



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

June 26, 2024

John Stankey
Chief Executive Officer
AT&T Services, Inc.
208 S. Akard Street
Dallas, TX 75202

Dear Mr. Stankey:

As you know, the use of Artificial Intelligence-generated voice cloning to mimic the voices of politicians, celebrities, or even family members, can be used to sow confusion, scam consumers and spread misinformation.

We already see it happening here in the United States. Just two days before a primary election in January, a fraudulent robocalling campaign that used AI to clone the voice of President Biden targeted voters in New Hampshire. When this happened, we acted swiftly. The Federal Communications Commission issued a Declaratory Ruling that made clear that “artificial or prerecorded voice” robocalls using AI voice cloning technology violate the Telephone Consumer Protection Act. We partnered in this effort with State Attorneys General, including the New Hampshire Attorney General, who is one of 49 State Attorneys General who have signed on to a Memorandum of Understanding to work with this agency on junk robocalls. This ruling gives our state colleagues the authority to go after bad actors behind these calls and seek damages under the law.

When we identified the carrier behind this scam, we immediately sent a cease-and-desist letter and allowed all other carriers to stop carrying this traffic. And in May, we took two enforcement actions. First, we adopted a \$6 million fine for the party responsible for the scam calls. Second, we adopted a \$2 million fine for the carrier that put these junk calls on the line and apparently failed to follow our call authentication rules.

This is just the beginning. We know that AI technologies will make it cheap and easy to flood our networks with deepfakes used to mislead and betray trust. It is especially chilling to see AI voice cloning used to impersonate candidates during elections. As AI tools become more accessible to bad actors and scammers, we need to do everything we can to keep this junk off our networks.

At the FCC, with this call and others, we have worked with the telecommunications industry to combat robocalls through the Industry Traceback Group. We appreciate the cooperation from this group, which facilitates information sharing from wireline, wireless, VoIP and cable companies to track and help stop illegal robocalls. Going forward we know that this work will be even more critical. To further assist us at the FCC to keep illegal robocalls, and especially those using AI-generated voices, off of our networks we request you respond to the questions below regarding your efforts to stop these calls from reaching consumers.

- (1) Please describe the steps your company takes to authenticate calls, in line with the FCC’s STIR/SHAKEN rules and policies.

- (2) Please describe your Know Your Customer Practices. Include in your response:
 - a. How do you verify the identity of your customer—both the company and individual point of contact?
 - b. How do you verify your customer’s phone, email, and address information?
- (3) Does your company have dedicated resources to respond to FCC requests for information related to suspected illegal robocall campaigns?
- (4) Does your company have dedicated resources—human and/or technological—capable of identifying generative AI voice?
- (5) What is your company’s involvement/contribution to the Industry Traceback Group?
- (6) What other steps has your company taken to address the threat of unauthorized AI-generated messaging campaigns during elections?

Please send your response to Priscilla Delgado Argeris via email (priscilla.argeris@fcc.gov) by July 15, 2024.

Sincerely,

A handwritten signature in black ink, appearing to read "Priscilla Argeris", with a long horizontal flourish extending to the right.

cc: Rhonda Johnson



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

June 26, 2024

Christopher Winfrey
President and Chief Executive Officer
Charter Communications
400 Washington Blvd. -UT 1
Stamford, CT 06902

Dear Mr. Winfrey:

As you know, the use of Artificial Intelligence-generated voice cloning to mimic the voices of politicians, celebrities, or even family members, can be used to sow confusion, scam consumers and spread misinformation.

We already see it happening here in the United States. Just two days before a primary election in January, a fraudulent robocalling campaign that used AI to clone the voice of President Biden targeted voters in New Hampshire. When this happened, we acted swiftly. The Federal Communications Commission issued a Declaratory Ruling that made clear that “artificial or prerecorded voice” robocalls using AI voice cloning technology violate the Telephone Consumer Protection Act. We partnered in this effort with State Attorneys General, including the New Hampshire Attorney General, who is one of 49 State Attorneys General who have signed on to a Memorandum of Understanding to work with this agency on junk robocalls. This ruling gives our state colleagues the authority to go after bad actors behind these calls and seek damages under the law.

