FACEBOOK, INC.

Moderator: Tom Reynolds
April 26, 2019
11:00 a.m. ET

Operator: This is Conference # 9549757

Operator: Hello and welcome to today's Facebook Press Call.

There will be prepared remarks and a Q&A to follow. To ask a question after the prepared remarks conclude, please press "star," "1."

Now, I'd like to turn the call over to Tom Reynolds who will kick this off.

Tom Reynolds: Thanks, operator, and thanks, everybody, for joining the call today. This is Tom Reynolds from the Facebook Communications Team.

With just under a month before voting begins for the European Parliament elections, we wanted to share an update on the many efforts we've undertaken to help quiet the spread of misinformation and prevent foreign interference.

On today's call we have Nick Clegg, Facebook's Vice President of Global Affairs and Communications; Samidh Chakrabarti, who is our Director of Product Management for Civic Engagement and Elections Issues; Antonia Woodford, the Product Manager on our Integrity Team; Nathaniel Gleicher, Head of Facebook's Cyber Security Policy; and Richard Allan, our Vice President for Global Policy.

Each speaker will give some brief remarks and then we'll open up for questions. As a reminder, the call is on the record with no embargo. A full transcript will also be posted in our newsroom shortly after the call concludes.

And with that, let me hand it over to Nick to get us started.

Nick Clegg: Thanks, Tom, and thanks, everybody, for joining us. It might be 20 past 8 here in California, but I'm conscious of the fact that it's early Friday evening just before the weekend for many of you, so I'm particularly grateful that you have joined us today.

And as Tom mentioned, we wanted to lay out for you the work we've been doing over the past 15 months or so to help protect the upcoming EU elections. For Facebook, this work -- increasing our and strengthening our defenses with each election -- has been a journey with a real learning curve because with each major election around the world we've become ever more sophisticated.

We develop smarter technologies, greater transparency, and better defenses. And as we head towards the start of voting in just under a month, the EU elections undoubtedly present one of the most complex challenges that we've faced -- 28 countries, 24 official languages, and a heightened atmosphere of political polarization.

If I compare the politics today to when I stood as a European candidate precisely 20 years ago, it is a completely different political environment in which we are operating. And we're also up again ingenious and aggressive adversaries. And so, we constantly need to work hard to stay ahead of them.

Commensurate with those challenges, our preparations for these elections represent one of the most sophisticated operations we've ever deployed to fight against misinformation, combat hate speech, and prevent foreign interference. For example, we now have nearly 40 teams working on elections across our family of apps.

We are launching a new Elections Operations Center in Dublin which will help our coordination and rapid response efforts. And with recent additions, we now partner with 21 fact-checking organizations in the European Union covering 14 languages. This marks a significant improvement and puts us in a stronger position than other social networks.

We continue to improve our systems for identifying the fake accounts and coordinate information campaigns that account for much of the interference, and we now remove millions of fake accounts every day. We've created a new standard for advertising transparency where anyone can search our political ad archive, see who had paid for an ad, and what are the ads they have run. We established and independent election research commission to study our impact when it comes to elections to help us find ways to improve even further in the future.

One quick word if I may about a figure that's been widely reported recently, the issue of how we're administering our system of political ads. As you know, I spoke to Antonio Tajani, the President of the European Parliament, last week about this. We have built our system around the legal responsibility, which is conferred upon national election authorities. The European Parliament and others have asked us to provide a temporary exemption for a prescribed list of (particular) groups (and) EU institutions.

We've said we are open to doing that, but we obviously need the consent of those bodies who have the primary legal responsibility for the conduct of these elections; namely, the national election administrations. And I hope that will be forthcoming in the days to come so that we can then move forward in a collaborative way.

And that I hope also illustrates an important final point I want to make, which is that we cannot do all this work on our own. We are actively working in partnership with EU institutions, with governments, with electoral administrations, with academics, with campaigning groups, and that is a collaborative approach that we are very keen to continue across the industry with governments across the European Union as we seek to make online campaigning as safe and as transparent as it possibly can be.

And with that, I will turn over to Samidh.

Samidh Chakrabarti: Thanks, Nick. I am Samidh Chakrabarti, Director of Product Management working on civic engagement in elections.

Now, as Nick mentioned, our work on preparing for these really important elections began early last year and is built on in-depth research and the detailed risk assessments to help customize our approach for the EU. With those findings, we've continued to build out our toolbox to help stop the spread of misinformation and to fight bad actors.

