Home Affairs Committee

Oral evidence: Hate crime and its violent consequences, HC 683

Wednesday 24 April 2019

Ordered by the House of Commons to be published on 24 April 2019.

Watch the meeting

Members present: Yvette Cooper (Chair); Stephen Doughty; Chris Green; Tim Loughton; Stuart C. McDonald; John Woodcock.

Questions 864–1023

Witnesses

I: Katy Minshall, Head of UK Government Public Policy and Philanthropy, Twitter, Marco Pancini, Director of Public Policy, YouTube, and Neil Potts, Public Policy Director, Facebook.

Written evidence from witnesses:

– Facebook
– Google
– Twitter
– Twitter (further evidence)
Examination of witnesses

Witnesses: Katy Minshall, Marco Pancini Company and Neil Potts.

Chair: I welcome our panel of witnesses to this Home Affairs Committee evidence session, which is part of our ongoing inquiry into hate crime. Could I ask the panel to briefly introduce yourselves and state the roles you play within your organisations?

Katy Minshall: My name is Katy Minshall, head of UK Government, public policy and philanthropy at Twitter.

Neil Potts: I am Neil Potts, public policy director at Facebook. I have oversight of the development and implementation of our community standards, which are the policies that we enforce to remove content on our platform. I also oversee the strategic response team, which focuses on crisis response and co-ordination throughout the company.

Marco Pancini: My name is Marco Pancini. I lead the public policy team for YouTube in Europe, the Middle East and Africa. I have 12 years’ experience, at Google and now at YouTube, of working on safety issues. I previously worked on safety in the industry at eBay.

Chair: Thank you very much, and thank you for your time. I will start with the Christchurch attack—a vile attack in which people were murdered and injured. The killer livestreamed his murders as terrorist propaganda. You have all accepted that, and I think you have all agreed that it should not be on your platforms.

However, versions of the video were still on each of your platforms many hours after the killings took place. There are reports in the New Zealand media this morning that some of those videos are still available and have been found on Facebook, YouTube and Instagram. You have all told us many times before about the systems that you have in place to take down terrorist material. Why have your systems failed so badly in this case?

Neil Potts: First, our hearts at Facebook go out to the victims of the tragedy in New Zealand and the recent Easter tragedy in Sri Lanka. In the case of New Zealand, first and foremost our priority was to help New Zealand law enforcement. We did that immediately after by sending members of our law enforcement response team to be on the ground, to support the investigation.

I would like to point out that we were able to remove the content and video within 10 minutes after it was flagged to us by New Zealand law enforcement. However, we saw more than 800 variants of that video appear on the platform. Within the first 24 hours, we were able to remove 1.5 million different copies, including 1.2 million at the initial upload stage, using our automated technology, and then an additional 300,000.

Unfortunately, we recognise that this was an adversarial space. The attacker used a network of his friends or colleagues on a separate
platform—8chan, in this case—to spread this, to make it go viral. They deliberately chose to be adverse to our policies and systems. They used things like splicing and cutting of the video, and filters to subvert our automation. Our automation is strong; we were able to immediately upload and share with our fellow colleagues of the Global Internet Forum to Counter Terrorism, but automation is not perfect. While it learns, it does have difficulty understanding different filters and different angles of the same video, and different uses of audio technology.

We realise that this is an adversarial space, and we want to make it hostile. But it is the case that, as more variants come online, they may appear on our platform. To date, we have shared with these companies here, as well as others within the GIFCT, more than 800 variants of that video—almost 900.

**Chair:** Do you think there are still versions of that video on your platform now?

**Neil Potts:** Chair, it is hard for me to say. I think we are doing an excellent job of removing it. The machine learning does learn over time, so as we see a video it can teach itself what to look for. Is there a possibility that one video exists that has a changed audio, a different filter or a different angle? It is possible. I am unfamiliar with seeing those copies. I know that we are doing a lot of work and investment there, but it is possible.

**Chair:** The Global Intellectual Property Enforcement Center is reported in the New Zealand media this morning as having found videos on your platform. Are you aware of that and have you taken those down?

**Neil Potts:** Chair, I am not aware of that, but I will definitely follow up with you on that and also make sure that my teams follow up with those folks in New Zealand to identify those copies and remove them. We will also add them to what we call our hash database and share them with the companies at this table.

**Chair:** The difficulty we have with this is that we have raised this issue with all of you many times before. There is this issue about uploading, re-uploading or taking a screenshot. Surely this is not new. Surely you have been aware of this as a problem when it comes to dealing with child abuse images, Islamist jihadi propaganda and all kinds of other videos and propaganda. I cannot believe that Christchurch was the first time you had people attempt to game your system.

**Neil Potts:** This is not the first time that people have tried to subvert our system, that is correct. In many cases, our systems are able to function very efficiently and remove the content. This time was unique because of the use of the live platform, the first-person perspective that the shooting took, and the media sharing many copies. People were then filming it with their phones, which created its own set of issues. We are committed to investing in artificial intelligence, machine learning and automation to surface and remove these videos as quickly as possible, but there is still
progress to be made with machine learning. It is not perfect or infallible today.

Q868 Chair: But you have had live streams before where you have had problems. This is not the first time you have had a livestream video that has been a problem.

Neil Potts: That is correct, but this is the first time we have—fortunately, events like Christchurch are very rare. This is the first case where we have seen this type of activity. It takes a machine multiple times—thousands of times, even—to recognise the type of violence or imagery it is seeing so that it can learn for itself and enact our proper policies.

Chair: What other organisations say is that you refuse help from outside organisations and you do not invest enough money in this kind of thing and that is why you have still got such a problem with being unable to take it down fast enough.

Neil Potts: I strongly object to that, Chair. We have made significant investment since the last time we appeared before your Committee. My colleague Simon Milner appeared in 2017. There are three areas where we have made tremendous investment in resources and our people. We now have more than 30,000 people who work on safety and security. Many of them are subject matter experts who write the policies and have law enforcement, intelligence and other backgrounds. They study counter-terror. We have more than 15,000 content moderators. Importantly, we have a full suite of engineers who focus directly on these issues to build out our product.

The second part is our product. Our artificial intelligence automation is not perfect. We have made significant investment, but it will take time for our artificial intelligence to improve. It is not infallible, but it is a big lever for us to pull and is leverage against this type of harmful content.

The third part is our partnerships, such as with companies like those at the table and in the GIFCT. We are committed to that, but we also work with a full variety of external advisers, academics, civil society and NGOs, as well as with government. We realise that these are tremendous problems and that we need to take all those measures to combat it.

Q870 Chair: But again, given that we have been raising this issue with you for some time, it is very hard to see why something as basic as just re-editing or splicing it and so on should cause you such problems. In March 2017—admittedly, this started as a YouTube issue—we first raised the issue about National Action videos, which was clearly illegal, far-right, extremist propaganda. In December that year, we raised again with YouTube the fact that that video kept appearing.

In an evidence session that all three of your companies were represented at, we were told that “they are sometimes manipulated, so you have to work out how they have manipulated them in order to take the new versions down. We are now looking at removing them faster...I think we will be closing that gap with the help of the machines”. I raised that
particularly with Simon Milner at that time. We raised it again with William McCants from YouTube in March 2018. He said: “Sometimes when there is a variation the technology will not automatically take it down; it will send it for review.” This hashing technology was developed years ago, and we have been raising this issue with you about people trying to game the system for years. That is why it is so hard to believe that this was still so difficult for you to deal with. The way you talk about it suggests that this was just a new thing that you had to deal with in the awful circumstances of Christchurch.

**Neil Potts:** I want to be clear: the thematic overview of these issues is not new. These challenges have existed, and we have worked and invested heavily to remedy them on our platform, and to combat this type of hate. This instance of the video, this type of video, was new. We had not seen that before and our machine learning had not seen that before. Therefore, it is harder for our machine learning—

**Chair:** Why was it a new type of video?

**Neil Potts:** Not to be too glib about it, this was essentially a first-person shooter video. We had someone using a GoPro helmet with a camera focused from their perspective of shooting. If we had different angles and it was a third-party video that showed it, perhaps our systems would have been faster, because we have seen that type of content before. We had not seen content from the actual angle of the shooter or the attacker.

**Chair:** Everybody knew—you knew—within a very short time of this happening, that this was a huge shooting attack, a criminal attack, and a terrorist attack. That was known very quickly. I do not understand why the angle of the camera was significant in terms of you then being able to take down all the material—the uploads and the re-uploads.

**Neil Potts:** I want to be clear: once we were made aware of the video we took it down extremely quickly—within 10 minutes. We immediately banked that video—bank is the term that we use for uploading to our database and sharing with our partners. That is one variant—we were very fast to get the variant from the shooter’s perspective. Other variants that did not resemble the exact shooter’s perspective, and the exact hash or digital fingerprint, made it more difficult. If you turn those angles certain ways, or you dub over soundtracks or add filters, that will subvert our system to some degree. Now the systems will learn quickly, but there is still time. In that space, some of those members on 8chan purposefully uploaded many copies, not only to Facebook but to YouTube and Twitter, with the purpose of spreading it wide. They uploaded it to message sharing sites that I have never heard of, with the intention of just making those things spread and go viral. Doing that presents a challenge to any AI.

**Chair:** It is very difficult to understand why, when these same issues were raised directly with you by us—if we were raising these issues in our very infrequent Select Committee hearings with you, I can’t believe that a whole load of other people, including police and law enforcement, were not raising them with you far more frequently. It is hard to understand why it
should take so long to develop the technology to address this. You just referred to people who were deliberately doing this. Have you identified all the users who were doing that, and have they been banned from Facebook?

**Neil Potts:** We have obviously identified the shooter and he has been banned from Facebook. We have identified and removed content from users who were sharing it. We do not have direct links back at this time to people who were within his core set of individuals on that 8chan system to share it, but we have removed numbers of individuals who were sharing that content.

**Q874 Chair:** So you have removed all the individuals who were deliberately sharing and uploading and changing the content in order to game your system. Sheryl Sandberg has talked about a community of “bad actors”. Have you identified all those people, and have you banned them from Facebook?

**Neil Potts:** We have identified some people and banned them from Facebook. There are also people who uploaded videos that were shared by bad actors—a bad actor shares the video, and someone else downloads it, but without the intention of knowing that they are being a bad actor, and they upload it. Then we just apply our normal penalties. We remove the video and they get certain escalating penalties, but they will not necessarily be removed from Facebook.

**Q875 Chair:** Okay, but you have removed the people who you think were doing that deliberately.

**Neil Potts:** We have, yes.

**Q876 Chair:** Have you reported them to the police?

**Neil Potts:** We are working closely with New Zealand law enforcement.

**Chair:** Have you reported them to the police?

**Neil Potts:** It is an active investigation, and I want to respect that. I am not a lawyer for the company.

**Q877 Chair:** The reason why this is significant is that we have been told by the counter-terror chief here, Neil Basu, that very often the social media companies do not report to the police incidents that clearly involve breaking the law, and that although you might remove content, you do not refer it to the police. That is why I think that there is a significant question about whether or not you have referred information to the police about individuals who were deliberately uploading in order to spread terrorist propaganda.

**Neil Potts:** Yes, Chair. I just want to point out that we do work closely with law enforcement. If there is an imminent threat of harm or risk, we do refer those things proactively to law enforcement. I am not familiar with the person whose statement you mentioned, but we do refer to law enforcement many cases of imminent threat. We also respond to requests for data and information when we receive proper legal process. I believe
that that is happening in New Zealand and we are responding, but I do not have the information on exactly what we have shared with them at this time in the investigation that is ongoing.

Q878 Chair: Just in terms of your policies, if you identify illegal content—not simply content that violates your standards, but death threats, the sharing of terrorist propaganda and so on—you rightly remove it, but do you also report it to the law enforcement in that country? Assistant Commissioner Neil Basu, by the way, is head of counter-terrorism for the Metropolitan police and for the whole of this country.

Neil Potts: I apologise for not knowing him.

We do. In the case that we think—I won’t say that we are certain—that there is an imminent threat of physical harm, we refer it. Whether it is terrorism, other types of crime, threats against a public individual—unfortunately members of this body have received threats—or threats against a private individual, we will refer it to the local law enforcement in the hope that it will intervene.

Q879 Chair: Okay, but that is where there is “life or limb” risk. Where there is no such risk, but where the posting of a video or something else is itself an illegal act, such as the promotion of terrorist propaganda, would you report that to the police?

