BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

MIKE ROGERS, ALABAMA
RANKING MEMBER

One Hundred Sixteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

November 26, 2019

Mr. Mark Zuckerberg
Founder, Chairman, and Chief Executive Officer
Facebook
1 Hacker Way
Menlo Park, CA 94025

Dear Mr. Zuckerberg:

As the 2020 elections approach, we are writing to request clear and detailed information on Facebook, Instagram, and WhatsApp's policies and processes for user reporting of suspected election interference on Facebook, Instagram, and WhatsApp. The U.S. Intelligence Community has determined that foreign adversaries are increasingly using social media platforms to spread disinformation with the intent to undermine the integrity of U.S. elections.[1] As Chair and Vice Chair of the Committee on Homeland Security, we believe Facebook, Instagram, and WhatsApp must remain vigilant as these attacks on our democratic institutions continue to utilize social media and evolve.

Social media has become part of our everyday lives, allowing us to connect with one another and share news, media, and information more easily and widely than ever before.[2] At the same time, foreign adversaries are exploiting social media "to seek political, economic, and military advantage over the United States and its allies."[3]

On Tuesday, October 22, 2019, the Committee on Homeland Security's Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation held a hearing entitled "Preparing for

---

[1] *8 U.S. Intelligence Groups Blame Russia for Meddling, but Trump Keeps Clouding the Picture*, New York Times (August 2, 2018).

[2] Pew Research Center, *Share of U.S. adults using social media, including Facebook, is mostly unchanged since 2018* (August 2019) (www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/)

[3] Senate Permanent Select Committee on Intelligence, Testimony of Daniel Coats, Director of National Intelligence, *Hearing on Worldwide Threat Assessment of the U.S. Intelligence Community,* 116th Cong. (January 29, 2019).

the Future: An Assessment of Emerging Cyber Threats."[4] Members heard testimony from experts in industry and academia on the next generation of cyber threats, including online misinformation and disinformation. Witnesses provided testimony on how advancements in artificial intelligence, quantum computing, and other technologies can both enable and undermine national security by introducing new vulnerabilities and changing the overall threat landscape.[5]

Members had the opportunity to question witnesses on the policies and processes that social media platforms have in place to allow users to report suspected content containing misinformation or disinformation. We were concerned to hear that not one of these subject matter experts was able to understand and clearly communicate these policies and processes. For example, one witness shared that "the only way [he] was able to report a fake LinkedIn profile that had connected with [him] was to tweet at LinkedIn" from his public Twitter account.[6]

Policies that affect users of social media platforms must be accessible and understandable to those users, in addition to industry experts and the platforms' employees. Yet our constituents in Illinois and Mississippi report difficulty finding clear guidelines about how to identify and report potential misinformation and disinformation on Facebook, Instagram, and WhatsApp.

Our constituents and many other Americans are rightly concerned about the potential risks of false information on Facebook, Instagram, and WhatsApp poses to the security of our elections and public confidence in our democracy. In order to ensure Facebook, Instagram, and WhatsApp users have the necessary resources to help combat the spread of online misinformation and disinformation, we respectfully request that you provide responses in writing to the following by December 18, 2019:

1. Please provide a detailed description of Facebook, Instagram, and WhatsApp's internal and external policies relating to false content on Facebook, Instagram, and WhatsApp's platform.

2. Please provide a detailed description of the process for Facebook, Instagram, and WhatsApp users to report suspected false content to Facebook, Instagram, and WhatsApp. Please also describe Facebook, Instagram, and WhatsApp's processes and policies for reviewing and adjudicating reports of false content or election interference,

---

[4] House Committee on Homeland Security, *Preparing for the Future: An Assessment of Emerging Cyber Threats,* 116th Cong. (October 22, 2019).

[5] *Id.*

[6] *Id. See* also: Council on Foreign Relations, *Hey LinkedIn, Sean Brown Does Not Work at CFR: Identity, Fake Accounts, and Foreign Intelligence* (September 2019) (www.cfr.org/blog/hey-linkedin-sean-brown-does-not-work-cfr-identity-fake-accounts-and-foreign-intelligence).; Rob Knake (@robknake), Twitter (September 10, 2019, 1:23 PM) (twitter.com/LinkedInHelp/status/1171477556333166592).

including any process for users to appeal Facebook, Instagram, and WhatsApp's decision on the report.

3. What guidance does Facebook, Instagram, and WhatsApp provide to allow users to identify and report posts or content that contains suspected misinformation or disinformation?

4. On average, how long does it take Facebook, Instagram, and WhatsApp to review and respond to a user report of misinformation or disinformation?

5. Do you believe Facebook, Instagram, and WhatsApp have a responsibility to ensure information shared by users and third-party advertisers on your platform is accurate?

6. How often does Facebook, Instagram, and WhatsApp evaluate and update their Advertising and Community Standards policies, specifically those relating to misinformation, disinformation, and election interference?

    a. Please provide a detailed timeline of changes Facebook, Instagram, and WhatsApp have made to these policies and processes since November 8, 2016.