As Nick mentioned, a key piece in that site is stopping fake accounts and every day we block millions of them; often at the point of creation before they can do any harm. And last year we significantly advanced these defenses. First, through better AI and machine learning, we've gotten better at detecting and blocking fake accounts created through automation. We've also created new tools to proactively identify fake accounts specifically targeting civic issues, like elections. And finally, we improved and accelerated manual review of suspect accounts.

Our improved technologies have also improved automatic translation at scale. Translating more content into more languages helps us better and more quickly detect material that violates our policies. It also expands access to the products and service offered on our platforms. We've recently had 24 new languages added to our system and we continue to expand this work and that's going to be critical for the EU.

Two other areas I want to highlight include our work to battle voter suppression efforts and new transparency efforts for pages with lots of followers. On fighting voter suppression, we've gotten more proactive in this work. Rather than wait for reports from our users, our teams now use trained algorithms to actively conduct sweeps tuned to identity violating content. For example, it might be content that promotes the wrong date of an election, or who can and can't vote in an election. And if we find it, then we can remove it and we can remove all bad content in bulk from the platform.

On increased transparency, we're beginning to require page admins with large followings to enable two-factor authentication for increased security and they must also confirm their locations. These steps help preventing of hacking and reduce the ability of foreign page admins to promote civic content targeting an audience in another country.

Lastly, I want to briefly mention our Elections Operation Center located in Dublin focused on the EU elections. This initiative builds on the work we did for Brazil and the US elections last year. Its structure allows our global teams to better coordinate in real time across regions and with our headquarters in California. It'll also accelerate our rapid response times to fight bad actors and bad content because we know in an election, every moment counts.

The teams in the ops centers serve as another layer of defense, building on a lot of the work that Nick outlined and it'll include representatives from threat intelligence, data science, engineering, research, community operations, and legal, amongst others.

So with that, let turn it over to Antonia for a deeper dive into our work to fight misinformation.

Antonia Woodford: Thanks, Samidh. I'm Antonia Woodford, a Project Manager with our integrity team focused on misinformation.

Our efforts to fight false news rely on increased investments in both technology and people, with the goal of reducing opportunities for manipulation, while still allowing for open discussions. Our effort follows a three pronged approach which we call remove, reduce, and inform.

When something violates our policies we can remove it from Facebook altogether. When we know something can be a problem but there are legitimate reasons for it to exist on Facebook, then we can reduce its presence by using news feed ranking. And finally, we can inform people by getting them context about the posts their seeing in their news feed so they can decide for themselves what to read, trust, and share.

When it comes to removing problematic content, if misinformation violates our community standards and contains content like hate speech, or calls to violence, we'll remove that content outright. Samidh mentioned our increased work on voter suppression misinformation, which we also remove. As context, during the US midterms our election war room found and removed

45,000 pieces of voter suppression content, more than 90 percent of which we identified proactively before it was reported to us.

Fact checking is another area we've been expanding over the past couple of months. We use machine learning to send potentially false posts to third party fact checkers to review. And these fact checkers review the content, check the facts, and rate its accuracy. This includes links and text posts as well as photos and videos. If fact checkers find a post to be false we'll greatly reduce its distribution in news feed so fewer people will see it and share it.

As Nick mentioned, we now work with 21 fact checking partners in Europe, who review content in 14 different languages. This includes five new partners we added just this week as part of an international fact checking network consortium called FactCheckEU, whose members will review content on Facebook and publish fact checks on the FactCheckEU Web Site. And finally, as part of the inform actions, in addition to notifying people that have shared false news and displaying articles from fact checkers alongside fact checked content, we're helping people better separate misinformation from credible information and decide for themselves what to trust, by partnering with local organizations across Europe through youth outreach, academic grants, and Newsroom training.

This includes efforts such as our partnership with the European Youth Forum to help young people spot false news online. In Germany we support Zeitverlag and Digibits, who educate young students and teachers in schools about false news and how to fact check. And in Poland last year we held media literacy workshops for journalism students at five major universities and launched a media literacy campaign.

With that, I'll turn things over to Nathaniel.

Nathaniel Gleicher: Thanks, Antonia. I'm Nathaniel Gleicher, Head of Cyber Security Policy for Facebook.

One area we have significantly grown over the past two years is our security work to combat information operations -- any coordinated effort to manipulate

or corrupt public debate for a strategic goal. In particular, combating election interference. Our focus in this effort is on three major areas.

First, growing our team of expert investigators who focus on the most sophisticated actors and threats. Second, based on the insights we gained from these investigators, we're building and continuing to improve our automated tools that help scale our defenses. And third, we're continually making product changes that makes life harder for the bad actors trying to engage in this type of manipulation.