Neil Potts: I think those are case-specific. It is hard to answer in the hypothetical. If it is just one posting of a piece of propaganda, I would say that we most likely would not. We do investigations, but if we find that the person is somehow connected to an organisation and/or contemplating some other large-scale attack, we would then refer it.

Q880 Chair: Sure, but there is a criminal threshold involved—the material itself might pass a criminal threshold. I understand that you will have very sensible policies for where there is an imminent risk; I am asking you about the situations in which there is not an imminent risk, but nevertheless there is evidence that in that country a crime has been committed. Would you refer that to the police?

Neil Potts: I think it would depend on the crime. If we understood what crime was being committed—there are obviously different scales of crime.

Q881 Chair: A crime is a crime.

Neil Potts: There are misdemeanours and then there are capital crimes.

Q882 Chair: A misdemeanour—okay, if it is not a crime, it is not a crime and I would not expect you to report it. I am just trying to understand whether Facebook reports crimes on your platform to the police.

Neil Potts: We do not report all crimes to the police. Again, we do report those imminent threats and we do respond to requests for information about crime.

Q883 Chair: Okay, and how do you decide what counts as a crime? Who are you to decide what is a crime that should be reported and what is a crime that
should not be reported on your platform?

Neil Potts: We have a very developed process. We have teams who come from law enforcement backgrounds—FBI, UK law enforcement and other law enforcement agencies globally—to help us to develop those processes, where we then create our own credible threshold of what we believe is imminent, and then we will pass that on.

But to be frank, part of this hearing is to discuss potential regulation and oversight from Government. These are areas where there are tough decisions, and they are decisions that we and these companies here are making on our own. These are places where Government can give us more guidance and more scrutiny about what we should be sharing.

Q884 Chair: Let me turn to Twitter. How long did it take you to remove the copies of this video?

Katy Minshall: Thank you, Chair, and thank you for inviting Twitter to testify.

The effort is ongoing. So far, we have removed 26,700 tweets. First, we should state that the video was not uploaded to Twitter, in its original form. You cannot, as an average user, upload a video of more than two minutes and 20 seconds. Like other companies, we saw multiple variants of the video—we saw 300 different copies on our platform—but, similarly to Facebook, we removed the perpetrator’s account before the New Zealand police asked us to and before he was arrested.

Q885 Chair: What have you done to be able to identify different versions and variants of this video, or have you simply relied on Facebook or others to tell you which are the different variants?

Katy Minshall: There are a few things. Brad Smith wrote a blog for Microsoft that puts it very well. There are two big lessons learnt for all of us. The first is exactly this issue: we all need to get better at identifying different variations of this content, and that has to be a priority. Secondly, the importance of a crisis response or command centre was another lesson. The GIFCT that we all work through was set up principally for programmatic work. It is effective with things like research, tech innovation and hash databases. On the day, although we were able to respond to the emergency and set up a specific repository for Christchurch content, we all felt that it was not particularly process-driven. A priority for all of us is to look at something like a command centre for the future.

Q886 Chair: You talk about learning lessons; the trouble is, we explicitly raised the issue of deliberate attempts to change videos to be able to post them again 18 months ago. It is so difficult to understand why this was a shock to you all when it happened in this case. Why are you always so reactive?

Katy Minshall: I think that at Twitter specifically, because of the limits on video length, we tend to see URLs being shared rather than the original content. Something we have done over the past year is set up a different database for URLs. When we add something to the database, we can all proactively surface that content on our platform. In thinking about
different versions of videos, that is part of the effort to try to think about how the video is emerging on different platforms in different locations.

Q887 **Chair:** Have you made efforts to identify the people who were deliberately spreading this terrorist propaganda on your platform?

**Katy Minshall:** It is a really difficult challenge. The first thing I should say is that we did our own analysis at Twitter and found that 70% of the video views were shared by 62 verified accounts—traditional media outlets. There is a lesson there in terms of our partnership with the wider media ecosystem on the day, which Neil Basu has raised.

To come back to your point on working with the police, I was at a police conference on the morning of the attack, running a training session to guide police officers in how they can make requests to Twitter for data. We were having meetings with the College of Policing to think about how we can scale that across the country, and with NTAC to discuss the upcoming implementation of the CLOUD Act. We take very seriously our partnership with law enforcement and the concerns they raise.

Q888 **Chair:** So 30% were not the mainstream media. The 70% were mainstream media?

**Katy Minshall:** Yes.¹

Q889 **Chair:** What discussions have you had with them?

**Katy Minshall:** This is something that I raised with the Home Office on the morning of the attack and in discussions since. We would welcome opportunities to be part of that discussion. As Mr Potts was saying, we saw users inadvertently breaking our rules by sharing content while condemning what happened and expressing solidarity with the victims. On our part, another bit of this is to clarify our rules and provide greater understanding to our users about those issues—when they might inadvertently break the rules, and the actions we will take.

Q890 **Chair:** So have you made an effort to distinguish between people who were thoughtlessly sharing in order to condemn, mainstream media who were making a very poor editorial judgment that they later changed, and those who were deliberately promoting it in the same way that Facebook talks about those who were doing so in order to escalate and promote terrorist material? Have you made that distinction, and have you tried to identify those who were doing it deliberately to spread terrorist propaganda?

**Katy Minshall:** We are in the midst of our own internal review, and I will of course keep the Committee updated. To come back to the point on terrorist content on our platforms, Twitter has now removed 1.4 million accounts for the promotion of terrorism. I think the director of the FBI was asked, “Would you like platforms to give you that dataset?” It’s

¹ **Note by witness:** We had 62 verified accounts globally upload clips of the NZ video, which resulted in 70% of all views of the video. While there were some celebrities who shared to condemn etc, this represents a large crossover with media.
complicated. Already, terrorism is often described as trying to find a needle in a haystack and the last thing we want to do is to provide a great deal more hay. That is very much a question for law enforcement.

Q891 Chair: Isn’t the reality of your problem that even if you were willing to do this, it wouldn’t really make a difference because you don’t know who any of those people are because of your policies on anonymity?

Katy Minshall: Like I said, we work closely with the police and when they make requests to us for information we can provide—

Q892 Chair: I know, but I am not asking about when you react. I am asking, if there were people on your platform who were deliberately spreading terrorist propaganda, are you able to identify them and to report them? Yes or no?

Katy Minshall: We are in similar position to Facebook. If there was a threat to life, we are able to work proactively—

Q893 Chair: I know; I am not asking about a threat. I am asking whether you are capable of identifying people who may be spreading terrorist propaganda on your platforms.

Katy Minshall: Like I said, when there is a threat to life, we will reach out to law enforcement, where we have relationships.

Q894 Chair: I’m not asking about whether there is a threat to life. I am asking about people who are spreading terrorist propaganda and who are breaking the law, and whether or not you are capable of identifying them and reporting them to the police. Are you capable of doing so? Yes or no?

Katy Minshall: There are plenty of signals we can use that I would rather not go into in a public setting, but I am very happy to follow up with the Chair after this session.

Q895 Chair: That would be very helpful.

YouTube, what did you do to take down material and do you believe, as reported in the New Zealand media today, that there are still videos from the Christchurch shooting on your platform?

Marco Pancini: Thank you, Chair. I will not repeat some of the things that were already mentioned by my colleagues, but there are three elements that were very important on the day. First and foremost, the use of our algorithms and the use of our machines. We invested a lot in that, and I think that in terms of capturing the original video the machines did their job. Once we got the original video from law enforcement, we were able to hash the video, identify the video and block the same video.

In relation to the re-upload—at the end of the day, we are talking about something like 200,000 pieces of content that we took down—the challenge was, as Katy said as well, the presence of pieces of the video in different uploads by authoritative sources. What we learned from that—this is the second big improvement that we made for the future to change our policies—is to make sure that now if there is a match of the same
pieces of video uploaded on the platform, instead of going up online, they go directly for review. I would like to look into this piece of news, which I am not aware of, to try to better understand how it is possible that pieces of the video identified by the machine were still not sent for review—and I assume that after review only authoritative sources would have been authorised to upload.

I would also like to stress one other point, which is the collaboration between our companies. That is something new and something positive, which was not there in the past. During the day we were able to share thousands of pieces of videos across the different platforms. That really helped us to catch up with the huge amount of uploads. The second is the collaboration with law enforcement. Of course, I mentioned the collaboration with New Zealand law enforcement, but when these things happen, our team—I did it in the past—get in touch directly with law enforcement, at European level, at APAC level and in all the different regions, to try to understand better where we need to focus our efforts and where we can work together in order to make sure that we are up to the threats.

This was absolutely horrific. When we woke up in the morning and we took over from our colleagues in APAC, we were absolutely shocked by everything that was happening, but we did everything that was possible. I think in the areas that you identified—particularly the fact that in the aftermath of the event our machine was not capable of distinguishing, for example, when something was glorification and when something was an authoritative source—we have now made an improvement, which is blocking all the different pieces of content from going online. Hopefully, as we have seen this week in Sri Lanka, issues like that will not happen again.

**Chair:** But again, it was specifically YouTube that raised this and talked to us about this in previous evidence sessions. William McCants told us 12 months ago: "Sometimes where there is a variation the technology will not automatically take it down. We will send it for review. We are fine tuning our technology so we spot even smaller clips." But 12 months on, you are still not able to do that.

**Marco Pancini:** That is the improvement that we made, unluckily because of this horrific event: the rule that William described to you, so that if the image is identified, there is doubt—it is not the same video—then it goes for review. In the future, in cases of horrific events like Christchurch, the content is not going up online and then being reviewed. It is blocked, it is reviewed, and only after being approved can it go online.

**Chair:** So up until now, although it gets sent to review, it has basically still been allowed on YouTube.

**Marco Pancini:** To put it in the right context, when we are saying that it is sent for review, we need to consider that for this kind of violation, for example, 90% of the content that is sent for review and is then taken down—so, terrorist propaganda or that kind of violation of our policies—is
taken down with fewer than 10 views. The machine, in the context that was described by William, is already working and allowing us to take down a lot of content in a very fast way. What we are changing, because of the unprecedented and specific threat that a fact such as Christchurch represents, is even in this case not to let the content go up online, but to send it for review and only when it is approved will it be available online.

**Q898** Chair: Okay, but again, the New Zealand media report today has a quote from Eric Feinberg of the Global Intellectual Property Enforcement Center, who talks about the YouTube video that they found some time after the attack. It has now been removed as a result of them reporting it—only as a result of them reporting it—about which, “He said hundreds of thousands of people had accessed the videos. ‘The YouTube video we took down...had over 720,000 views.’” Is that correct?

**Marco Pancini:** I am very sorry, but I am not aware of this piece of information. If it is possible, I would like to go back to the team and ask for confirmation, because the rule that we implemented after Christchurch would not allow pieces of content that are linked to any glorification of that fact to go up online.

**Q899** Chair: Okay, but again, that is something that we have repeatedly raised with you. For some of this, at the time of the Christchurch attack, it had a content warning up. So you had material, bits of these videos that were up, within eight hours, with a content warning. You had enough information to flash it up as a problem, but not to take it down.

**Marco Pancini:** Again, if we look at the policies that we have implemented and the algorithm that we have implemented, there are different levels of implementation and enforcement of the policies. If it is about the same video, the same video is blocked. If it is about pieces of the same video, they are sent for review. In the case of something like Christchurch, we have changed our policies, so it is not even going up online—it has to be reviewed by a human. In any case, if there is doubt, it is escalated. In the comprehensive approach that we are taking to this kind of content, there can always be issues like the one that is mentioned—and I want to look into that and come back to you with more information—but I think we have a robust approach to try to face the threat.

**Q900** Chair: Again, have you identified people who you believe to have been deliberately promoting this to deliberately promote terrorist propaganda?

**Marco Pancini:** Of course, we have identified, and violation of this kind—

**Chair:** Have they been blocked?

**Marco Pancini:** Violation of this kind will lead to blocking the account and taking down the channel. Absolutely. In terms of working with law enforcement, it is a very delicate issue. Why? Because there are two elements to take into consideration. On one side, the need to collaborate together with law enforcement to make sure that the evidence from the crime is collected in a way that is in line with the law of the country where
the crime is committed. That requires, in most cases of this kind of very
dangerous act, freezing the evidence, waiting for a request from law
enforcement to acquire the evidence and then delivering the evidence.
That is in order to make sure that the evidence can be acquired in a form
that means it then can be actually used against the criminals.

**Q901 Chair:** So you wait for a request from law enforcement in order to give
them information. You don’t identify something that is illegal on your
platform and report it to the police.

