FACEBOOK, INC.

Moderator: Tom Reynolds
October 26, 2018
9:30 a.m. PT

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," "one."

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

Tom Reynolds: Thanks, operator, and thanks, everyone, for joining us this morning and happy Friday. I'm Tom Reynolds from Facebook's Communications Team.

A few minutes ago, we announced that we have removed dozens of Pages, Groups and accounts that originated in Iran and were engaged in coordinated inauthentic behavior. Nathaniel Gleicher, Facebook's Head of Cybersecurity Policy, is here with me today to talk though the news with you, and then we'll take some questions.

Before we get started, just a little bit of housekeeping. The call is on the record and with no embargo.

With that, let me turn it over to Nathaniel.

Nathaniel Gleicher: Thanks, Tom.

This morning we removed 82 Pages, Groups and accounts that originated from Iran and have violated our policy against coordinated inauthentic

behavior. These included 30 Pages and 33 Facebook accounts as well as three Groups on Facebook and 16 accounts on Instagram.

Coordinated inauthentic behavior is when people or organizations create networks of accounts to mislead others about who they are or what they're doing, and we prohibit it on Facebook because we want people who use our services to be able to trust the connections they make here.

Our Threat Intelligence team first detected signs of this activity late last week and we quickly launched an investigation. Manual reviews of these accounts linked the activity to Iran. They also identified some overlap with the Iranian accounts and Pages we removed in August.

However, our investigation is still in its early days, and while we have found no ties to the Iranian government at this point, we can't say for sure who is responsible. As we've explained on previous calls, it's often hard to know for sure exactly who's behind this type of activity, and that's proven to be the case with this investigation so far as well.

In most cases, the page administrators and account owners attempted to hide their true identities by passing themselves off as U.S. citizens, and in a few cases, U.K. citizens. These accounts frequently posted about politically charged topics such as race relations, opposition to political leaders, and immigration.

And their activity was targeted at people using Facebook in the United States and in the U.K. About one million accounts followed at least one of these Pages, and about 25,000 accounts joined at least one of these Groups, and more than 28,000 accounts followed at least one of these Instagram accounts.

In terms of advertising, we found less than $100 in spending so far on Instagram and Facebook across two ads paid for in U.S. and Canadian dollars. Given that the U.S. midterm elections are just a few weeks away, we took action as soon as we completed our initial investigation. We've also already shared what we know with U.S. and U.K. government officials, U.S. law enforcement, Congress, other technology companies, and The Atlantic

Council's Digital Forensics Lab, its forensics research lab which is doing additional analysis into the investigation themselves.

Today's action follows similar takedown efforts we announced earlier this summer, including another set of Pages, accounts, and Groups tied to Iran. We continue to get better at finding and taking down these bad actors using a combination of machine learning and manual investigations. But we face smart well funded advisories who will never give up and constantly change tactics as we improve.

The adversarial nature of this work means that we will need to continue to invest heavily in safety and security -- not only to prevent election interference on Facebook but also to protect the authenticity of the connections and conversations across our services.

Tom Reynolds: Thanks, Nathaniel.

Operator, we can open it up for questions.

Operator: 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 "one."

Your first question comes from the line of Jo Ling Kent of NBC News. Please go ahead.

Jo Ling Kent: Hey, guys. Thanks so much for doing this call with us.

My question is, what has been the response from the U.S. government, (and) not in -- just in relation to this particular case -- but in the final 10 days to the midterms? I know you touched on that briefly, Nathaniel, but are you satisfied with what you're getting in terms of intelligence and responsiveness from the U.S. government?

Nathaniel Gleicher: Thanks, Jo Ling.

Yes, we work closely with the U.S. government. We have been in contact with law enforcement -- both the Foreign Influence Task Force at the FBI and the Department of Homeland Security. As with all of our major takedowns

we reached out to them before taking this action to ensure they knew what was happening and that they could run any investigations they needed to run.

More generally, in the days leading up to the elections we have been in close contact with them, we worked closely with them, and one of our priorities is to make sure that as our government partners identify particular threats, they're able to quickly reach out to us. That includes federal law enforcement. It also includes, by the way, state elections officials -- the people who are actually on the ground and running polling places.

Because as we lead in to the final days before the midterms our expectation is that they will be seeing challenges and that we have made sure that they can reach out to us and that we can work with them quickly to identify those and respond. That's exactly why we have built the war room that there's been a lot talk about and pulled these teams together -- so that as our partners in government and elsewhere identify things we can respond to them very quickly.

Operator: Your next question comes from the line of Chris Fox of BBC News. Please go ahead.

Chris Fox: Hi.