Our teams are constantly working to identify threats, looking for patterns, researching bad actors and designing new detection methods and really looking to catch any small mistakes by those who want to do harm. We've announced dozens of takedowns of coordinated inauthentic behavior across the world, from Asia to Europe to the Americas. We're constantly following up on thousands of leads of potential activity globally, including information shared with us by law enforcement, industry partners and civil society groups.

To our security teams, it doesn't matter who the actors are or what their goal is. We take action based on their behavior; not who they are or what content they're posting. As I mentioned, finding this activity requires a mix of human and automated efforts. Our human expert investigators track and catch the newest tactics that cutting-edge threat actors develop. As we identify new techniques, our product teams develop scaled automated solutions to combat these new tactics, enabling our human investigators to keep focused on the most sophisticated bad actors.

Over time, this cycle means we can continually adapt our platform to make deceptive behaviors much more difficult and costly. We've already begun to see important impacts from our efforts to run this security cycle. For example, when we work to detect and remove fake accounts and as we require additional verification for political ads.

Finally, based on our elections security work around the world over the past two years, we've seen how important it is have strong partnerships between industry, law enforcement, policymakers, electoral commissions, journalists,

researchers and civil society groups. Our ongoing relationship with the Atlantic Council's Digital Forensics Research Lab and our recent work with Avaaz, are great examples of this collaboration. They help us find potential bad activity and assist in analyzing the content we action related to coordinated inauthentic behavior.

While these efforts are global, we also customize our work to individual countries based on research and threat assessment that begin many months before ballots are cast. Earlier this year, we announced the launch of the Integrity and Security Initiative under the leadership of the BSI. The initiative brings together experts from the public sector, industry -- including Facebook, Twitter and Google -- as well as scientists from universities and think tanks. With this initiative, we aim to build a better and more comprehensive understanding of election interference and thereby help guide policymaking in Germany and across the EU.

Now let me turn it over to Richard.

Richard Allen: Thanks very much, Nathaniel.

I'd like to close by briefly highlighting some of the major changes that we'd be making to political and issue advertising on Facebook in the run-up to the elections. These tools help us to deliver on two key goals that experts have told us are important for protecting the integrity of elections. First, preventing online advertising from being used for foreign interference and second, increasing transparency around all forms of political and issue advertising.

To help prevent abusive interference, all political advertisers in the EU now need to get authorized in the country where ads are being delivered if these relate to the European Parliamentary elections. We ask them to submit documents and we use technical checks to confirm their identity and location. We recognize that some people can still and try and work around any system. But we're confident that this will be a real barrier for anyone who's thinking of using our ads to interference in an election from outside of the country.

Importantly, this means that the people who are reaching you without identifying as relating to politics or issues have been authorized as being in

your country and will be required to provide accurate information about who they are. This will help relevant authorities investigate them if they have any suspicions. There are many issues that only election regulators an effectively decide -- for example, if campaign finance rules have been followed -- and our new tools will help them in this important work.

And Nick mentioned earlier the question of cross border ads that's been raised in the EU. And again, I wanted to reiterate why we arrived at this decision. We did an analysis earlier this year and one of the things that came out of that analysis was that we -- one of the risks that was presented in this election would be that somebody would set an organization up in one EU country in order to direct advertising to influence an election in another EU country.

And just to be clear, I am sitting in the U.K. today. If I were to do that, I would not be breaking any U.K. law, which only governs ads and political activity inside the U.K. I'd be unlikely to be breaking the law of (third) country and even if I was, it'd be very hard for them to come and get me in the U.K. So that was the core rationale for why we ended up determining that the safest option was to allow people only to advertise in the countries where they've been authorized.

Finally, just to flag that, to increase transparency, all of the ads related to politics and issues on Facebook and Instagram in the EU must now be clearly labeled, including a paid-for-by disclosure from the advertiser at the top of the ad. This means that you can see who is paying for the ads and for any business or organization, their contact details. And when you click on the ad, you'll be able to see some additional information around the budget associated with that ad and some details of the people that -- who saw it.

We also understand that many people are getting -- are interested in getting information about the ads run by political campaigns. And this is especially useful for election regulators and watchdog groups, including the media. We built a new tool called Ad Library to make it easier for everyone to find out about political or issue ads on Facebook and ads will be kept in that library for seven years. As well as being able to browse and search that on Facebook, we've also created an application programming interface, or API, so that those

with more expertise can in an automated way analyze all of the ads that have been run on Facebook and hold both the advertisers and ourselves accountable.