**Marco Pancini:** According to the different jurisdictions, we work together
with law enforcement in order to make sure that, in respect of the due
process of law, we hand over the information in a way that makes sure
that the criminals can be prosecuted.

**Q902 Chair:** But again, this comes back to the issue raised by Assistant
Commissioner Neil Basu, who said that all your platforms are removing
things that are illegal but you are not reporting it to them. Do you actively
report to the police within a jurisdiction if you identify content that is
illegal—not just against your guidelines although not illegal, but material
that itself is a crime? Do you report those cases to the police?

**Marco Pancini:** We have policies that are in line with the ones of our
colleagues, but I want to stress—

**Chair:** So the answer is no.

**Marco Pancini:** I want to stress that it is very, very important to work
together on these issues—I did this also in the past, when I was working,
of course, on issues of less relevance, like e-commerce—with law
enforcement in order to make sure that the evidence is acquired in the
right way. Because then—

**Q903 Chair:** That’s fine. It’s very good that you do that and that you want to
take the right kind of digital evidence. That’s fine. The issue is whether
you are letting law enforcement know about crimes being committed on
your platforms. This is a real concern, because you are effectively making
these crimes possible—you are facilitating these crimes. I accept that you
are doing much more than you were 18 months ago to respond to them
and to take that material down, but you are not actually reporting the
crimes that your platforms are making possible. Surely that is a serious
problem for people right across the world who want to make sure that
crimes are not being committed.

**Marco Pancini:** It’s a very fair point. I want to stress that we discuss
these issues with Europol every week; we have a conference call with the
people at Europol every week, and we came to a place where we decided
that the best way is to work together and identify, for example, trends,
identify areas where we want to improve, and then find the right process,
according to the applicable laws, to make sure that the evidence is
acquired in the proper way.

**Q904 Chair:** I have been concentrating on something that is a very clear-cut
case. It’s about terrorist propaganda, and you all accept that it is wrong, is
illegal and should be removed. But it seems to me that time and again you are simply not keeping up with the scale of the problem, the scale of criminal and terrorist activity, and doing the things that we all, as communities across the world, need you to be doing.

Do you have a concern about the way the Sri Lankan Government has responded? Actually, countries and Governments are being forced into this very strong reaction, because they have no confidence in your ability to sort things, and even if it might have all kinds of wider repercussions, of banning your platforms for a temporary period. Even if that causes huge problems for people, they are being forced to do it because, they say, they don’t have confidence in your abilities. Aren’t you concerned that that is going to happen more often if you can’t get your act together? Who would like to respond?

**Marco Pancini:** I would like to first stress that our focus, after the horrific events in Sri Lanka, was first and foremost to make sure that we applied the procedures that we described before. So we identify the attackers. We work together with law enforcement in making sure that, if they have a channel or if they have a presence on the platform, this is closed. We make sure that when people are searching for information on what is happening, they find authoritative sources. Also, we are working together with law enforcement again in trying to understand how the facts are developing and who the group is that is actually accused of the facts, and then we take action on the channel. This is something that we have done in the last hours. So that was our focus. On the decision of the Government, of course it is a decision of a Government and we need to respect it. There are voices from civil society and voices from journalist organisations that are raising concerns about the fact that this is also impairing their ability to communicate and understand better what is happening there, but this is a different issue. Our focus at the moment was not answering to the decision of the Government from Sri Lanka, but to make sure that we had our house in order.

Q905 **Chair:** My question is whether you think that you have any responsibility to ensure that countries do not end up in that situation, needing to react in that way or deciding that they want to react in that way, because they can have confidence in your platforms to be able to act in the way that they need you to.

**Neil Potts:** Thank you, Chair. I appreciate that question. As my colleague said, ethnic violence and the targeting of someone at worship is one of the most despicable acts. Our hearts go out to those who were impacted by the bombings on Easter. I believe that we have a responsibility under our policies to enforce our community standards, to ensure that that type of hate, terrorism and violence is not on our platform, and we do that swiftly. In the immediate aftermath of this attack we designated the event and designated the individuals as terrorists, and we removed that content, sharing much of it with our colleagues here.

Where we have seen other types of ethnic violence or terrorism we have invested significantly, as we have in Sri Lanka, with the 30,000 people
who now work on safety and security. We have dedicated teams that focus on these markets. We have language experts and subject experts, with the challenges that they face, and we really want to work with partners on the ground so that we better understand the situation.

As my colleague said, communication after any event of this type is important. It is a way for families and loved ones to connect, so we feel that it is better to have an open internet, because that is how people are able to know if someone is safe. On Facebook, we have a system called Safety Check, whether after a natural disaster or an event like this. Many people used Safety Check after the events in Sri Lanka. Obviously, they cannot do that now, because of the blockage of the internet.

We would rather see the internet open, but we share many of the concerns of the Sri Lankan Government. Their constituents and citizens are our community, and we have the same goals of wanting to keep them safe. We respect their way of going about that. We think it would be better for communication to be open, but we do understand.

Q906 **Stephen Doughty**: My problem is that I don’t think you are even getting some of the basics right in terms of the material that is used to radicalise those who carry out such horrific attacks in the first place. When all three of your respective companies appeared before this Committee some time ago, you all admitted that you were not proactively searching for other organisations, such as far-right or extreme right-wing organisations, Northern Ireland terrorist organisations and others. It was basically an admission that the entire focus had been on Islamist organisations, and that you were not routinely searching for proscribed or other problematic organisations.

I have raised some very specific concerns about far-right content, particularly relating to an organisation called Radio Aryan, and another organisation called System Resistance Network.

Ms Minshall, you said a moment ago, “We all need to get better at identifying content,” beyond videos and everything else, and you have a URL database. Why did you have for so long an account on your site actually called @RadioAryan, which was providing links to the most disgusting antisemitic, Islamophobic, homophobic, racist far-right content? Why did you allow that account to exist?

**Katy Minshall**: I will first just outline our rules in this space, because I think that would be helpful for the Committee.

Q907 **Stephen Doughty**: No, I would like to know why that account was allowed to exist and why it was subsequently taken down only after a media report involving myself and others.

**Katy Minshall**: At the beginning of your question you asked about proactive searching. We said last week that it was unacceptable that we were solely relying on user reports to find and identify violations of our rules. Now, 38% of the enforcement action that we take on abuse is identified through our own internal criteria.
Q908 **Stephen Doughty:** That is very interesting, but why was that account allowed? At a very basic level—we are not taking about a link, but an account—the account was called @RadioAryan on Twitter. Why was that allowed to be up on your site for so long?

**Katy Minshall:** I am not familiar with the details of that specific account.

Q909 **Stephen Doughty:** Even though it was reported to you by myself.

**Katy Minshall:** I am not familiar with that.

Q910 **Stephen Doughty:** Okay, so even though you have now removed the main account, you also have accounts—I looked last night—linking to that content. You have other accounts linking to The Daily Stormer—a well-known US neo-Nazi site—which includes a link to an article I found in three minutes last night, saying that the New Zealand killer bears no responsibility and it was a legitimate revenge attack. I am not talking about deeply hidden organisations or links. Why are there links to very well-known organisations like that in full public view on your platform?

**Katy Minshall:** I am aware of high-profile accounts and individuals on the platform. When those accounts are reported to us, we take it very seriously, and we review those contributions.

Q911 **Stephen Doughty:** Well, you didn’t—it took weeks for you to remove Radio Aryan when I reported it to you.

**Katy Minshall:** We’ve have now designated almost 100 white supremacist, nationalist or separatist groups to date—

Q912 **Stephen Doughty:** But apparently not The Daily Stormer, which is one of the most well-known neo-Nazi websites in the US.

**Katy Minshall:** We have a number of ongoing assessments that we do day in, day out. In terms of one of the challenges we have, people often say about the police that they can't arrest their way out of a problem. We have no interest in having violent extremist groups on our platform, but we can’t ban our way out of this problem.

Q913 **Stephen Doughty:** That’s just words. This is the basics. We are not talking about deep, hidden content; we are talking about the basics of very well-known, publicly reported and identified organisations that are of concern to law enforcement organisations across the world, as well as to a range of organisations such as Hope not Hate that have identified them and to members of the Committee. You are still providing links to the most basic of these organisations.

**Katy Minshall:** For us, the priority will be using technology to identify accounts that break our rules. Safety is our top priority as a company, and we will continue to invest in tools that help us to surface those accounts.

Q914 **Stephen Doughty:** So will you ensure that Radio Aryan, System Resistance Network, The Daily Stormer and other organisations like that are not available as links on your platform, and are put into those URL databases and other automatic systems that you have?
**Katy Minshall:** As I said, I am not familiar with the details of those accounts, but if we identify a breach, we will take action.

Q915 **Stephen Doughty:** It is simply not good enough. These have been reported to you on multiple occasions. Facebook, I similarly raised concerns directly with your team about links to such organisations. It took you weeks to remove links to Radio Aryan from Facebook—I got to the stage of raising it directly with your staff in the UK. Can you explain why you still have links to The Daily Stormer, System Resistance Network and some of these other sites, including Gab? I found a link last night to a page that said, “If Muslims are the bullets, the system is the gun in the hand of the Jew”. Can you explain why Facebook is routinely allowing links to such organisations? Again, we are not talking about deeply hidden organisations—these organisations are well known, and anyone can find them within minutes on your platform.

**Neil Potts:** Thank you for raising Radio Aryan—I think we were able to designate it as a hate organisation and remove it from our platform within one week of you raising the issue with us, which is very fast. We have a very deliberate process, but thanks to your efforts, we were able to do that. That is not to say that someone could share information about Radio Aryan on our platform and we would find it immediately, but once we are made aware of it, we will remove it. There is no room for praise, support or representation of that organisation, or any hate organisation.

Q916 **Stephen Doughty:** So why have you still got links, this morning, to System Resistance Network and The Daily Stormer?

**Neil Potts:** I know that we have black-holed or placed on our URL database The Daily Stormer. I am not exactly sure what you have—

Q917 **Stephen Doughty:** I have multiple links here. You claim that these things are being looked at, yet people can just find them. I can find page after page after page linking to its article—I won’t use the terms, but they are utterly offensive terms relating to Jews, Muslims and black people, and they are in full view on Facebook this morning. Clearly your systems aren’t working.

**Neil Potts:** To be clear, we have 2.7 billion users on our platform who share billions of pieces of content every day. We have millions of reports against that type of content. Some of it is proactive; some is user-generated. We do an extremely good job of finding that information and removing it when it violates our terms, but that is not to say that everything is perfect.

Q918 **Stephen Doughty:** These are direct links to The Daily Stormer website. That is a very easy thing to search for. We are not talking about a video that has been altered or music that is added. We are talking about the most basic thing, which is a link to a well-known neo-Nazi website, and it is all over your platform. Why is it not being found?
**Neil Potts:** Mr Doughty, I am happy to follow that up with you afterwards. I would need to see the actual link to ensure that it is one that we have identified and put into our URL database.

**Q919 Stephen Doughty:** It is the link to the actual website. It is there for everyone to see. It is the most basic thing.

**Neil Potts:** I understand your concerns. I am happy to take that feedback. I want to make sure that we are removing that, so could I follow up with you afterwards? I would need to—

**Q920 Stephen Doughty:** So you will remove links to The Daily Stormer?

**Neil Potts:** Absolutely.

**Q921 Stephen Doughty:** And System Resistance Network.

**Neil Potts:** Absolutely. They are both banned.

**Q922 Stephen Doughty:** And you will proactively search for the range of neo-Nazi and far-right organisations that have been identified by groups such as Hope not Hate.

**Neil Potts:** We have long held that white supremacist organisations and far-right organisations that have—let me rephrase this. Our policies around terrorism and hate are ideological and apathetic: we do not care whether you claim to be a far-left or a far-right group—if you have a deep link to violence or a deep link to hate, we remove you, we designate you.

**Q923 Stephen Doughty:** But you clearly don’t, Mr Potts.

Can I turn to YouTube? Similarly, do you have content linking to Radio Aryan on your site?

**Marco Pancini:** As far as I know, no—we do not have any.

**Q924 Stephen Doughty:** Okay. Well, last night I found a link to one of their full radio broadcasts within a moment, which—I am sorry to use the words—talks about going after “niggers” and “faggots”. A full broadcast was there from an individual providing multiple links to neo-Nazi organisations. I found another set of videos and music—again, white supremacist and neo-Nazi organisations. I found people providing links to Britain First, which, as you will be well aware, is an organisation that, I believe, has been banned from some of the other platforms. I found huge amounts of videos—for example, “Homosexuality and the Campaign for Immorality”—from far-right and Islamist organisations, talking about going after gays, advocating stoning, and all sorts of different things. It is just a cesspit. Why are those links on your site?