When we identified the carrier behind this scam, we immediately sent a cease-and-desist letter and allowed all other carriers to stop carrying this traffic. And in May, we took two enforcement actions. First, we adopted a \$6 million fine for the party responsible for the scam calls. Second, we adopted a \$2 million fine for the carrier that put these junk calls on the line and apparently failed to follow our call authentication rules.

This is just the beginning. We know that AI technologies will make it cheap and easy to flood our networks with deepfakes used to mislead and betray trust. It is especially chilling to see AI voice cloning used to impersonate candidates during elections. As AI tools become more accessible to bad actors and scammers, we need to do everything we can to keep this junk off our networks.

At the FCC, with this call and others, we have worked with the telecommunications industry to combat robocalls through the Industry Traceback Group. We appreciate the cooperation from this group, which facilitates information sharing from wireline, wireless, VoIP and cable companies to track and help stop illegal robocalls. Going forward we know that this work will be even more critical. To further assist us at the FCC to keep illegal robocalls, and especially those using AI-generated voices, off of our networks we request you respond to the questions below regarding your efforts to stop these calls from reaching consumers.

- (1) Please describe the steps your company takes to authenticate calls, in line with the FCC’s STIR/SHAKEN rules and policies.

- (2) Please describe your Know Your Customer Practices. Include in your response:
 - a. How do you verify the identity of your customer—both the company and individual point of contact?
 - b. How do you verify your customer’s phone, email, and address information?
- (3) Does your company have dedicated resources to respond to FCC requests for information related to suspected illegal robocall campaigns?
- (4) Does your company have dedicated resources—human and/or technological—capable of identifying generative AI voice?
- (5) What is your company’s involvement/contribution to the Industry Traceback Group?
- (6) What other steps has your company taken to address the threat of unauthorized AI-generated messaging campaigns during elections?

Please send your response to Priscilla Delgado Argeris via email (priscilla.argeris@fcc.gov) by July 15, 2024.

Sincerely,

A handwritten signature in black ink, appearing to read "Priscilla Argeris", with a long horizontal flourish extending to the right.

cc: Elizabeth Andrion



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

June 26, 2024

Brian L. Roberts
Chairman & Chief Executive Officer
Comcast
1701 John F. Kennedy Boulevard
Philadelphia, PA 19103

Dear Mr. Roberts:

As you know, the use of Artificial Intelligence-generated voice cloning to mimic the voices of politicians, celebrities, or even family members, can be used to sow confusion, scam consumers and spread misinformation.

We already see it happening here in the United States. Just two days before a primary election in January, a fraudulent robocalling campaign that used AI to clone the voice of President Biden targeted voters in New Hampshire. When this happened, we acted swiftly. The Federal Communications Commission issued a Declaratory Ruling that made clear that “artificial or prerecorded voice” robocalls using AI voice cloning technology violate the Telephone Consumer Protection Act. We partnered in this effort with State Attorneys General, including the New Hampshire Attorney General, who is one of 49 State Attorneys General who have signed on to a Memorandum of Understanding to work with this agency on junk robocalls. This ruling gives our state colleagues the authority to go after bad actors behind these calls and seek damages under the law.

When we identified the carrier behind this scam, we immediately sent a cease-and-desist letter and allowed all other carriers to stop carrying this traffic. And in May, we took two enforcement actions. First, we adopted a \$6 million fine for the party responsible for the scam calls. Second, we adopted a \$2 million fine for the carrier that put these junk calls on the line and apparently failed to follow our call authentication rules.

This is just the beginning. We know that AI technologies will make it cheap and easy to flood our networks with deepfakes used to mislead and betray trust. It is especially chilling to see AI voice cloning used to impersonate candidates during elections. As AI tools become more accessible to bad actors and scammers, we need to do everything we can to keep this junk off our networks.