I was just wondering whether you can share how many people saw the posts that were on these fake Pages and how many posts there were, and how many people clicked that they were attending the fake event?

Nathaniel Gleicher: We're still investigating those details. We first identified this activity about a week ago and so we've moved pretty quickly to get this out, but we're still looking into the specific details about this. As we learn more we'll continue to share it.

Operator: Your next question comes from the line of Sheera Frenkel of New York Times. Please go ahead.

Sheera Frenkel: Hi.

I was wondering, you said you found this on manual review? Can you tell us a little bit more about that? And specifically, was it linked to the Iranian state media accounts that you removed in the past?

Nathaniel Gleicher: That's a great question.

We found this, as we said, based on our own internal investigations. There were some links back to the Iranian assets we removed in August. But we haven't seen direct links back to the Iranian state media in the way that we saw some links back in August; we haven't seen that here.

And I should say that our internal investigations into this involve a combination of -- we have manual teams of investigators that are looking for specific threads they can pull. And obviously something we said in August was that we'd continuing to investigate this type of activity, so we continue to pull those threads.

And in addition we have data science teams that work really closely (where) those manual investigators are looking for patterns that they can see in larger behavior to identify potential inauthentic behavior. And in this case, our investigations here involve both of those techniques working together.

Operator: Your next question comes from the line of Donie O'Sullivan of CNN. Please go ahead.

Donie O'Sullivan: Hey.

Is there a reason you guys are holding back on the event information? I mean surely you guys could count up the number of attendees. Did real events happen in the U.K. and the U.S.?

Nathaniel Gleicher: We're not holding back on that at this point, Donie. It's just a question of what we're prioritizing in the operation and the focus of the operation based on our analysis and what we've seen so far. The primary focus of the operation was messaging through the large Pages and it wasn't as focused on the events.

I mean, as I said earlier, we can pull that information and we can make sure that people are aware of the detail.

Operator: Your next question comes from the line of Courtney Norris of PBS NewsHour. Please go ahead.

Courtney Norris: Hey.

Yes, I was just curious if you guys could -- I mean, obviously, you said this was first identified a week ago -- but on Election Day if this is discovered that day, what is the response time and can you give a little color to how local election officials will reach out to you?

Nathaniel Gleicher: Sure.

One of our -- I mean, our major priority has been as we head into an -- into the elections, the time -- the opportunity for time response shortens and the need to be able to move quickly gets more and more important. The reason we pulled together 20 of the top teams that work on our investigations and response into the war room is so that we can move much more quickly. Because our expectation is as things do develop in the sort of 11th hour, we're going to need to move fast and we need to be ready for that.

We've done a couple of things to make sure that that happens. First, just bringing the teams together in the war room and also establishing the broader relationships back from those 20 teams to all the different people that work on elections and safety and security at Facebook has helped us move much more quickly.

So in our work on the Brazil elections we found that there were cases where, as an example, new waves of hate speech were surfaced and we were able to identify that and then develop and respond at scale within just a couple of hours. So that's a -- really important evidence of our ability to move much more quickly and it's what we're focused on.

In addition, building those relationships with the people on the ground is a critical part of this because they are ones who are going to see it first and we

want to make sure that they can get to us quickly enough so that we can drive and respond to that quickly.

And then the last thing that we've done, or at least another thing that we've done, is we've been consistently running tabletop exercises to make sure that we've thought through as many of the different types of threats that we could anticipate so that we would know and have practiced how to respond.

And in addition, to your point, we've also though about if multiple threats develop at the same time or multiple incidents occur, how will we respond to them in parallel and do we have the resources in place. We've made sure to put the resources in place so that we'll be able to escalate quickly to manage multiple incidents if they develop.

Operator: Your next question comes from the line of Matt Oliver of Daily Mail. Please go ahead.

Matt Oliver: Hi.

I was just wondering if you could give a bit more color perhaps on what these posts in the U.K. were about? I mean, can you -- you mentioned that they were trying to (stoke up) various different types of behavior, but what were they actually talking about?

Nathaniel Gleicher: So when we conduct an operation like this and we run a takedown, the actions that we take are based squarely on behavior; they're not actually based on content. And so we are careful not to spend too much time characterizing the nature of the content because the enforcement that we take is based on the behavior.

I mentioned at the beginning that the -- that the content was focused on politically charged topics like race relations, opposition to political leaders, and immigration. And that was through both in the content focused in the U.K. and in the U.S. I would say in general, the majority of the content and engagement was focused in the U.S.; there was less focus in the U.K.

A couple of things you can do to understand this better. First is, the newsroom posts that we put up include samples -- think there are about seven samples -- of the type of content that are designed to be representative of the content itself and reflect the higher follower count Pages. That includes a couple of samples from the U.K.