**Marco Pancini:** Let me take a step back and put things in perspective. In looking at content when it is uploaded on the platform, we take into consideration two pillars: one is the law; the second is our policies. Our policies do not allow any kind of that abuse, so I really need to link into the content that you are reporting to me with our team.

**Q925 Stephen Doughty:** But there is loads of it. Again, we are not talking
about deeply hidden content; we are talking about stuff in full public view. We are talking about basic links—link after link after link—to neo-Nazi and far-right extremist organisations, all in the comment pages, and people commenting on it afterwards. Not only that, but actual links to full audio recordings of neo-Nazi broadcasts advocating violence against Muslims, Jews, gays, and the state—the violent overthrow of the state. How is that content getting through if you have these policies in place?

Marco Pancini: I have worked for years with NGOs from all over Europe on these kinds of issues, in the context of the European code of conduct against hate speech. We are working together with NGOs from 26 countries—now 27. Absolutely, it is an important issue. We are focusing on improving the enforcement of our policies, working with experts and NGOs.

Just to give you a number, in the last two years, thanks to the work that we have done with these NGOs in the context of the code of conduct, we were able to pass from a tick-down rate of 40% to 80% for the referrals that we are receiving on these kinds of issues across all of Europe, so the situation is improving. Still, I fully understand that there are areas such as the one that you are highlighting that we need to look into, and—

Q926 Stephen Doughty: I’m sorry, but why is it that every single time all three of your companies appear before this Committee, members of the Committee, including myself, the Chair and others, are able to find content within minutes? We are not talking about weeks of research or about looking for complicated hidden stuff on the dark web or stuff that has been altered. We are able to find stuff within minutes or seconds. I was able to find the attack video in Christchurch within seconds on various of your platforms. Your systems simply are not working. Quite frankly, it is a cesspit, and it feels as if your companies really do not give a damn. You give a lot of words and a lot of rhetoric. You do not actually take action. You do not even know that this content is on there. You are appearing before us this morning, and you have not even looked up the organisations that we have raised. It is all on there.

Marco Pancini: We need also to remember that there are 2 billion users that come every month on our platform to find content, to learn something and to share something. Of course, this is absolutely a horrific issue, and we need to do a better job in trying to understand—actually, we are doing a better job in trying to understand—how to stay up to the threat.

For example, there is something I would like to mention. Since the last hearing, we introduced a team called the intel desk, which is dedicated to making sure that we better understand the trends of violation of our policies, of far-right organisations, of extremists—

Q927 Stephen Doughty: That is all wonderful, but they are clearly not doing a very good job. Quite frankly, I find it extraordinary that I can find all this hate content directed at the LGBT community on YouTube, and yet I know for a fact that you block and restrict positive LGBT content by your own
YouTube creators—block it so it is restricted. Yet, last night, I could find videos advocating violence and hatred towards the LGBT community. Quite frankly, your policies mean nothing, because you are not following them through. Chair, I have had enough of listening to this.

Marco Pancini: I would like to look into this content and come back to you, in any case, if possible.

Stephen Doughty: You are all three of you not doing your jobs.

Q928 John Woodcock: Can I take you back to the issue of what you share and the requirements on you to share with law enforcement agencies? If the UK Government put a requirement on all of you as companies to share the identifying IP address data for every account that breaches your policies, what would be your response to that?

Marco Pancini: I can tell you that, from my personal experience, we are also discussing these issues with the European institutions in the context of the EU evidence initiatives, which are very similar to some of the ideas that, by the way, are in the “Online Harms” White Paper. Of course, the focus on trying to find a way to make sure that the evidence is preserved and that there is the right level of collaboration with law enforcement is something that we are very open to discussing.

Q929 John Woodcock: You all talk about active collaboration, and I am sure that is the case in specific instances, but what would be the bar—what would be your objection, or would you have no objection—to simply routinely sharing that identifying data with the appropriate law enforcement agencies? Ms Minshall, you made the point about needles and haystacks. We can take that as read, but if a Government says, “Actually, we want all of that data available as you either ban the user or restrict a particular piece of content,” what would Twitter’s response be?

Katy Minshall: My understanding is that that is exactly the issue that the CLOUD Act is intended to address.

Q930 John Woodcock: But it does not go as far as that at the moment. No one is suggesting that. Are you being unspecific because you are not sure?

Katy Minshall: As it stands, if there is a threat to life or serious harm, we can proactively reach out to law enforcement where we have relationships. US law would prevent us going beyond that. For some time, all of us have raised that as an issue, and the CLOUD Act is intended to address that exact gap.

Q931 John Woodcock: But if the UK changed its law to require everything available to be routinely shared—yes there is a different path that the US is going down, but it does not go as far as doing that—could you do it? Would you object to doing it?

Katy Minshall: This is something I would have to look at in terms of the implementation of the CLOUD Act, the details of which I am not sure of, but it is also a question for the White Paper on online harms, in which
there is a very thoughtful section on illegal content. More detail on where the regulator ends and law enforcement begins would be very welcome.

**Q932 John Woodcock:** Indeed, but this is clearly a live issue, and there is an active debate about the level of responsibility being taken by your platforms, as we have seen today and as we have seen with every terrorist atrocity. We clearly have a question being posed on the mechanisms in place. I am surprised that you cannot give me an answer. If it is a bad idea, you need to tell us why it is a bad idea, because these are the directions we are going to go down. Mr Potts, did you have a view on this?

**Neil Potts:** I would say that we want to comply with the law where we can. Where there are different regulatory frameworks in different areas, as Ms Minshall mentioned, and where they conflict, we have to essentially de-conflict those and make sure we solve that for those issues. We are a US-based company, but we operate internationally. We are a US-based company, and we must adhere to the US-based laws as well. We do respond to legal requests from Government for that information. If you request information about any of our users—data, location—we will comply with that, if the request is legal, just—

**Q933 John Woodcock:** So if the UK Government makes a standing request that everything that every user who creates content that you then ban is routinely shared with UK law enforcement agencies, that is fine.

**Neil Potts:** I want to be sure that I fully understand your question. Are you talking about every piece of content that we would remove under our standards, but that is not necessarily illegal?

**John Woodcock:** Yes.

**Neil Potts:** If you have a specific proposal, I am happy to take it back to the team. I want to make sure I fully understand that—it seems like a very grand proposal.

**Q934 John Woodcock:** Okay, let’s restrict it to not necessarily offensive but to terrorist-related activity. For all platforms there is a large volume of cases where you take down material but are not required to share it with UK law enforcement agencies. If the UK passes a law to say that you must automatically share the IP data related to those accounts, which clearly you have, would you have an issue with doing that?

**Neil Potts:** I’m happy to take that back to the team to get you a direct answer. To make sure I fully process your question, I want to point out that even in the space of terrorism there are different levels. We spoke earlier about deliberate actors; we want to ensure that we follow the correct due process of those people. There are people who may be sharing for awareness in a way that violates our community’s policies. Doing that would seem to be a bit over-broad. For example, if someone wants to share awareness of the attack in Sri Lanka in a way that violates our policies, where it is not clear that they are condemning but are just
sharing something without a caption, that puts us in a difficult position to assess someone’s intent behind the sharing.

**Q935**  
**John Woodcock:** I understand that, and it is a valid point. You said at various points that you want Government’s help. The Government may say, “We are taking control of overall terrorist policy, and we instruct you to share that and we will make the assessment of what has been shared in a non-criminal way or what might have been below the criminal bar, but nevertheless flags up activity that a UK programme such as Prevent may want to take into account.” What I am getting at is whether you think there are legal bars to your applying that, and whether you would have objections as a company. If you do not have the answer now, I would appreciate a corporate response from all three of you. Does anyone have anything to add?

**Neil Potts:** I am happy to take that back to our teams and follow up with your office.

**Q936**  
**Chris Green:** Ms Minshall, who is responsible for content on Twitter?

**Katy Minshall:** Many different teams have a role in content on Twitter, from our engineers to our safety teams.

**Q937**  
**Chris Green:** Twitter as a whole is responsible for its content. Individuals who tweet whatever they tweet and share have personal responsibility, but ultimately, you are responsible for it. Does the content on Twitter reflect your moral character as an organisation?

**Katy Minshall:** Let me be very clear: some of the examples raised today and previously in this Committee do not meet my moral threshold and are abhorrent. Our role is to identify that content as quickly as possible and remove it from the platform.

**Q938**  
**Chris Green:** Within Twitter and social media more broadly, there are teams of moderators who look at content and stop it from being broadcast or re-broadcast. How many people do that for Twitter?

**Katy Minshall:** Let me give an overview of our strategy more broadly rather than focusing specifically on the number of people we employ operationally. As I said, technology is critical for us as a company. Algorithms do not need weekends and they do not need to sleep. Not only does technology help us to find content that breaks our rules, it helps us to prioritise reports and block spam accounts without human intervention. In the first half of last year, there were about 230 million attempts to come on to Twitter that violated our spam policies.

**Q939**  
**Chris Green:** Are those non-human interventions fast enough and good enough yet?

**Katy Minshall:** We have seen success in a number of areas.

**Q940**  
**Chris Green:** Clearly, there is a distinction—this is the impression that I got—between Facebook and Twitter in the responses to Mr Doughty’s points. The answers were far better from Mr Potts’ organisation than from yours. Why is that? Why are you not keeping up?
Katy Minshall: Sorry, can you clarify the question?

Chris Green: In terms of some of the organisations that could and perhaps should be proscribed, and which should not be shared on Twitter, we heard evidence that there was a difference in the response and in shutting down this content.

Katy Minshall: On proscribed organisations, there are a number of groups that we proscribed several years ago. We are different platforms.

Chris Green: Not just proscribed organisations, but others that clearly do not share the values that Twitter would want to broadcast.

Katy Minshall: Sorry, could you clarify the question?

Chris Green: Sorry. At the moment, there is significant and quite repugnant content on Twitter that, it seems, has been more effectively shut down on Facebook and other platforms than it has been on Twitter. Isn’t Twitter keeping pace?

Katy Minshall: I’m not sure that that is a characteristic or something I recognise.

Chris Green: Would you say you’re keeping pace with other organisations?

Katy Minshall: Yes. We are in a very different place from where we were two years ago, and regular Twitter users will have seen a step change. We have indications that our automated systems are having an effect. On something like malicious automation, we are seeing the number of human reports go down because our tools are catching those attempts before humans see them.

Chris Green: Why are you unwilling to give a figure for the number of people involved in moderation?

Katy Minshall: I will share the figure. I just wanted to give that context. We have 1,500 people working on policy enforcement of content moderation.

Chris Green: What jurisdiction do these people reside in? Are many of them in the UK or the US? Where are they?

Katy Minshall: We are a global company, and they are based all over the world.

Chris Green: So a fair distribution around the globe. Over time, there is increasing pressure from society and politics for more and more censorship, essentially—more and more control. At the moment, it does not seem as though you are actually meeting the mark, which is what society would expect and politicians would certainly hope for. At what point do you think we would have confidence that some of these extremist organisations would be excluded? Would we expect it to be within a day?

Katy Minshall: On scale, we see 500 million tweets a day. One in a million happens 500 times, and we will never get to a 100% success rate
on any of these issues in the near term. We look at our metrics compared to the same time last year: we are now removing three times the number of abusive accounts within 24 hours. That uptick in speed has been independently validated by the EU code of conduct.

**Q948 Chris Green:** Taking a slightly different approach, social media is used by all sorts of different people. In society more broadly, we know whom not to talk to and whom to avoid. In terms of newspapers and things, we know what we do not want to see. Do we ultimately have to take the same approach to social media? We know that there will be unpleasant and repugnant stuff on there, and we have to take a similar kind of approach to the one that we would take more broadly. Is that something we just have to accept?

**Katy Minshall:** That is a decision for lawmakers, and the Government have put forward a proposal. From our perspective, there are plenty of really positive aspects of the White Paper—not least the creation of a new regulator, which could be a big step forward. To come back to some of the challenges, the crux of any tech regulation is international enforcement. There are over 2 million apps on the Android app store, and the overwhelming majority are not based here and do not have people in the UK. The key question is how you enforce a standard of behaviour across the internet that has the capacity to involve those organisations as well.