These changes will not prevent abuse entirely. We're up against smart, creative and well funded adversaries who change their tactics as we spot and block their abuse. But we believe that they will help prevent future interference in elections on Facebook and that's why they're so important.

Tom.

Tom Reynolds: Thanks, Richard.

Before we take questions, I understand a few folks were a little bit late joining. I just wanted to reiterate that the opening comments so far and the transcript of the full call will be available quickly after on the Facebook Newsroom for -- to help with your reporting.

With that, operator, we can turn it over to questions.

Operator: Thank you. We will now open the line for questions. Please limit yourself to one question per person. To ask a question, press "star" followed by the number "1." Again, please press "star" followed by the number "1" to ask a question.

Your first question comes from the line of Madhu Murgia from Financial Times. Your line is open.

Madhu Murgia: Hi there. This is Madhu Murgia from the Financial Times.

You -- one of you mentioned how you start seeing threats circulating quite a lot in advance of the actual election process. And I wondered if maybe Nathaniel or any of the others working closely on this could tell me a little bit about the trends and threats in Europe at the moment? What do they look like? What trends are you seeing in terms of the discussions happening on Facebook in relation to the election with -- if you have specific examples of stories that are already circulating at scale that might be fake, for example?

Nathaniel Gleicher: That's a great question. Thank you.

As I mentioned, we have teams that are continually investigating to look for evidence of what we call coordinated inauthentic behavior. One of the key things that I want to mention though is, as we're looking to investigate for groups trying to manipulate or deceive or engage in election interference, one of the key things this team focuses on is behavior and patterns of behavior as opposed to the particular content that people might be sharing.

So in this context, we've actually already brought together teams of people. A couple of months ago, we had a team of people come together in Europe to work through a series of scenarios to think about the types of threats we anticipate for the European Union Parliamentary elections to make sure we're prepared and ready to respond to those.

And since then, we have been continuing to run our proactive investigations to understand the types of threats that are out there. Whenever we conduct these investigations, as we identify evidence of foreign interference or coordinated inauthentic behavior, we immediately drive our investigation to conclusion so that we can remove that from the platform and we announce it publicly to make sure that people are aware of the types of behavior we're seeing.

So as we continue to identify and respond to this type of behavior, we will be making sure that -- we will be making sure that your colleagues in the press, our civil society partners, and policymakers understand what we've seen and the actions we've taken. Over the course of recent months and over the last year, we've done takedowns involving activity around the EU including content that targeted people in the United Kingdom, including content in other countries, and we've announced each of those and you'll see us continue to do that going forward.

Operator: Your next question comes from the line of Mark Scott from POLITICO. Your line is open.

Mark Scott: Yes. Good afternoon, everyone.

I just wanted to follow-up on the (F.T.'s) question regarding inauthentic behavior. You've now had the transparency tool up and running in Europe for, what, a couple of weeks now, maybe 10 days? Can you give us any sense of the type of activity you're seeing? Is it -- have you seen any, either foreign interference or domestic, who's coordinating messages in an -- in an illegal manner in the last 10 days?

Thank you.

Nathaniel Gleicher: Sure, I can take that one.

And I think it's actually a great question because there's another piece which we -- which we mentioned when we were talking -- we mentioned that our teams are continually looking for this type of deceptive, bad behavior, this coordinated inauthentic behavior. But in addition, partnerships with external organizations that do their own investigations are absolutely critical.

And one of the goals of the transparency tools we've built out is so that investigative journalists, civil society investigators, can find and identify bad behavior themselves. They can dig into the details here and then we can work with them to make sure we take sure we take action on this type of behavior.

A great example of this is Avaaz recently raised to us three separate investigations that they'd identified into potential networks of bad behavior in the context of Spain. Working with them, we identified, while these networks weren't engaged in what we would define as coordinated inauthentic behavior, we did see widespread use of fake accounts. And we took action and removed those fake accounts which radically reduced the scope and capacity of the actors in this case.

So that type of investigation, building on the transparency tools that we have is absolutely critical, and we've seen that no one organization can do this by itself. So part of what we're doing is building up our own capacity to run these investigations, but an equally critical part is building up transparency tools so that external partners can run their investigations and building our partnerships with civil society, with law enforcement, with government actors around the region and around the world.

Operator: Your next question comes from the line of Kristin Becker from ARD. Your line is open.

Kristin Becker: Good afternoon from Germany.

My question is regarding sort malicious actors. Can you say something about who they have been targeting so far in Europe most? Like which countries basically and who they are or what kind of findings you have about them?