In addition, and part of the reason why we will work with the Atlantic Council on something like this, we have shared with the Atlantic Council a link so that they can understand the nature of the content as well. They are going to do and are currently doing their own analysis of the trends that the content focused on, the nature of what it was, and they're going to be publishing their own report which will give much more detail on the nature of the content and the engagement.

That should be coming out soon -- they obviously need to develop that -- but that should also give a better sense specifically about the content and the focus.

Operator: Your next question comes from the line of Christopher Bing of Reuters. Please go ahead.

Christopher Bing: Yes, thank you for setting up this call.

I was interested in knowing if Facebook has seen improvements in the tactics and procedures and operational security of these posters since the first Iranian take down? For example, in this case, they're paying with U.S. dollars for the advertising purposes. But I'm wondering if they're using VPNs or if they've learned from the first take down in any way?

All right. Thank you.

Nathaniel Gleicher: Sure. That's a great question, Chris. Thanks.

A couple of details. First, it's important to note that in the ads context, it's a very small ad spend here; it's less than $100. So the -- and we're really only talking I think about two ads that ran so those did run with U.S. and Canadian dollars, but they clearly weren't a focus of this operation.

More generally, there are parts of this that were and did have better operational security that we identified. As with any operation, I think it's important to realize that this cluster of accounts -- this cluster of assets overlap. It doesn't necessarily mean this is all one tightly coordinated group.

And so some pieces of this had better operational security than others. That's been consistent with what we've seen not just in August, but across the -- across the spectrum of our investigations. We will see some actors that have better operational security and others that have a little bit less -- including involved in the same cluster.

And I should note that in this case, when we think about the timeline for this, we're continuing to look and see the scope of this but in general, the operations here, we saw some improvement in operational security but there was spectrum across all the actors.

Operator: Your next question comes from the line of Ryan Mac from BuzzFeed News. Please go ahead.

Ryan Mac: Hey, guys. Thanks for having the call.

Two questions. One, did you see any -- I saw the examples that you guys put up -- but have you guys seen any examples of posts that touch on the midterm elections?

Other question is, are you sharing -- are you sharing any of this information or kind of information with other companies?

Thanks.

Nathaniel Gleicher: Sure. So there were two questions there.

The first is to say, so we're not in a position to assess the motivation of these bad actors and what they were or were not attempting to accomplish. And so understanding exactly what they're targeting is always a little tricky. We previously discussed some of the challenges of making these types of determinations.

In this context, this content appeared consistent with what we've seen in other major operations, which is that is was targeting broad divisions and was sort of focused as we've seen with these previous -- with these -- with previous operations. It was sowing discord and it was trying to target socially divisive issues as apposed to being specifically targeted on events that are about to occur.

You also asked if we worked with our other partners. As with any operation like this, we engage with our industry partners. We make sure that they know what action we're taking and that they can see the activity that we're seeing so that they can run their own investigations and determine if there's parallel content or connected behavior on our their own platforms that should take action on. And my understanding is those investigations are ongoing.

Operator: Your next question comes from the line of Karissa Bell of Mashable. Please go ahead.

Karissa Bell: Hi. Thanks for taking my question.

You guys said that you guys first detected the account activity a week ago, but can you provide any clarity on when these accounts were created and how long they were posting this type of content for before you were able to detect it?

Nathaniel Gleicher: The earliest asset included in this set dates back, as I understand it, to June of 2016 **[CORRECTION**: **The earliest asset included in this set dates back to January 2016.]** The majority of the activity that we saw in this set is over the last year. And there's obviously -- part of what happens is when these are initially created and there's less activity, there's less threads to pull to identify them. As they get more active, there's more opportunity that we have to engage and find it.

Operator: Your next question comes from the line of Issie Lapowsky of WIRED. Please go ahead.

Issie Lapowsky: Hi.

I was actually going to ask about how recent these accounts are -- you say over the last year -- but I see that they were actually capitalizing from the content you shared so far on the (Kavanaugh hearing). So is a lot of this very recent, happening now? To what extent have they been capitalizing on other recent news events like the caravan?

And separately, with regard to these mail bombings that have been happening, I wonder how you guys are addressing fake news as it arises about that as we've been seeing this week?

Nathaniel Gleicher: Sure. So there were a couple of questions there.

Your first question was about the timeline for this engagement, and one thing that I would add to my previous answer, so we saw -- we saw these actors engaging, as I said, primarily over course of the last year. As with any operation like this, over time as they engage, they will react to public events, and particularly divisive public events so that they can connect to that. So it's not surprising that we would see content linked to recent public events.