**Q949 Chris Green:** I don’t think that this tweet would get over the line, in terms of being banned. However, I think you will appreciate that, whether on the hard right or on the left of our politics, there is a lot of repugnant stuff out there. I will just read you this tweet. It was about a video that actually showed Guatemalan soldiers beating young people, and it was put out by someone who I think is on the left of politics, who said: “Why does this secretly recorded video appear to show your cowardly soldiers brutally beating up Palestinian children, again?” That was directed to @IsraeliPM, and the suggestion was that the video showed the Israeli Defence Force. That tweet was widely seen on Twitter. We know the context in the UK of antisemitism and the targeting of the Jewish community and the genuine and legitimate fears that the UK’s Jewish community have. That tweet was not taken down by Twitter; I think it was deleted by the person who put it up. Do you think that it goes against your rules and should have been taken down by Twitter? Is that the case now? Or do you think, perhaps in the future, as the rules develop, it would transgress those rules?

**Katy Minshall:** I will take that specific tweet away because I am not familiar with whether it would break our rules or not. I will come back to you. On the broader question about whether we can do anything about content that does not break our rules, I think the answer is yes, absolutely. There are a couple of things I will point out. First, we now take into account a number of signals in how we organise content in communal areas, like in “search” and in “conversation”. If you are a Twitter user, you will see this “view more replies” section. Content goes through a machine-learning model, to try to understand the level of toxicity and whether or
not it violates our rules. We found that approach somewhat successful. It has decreased abuse reports by 4% and 8% respectively.

The other thing to point out is that, in a couple of months, we will begin trialling author-moderated replies in one country in which we operate. That will give users the ability to hide replies that they get to tweets. I think that there is plenty that we can do beyond our rules to support people in seeing the content that they wish to see.

Q950 Chris Green: Thank you. Mr Potts, how many moderators does your organisation have at the moment?

Neil Potts: We have over 30,000 people working in safety and security, and 15,000 of those are content moderators.

Q951 Chris Green: Fifteen thousand. I understand that the Committee was informed in December 2017 that that figure would be 20,000 by the end of 2018. Why aren’t you reaching that target?

Neil Potts: I think we are still growing, and I think we will continue to be on track with that growth in our content moderators. One of the big places of investment has been in our engineers and our artificial intelligence, which also do the job of what moderators do. We are able to surface much more content that way; we proactively remove it and proactively surface to moderators a better quality of report, so that they can apply our policies.

In fact, we are very transparent about that. We have our community standards enforcement report. I am pleased to say that the next edition is coming out in May. I believe that we are now at over half of all abuse types being surfaced proactively by our automation. That does not rely on a user report or a human but on the AI surfacing it to our reviewers, saying, “This seems like it violating. Let’s review it and let’s remove it.” In that case, it is bearing fruit.

Q952 Chris Green: On artificial intelligence and the advantages that that gives, obviously there will be a learning process, and over time artificial intelligence will be more and more effective. That will also reduce the time between someone raising a concern with the police or with you and your assessing that material and your response—blocking it.

Neil Potts: I think that is correct, Mr Green. I think the way that we think about these issues is really about prevalence, as a metric. What we mean by prevalent, as I think Mr Pancini mentioned, is the views that any piece of content receives. You want to try to limit those views. Now, if there is a piece of content on the platform for one minute, one hour or one day and it never receives any views, it is probably less impactful than something that is getting hundreds or thousands of views, so by using artificial intelligence and automated technologies, we are able to identify what is going more viral or receiving that engagement. That allows us to surface it and review it sooner.

Q953 Chris Green: With YouTube, there is a concern more broadly that I would like you to respond to: the moderators are not necessarily employees of
the company, so how effectively can we hold you to account for the quality of their moderation?

**Marco Pancini:** Let me take a step back and give you an overview on our approach, and then I will answer your very good question, Mr Green. In the last two years we have made progress in that specific space. Thanks to technology that we have deployed, of the 8.7 million pieces of content that we removed in the last quarter of last year, 71% were flagged by machine. Of that 71%, 73% were taken down with no views. That is exactly the point that Neil was making. For us, the goal is to reduce the number of views that the violative content gets on the platform. Of course, the challenge will always be to ensure that we have less and less violative content, but in a certain sense that is out of the control of an open platform, something that is also acknowledged in the “Online Harms” White Paper. Reducing the number of views and—this is the second point—people and machines working together in doing that job are the key elements.

The third point is that we continuously update our policies; we have made 30 changes in the last month, basically since the last hearing. It is also a way to keep up with these developments. The point that was made before and in the previous hearing about the need to be proactive is something that we as an industry are now doing. For the intel desks that we have at YouTube, our chief of the intel desk is a former FBI intelligence deputy. He reports directly to our CEO and they discuss those issues. That is a way to understand, region by region, market by market, where the threat is moving and evolving.

On your question about moderators, first, they are a mix of YouTube employees and external vendors helping us to do the job in that kind of way. They all have the same level and kind of training, done by YouTube people. We created those training courses, which last something between three and six weeks, together with external experts. The moderators go through the same level of training, and they also go through the same level of development. Tenure, expertise and understanding of the issues are important for moderators to become more and more expert, and then to be dedicated to the more delicate issues, such as for example reviewing proscribed groups or terrorist organisations, where you need to understand the context and know the logo and the language to be effective.

All that said, the element of ensuring a high standard across all the different reviewers is present, but it is important to stress that the progress we have made has been thanks to our comprehensive approach. That includes technology, people and policies.

**Q954 Chris Green:** In terms of the moderators, whether they work directly for you or not, YouTube, Facebook, Twitter or whoever is held equally to account, whether it is your employee or a contractor?

**Marco Pancini:** Of course.

**Q955 Chair:** Let me just quickly clarify the figures: is it right, YouTube, that less
than 1% of the videos that are flagged to you by users for hateful and abusive content, promotion of violence and extremism or harassment and bullying are actually removed?

Marco Pancini: Actually, I am not aware of this metric.

Chair: Isn’t that the kind of figure, or at least the sense of proportion, that you ought to have? My understanding from your YouTube report on users flagged in the last quarter that you have got records for—until December—is that around 12 million videos were flagged by users for hateful or abusive content, violent or repulsive content, or promoting terrorism. It looks as though about 110,000 videos were removed in the same quarter. It is not clear whether the ones that were removed included the ones that you identified automatically or whether it is just the ones that were flagged, so it might be a much smaller proportion of the ones that have been flagged to you.

Marco Pancini: Just to summarise—I hope I understood your question correctly—in terms of efficiency, as I mentioned before, in the last quarter of 2018, 71% of the flags that led to removal came from machines. Of course, the machines work. Thanks to algorithms, the artificial intelligence is very precise. Then we have another source of flags, which is the expert trusted flaggers we work with in different countries. We have six organisations here in the UK, which do an incredible job and, for example, the police are also part of the trusted flaggers. The number of flags is much less than the number generated by a machine, but the efficiency and precision of the trusted flaggers is very high—80%. Then we have normal users, but the quality of the flags we receive from everyday users is lower than that of the flags from trusted flaggers and machines. Those are the numbers. I can come back to you with a more specific breakdown.

Chair: Okay. What you have just said suggests that it is worse than 1%. That suggests that less than 0.5% of the content that is being actively flagged by users as violating those standards is actually being removed. That is tiny. Even Twitter is talking about taking action on somewhere between 3% and 10%, depending on the category.

Marco Pancini: We review every flag that we receive. In terms of efficiency, I need to look into the data.

Chair: I am surprised that this isn’t kind of thing for which, even if you didn’t have the precise figure in your head, you would have a rough sense of a ballpark. Maybe it is 10%, 5% or 2%.

Marco Pancini: Forty per cent.

Chair: Forty per cent of the—

Marco Pancini: I need to check, but—

Chair: That would be really helpful. I accept that I may be misreading the data. It would be very helpful to have the same precise data from all the social media platforms. Twitter seem to provide it in some form. For Facebook, as far as I can see, we have information about the amount you
have taken down, but not what it is as a proportion of the cases flagged, so that would be very helpful to have.

Q959 **Stuart C. McDonald:** In a moment I will ask some specific questions about the use of algorithms, but before I do I have a more general question. To what extent would each of you accept that the growth and recent success of the far right and other extreme ideologies is down to how they are able to use your platforms?

**Katy Minshall:** I think that the far right’s use of digital tools is well documented. What is particularly striking—this is something that previous witnesses have raised with this Committee—is the sheer variety of the platforms that are being used. We see people leaving Twitter all the time saying, “Follow me on x,” or, “Add me on y platform.” There is a likely risk over the next few years that the better our tools get and the more users we remove from our platform, the more they will migrate to other parts of the internet where nobody is looking—indeed, maybe nobody can look, because they are private, encrypted communications.

Q960 **Stuart C. McDonald:** That may be true, but isn’t the problem that, first of all, it is on the mainstream platforms like Facebook, Twitter and YouTube that they are brought into the fold? Sure, later on in the journey they are pushed into places where more extreme material can be found, but as a starting point it is their use of these three platforms and one or two others that is incredibly significant. Would you accept that?

**Katy Minshall:** Again, I would go back to the words of Neil Basu. This is an issue across the entire media ecosystem.

Q961 **Stuart C. McDonald:** Mr Potts?

**Neil Potts:** First, I want to say that violence, whether from the far right or other groups that espouse hate and terrorism, isn’t allowed on our platform. We want to make it a hostile environment—as hostile as possible. If the question is about radicalisation, that is a very complex issue. I believe studies show that radicalisation happens in many forms. It can happen at the local pub, it can happen within the family or the church, and it can happen online. Any solution we focus on needs to be comprehensive, attack all those areas and get to the root of what hate is and why the ideology exists. I want to be sure that, when we think about these things, we think of them in those comprehensive terms. I still think there is a lot of study to be done, but I do think that radicalisation can prosper throughout all those areas.

Q962 **Stuart C. McDonald:** But movements such as racist political ideologies that do not even go as far as radicalising anyone to an act of terrorism have had considerable success through use of your platforms. Do you accept that?

**Neil Potts:** I think any type of movement can have success both on social media—online—and offline. I think it is accurate to say that these ideologies largely start offline. They may be able to spread online and reach other individuals. We take that seriously and invest in ways of
stopping that hate on our platform, but I appreciate your point that it can happen in many forms.

Q963  **Stuart C. McDonald:** Mr Pancini?

**Marco Pancini:** There are at least two areas in which I would like to add to what my colleagues said about where we need to work together. First, we need to make sure that the technology or the solution that we, as big companies, implement can be shared with smaller platforms. We have already seen the risk of a spillover effect in the context of Daesh, and that could also happen for far-right groups. That is something we can fight together through, for example, the activity we are doing with the GIFCT to train small platforms on how to use our database of hashes and how to be better prepared for the new threats of radicalisation that, for example, far-right groups present. The second point is the work we have done and can do together to create anti-radicalisation programmes in schools. In 2018, we had a programme that reached something like 2 million students here in the UK.

Q964  **Stuart C. McDonald:** But just to go back to the basic question, do you accept that extreme right-wing and other hateful ideologies are having success, and that a large part of that success is down to how they exploit or are facilitated on platforms such as your own? We are all here trying to work out a solution to something. I just want to be absolutely clear that we all agree there is a problem here.

**Marco Pancini:** We are aware of the problem, of course. These are abuses of our policies that we do not accept. We are studying this phenomenon. What I was trying to stress is that, as much as we are making progress on extremism online, the risk of the spillover effect is something we need to take into consideration.

Q965  **Stuart C. McDonald:** There was mention there of the spillover from offline to online. When your platforms take action, either in relation to a specific post or piece of material or to ban a channel or a particular account or user, to what extent are those decisions based entirely on what has gone on on your own platforms, what has gone on on other platforms, or indeed what has gone on offline altogether?

**Neil Potts:** Maybe I will start. As you may know, we recently banned a number of groups and organisations in the UK, including Britain First, the English Defence League and others. We look at a series of signals on our platform, on other platforms and offline. For example, if we know that an organisation is engaged in violence offline—whether it is hosting events that espouse violence or it is actually carrying out violence—we take those signals in as well. We obviously work with our partners—civil society and academics—to understand this better. We take input from Government and law enforcement, as well as organisations, to be better able to understand those trends.

Q966  **Stuart C. McDonald:** Is it similar with Twitter?

**Katy Minshall:** It is similar. We have criteria by which we designate violent and extremist groups. We are informed partly by national and
international lists; otherwise, it is pretty much three things. First, does the group identify, either through its stated purpose or its actions, as an extremist group? Secondly, does it use violence to further its cause? Thirdly, does it target civilians? All of that considers the offline context.