7. Reports indicate third-party fact-checkers have urged Facebook to share more data to curb the spread of misinformation.[7] What is Facebook doing to engage with all 54 fact-checking partners to ensure each has the information needed to effectively evaluate content?[8]

8. Please provide a detailed list of experts with whom Facebook, Instagram, and WhatsApp consults when developing policies and processes to ensure users see accurate information about U.S. elections.

Thank you for your prompt attention to this matter.

Sincerely,

Bennie Thompson
Chairman

Lauren Underwood
Vice Chair

[7] *Facebook Fact-Checker Says Company Must Share More Data to Fight Misinformation,* Reuters (July 30, 2019).

[8] *Id.*

BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

MIKE ROGERS, ALABAMA
RANKING MEMBER

One Hundred Sixteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

November 26, 2019

Mr. Jack Dorsey
Chief Executive Officer
Twitter
1355 Market Street
San Francisco, CA 94103

Dear Mr. Dorsey:

As the 2020 elections approach, we are writing to request clear and detailed information on Twitter's policies and processes for user reporting of suspected election interference on Twitter. The U.S. Intelligence Community has determined that foreign adversaries are increasingly using social media platforms to spread disinformation with the intent to undermine the integrity of U.S. elections.[1] As Chair and Vice Chair of the Committee on Homeland Security, we believe Twitter must remain vigilant as these attacks on our democratic institutions continue to utilize social media and evolve.

Social media has become part of our everyday lives, allowing us to connect with one another and share news, media, and information more easily and widely than ever before.[2] At the same time, foreign adversaries are exploiting social media "to seek political, economic, and military advantage over the United States and its allies."[3]

On Tuesday, October 22, 2019, the Committee on Homeland Security's Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation held a hearing entitled "Preparing for

---

[1] *8 U.S. Intelligence Groups Blame Russia for Meddling, but Trump Keeps Clouding the Picture*, New York Times (August 2, 2018).

[2] Pew Research Center, *Share of U.S. adults using social media, including Facebook, is mostly unchanged since 2018* (August 2019) (www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/)

[3] Senate Permanent Select Committee on Intelligence, Testimony of Daniel Coats, Director of National Intelligence, *Hearing on Worldwide Threat Assessment of the U.S. Intelligence Community,* 116th Cong. (January 29, 2019).

the Future: An Assessment of Emerging Cyber Threats."[4] Members heard testimony from experts in industry and academia on the next generation of cyber threats, including online misinformation and disinformation. Witnesses provided testimony on how advancements in artificial intelligence, quantum computing, and other technologies can both enable and undermine national security by introducing new vulnerabilities and changing the overall threat landscape.[5]

Members had the opportunity to question witnesses on the policies and processes that social media platforms have in place to allow users to report suspected content containing misinformation or disinformation. We were concerned to hear that not one of these subject matter experts was able to understand and clearly communicate these policies and processes. For example, one witness shared that "the only way [he] was able to report a fake LinkedIn profile that had connected with [him] was to tweet at LinkedIn" from his public Twitter account.[6]

Policies that affect users of social media platforms must be accessible and understandable to those users, in addition to industry experts and the platforms' employees. Yet our constituents in Illinois and Mississippi report difficulty finding clear guidelines about how to identify and report potential misinformation and disinformation on Twitter.

Our constituents and many other Americans are rightly concerned about the potential risks false information on Twitter poses to the security of our elections and public confidence in our democracy. In order to ensure Twitter users have the necessary resources to help combat the spread of online misinformation and disinformation, we respectfully request that you provide responses in writing to the following by December 18, 2019:

1. Please provide a detailed description of Twitter's internal and external policies relating to false content on Twitter's platform.

2. Please provide a detailed description of the process for Twitter users to report suspected false content to Twitter. Please also describe Twitter's processes and policies for reviewing and adjudicating reports of false content or election interference, including any process for users to appeal Twitter's decision on a report.

---

[4] House Committee on Homeland Security, *Preparing for the Future: An Assessment of Emerging Cyber Threats,* 116th Cong. (October 22, 2019).

[5] *Id.*

[6] *Id. See* also: Council on Foreign Relations, *Hey LinkedIn, Sean Brown Does Not Work at CFR: Identity, Fake Accounts, and Foreign Intelligence* (September 2019) (www.cfr.org/blog/hey-linkedin-sean-brown-does-not-work-cfr-identity-fake-accounts-and-foreign-intelligence).; Rob Knake (@robknake), Twitter (September 10, 2019, 1:23 PM) (twitter.com/LinkedInHelp/status/1171477556333166592).

3. What guidance does Twitter provide to allow users to identify and report posts or content that contains suspected misinformation or disinformation?

4. On average, how long does it take Twitter to review and respond to a user report of misinformation or disinformation?

5. Do you believe Twitter has a responsibility to ensure information shared by users and third-party advertisers on your platform is accurate?

6. How often does Twitter evaluate and update its rules and policies, specifically those relating to misinformation, disinformation, and election interference?

    a. Please provide a detailed timeline of changes Twitter has made to these policies and processes since November 8, 2016.