Nathaniel Gleicher: Sure.

As you'd expect when we're talking about our own work and our investigations, we have to be a little bit careful in how many details we provide because it's really critical that when we take disruption actions it is as effective as possible. Whenever we identify and take down a network like this we put out a blog post that details what we can confirm about the actors behind it and what we can confirm about the behavior they engaged in.

One of the things you'll see is that we're very careful to only describe what we can validate based on our technical investigations. So you'll see in a number of the newsroom posts descriptions of who we think the actor might be. If we describe that it is because we can prove that based on the technical identifiers. If we don't detail that in a news post -- newsroom posts it's because while we can see they're engaged in coordinated inauthentic behavior, we do not have the technical evidence to prove who they are.

And the key for us is we don't need to know who is behind something in order to take action against deceptive behavior and violating behavior. That's to make sure that, because often it can be challenging to determine who exactly is directing this behavior, we can still take rapid action as it develops.

Operator: Your next question comes from the line of (Raphael Bellinari) from (Late Echo). Your line is open.

(Raphael Bellinari): Yes. Hello, everyone.

Just following up on the previous question, could you give a few figures on the number of fake accounts that you took down in the recent days or weeks, perhaps also the number of political advertisers that failed to meet your standards?

And also just on a second note, how did you improve and learn from previous bugs and mistakes perhaps after you launched the EU election center in the US -- there was the election in Brazil and there was a huge misinformation campaign on the app -- so how did you learn from previous bugs? Yes.

Nathaniel Gleicher: Great. I can take the first part of the question.

Our ability to be able to detect and block fake accounts that are not just created through automation but also manually-driven fake accounts that are created by people has definitely continued to improve over time and we're at the point now that we really block millions of fake accounts every day. We don't have a specific geographic breakdown of that because really this is a global problem and we apply these technologies to be able to work at global scale irrespective of where they appear to be coming from. I think that addresses the first part of your question.

Yes, and then I'll turn it over to Richard to -- yes.

Richard Allan: (Yes, it's Richard).

Just on the (learnings point). One of the other trends that we've seen that's very interesting are changes in the legislation related to elections. Brazil, in particular, they passed a law which requires any politician who wishes to place electoral ads to use only services that meet certain transparency requirements. So that created a very strong incentive for Brazilian politicians to sign up to the transparency -- the ad transparency tools. Canada has also recently completed a law that they're starting to implement requiring politicians, for example, to give accurate disclaimers.

So we have been learning in terms of technology and the ads transparency tools that we've got now are state of the art based on what we're able to provide. And I think they will capture a very large proportion of political ads

run in this election. But we're also very conscious this needs to run in parallel with legal reform that makes clear what the obligations are of a political advertiser when they're using platforms like ours.

Samidh Chakrabarti: And this is Samidh. I'll take the last part of your question also in terms of learnings from prior elections.

I think it's important to recognize that over the last several years we've actually been working on a number of elections all around the world. Each ones, of course, present their own unique challenges, but from each one we learn a great deal and we're able to then apply those learnings to future elections. So our defenses cumulatively get better with every single election.

So you asked about Brazil, for example. So Brazil was an election that was the first time we created an Election Operation Center for any election where we brought together a cross-functional team to be able to rapidly respond to issues as they arise. And so from that, we actually had a great number of operational learnings in terms of how to be even more efficient in decision-making, how to share information that's necessary internally between functions in order to come to more rapid decisions. And those are learnings that we're absolutely applying as we open up this dedicated Election Operation Center in Dublin for the EU election.

And one of the reasons I think this is particularly important and those learnings are extremely applicable is that we really need to operationally look at this as -- and be prepared for essentially 28 elections running in parallel. And so the learnings operationally from Brazil are absolutely instrumental in helping us be able to handle a large number of elections happening in parallel as constitutes the EU Parliamentary elections.

Nathaniel Gleicher: And then one last note just make is that one of the clear learning for us from all of the elections we've run is how critical it is to have close collaboration from government and industry to ensure that we can protect these elections. We benefited greatly from that partnership around the US midterms, for example, and one of the things we've been especially focused on over the last -- over recent months is making sure that we have these

partnerships, both at the national level with the -- with the member countries around the EU, and with the European Commission and the work that they're doing.

Tom Reynolds: Operator, we can take the next question.

Operator: Your next question comes from the line of Dave Lee from BBC News. Your line is open.

Dave Lee: Hi there. Thanks for taking the question.