Marco Pancini: It is absolutely important to work together with experts. For example, the reason why we are giving £1 million to the UK-based Institute for Strategic Dialogue is to better understand the development of this phenomenon. We need to work on better understanding the behaviour of these organisations on our platform, but also to put that into the broader context of the issue at large in our society. That is what can really help us to make progress in better addressing the problem.

Q967 Stuart C. McDonald: I am going to turn now to the question of algorithms. Most of my questions will be directed to YouTube, Mr Pancini. Several users have reported being directed to offensive content, a lot of which promoted extreme right-wing ideologies—video has been recommended to them, even though they have not been engaging in anything remotely similar. Why do algorithms promote that sort of far-right content to people who aren’t even showing any signs of being interested in it?

Marco Pancini: Products like “Up next” or “Recommended” videos are very useful if you are, for example, going on the platform, YouTube, and you search for music. If you want to have a suggestion of other kinds of music that you may like or other users that have looked at that specific video liked, “Up next” is a great tool to discover that.

Q968 Stuart C. McDonald: Sure. Absolutely.

Marco Pancini: The challenge for speech is that there are different dynamics. Speech is very different to cooking suggestions or musical preferences, which are, by the way, the vast majority of the reasons why people come on to the platform. Nevertheless, this is a very important challenge. We are looking into that. There are different measures that we are implementing. I would like to mention at least two. One is to make sure that authoritative content is coming up and has more visibility. That is a way for us to address the specific issues and speech-related issues. The second is to make sure that the controversial content and content that can be offensive has less visibility. Those are the two areas where we are investing, and all of that is in the context of—

Q969 Stuart C. McDonald: But it does not seem to be working at all well. One of the members of the Committee staff here did an experiment in preparation for the hearing. They opened up a new YouTube account and all they searched for were terms such as “British news”, “British politics”, “football”, “music”, “TV” and “games”. Suddenly, through searching with those perfectly innocent terms, they were being recommended towards right-wing commentators and very controversial psychologists, who, essentially, hold what I regard as racist views, and a far-right political figure in the United Kingdom. I am not really getting any idea from you about how this is happening. Why is that happening?
Marco Pancini: It is in our interest to get this right—I want to make that very clear—because this kind of content does not drive any engagement and actually advertisers are not interested in supporting this content. The problem is that in looking at political speech, or speech in general, the suggestions that the user may have are suggestions that can go right across the spectrum, from slightly more extremist, mainstream, to absolutely not related or not extremist-related. Indeed, there is also the possibility that there is a trajectory towards content that is more extremist, but that is not our intention. That is not why we designed the algorithm. That is why we want to find solutions to make sure that it is not happening.

Stuart C. McDonald: Surely you should have a much more precautionary way of approaching it. Fine, the music side of things seems to work absolutely well, but if you are directing perfectly innocent users towards extremist, hateful content, surely the better thing to do, rather than carrying on regardless and saying, “We will see if we can fix it in the future”, is to stop the algorithms applying to certain types of content or directing people to certain types of content. I cannot really see an excuse for why these algorithms are staying in place.

Marco Pancini: It is a very good question, Mr McDonald. Just to give you a number to show you how the situation is not so black and white, 80% of the views that the BBC gets come from “Up next”. That means that there is this challenge, and it is complex, and we need to find ways to improve the quality of the result of the algorithm. It is in our interest and we are working on that.

Stuart C. McDonald: In terms of what the algorithms tend to recommend, you will be aware of the AlgoTransparency website, which collects information about the most recommended videos on YouTube each and every day. Again, the Committee staff did an analysis of the most recommended videos for the first couple of weeks of April. In terms of news sites, for example, 39 of the 44 political videos that were recommended were overtly partisan to the American right and controversial right-wing figures, and had been promoted pretty intensely. Can you explain why that is happening, and how can you defend what is basically political bias?

Marco Pancini: There is no political bias. That is not in our business interest, actually.

Stuart C. McDonald: It may not be direct bias.

Marco Pancini: There is a challenge. We are developing products that are going to ensure, when it is about speech, breaking news or political speech, that content that is labelled as authoritative has more visibility. Those products will be rolled out in the coming months. If possible, I would like to keep you updated on those changes in order to make sure—

Stuart C. McDonald: I think that needs to be done absolutely urgently. In fact, if those algorithms are not correct now, they should just be stopped; they should not be applied to certain types of content. That is
dealing with people who are perfectly innocently searching terms such as “politics”, “football” or “news”. Some people will start off down a road and are interested and deliberately search for a controversial commentator who they are intrigued by. Even there, is it right that your channel picks up on that and essentially reinforces their path down that road, by recommending further right-wing, extremist or hateful content and videos? In that sense, the algorithm deliberately tries to find similar stuff to what they have already looked for. How can you justify doing that?

Marco Pancini: Actually, we do not have any evidence that more extreme content is more engaging for users. Users are not interested in more and more extreme content. The challenge is for specific areas like the one that you have highlighted; finding product solutions to make sure that the users who come on the platforms find content that is in line with our interests, of course, but which is not offensive.

Q973 Stuart C. McDonald: But you realise how frustrating this is? I hope those products arrive tomorrow; we cannot wait for that. Some 70% or 80% of the viewing that happens on YouTube is of recommended content. That is such a significant part of the product that if it is wrong, fundamentally, we have significant problems with the channel altogether.

Marco Pancini: That is why I mentioned the figure of 80% of views of the BBC come from “Up next”. It is actually a great tool for the BBC and, by the way, for other broadcasters. It is a very important tool to give visibility to authoritative content.

Q974 Stuart C. McDonald: That is great, but if, at the same time, certain extremist and hateful videos are getting up to 1 million views at a time because of the way that your algorithms work, I do not care if the BBC gets a few extra hits. My concern is that 1 million extra people have seen that content and are being pushed along a path to extremism and hate. Everyone on this panel seems concerned about protecting free speech, which is great—absolutely—but they seem less concerned about pushing folk, inadvertently or otherwise, down a path to hatred and extremism. Why is that not just as much—if not more—a concern as protecting free speech?

Marco Pancini: I want to reassure you that we care about this issue—we care deeply about this issue. We want users who come on YouTube to have a positive experience. We want the 2 billion users who come on YouTube every month to have a positive experience and we want to invest in products that give more visibility to authoritative sources. Today, if you look for breaking news, you already get more authoritative sources than in the past. That is the direction that we are taking. I would be very happy to update you on the official product launches that we are planning in the UK, to ensure that you can see the evidence.

Q975 Stuart C. McDonald: Ultimately, the problem is also that the far right are showing themselves capable of exploiting your algorithms. I do not know if you are aware of the report by the Data & Society research institute about the alternative influence network, for example. Have you heard of that report?
Marco Pancini: It does not come to the top of my mind, but I think I know what you are talking about.

Q976 Stuart C. McDonald: Basically, significant influencers, who may be sympathetic to extreme right-wing views, bring on extreme right-wing figures. They have a nice cosy chat, do not challenge any of their views, and it is all seen as nice and rebellious. By doing that, the 1 million followers of that internet or YouTube personality are suddenly directed towards the extreme individual who was invited on to that show. Do you accept that your algorithms are vulnerable to exploitation in that way?

Marco Pancini: We are also working on specific tools in relation to this issue to give visibility and transparency. If the news outlet is state sponsored, we are working together with the European Commission on something called the code of conduct to protect the European election, where we are working with fact checkers and third parties in order to make sure that information can be verified.

There are ways to find solutions for this problem. The message that I would like to give you is that we are aware of the issues and we are working on that. It is not in our interest to have this effect on our users. We want users to have a safe experience.

Q977 Stuart C. McDonald: Would you be happy for an independent regulator to have oversight of your algorithms?

Marco Pancini: Absolutely. The solutions that are in “Online Harms” are all interesting solutions. We are looking forward to providing our feedback in the context of the public consultation. But this is a direction we have seen in other fields. For example, the AVMS directive is going in the direction of giving more power to the regulators in relation to some of the activities of our platforms. That could actually be the effort to build the trust between the industry and the institutions.

Q978 Chair: The trouble is, Mr Pancini, you have had this issue about your algorithms pushing people towards more and more extreme content raised with your company repeatedly. Yesterday, I did a search on YouTube for a relatively popular right-wing US YouTuber. As a result, I immediately had recommended on my home page, as the third recommendation, another channel from somebody who has promoted racist and homophobic language.

As a result of clicking that, on my YouTube channel this morning, on my home page, the first and fourth recommended videos that come up are for the former leader of the EDL, somebody who has been banned on both Facebook and Twitter. I have never searched for his videos but they are coming up. Videos with him included in them and promoting him are coming up as the first and fourth recommendation. How on earth is that happening?

Marco Pancini: “Up next” recommended—

Q979 Chair: This is not “Up next”; this is on “Recommended”. This is just coming up as recommended on my home page—the recommended videos
for me to watch.

Marco Pancini: The logic behind this product is to provide to users, who have seen a specific set of content, suggestions that are in line with the content that they have seen before.

Chair: With each one, the next thing being recommended for me was something that was more extreme than the first thing I had looked at. The first thing I looked at was a right-wing US site. The second thing was more extreme and clearly included somebody who used racist and homophobic language. The third thing was even more extreme and was somebody who was promoting Islamophobia and was cited as a cause of radicalisation in the Finsbury Park attacks. How is that happening? It is a clear example of YouTube—your platform—recommending increasingly extreme content.

Marco Pancini: This is happening in the context of speech and political speech because the logic of “Recommended” or “Up next” is based on the behaviour that the user had on the platform, which works for 90% of the experience that the users have on the platform. Of course, I am absolutely aware of the challenges that these represent for specific areas like breaking news and political speech. That is why we need to work on product solution. We are working on product solution in order to reduce the visibility.

Chair: The only thing you talked about in your product solution is the authority level of news. If I search for the BBC, I might get Sky and I might get other similar news channels. That is not about far-right extremism. I want to know what you are doing to stop your channel promoting further and further extremist material, with your channel and your algorithms effectively radicalising people.

Marco Pancini: We have an approach that is very clear. First and foremost, we look at the law. If the content is illegal, the content has to go down. If the content is against our policies, with the approach that I described before, we enforce this policy, but I agree that there are areas—

Chair: You are recommending it; you are promoting it. This is not about whether or not you have got it on. There is a separate question for you about why you have not banned something that is currently being banned from Twitter and Facebook, and for specific reasons and evidence, but the question is why you are promoting it.

Marco Pancini: We actually found solutions, and this is about the 30 policies that we launched in the previous year to reduce the visibility of this content. In relation to some of these examples, we have evidence that because of the action that we took, these speakers lost a lot of visibility. They are becoming basically—

Chair: Seems pretty visible to me. This is the top recommended video, just as a result of me searching for one channel and then clicking on another that was recommended to me. That is all I have done to get this to be the top promoted video for me.

Marco Pancini: I am not here to defend this kind of content.
Chair: No, but your predecessors have already said that you were supposedly doing something about this. We raised this with your company in December 2017, so almost 18 months ago. Dr Lundblad admitted at that point, “Clearly, this becomes a problem when you have content where you do not want people to end up in a bubble of hate”. He said that you need to “make sure that we use machine learning”. That was 18 months ago. It still has not happened.

Six months later, I asked William McCants; I said the same thing, because at that time I had been looking for some of the National Action videos. Again, at that point I got similar kinds of videos—extremist videos and white supremacist videos—being promoted at me. I said, “Does that cause you some serious alarm?” He said, “Personally, it causes me a lot of alarm...I will take this back to our team and see why this is happening...It is important for the company and for our bottom line for the recommendation engine to work as it is intended...It should not be serving up videos that incite or inspire hate.”

How is that any different from what you have just said to us now? You are not doing anything about this, despite the fact that you have been warned, not just by this Committee but by law enforcement, and by people across the world, not just in this country, that your algorithms are pushing people towards more and more extreme content.

Marco Pancini: In relation to the specific issues that you mentioned, on the proscribed groups, we took action. In the last year, we took down 100 pieces of content. We have a proactive approach; we are doing exactly in line with the expectation that you have. Our focus is really to have an impact on this kind of content and reduce—

Chair: You are still coming back to the same thing: you are talking about removing content. I think there is a big problem with you not removing content that is extremist, but let us put that aside; that is not the question I am asking you about. I am asking you about what you are promoting, what you are recommending, and what your algorithms are doing. The algorithms that you profit from are being used to poison debate.

Marco Pancini: There is no intention from our side to promote speech that is an abuse of our policies. We want to enforce our policies against this kind of content, whenever it is against our policies, whenever it is illegal. There is a series of content that is not illegal, that is not against our policies—

Chair: What are you doing about your algorithms?