At the FCC, with this call and others, we have worked with the telecommunications industry to combat robocalls through the Industry Traceback Group. We appreciate the cooperation from this group, which facilitates information sharing from wireline, wireless, VoIP and cable companies to track and help stop illegal robocalls. Going forward we know that this work will be even more critical. To further assist us at the FCC to keep illegal robocalls, and especially those using AI-generated voices, off of our networks we request you respond to the questions below regarding your efforts to stop these calls from reaching consumers.

- (1) Please describe the steps your company takes to authenticate calls, in line with the FCC’s STIR/SHAKEN rules and policies.

- (2) Please describe your Know Your Customer Practices. Include in your response:
 - a. How do you verify the identity of your customer—both the company and individual point of contact?
 - b. How do you verify your customer’s phone, email, and address information?
- (3) Does your company have dedicated resources to respond to FCC requests for information related to suspected illegal robocall campaigns?
- (4) Does your company have dedicated resources—human and/or technological—capable of identifying generative AI voice?
- (5) What is your company’s involvement/contribution to the Industry Traceback Group?
- (6) What other steps has your company taken to address the threat of unauthorized AI-generated messaging campaigns during elections?

Please send your response to Priscilla Delgado Argeris via email (priscilla.argeris@fcc.gov) by July 15, 2024.

Sincerely,

A handwritten signature in black ink, appearing to read "Priscilla Argeris", with a long horizontal flourish extending to the right.

cc: Jordan Goldstein



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

June 26, 2024

Mark Greatrex
President
Cox Communications
6205-A Peachtree-Dunwoody Rd.
Atlanta, GA 30328

Dear Mr. Greatrex:

As you know, the use of Artificial Intelligence-generated voice cloning to mimic the voices of politicians, celebrities, or even family members, can be used to sow confusion, scam consumers and spread misinformation.

We already see it happening here in the United States. Just two days before a primary election in January, a fraudulent robocalling campaign that used AI to clone the voice of President Biden targeted voters in New Hampshire. When this happened, we acted swiftly. The Federal Communications Commission issued a Declaratory Ruling that made clear that “artificial or prerecorded voice” robocalls using AI voice cloning technology violate the Telephone Consumer Protection Act. We partnered in this effort with State Attorneys General, including the New Hampshire Attorney General, who is one of 49 State Attorneys General who have signed on to a Memorandum of Understanding to work with this agency on junk robocalls. This ruling gives our state colleagues the authority to go after bad actors behind these calls and seek damages under the law.

When we identified the carrier behind this scam, we immediately sent a cease-and-desist letter and allowed all other carriers to stop carrying this traffic. And in May, we took two enforcement actions. First, we adopted a \$6 million fine for the party responsible for the scam calls. Second, we adopted a \$2 million fine for the carrier that put these junk calls on the line and apparently failed to follow our call authentication rules.

This is just the beginning. We know that AI technologies will make it cheap and easy to flood our networks with deepfakes used to mislead and betray trust. It is especially chilling to see AI voice cloning used to impersonate candidates during elections. As AI tools become more accessible to bad actors and scammers, we need to do everything we can to keep this junk off our networks.

At the FCC, with this call and others, we have worked with the telecommunications industry to combat robocalls through the Industry Traceback Group. We appreciate the cooperation from this group, which facilitates information sharing from wireline, wireless, VoIP and cable companies to track and help stop illegal robocalls. Going forward we know that this work will be even more critical. To further assist us at the FCC to keep illegal robocalls, and especially those using AI-generated voices, off of our networks we request you respond to the questions below regarding your efforts to stop these calls from reaching consumers.

- (1) Please describe the steps your company takes to authenticate calls, in line with the FCC’s STIR/SHAKEN rules and policies.