This may be for Nick, I guess. We heard earlier this week that Facebook had put away $3 billion in preparations for (regulators' fine) in the US. I'm just curious, are you doing the same in preparation for (a fine) from the European Union and what might that look like size-wise?

And in a similar vein, to what degree is the company concerned that the regulators might (force) changes in governance at Facebook as well as monetary fines?

Thanks.

Nick Clegg: David, I'm going to disappoint you because (there's not a lot) that I can (say) -- so I can't, as you can imagine, say much about the FTC process. That's a process which is -- which is ongoing. We're working with the FTC as they discharge their regulatory duties and in conformity with the law governing (denouncements), we revealed the estimates the we did in the earnings call earlier this week. But that is all contingent on a process coming to completion which hasn't yet come to completion.

Similarly, as for the inquires that are going to proceed or not from regulators elsewhere in the EU and other jurisdictions, quite rightly that is -- that (tempo and) that content (is entirely) determined by them, not by us, so I can't -- I just -- you'll have to refer to the -- particularly to the Irish Data Protection Authority who (is also) the principal data protection authority to whom we're accountable in the European Union. I think they've made public that they're looking at a number of -- a number of issues and we will wait just

as much as everybody else will have to to see what next steps they want to take.

The only final point I would make is that a company the size of Facebook, operating as we do around the world, it is right that we're seen to be held to account as we proceed. I mean, accountability -- with success comes accountability. And we take our responsibilities -- legal and otherwise -- very seriously, and we think it is right that the mechanisms of accountability operate effectively going forward.

Operator: Your next question comes from the line of (Manoi Mochado) from (New El Salvador). Your line is open.

(Manoi Mochado): Hello. Good morning, good afternoon. My name is (Manoi Mochado) from (El Salvador).

The question I ask is about Facebook. (Similarly to) Facebook and WhatsApp -- (similarly) to what you are doing in India), are you doing anything to make your fact check and (software determination) of fake news in WhatsApp to European users?

Nathaniel Gleicher: Great. Thanks for the question.

We've been working on these election integrity measures across the entire Facebook family of applications, and every single application takes the responsibilities here extremely seriously, and that includes the team at WhatsApp. WhatsApp has been working extremely hard to put a number of measures in place to protect against potential abuse of their platform around elections.

And I think one thing that's really important to understand is that WhatsApp is actually a fundamentally different kind of platform and service than Facebook. It is fundamentally a private messaging application and therefore the vectors for abuse are actually quite different than one might see at Facebook. And so, some of the things that the WhatsApp team has done to stay ahead of any sort of potential abuse is that they've actually created a

bunch of really important computational techniques to crack down on spammy behavior.

So since WhatsApp is a private messaging platform more so than a broadcast mechanism, spamminess would be the vector by which people would try to abuse the platform. So that is exactly why they have done an immense amount of work to computationally crack down on spammy accounts. And they're also at the point that they are banning millions of fake accounts every month in order to stay ahead of this.

Another part of this is actually to -- the WhatsApp team has worked to constrain the virality of their platform and have instituted a global limit on the number of times particular messages can be forwarded. So that global limit is currently five. And so that's (led) to also reduced risk of things like by viral misinformation.

And then the final component of their work has really been around creating tools and putting information into the app that helps empower people to control their WhatsApp experience more. And so they've done an immense amount of work for example to help people better control how they're added to groups, they've added indicators to messages to show when they've been forwarded so that people know if it's original content or something that's being -- that's being forwarded. And so all these things, they've really taken together a comprehensive approach, which is what's required when you're dealing with complex challenges like this.

No single measure is going to work and so all these measures have been working in concert together around the computational techniques, the crackdown on spammy behavior, constraining (virality) in various ways and empowering people to control their experiences.

Operator: You next question comes from the line of (Simon Cruz) from (Berlin SJE). Your line is open.

(Simon Cruz): Yes, hi, everyone.

I was wondering how confident people from smaller countries and smaller language areas can be that Facebook is also devoting resources to monitoring content, for example in Danish or the Nordic languages? I suppose it's almost inevitable that small language areas will be less resourced so it could open a possibility to make them more vulnerable to misinformation campaigns. How would you -- how would your answer to that?

Nathaniel Gleicher: I'll take part of that question, for sure.

We really are being prepared across all 28 potential elections here, and that has meant that one of the key challenges that we identified is having in parallel -- to have our systems be prepared for the multiplicity of languages across the EU. And so that's actually one of the chief reasons that we have invested so much over the last year and a half on automatic translation technologies, to be able to do this at greater scale, to be able to train our integrity defense measures, to be able to account for languages across the entire European Union.