Marco Pancini: On the algorithms, we are making broader changes in order to make sure that whenever a user is searching for breaking news or for political speech, the results they are going to get are authoritative sources.

Chair: I am not asking you about authoritative news. This is not the DCMS Committee; we are not asking you very good questions about fake news. I am asking you about extremist content, and your algorithms that are promoting it.
Marco Pancini: On extremist content, we are going to tackle the visibility. Whenever content is offensive—still not against our policies, not illegal, but offensive—we put this content in a situation where this cannot be searched, cannot be recommended.

Chair: Sorry, but this just has been recommended.

Stephen Doughty: This is just absolute rubbish from you. When I was searching last night, it is not just the algorithms; it is your actual channels that people are then being encouraged to subscribe to.

I have a channel here from a well-known extreme right-wing person who used to be linked to the BNP, a self-described Nazi and so on. It is just video after video on a subscriber channel with 86,000 subscribers—which is fairly high, as you know—with videos like “Black man throws white boy off balcony”, “Bullied to death for being white”, “Treason from Parliament”, “The media promotes anti-white violence”, “How the Israel lobby controls”—you know. It is video after video after video of curated content by one of your subscriber channels. The example that I gave to you earlier on was also a subscriber channel. It is somebody who boasts, on that channel, that they have closed down one of their other channels and opened a new one sharing those speeches talking about “niggers” and “faggots”. What on earth are you doing? It is the algorithms. It is the channels. You are essentially accessories to radicalisation—accessories to crimes.

Marco Pancini: It is not in our business interest to have users going through these bad experiences—

Stephen Doughty: So why are you doing it?

Marco Pancini: First, I would really love to look into this content together with our team and come back to you with a specific answer in relation to that.

Stephen Doughty: That is what you say every time: “We’ll look at it.” “We don’t want to do this.” You are not actually taking the action.

Marco Pancini: Actually, we took action. We had 30 policy changes. The content in question—a lot of the content that you have mentioned today—is content that cannot be shared, cannot be commented on, is not even—

Stephen Doughty: But it is being shared and commented on.

Marco Pancini: That is why I want to look into the specific example that you are making in order to come back to you and give you an answer, because it was actually our responsibility to look into the comments that you made and come with specific solutions.

There are improvements—the numbers that I mentioned to you before. The fact is that in relation to the worst of the violations, including some of the violations that you are mentioning, 90% of the content that we took down had fewer than 10 views. That is actually a number that shows how we made progress on enforcement. In the area where—
**Chair:** But it does not deal with your algorithms. Chris Green, did you want to come in on that point?

**Q990 Chris Green:** Yes. We are going through a very curious political time at the moment. In 2009, Nick Griffin was elected to the European Parliament to represent the north-west of England. There was another member of the BNP elected to represent Yorkshire and the Humber. Is there any circumstance in which a Member of the European Parliament or a Member of the British Parliament could be banned from YouTube, Facebook or Twitter?

**Katy Minshall:** Any user on Twitter is subject to our rules. Something we are looking at is if there are occasions where it would be helpful to have a public interest interstitial, in that there may be times when individuals in public life say something that is against our rules and, by removing it, we decrease awareness of that violation, and whether it is of value to have a note saying, “This breaks our rules but we’re leaving it up because it’s in the interest of the wider public to be aware of.”

**Q991 Chris Green:** In that context, I suppose it is a bit like the BBC “Question Time” programme. Nick Griffin appeared on it, which actually damaged him and the reputation of the BNP, because his performance could be seen by a whole series of people. Could you think of a circumstance where you would actually ban an MP or MEP?

**Katy Minshall:** Every Twitter user is subject to our rules.

**Q992 Chris Green:** And from Facebook and YouTube?

**Neil Potts:** Similarly, all Facebook users in our community are subject to the rules, which raises a very interesting point for Members of Parliament or others who have stood in elections, and how we go about making those decisions to ban organisations, for example Britain First and the BNP, who have stood in recent elections. We take those decisions very seriously. They are very hard. I think this is a place where regulation can be helpful to give us a steer on the correct ways to operate. We want to be respectful of political speech, but we also do not want abusive users and users who subscribe to hate ideology to be on our platform. In the case of Britain First and the BNP, we have moved to banning those and all those affiliated, but we recognise that it is a very difficult decision.

**Marco Pancini:** Same for us. We look at a piece of content, and if the content is against the law or against our policies, we take action.

**Q993 Tim Loughton:** Apologies—I was not here at the beginning of the session, so I hope that I do not repeat anything. Mr Pancini, you seem to be in denial that it is not just the individual sites that are lingering on your platforms that we are primarily concerned about. There seems to be a systemic problem that you are actively, because of the way your sites and algorithms are structured, signposting and promoting extremist sites. Theoretically, if I were to search for “black boots” on your site, ultimately I would be signposted to a Nazi sympathiser group—in its extreme, it seems to work—but you do not appear to see the significance of that.
Marco Pancini: We do. We take this issue very seriously. We understand that, for specific areas, there could be an effect that is not intended. That is why we are investing in products in the different areas that I described before, to ensure that authoritative sources are coming up—

Q994 Tim Loughton: We keep coming back to authoritative sources and fact checking. On some of the sites that we have heard about, where it says “All Jews should be killed” or “Black people need to be murdered”, you don’t need fact checkers to see that those are completely unacceptable. If somebody starts off looking for extremist sites—be it terrorism, extreme right wing or left wing, or whatever—and as a result of which they are looking at more extremism, so there is a clear pattern of behaviour, does that flag up any warnings to your moderators, indicating that here is somebody who is looking at stuff that is clearly potentially dangerous? Would that therefore initiate action by you towards that person doing the browsing?

Marco Pancini: That is a very good question; thank you, Mr Loughton. We made some experiments together with Jigsaw, our think-tank that is looking into these issues, to ensure that when a user is searching for extreme content, we also suggest content that is going in the direction of tackling the radicalisation issues in their behaviour. In specific areas there are tools that can be put in place.

Where it is a bit more challenging—but again, with our products and our policies we are tackling the issue—is the area around political speech that can sometimes become controversial. In public debate we have thousands of examples of this. This is where it is more challenging. This is where we are looking into products to ensure that it is not just about being authoritative—I want to be very clear—but about providing different ways, for example a contextual box or making reference to sources that can help the user who is looking at a video—

Q995 Tim Loughton: Okay, I don’t think I understand most of that. We have raised this on countless occasions with another group of your predecessors. They always say, “We are looking into this,” rather than, “This is actively going to be put into force.”

Can any of you conceive of a situation—this goes for dangerous radicalisation and political terrorism or whatever, as well as for people with eating disorders and people who are self-harming, which is a particular concern that I have—where if somebody is exhibiting a pattern of behaviour, for example looking at sites linked to “How do I kill myself?” or “How do I harm myself?”, it would flag up a warning message on your platforms, about which you would proactively take some action? I do not mean showing an authoritative source or a BBC site on slimming advice, but something that would specifically flag up that there is potentially somebody here who is going to get up to mischief to somebody else or to themselves, and therefore third parties need to be informed about it. Is that doable on any of your platforms now, or is it intended to be?
**Katy Minshall:** This is a major priority for us. You will have seen our CEO talking about looking at everything from the fundamentals of Twitter right through to our partners on the ground.

I draw your attention to two things that we are doing. First, we have a partnership with the University of Oxford, looking specifically at how exposure to a variety of different viewpoints can reduce prejudice on Twitter. Secondly, we now give all our users the opportunity to turn the algorithm off on Twitter. If you click twice in the top right-hand corner of the app, the algorithm is off. You can see all the content just in order of the users you follow.

**Neil Potts:** Mr Loughton, I think that is a great question. I think a lot of this discussion is about the discoverability of content and how you can reduce the incentive of people who interact with borderline content. We have found in our research—every company has its own research—that no matter where you draw the line with prohibited content and reliable content, people tend to engage more around the borderline content.

Our CEO, Mark Zuckerberg, has spoken about wanting to flip the calculus on that, to make it less likely that you will engage with borderline content. We can do that through algorithmic changes and things such as suggestions, where we now invest in not suggesting things that are borderline, even if they are not violations. I think, Mr Doughty, you mentioned a number of groups. I think those are really violating on Facebook, so I hope they would not be referred, but even things that come close to that, we want to flip that calculus to make sure that we are not surfacing them to you—that they stay buried, and then, once we do designate that, they will be removed. Mr Loughton, your point about whether it is someone who is searching for extremist content, or someone searching for issues around suicide and self-harm, we do a lot in that space to surface resources to those individuals. For extremist content, for example, after a white nationalism and separatism announcement in the United States, we are now redirecting individuals who search for that content on Facebook to a group called Life After Hate. It is a group of former extremists that offer resources, offer intervention, for people that are searching for that. I think those are big steps. Similarly with suicide—

Q996 **Tim Loughton:** How many sites are you doing that for?

**Neil Potts:** We are partnering with Life After Hate now in the United States. We are looking to roll that programme out more globally. I know here in the UK we work with the Online Civil Courage Initiative, or one of our current speech initiatives, where they have Hope not Hate, they have the ISD, others that work with that group, where we think that there would be a likelihood that we offer redirection services, so that we can have intervention.

Q997 **Tim Loughton:** How many sites are you redirecting from now?

**Neil Potts:** It would be searches on our platform. Maybe I am not understanding your question, sir.
Q998 **Tim Loughton:** You are saying that if somebody is looking for these extreme sites then they can be redirected to something that is—it may be, for Mr Pancini, an authoritative news source, but you are saying it is something that may be an antidote in some form to whatever hate extremist site they have alighted on.

**Neil Potts:** It is a number of search terms, and I would have to come back to follow exactly the search terms. So it is not just sites—

Q999 **Tim Loughton:** The point is we have had all this “We are looking at”, “We are in discussions with Oxford University”, “We are dealing with all these groups”. These discussions have been going on for ages. You have the personnel, the technology and the algorithms now to clamp down on this stuff. I never cease to be amazed how many products I never knew I couldn’t live without that I am told when I just do basic searches on any of your platforms. If you put a fraction of that effort, in trying to promote the sale of goods and get the revenue commission from doing so, into coming up with algorithms that actively redirected people now to antidotes to hate sites, or didn’t signpost them to the sort of sites that the Chair has come up with, we might start to take you seriously. So let’s drill down into some of your numbers, Mr Potts. You told us just now that 15,000 of your employees are involved in content moderation. That was the figure you gave?

**Neil Potts:** That is correct, sir.

Q1000 **Tim Loughton:** Right, even though it is below the 20,000 target for 2018 that one of your predecessors indicated and even though, at the last quarter alone, your revenues went up by 61% to $16.9 billion. So there is no lack of money to invest in those people. So of those 15,000 people, how many of them are actually designing algorithms that will redirect, prevent hateful content, or react and quickly take down hateful content, actually moderating sites that come up? How many of those 15,000 are doing that rather than moderating algorithms that will try and sell me more product?

**Neil Potts:** I am sorry, I want to be clear; I would have to check the transcript of Mr Milner’s comments. We now have 30,000 people who work in safety and security. That includes subject matter experts, whether they are in counter-terror or safety, around things like suicide, safety around other health issues. We have 15,000 in what we call content moderation, who specifically focus on enforcing the policies. That is within that 30,000. We also have thousands of engineers who build out the algorithms. So I think the number—I am having a little difficulty trying to parse the number for you; I want to be clear—of 30,000, which is obviously more than 20,000, are the 30,000 people who are working in this area that work together in concert across to scale all these policies to our global community, so in many ways I think we not only have met the 20,000 but we are beyond that.

Q1001 **Tim Loughton:** What are these 15,000 doing?


**Neil Potts:** The 15,000 that we speak of—they are specifically content moderators who enforce our policy based off user reports, based off proactive algorithms that surface likely violating content to them. Those people, based in over 20 different offices globally, speaking over 50 languages, work on the process to ensure that reports are being reviewed quickly, that we can enforce those within a very quick turnaround time.

Q1002 **Tim Loughton:** So they are there purely and exclusively to remove or prevent or respond to harmful content.

**Neil Potts:** They are, and they build the processes to help us both scale that and be quicker in our response.

Q1003 **Tim Loughton:** Purely dealing with harmful content.

**Neil Potts:** Harmful content in all of our abuse types. You have types of abuse such as spam, financially motivated bad actors. There are things like credible violence, terrorism, the sharing of private and identifiable information.