- (2) Please describe your Know Your Customer Practices. Include in your response:
 - a. How do you verify the identity of your customer—both the company and individual point of contact?
 - b. How do you verify your customer’s phone, email, and address information?
- (3) Does your company have dedicated resources to respond to FCC requests for information related to suspected illegal robocall campaigns?
- (4) Does your company have dedicated resources—human and/or technological—capable of identifying generative AI voice?
- (5) What is your company’s involvement/contribution to the Industry Traceback Group?
- (6) What other steps has your company taken to address the threat of unauthorized AI-generated messaging campaigns during elections?

Please send your response to Priscilla Delgado Argeris via email (priscilla.argeris@fcc.gov) by July 15, 2024.

Sincerely,

A handwritten signature in black ink, appearing to read "Priscilla Argeris", with a long horizontal flourish extending to the right.

cc: Barry Ohlson
Jennifer Prime



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

June 26, 2024

Hamid Akhavan
CEO and President of DISH and EchoStar
9601 S Meridian Boulevard
Englewood, CO 80112

Dear Mr. Akhavan:

As you know, the use of Artificial Intelligence-generated voice cloning to mimic the voices of politicians, celebrities, or even family members, can be used to sow confusion, scam consumers and spread misinformation.

We already see it happening here in the United States. Just two days before a primary election in January, a fraudulent robocalling campaign that used AI to clone the voice of President Biden targeted voters in New Hampshire. When this happened, we acted swiftly. The Federal Communications Commission issued a Declaratory Ruling that made clear that “artificial or prerecorded voice” robocalls using AI voice cloning technology violate the Telephone Consumer Protection Act. We partnered in this effort with State Attorneys General, including the New Hampshire Attorney General, who is one of 49 State Attorneys General who have signed on to a Memorandum of Understanding to work with this agency on junk robocalls. This ruling gives our state colleagues the authority to go after bad actors behind these calls and seek damages under the law.

When we identified the carrier behind this scam, we immediately sent a cease-and-desist letter and allowed all other carriers to stop carrying this traffic. And in May, we took two enforcement actions. First, we adopted a \$6 million fine for the party responsible for the scam calls. Second, we adopted a \$2 million fine for the carrier that put these junk calls on the line and apparently failed to follow our call authentication rules.

This is just the beginning. We know that AI technologies will make it cheap and easy to flood our networks with deepfakes used to mislead and betray trust. It is especially chilling to see AI voice cloning used to impersonate candidates during elections. As AI tools become more accessible to bad actors and scammers, we need to do everything we can to keep this junk off our networks.

At the FCC, with this call and others, we have worked with the telecommunications industry to combat robocalls through the Industry Traceback Group. We appreciate the cooperation from this group, which facilitates information sharing from wireline, wireless, VoIP and cable companies to track and help stop illegal robocalls. Going forward we know that this work will be even more critical. To further assist us at the FCC to keep illegal robocalls, and especially those using AI-generated voices, off of our networks we request you respond to the questions below regarding your efforts to stop these calls from reaching consumers.

- (1) Please describe the steps your company takes to authenticate calls, in line with the FCC’s STIR/SHAKEN rules and policies.
- (2) Please describe your Know Your Customer Practices. Include in your response:

- a. How do you verify the identity of your customer—both the company and individual point of contact?
 - b. How do you verify your customer’s phone, email, and address information?
- (3) Does your company have dedicated resources to respond to FCC requests for information related to suspected illegal robocall campaigns?
- (4) Does your company have dedicated resources—human and/or technological—capable of identifying generative AI voice?
- (5) What is your company’s involvement/contribution to the Industry Traceback Group?
- (6) What other steps has your company taken to address the threat of unauthorized AI-generated messaging campaigns during elections?

Please send your response to Priscilla Delgado Argeris via email (priscilla.argeris@fcc.gov) by July 15, 2024.

Sincerely,

A handwritten signature in black ink, appearing to read "Jimmie Ramm", with a long horizontal flourish extending to the right.

cc: Jeffrey Blum



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

June 26, 2024

Nick Jeffery
President and Chief Executive Officer
Frontier Communications
1919 McKinney Ave.
Dallas, TX 75201

Dear Mr. Jeffery:

As you know, the use of Artificial Intelligence-generated voice cloning to mimic the voices of politicians, celebrities, or even family members, can be used to sow confusion, scam consumers and spread misinformation.