And our systems are much better prepared for this as a result of that than they've ever been before.

Antonia Woodford: And I can also talk a little bit about some of our fact checking work.

We've been really focused on trying to get fact checking coverage across the EU, and so just this week added five new partners that are participating in an international fact checking network consortium. So now all of the IFCN certified fact checkers in the EU that are publishing fact checks are part of our program and are able to review and rate content on Facebook. And that covers 14 different languages with 21 different partners.

Nathaniel Gleicher: And then the last thing that I would just say is, as we pull all of this together, the teams that are looking for this type of deceptive behavior, I mean, we often talk about having 30,000 people across the company that think about security and safety. And part of the reason for that is it gives us the language skills we need around the world and in the EU.

Whenever we're running an investigation, we're able to rapidly ramp up the linguistic skills and the local cultural and regional skills that the team needs to understand the threat and to run that investigation quickly.

Operator: Your next question comes from the line of Mark Di Stefano from BuzzFeed News. Your line is open.

Mark Di Stefano: Good day.

A few months ago Facebook put Tommy Robinson on a dangerous persons list, so support for him on the platform was effectively banned. Now, Tommy Robinson is actually running in these elections and a couple weeks ago you also took action against groups like Britain First in the U.K., (they also are) running in the (EU as well).

I wanted to get a sense of how many people Facebook have that are monitoring and removing white nationalists and far right content; that's my first question.

And then the second one, when can other countries -- and so I'm thinking of maybe France and Hungary -- when can other countries expect their similar style crackdown where the top far right white nationalist groups are going to be placed on those lists?

Richard Allan: Yes. Richard Allan here.

Let's be clear, when somebody -- we have a process whereby we look at indicators to try and reach an objective view of whether an individual -- an individual represents white nationalists or represents a hate figure, and if that's the case, then they are not permitted to have a presence on the Facebook platform. And that's irrespective of whether or not they're in a political party (or standing) for an election.

So that designation is about the behavior and the effect that that individual is having, and (to say the) fact they're standing for an election does not mean that they automatically have a right to a presence. So that's how we will treat individuals.

To your question on how many people within the safety and security team that Nathaniel just referred to, there are a number of experts who work in this space who are, themselves, often from civil society or have an expertise and understanding what the markers are for somebody or an individual or group or a hate organization.

They are actually active in multiple languages, so we do have individuals who've been designated as hate figures actually in the countries that you named. For example, there are individuals already and groups in France and Hungary and Germany and so on that have actually been designated for some time. It's a consistent policy approach.

Obviously, there is more attention on it recently and so when we recently designated a number of groups in the United Kingdom, we told people about that, I think you can expect that to happen again, that where we make significant designations then there will be a public announcement. But I do want to be clear that the -- that the approach, the policy is global, and there are individuals and organizations in pretty much every country in the world who may have fallen on the wrong side of that line and may already be banned from having a presence on Facebook.

And I would expect that there will be more. Obviously, having a larger safety and security team allows us to do more of these investigations and do the assessments properly so that we can treat people fairly but also ensure that our policies are correctly enforced.

Tom Reynolds: Great. Operator, we're going to have time for two more questions, please.

Operator: Your next question comes from the line of (Stefan Manjess) from (ZDS). Your line is open.

(Stefan Manjess): Thank you.

I just have one question regarding the report about the Code of Practice that Facebook signed with the European Union. The European Commission criticized in their statement a couple of days ago that Facebook and Google

and Twitter don't give enough access to data for researches and fact-checkers when it comes to fake accounts.

Can you or can one of you just say whether you're going to give more access to researchers or why you haven't so far?

Thank you.

Richard Allan: Yes. It's Richard here.

We are -- so there are two things just to be clear about in the report that the EU have issued. I think that was the one they released recently -- was overall positive, so they made some very positive comments about the activities we've undertaken. (I mean the first), just to be clear there they were certain data items that they have asked for from us that we're not in a position to provide because we don't record the data in that way.

We've explained that to them and we understand why they're disappointed. They wanted something but we're simply not able to provide those specific data items because we're recording things that -- differently on our systems and we want to be accurate when we put data out. That's the first part.

The second part is this question of access by researchers. We have a program that we've been developing actually over, I think, more than a year now to make sure that there are data sets that are available to researchers who are looking at issues like misinformation and false news. Again, we understand that researchers want that data as quickly as possible and we're working hard to do that.