We saw the increased engagement over the course of the last year. It isn't just a result of the last month or so or something like that; it has been a bit longer. It's also worth noting -- and I did want to point out -- we identified this about a week ago, and we moved from detection to disruption in the course of a week which is a really important marker for us. We've been pushing to be able to identify and action this stuff much more quickly.

And this was in an opportunity for us to do that leveraging the war room resources and the additional resources we've put in place. We've really shortened the time horizon to respond given the impending election.

To your question about misinformation more generally, as with all of these, we investigate these to determine if there is misinformation involved as public debates ensue. When content is identified as false by our fact checkers, that content gets down-ranked in News Feed, it gets reduced in News Feed, and that radically reduces the distribution of that content.

We also -- with all of these we'll have our threat intelligence teams engage to determine if there is any inauthentic driver behind these networks. And we continue to run those investigations.

Operator: Your next question comes from the line of Tara Deschamps of Canadian Press. Please go ahead.

Tara Deschamps: Hi there.

You mentioned that advertising was paid for in Canadian dollars. Do you have any reason to believe that Canadians may have been behind or targeted with these accounts?

Nathaniel Gleicher: No. There were only two ads that were run. They were very small ad spend. We don't have any reason to believe that there was any targeting to Canada in this context.

Operator: Your next question comes from the line of Edgar Alvarez of Engadget. Please go ahead.

Edgar Alvarez: Hi.

You touched on this a little bit, but I'm wondering in terms of the -- in particular with the account that was followed by 1.2 million, I'm wondering -- or when that page was found -- if you can share that?

Thank you.

Nathaniel Gleicher: So what we said actually was that there were a total of approximately 1 million followers across all the Pages. And those Pages were, as we said, were created -- some of them were created as early as 2016, but the majority of activity engagement was much more recently over the last year and it spreads out across that year as you would expect over time.

Tom Reynolds: Operator, we're going to have time for two more questions, OK?

Operator: Your next question comes from the line of Ali Breland of The Hill. Please go ahead.

Ali Breland: Hi, you guys have done a really good job of revealing these kinds of things from Russia and Iran to us. The United States government was engaged in a coordinated, inauthentic misinformation campaign. Would you pressure the same way, be as transparent and take the same kind of steps to reduce it if it happened to a foreign adversary?

Nathaniel Gleicher: Yes. Part of the key of our operations here is that we engage based on behavior -- not based on content and not based on the nature of the actor. And that's been a very intentional choice on our part.

We obviously have steps that we can take to down-rank and engage with content -- particularly content that violates our community standards. But when we're talking about coordinated inauthentic behavior, what matters is, is the actor engaging in behavior that is inauthentic, that misleads users as to, for example, the source or origin of content, and that as such violates our policies?

If they do, we will take action on them regardless of who the actor is.

Tom Reynolds: Thanks.

Operator, this will be our last question.

Operator: Your last question comes from the line of Sean Gallagher of Ars Technica. Please go ahead.

Sean Gallagher: Hi. Thank you.

First, I wanted to ask if you were looking at releasing any of the information from these accounts or Pages in the same way that Twitter did with the accounts they identified as being associated with Iran actors just last week -- either from this particular takedown or from the takedown in August?

And if you're looking at any other exposure of this data to researchers outside of Facebook and Atlantic Council?

Nathaniel Gleicher: Sure.

You're hitting on what I think is a really important point. When we take these actions, we have a couple priorities. One of them is we want to rapidly disrupt the behavior. The second is we want to make sure that law enforcement understands it and can continue their investigation. The third is we want to make sure that the public is aware of what's happening. And then the last is we want to make sure that researchers can study this.

And one of the key things that we need to balance as we do this is, how we share as much information as possible, address any legal constraints we might have around sharing that information, and also think about the privacy implications it has for our users and for people -- innocent people who might be looped up in this in some way. Because obviously the point of these operations is to engage with people.

Partly the way we do that is we release samples of the content and we partner with an organization like the Atlantic Council so that they can do this analysis. Obviously when they do their report, there will be additional information about the particular content and about the nature of the content that people will be able to review and understand better what is happening filtered through expert eyes so that the public can get a real sense of the activity.

To your question about researchers, one of the key things we've been working on is how do we make more information transparently available to researchers. We've partnered with organizations like Social Science One to be able to share more information for researchers to be able to do this research.

In the (context of) specific takedowns, we're continually thinking about how we can make it more transparent and how we can make sure that people can study it more comprehensively. We just have to make sure that we balance all the factors that are at play here.

Tom Reynolds: Great. Thanks, Nathaniel, and thanks, everybody, for joining us today. If you have any follow up questions, you can reach us at press@fb.com. And thanks again.

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

END