7. Please provide a detailed list of experts with whom Twitter consults when developing policies and processes to ensure users see accurate information about U.S. elections.

Thank you for your prompt attention to this matter.

Sincerely,

Bennie Thompson
Chairman

Lauren Underwood
Vice Chair

BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

MIKE ROGERS, ALABAMA
RANKING MEMBER

One Hundred Sixteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

November 26, 2019

Mr. Jeff Weiner
Chief Executive Officer
LinkedIn
1000 W Maude
Sunnyvale, CA 94085

Dear Mr. Weiner:

As the 2020 elections approach, we are writing to request clear and detailed information on LinkedIn's policies and processes for user reporting of suspected election interference on LinkedIn. The U.S. Intelligence Community has determined that foreign adversaries are increasingly using social media platforms to spread disinformation with the intent to undermine the integrity of U.S. elections.[1] As Chair and Vice Chair of the Committee on Homeland Security, we believe LinkedIn must remain vigilant as these attacks on our democratic institutions continue to utilize social media and evolve.

Social media has become part of our everyday lives, allowing us to connect with one another and share news, media, and information more easily and widely than ever before.[2] At the same time, foreign adversaries are exploiting social media "to seek political, economic, and military advantage over the United States and its allies."[3]

On Tuesday, October 22, 2019, the Committee on Homeland Security's Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation held a hearing entitled "Preparing for the Future: An Assessment of Emerging Cyber Threats."[4] Members heard testimony from

---

[1] *8 U.S. Intelligence Groups Blame Russia for Meddling, but Trump Keeps Clouding the Picture*, New York Times (August 2, 2018).

[2] Pew Research Center, *Share of U.S. adults using social media, including Facebook, is mostly unchanged since 2018* (August 2019) (www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/)

[3] Senate Permanent Select Committee on Intelligence, Testimony of Daniel Coats, Director of National Intelligence, *Hearing on Worldwide Threat Assessment of the U.S. Intelligence Community,* 116th Cong. (January 29, 2019).

[4] House Committee on Homeland Security, *Preparing for the Future: An Assessment of Emerging Cyber Threats,* 116th Cong. (October 22, 2019).

experts in industry and academia on the next generation of cyber threats, including online misinformation and disinformation. Witnesses provided testimony on how advancements in artificial intelligence, quantum computing, and other technologies can both enable and undermine national security by introducing new vulnerabilities and changing the overall threat landscape.[5]

Members had the opportunity to question witnesses on the policies and processes that social media platforms have in place to allow users to report suspected content containing misinformation or disinformation. We were concerned to hear that not one of these subject matter experts was able to understand and clearly communicate these policies and processes. For example, one witness shared that "the only way [he] was able to report a fake LinkedIn profile that had connected with [him] was to tweet at LinkedIn" from his public Twitter account.[6]

Policies that affect users of social media platforms must be accessible and understandable to those users, in addition to industry experts and to the platforms' employees. Yet our constituents in Illinois and Mississippi report difficulty finding clear guidelines about how to identify and report potential misinformation and disinformation on LinkedIn.

Our constituents and many other Americans are rightly concerned about the potential risks false information on LinkedIn poses to the security of our elections and public confidence in our democracy. In order to ensure LinkedIn users have the necessary resources to help combat the spread of online misinformation and disinformation, we respectfully request that you provide responses in writing to the following by December 18, 2019:

1. Please provide a detailed description of LinkedIn's internal and external policies relating to false content on LinkedIn's platform.

2. Please provide a detailed description of the process for LinkedIn users to report suspected false content to LinkedIn. Please also describe LinkedIn's processes and policies for reviewing and adjudicating reports of false content or election interference, including any process for users to appeal LinkedIn's decision on a report.

3. What guidance does LinkedIn provide to users to identify and report posts or content that contains suspected misinformation or disinformation?

4. On average, how long does it take LinkedIn to review and respond to a user report of misinformation or disinformation?

---

[5] *Id.*

[6] *Id. See* also: Council on Foreign Relations, *Hey LinkedIn, Sean Brown Does Not Work at CFR: Identity, Fake Accounts, and Foreign Intelligence* (September 2019) (www.cfr.org/blog/hey-linkedin-sean-brown-does-not-work-cfr-identity-fake-accounts-and-foreign-intelligence).; Rob Knake (@robknake), Twitter (September 10, 2019, 1:23 PM) (twitter.com/LinkedInHelp/status/1171477556333166592).

5. Do you believe LinkedIn has a responsibility to ensure information shared by users and third-party advertisers on your platform is accurate?

6. How often does LinkedIn evaluate and update its Professional Community and Advertising policies, specifically those relating to misinformation, disinformation, and election interference?

    a. Please provide a detailed timeline of changes LinkedIn has made to these policies and processes since November 8, 2016.

7. Please provide a detailed list of experts with whom LinkedIn consults when developing policies and processes to ensure users see accurate information about U.S. elections.

Thank you for your prompt attention to this matter.

Sincerely,

Bennie Thompson
Chairman

Lauren Underwood
Vice Chair