There is a lot of complexity around it, particularly around issues related to privacy. We've got to make sure that in meeting the requirements that people have to be able to dot hat research, we don't undermine one of our other objectives which is to make sure we keep data safe and secure. We are committed to that, we're working hard at it, we understand that the (commission and others) want it as soon as possible. And we will deliver it soon as we can do so in a safe manner.

And there is a large consortium now working to that effect of people inside Facebook and independent people outside of Facebook.

Nathaniel Gleicher: One of the areas where we really worked on this is whenever we do takedown for coordinated inauthentic behavior, we announce the takedown publicly, we describe the nature of the behavior and we describe the accounts that we're taking action on. Obviously when we're announcing something like that, people want to understand what the content was and what the operation was and who was behind it.

We also partner with outside investigative groups. The Atlantic Council's Digital Forensics Research Lab is one, we've worked with (Grafica), we've worked with cybersecurity research companies. In each case what we'll do is we'll let them conduct their own analysis so that we get a separate, external, independent perspective on the nature of the content and the nature of the campaign.

And one of the key reasons we do that is when they conduct that analysis, they can commit to keep protected any privacy implicating information that might be included in that set. And so that's one way that we're working to bridge what is a really difficult divide.

How do we make sure that people understand the nature of the bad behavior that's happening while simultaneously protecting the privacy of the users that are on the site and ensuring that we're not hyperbolizing or sensationalizing these campaigns. Which, we know some of these actors want to engage in.

This is one way we work to balance this that has been effective and you'll see if you look at all of our Newsroom posts for each of our takedowns, the dozens we've done in recent months, you'll see links to these various analyses. You can see an external perspective.

Tom Reynolds: Thanks. Operator, we're going to have time for one more question, please.

Operator: Your last question comes from the line of (Julie Demot) from (ASP). Your line is open.

(Julie Demot): Hi, I've got two questions.

One is for Nick Clegg. You mentioned hiring an independent election commission (person). I'd like to know more about the role and what to expect from that person?

And for Samidh, you were talking about the improvements -- machine learning, manual review -- what were you not able to do before that you can do now?

Thank you.

Nick Clegg: Forgive me, could you just ask that first question again?

(Julie Demot): You -- Nick Clegg mentioned hiring independent -- somebody independent to check on the election, like an election commission but hired by (Facebook)...?

Richard Allan: ...the research commission, Nick, it was the research commission...

Nick Clegg: ...(sorry) -- I got it, sorry. I think we might be talking in slightly cross-purposes. What I was referring to was the independent election research commission, which Richard was just alluding to which we're doing with a network of academics, and where we are trying to -- as Richard just described earlier -- mindful of our legal responsibilities and ethical responsibilities to protect privacy, abide by data protection rules and so on, provide data to researchers so that they can better explore over time the (connection) between the information that (folk) consume on social media platforms and the way people behave in elections.

So that was -- I was referring to a research facility; not an independent person or a watchdog for this particular European election.

Nathaniel Gleicher: And I'll take the second part of the question which was around advancements that we've made around fake accounts.

Really the biggest advancements we made in the last couple of years is not just being able to protect against accounts that are created through automation or bots but actually against fake accounts that are created by real people. So

even back in 2016, our fake account defenses were quite robust against things like bots, but really what 2016 exposed was that the -- a form of manipulation was taking place where real people were basically creating fake accounts to do abusive things on our platform.

So what we've been able to do using artificial intelligence in the last couple of years is actually combine hundreds of thousands of different behavioral signals to be able to more accurately predict if an account is likely to be fake even when it's run by a real person. And so an example of this is that -- people who create fake accounts, the structure of the friend networks of those -- of those fake accounts actually look different than the typical Facebook user.

Also in how they behave on the platform also looks different than the typical Facebook user. So for example a fake account might be much more likely to join a bunch of groups early on in -- during their time on the site than a typical user. No one of these signals is really accurate enough to figure out whether something is a fake account, but that's where the artificial intelligence and machine learning come in. It allows to combine hundreds of thousands of these kinds of signals to make more accurate determinations.

So we believe that we are much more able to detect and block these kinds of manually-driven fake accounts than we were able to before, and that's one of the reasons that we're now able to block millions of fake accounts per day and keep our platforms more secure.

Tom Reynolds: So with that, we're going to have to conclude.

Let me just reiterate, first of all, thank you for joining us today especially in the various time zones where you might be. Second, we'll have a full transcript of both the opening comments and the Q&A as quickly as possible available on our Facebook newsroom. And then lastly, if we could be of any help with any follow up questions, you can reach us at press@fb.com.

And with that, thank you very much.

Operator: This concludes the Facebook press call. Thank you for joining. You may now disconnect your line.

END