We already see it happening here in the United States. Just two days before a primary election in January, a fraudulent robocalling campaign that used AI to clone the voice of President Biden targeted voters in New Hampshire. When this happened, we acted swiftly. The Federal Communications Commission issued a Declaratory Ruling that made clear that “artificial or prerecorded voice” robocalls using AI voice cloning technology violate the Telephone Consumer Protection Act. We partnered in this effort with State Attorneys General, including the New Hampshire Attorney General, who is one of 49 State Attorneys General who have signed on to a Memorandum of Understanding to work with this agency on junk robocalls. This ruling gives our state colleagues the authority to go after bad actors behind these calls and seek damages under the law.

When we identified the carrier behind this scam, we immediately sent a cease-and-desist letter and allowed all other carriers to stop carrying this traffic. And in May, we took two enforcement actions. First, we adopted a \$6 million fine for the party responsible for the scam calls. Second, we adopted a \$2 million fine for the carrier that put these junk calls on the line and apparently failed to follow our call authentication rules.

This is just the beginning. We know that AI technologies will make it cheap and easy to flood our networks with deepfakes used to mislead and betray trust. It is especially chilling to see AI voice cloning used to impersonate candidates during elections. As AI tools become more accessible to bad actors and scammers, we need to do everything we can to keep this junk off our networks.

At the FCC, with this call and others, we have worked with the telecommunications industry to combat robocalls through the Industry Traceback Group. We appreciate the cooperation from this group, which facilitates information sharing from wireline, wireless, VoIP and cable companies to track and help stop illegal robocalls. Going forward we know that this work will be even more critical. To further assist us at the FCC to keep illegal robocalls, and especially those using AI-generated voices, off of our networks we request you respond to the questions below regarding your efforts to stop these calls from reaching consumers.

- (1) Please describe the steps your company takes to authenticate calls, in line with the FCC’s STIR/SHAKEN rules and policies.

- (2) Please describe your Know Your Customer Practices. Include in your response:
 - a. How do you verify the identity of your customer—both the company and individual point of contact?
 - b. How do you verify your customer’s phone, email, and address information?
- (3) Does your company have dedicated resources to respond to FCC requests for information related to suspected illegal robocall campaigns?
- (4) Does your company have dedicated resources—human and/or technological—capable of identifying generative AI voice?
- (5) What is your company’s involvement/contribution to the Industry Traceback Group?
- (6) What other steps has your company taken to address the threat of unauthorized AI-generated messaging campaigns during elections?

Please send your response to Priscilla Delgado Argeris via email (priscilla.argeris@fcc.gov) by July 15, 2024.

Sincerely,

A handwritten signature in black ink, appearing to read "James Ramm", with a long horizontal flourish extending to the right.

cc: William Wilhelm



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

June 26, 2024

Kate Johnson
President and Chief Executive Officer
Lumen Technologies
100 CenturyLink Dr.
Monroe, LA 71203-2041

Dear Ms. Johnson:

As you know, the use of Artificial Intelligence-generated voice cloning to mimic the voices of politicians, celebrities, or even family members, can be used to sow confusion, scam consumers and spread misinformation.

We already see it happening here in the United States. Just two days before a primary election in January, a fraudulent robocalling campaign that used AI to clone the voice of President Biden targeted voters in New Hampshire. When this happened, we acted swiftly. The Federal Communications Commission issued a Declaratory Ruling that made clear that “artificial or prerecorded voice” robocalls using AI voice cloning technology violate the Telephone Consumer Protection Act. We partnered in this effort with State Attorneys General, including the New Hampshire Attorney General, who is one of 49 State Attorneys General who have signed on to a Memorandum of Understanding to work with this agency on junk robocalls. This ruling gives our state colleagues the authority to go after bad actors behind these calls and seek damages under the law.