Q1004 **Tim Loughton:** So they are not all involved in harmful content. Spam and other things like that are an inconvenience, but they are not the same as harmful content.

**Neil Potts:** That is a grey point about the definition of what you consider to be harmful content.

Q1005 **Tim Loughton:** It is not a grey point, it is an obvious response. You have just told me that all 15,000 people are dealing with hateful content, and now you say that actually a lot of them are dealing with spam, which cannot necessarily be construed as hateful content. We would just like to know what these people do. You are the first $1 trillion capitalised company in the world, and you have an awful lot of money to employ people to do being rather more than you are doing now, and to prevent hateful content, not design algorithms that want to sell us more. I would really like to meet some of those 15,000 people to find out exactly what their job is and how proactive they are being. Time and again you tell us what you are planning to do, and it does not come to reality. That is why now, regulation has become a thing.

Ms Minshall, you said just now that the new regulator proposed in the White Paper was a “big step forward”. Why?

**Katy Minshall:** Two things. First, in my experience with Twitter so far a great deal of really good work is going on, whether that is holding us to account, or support services or research. Having one organisation that can co-ordinate and convene all that good work would be particularly helpful from the perspective of users who sometimes do not know where to turn when they see issues online, and they don’t know the differences between our policies.

The second aspect is that part of the problem—this is what is driving the regulation—is the perception that tech companies such as ours that have come from the west coast are unaccountable alien organisations. Having
an organisation in the UK that is accessible to the public can help to restore some of that process and accountability for British citizens. There are lots of ways that could be positive, but we still need more detail on the operation of the new regulator.

Q1006 **Tim Loughton:** So you agree that you are unable to regulate yourself.

**Katy Minshall:** I believe that a number of actions have been taken over the past couple of years, particularly around the removal or terrorist content across the industry, that have had a really positive impact. It would be particularly good if the new regulation builds on that. With something like GIFCT—

**Tim Loughton:** This is a simple question. If you think we need a regulator to regulate your business, that must be a tacit admission that you are incapable of regulating yourself.

**Katy Minshall:** Our CEO has spoken about this. He sees our role very much as educators, and there are plenty of ways that regulation could be a positive step forward.

Q1007 **Tim Loughton:** What is the purpose of Twitter anyway?

**Katy Minshall:** Twitter exists to show entertainment, sport and news. It is about what is happening.

Q1008 **Tim Loughton:** What is your favourite social media platform?

**Katy Minshall:** Twitter.

Q1009 **Tim Loughton:** So why have you only tweeted six times this year?

**Katy Minshall:** As part of my role as a public-facing representative of Twitter, I take quite seriously what I tweet, which probably means there is a level of thought behind when I do tweet.

Q1010 **Tim Loughton:** Six tweets since Christmas. Why do you only have 413 followers? Would that be a good Twitter account, only to have 413 followers?

**Katy Minshall:** That is quite difficult to say.

Q1011 **Tim Loughton:** It is not very difficult. Why are you not taking your own product seriously? Why are you not using it to disseminate good, responsible practice for your company? You describe yourself as working for Twitter on your Twitter account, yet I can’t find a single example of where you have tried to promote good practice for social media users.

**Katy Minshall:** I am very happy to send you examples of where I have retweeted exactly that information.

**Tim Loughton:** I can’t find any.

**Katy Minshall:** It is there.

Q1012 **Tim Loughton:** How many years ago?
**Katy Minshall:** Within the last six months. There are multiple examples.

**Tim Loughton:** Well, it is not one of the six tweets you have done since Christmas. I just don’t think they are there. I find it extraordinary that as a representative and the public policy person for a major social media company, you are not making use of your company’s product to promote more responsible practice among your users.

**Katy Minshall:** What I would also say is that 40% of our users never tweet; they use Twitter on a daily basis to access content and not to tweet. There are a range of ways our users engage with the platform.

Q1013 **Tim Loughton:** Yes, but they don’t work for Twitter, do they? Which other countries regulate better, or do you, or perhaps Mr Potts or Mr Pancini, think that actually you don’t need to be regulated more than you are at the moment? What are your thoughts on having a regulator as proposed in the White Paper?

**Marco Pancini:** I would like to mention two experiences that I have had in the past years in this regard. One was with the European code of conduct. We started to discuss this code of conduct—it is self-regulation, but the European Commission was heavily involved—because there was a lack of trust that we could improve on the way we were dealing with the referrals that we were receiving from users and from NGOs. We started with a very tense relationship. We worked with the Commission and with the NGOs, and the first result of this was also not super-positive: we had a removal rate of around 40% in 24 hours, which is the threshold. Through three rounds of reporting, by keeping on working with the NGOs, by working on these issues and through all the improvements that we put in place, we have arrived, now, at a removal rate of 80% in 24 hours in relation to the monitoring that is happening, through NGOs, on our platform, of hate speech.

Q1014 **Tim Loughton:** So, are you in favour of a regulator?

**Marco Pancini:** That was self-regulation—just to give you an idea. Another example involves AVMS. With the new code of conduct, there is no regulator; it is self-regulation. It is us working together with NGOs. The NGOs, for a period of time, monitor our platform and they send to us a request. They take note of our answers. They go back to the Commission and give it the result, and the Commission publishes the result. So it is purely self-regulation. This is an example of something that is working, but—

Q1015 **Tim Loughton:** I’m not sure I got an answer to the question. Perhaps I will get one from Mr Potts. Are you in favour of a regulator, and can you signpost us to any countries that you think have tougher regulation?

**Marco Pancini:** I think there are situations where regulators can help. For example, in the context of AVMS, the fact that now, for specific services on our platform, there will be a regulator that will oversee our activities is something that is positive. On GDPR and privacy, there are regulators that are working with us on data protection issues. What I am saying is that I think our industry can successfully regulate itself in some specific areas
and show improvement in a very transparent way; and in other areas, working together with regulators can be a way to build trust. I think both solutions can be applicable to our industry.

Q1016 Tim Loughton: Mr Potts?

Neil Potts: Mr Loughton, I first want to say—I am saying this also to the Chair and all members of this Committee—that if you would like to visit our content moderators, we are more than happy to work with you to set that up. We have a large content moderation team, which sits in Dublin—our international headquarters. In fact, one of our largest engineering teams outside the headquarters—Menlo Park—sits here in London. They do much of the work to train the AI on finding harmful content for removal. So we are happy to set that up and happy to follow up with the team after this session.

As far as regulation is concerned, I think we recognise that we want Government to play a more active role in this space. Our CEO, Mark Zuckerberg, has spoken about four areas, one being harmful content; the others are election integrity, privacy, and data portability. You also asked for an example of where perhaps regulation is getting it right. I think that in the context of providing certainty to any industry, both for larger companies like ours and for smaller companies that are growing, in this space, it is always good. GDPR may be an example of where regulation, in a harmonious framework, is good. Every example—well, I would love to be able to work with our regulatory lawyers to review and to make sure that we can commit to those things, but those are areas where I think we recognise the value of government and really encourage it.

Q1017 Chair: Let me ask you a final few quick questions. The first is to Twitter. David Duke tweeted two days ago, blaming the awful attack in Sri Lanka on the “Zionist Occupied Government” and the “Zio media”. He is the former Grand Wizard of the KKK. You have banned Britain First. You have banned the former head of the EDL. Why have you not taken down David Duke?

Katy Minshall: I was not aware of that specific tweet. There may be a team that is already reviewing this; let me go away and I will come back to you as soon as possible.

Q1018 Chair: I think there is a real concern that you just have double standards for different people and that you are not consistently removing some of this extremist content.

Katy Minshall: Like I said, let me come back to you as soon as possible.

Q1019 Chair: Facebook, I welcome some of the work that you have announced recently on removing some far right extremists. You have said, “Individuals and organisations who spread hate...have no place on Facebook.” What are you doing about closed groups and secret groups?

Neil Potts: Thank you, Chair. Different services on Facebook have different problems, and closed groups or secret groups are one of those services. About two years ago, we started the safe communities initiatives,
to ensure that we were removing both harmful groups and content that was harmful that appeared in those groups.

We are not only reviewing content, whether it’s user-reported in those groups, with our proactive measures, with our artificial intelligence service, and we are also holding the group admins more accountable now. So, if I was a member of the group and I was posting harmful content that violated it, I would get my penalty, as normal, but those penalties would also read down towards the admins of those groups. As you eclipse a certain threshold, you run the risk of having the group removed, and you run the risk around being able to admin or moderate other groups as well.

Q1020 Chair: How do you know about those groups and what is happening, though, if you do not have users within them reporting things?

Neil Potts: Fortunately, we do have users even in some of these enclosed groups who will report things. We also run our automated services within the groups.

Q1021 Chair: Okay, let me tell you about one closed group that I had reported to me last night. It describes itself as a “direct action group”. It makes a reference to me and my family, and says, “Just shoot them. Criminals.” There’s another reference to somebody else, saying, “They should be shot.” And then somebody else says, “Kill them all, every fucking one, military coup, national socialism year one, I don’t care as long as they are eradicated.”

That group has over 30,000 members. The only reason that I know about it is that somebody sent me some screenshots about it last night. The comments are from several weeks ago, so your systems obviously have not flagged them or done anything about them. Isn’t the truth that you are providing safe places to hide for individuals and organisations that spread hate?

Stephen Doughty: Accessories to crime.

Neil Potts: Chair, we want to be hostile to those groups. Obviously, I am not aware of that group. I will follow up with you directly to make sure that we review that group, remove those actors and, where appropriate, work with law enforcement on any credible threat. We have enacted a number of measures following the unfortunate incidents in this House and the targeting of other elected officials in the world.

We are now more impactful in our enforcement against violence, intimidation and incitement around Members of Parliament and around other elected officials. So, not only do we remove credible threats but we remove even aspirational threats—something like if someone says, “I hope someone shoots them.” To a normal person, maybe that is just puffery or a hyperbolic statement, but we realise the position that you all are in and that those statements may turn into incitement, and we do remove those. We want to be more aggressive in that space—

Q1022 Chair: What are you doing to identify them, particularly the large ones? So you have got large sites that may be promoting racism, or
homophobia, or violent threats within those closed groups, and within secret groups. And it’s not possible for anybody else from the outside who might disagree strongly with their values to be able to see what they are doing, in order to be able to report them to you. And yet you are providing a forum for people with extreme views to escalate and organise. In this case, as I said, it describes itself as a “direct action group”, so it encourages others to take direct action, of whatever kind.

Neil Potts: Again, we want to use our artificial intelligence—really leverage the artificial intelligence—to help find that. It is the case, as we spoke about earlier, that artificial intelligence is not infallible at this stage; it will never be infallible. But we will work on that, to improve training and to improve the investment there to find these groups. And once I connect with you after this hearing, we will not only get groups removed but train our classifiers.

Q1023 Chair: You have had raised with you the possibility of legislation around these kinds of secret or closed groups, so you must presumably have looked at this, because it has been discussed in Parliament. So surely you should be taking a more proactive approach, particularly to these groups that have a large number of members.

Neil Potts: I hear your concerns, Chair. We are going to go back and rectify it—not only this group, but I will make sure that my leadership and those who I work with understand the urgency.

Chair: Look: I think, overall, you will have heard the concerns from every member of the Committee. We have taken evidence from your representatives several times over several years, and we feel as if we are raising the same issues again and again. We recognise that you have done some additional work, but we are coming up, time and again, with so many examples of where you are failing, where you may be being gamed by extremists or where you are effectively providing a platform for extremism.

You are enabling extremism on your platforms. For example, Mark Rowley, who is the former counter-terror chief, said that the Finsbury Park attacker “had grown to hate Muslims largely due his consumption of large amounts of online far-right material including, as evidenced at court, statements from former EDL leader…Britain First and others.” This is why it matters. There is evidence that the police and law enforcement agencies are giving us of radicalisation being done online that leads to people being hurt and killed, yet you are continuing to provide platforms for this extremism and continuing to show that, actually, you are not keeping up with it. Frankly, in the case of YouTube, you are continuing to promote it—you are continuing to pursue and promote radicalisation that in the end has huge, damaging consequences to families, lives and communities right across the country.

Particularly in the case of YouTube, I am just appalled that the answers that you have given us are no better than the answers that your predecessors gave us in every previous evidence session. As far as it
seems from your organisation in particular, very little has changed. I think you can see why Parliaments and legislatures across the world are despairing at your ability to do what you need to do to keep people safe. We hugely value the work that social media companies do, but we need you to keep us safe and you are not doing so.

Thank you very much for your evidence.