When we identified the carrier behind this scam, we immediately sent a cease-and-desist letter and allowed all other carriers to stop carrying this traffic. And in May, we took two enforcement actions. First, we adopted a \$6 million fine for the party responsible for the scam calls. Second, we adopted a \$2 million fine for the carrier that put these junk calls on the line and apparently failed to follow our call authentication rules.

This is just the beginning. We know that AI technologies will make it cheap and easy to flood our networks with deepfakes used to mislead and betray trust. It is especially chilling to see AI voice cloning used to impersonate candidates during elections. As AI tools become more accessible to bad actors and scammers, we need to do everything we can to keep this junk off our networks.

At the FCC, with this call and others, we have worked with the telecommunications industry to combat robocalls through the Industry Traceback Group. We appreciate the cooperation from this group, which facilitates information sharing from wireline, wireless, VoIP and cable companies to track and help stop illegal robocalls. Going forward we know that this work will be even more critical. To further assist us at the FCC to keep illegal robocalls, and especially those using AI-generated voices, off of our networks we request you respond to the questions below regarding your efforts to stop these calls from reaching consumers.

- (1) Please describe the steps your company takes to authenticate calls, in line with the FCC’s STIR/SHAKEN rules and policies.

- (2) Please describe your Know Your Customer Practices. Include in your response:
 - a. How do you verify the identity of your customer—both the company and individual point of contact?
 - b. How do you verify your customer’s phone, email, and address information?
- (3) Does your company have dedicated resources to respond to FCC requests for information related to suspected illegal robocall campaigns?
- (4) Does your company have dedicated resources—human and/or technological—capable of identifying generative AI voice?
- (5) What is your company’s involvement/contribution to the Industry Traceback Group?
- (6) What other steps has your company taken to address the threat of unauthorized AI-generated messaging campaigns during elections?

Please send your response to Priscilla Delgado Argeris via email (priscilla.argeris@fcc.gov) by July 15, 2024.

Sincerely,

A handwritten signature in black ink, appearing to read "Joseph Cavender", with a long horizontal flourish extending to the right.

cc: Melissa Mann
Joseph Cavender



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

June 26, 2024

Mike Sievert
President and Chief Executive Officer
T-Mobile
3618 Factoria Boulevard SE
Bellevue, WA 98006

Dear Mr. Sievert:

As you know, the use of Artificial Intelligence-generated voice cloning to mimic the voices of politicians, celebrities, or even family members, can be used to sow confusion, scam consumers and spread misinformation.

We already see it happening here in the United States. Just two days before a primary election in January, a fraudulent robocalling campaign that used AI to clone the voice of President Biden targeted voters in New Hampshire. When this happened, we acted swiftly. The Federal Communications Commission issued a Declaratory Ruling that made clear that “artificial or prerecorded voice” robocalls using AI voice cloning technology violate the Telephone Consumer Protection Act. We partnered in this effort with State Attorneys General, including the New Hampshire Attorney General, who is one of 49 State Attorneys General who have signed on to a Memorandum of Understanding to work with this agency on junk robocalls. This ruling gives our state colleagues the authority to go after bad actors behind these calls and seek damages under the law.

When we identified the carrier behind this scam, we immediately sent a cease-and-desist letter and allowed all other carriers to stop carrying this traffic. And in May, we took two enforcement actions. First, we adopted a \$6 million fine for the party responsible for the scam calls. Second, we adopted a \$2 million fine for the carrier that put these junk calls on the line and apparently failed to follow our call authentication rules.

This is just the beginning. We know that AI technologies will make it cheap and easy to flood our networks with deepfakes used to mislead and betray trust. It is especially chilling to see AI voice cloning used to impersonate candidates during elections. As AI tools become more accessible to bad actors and scammers, we need to do everything we can to keep this junk off our networks.

At the FCC, with this call and others, we have worked with the telecommunications industry to combat robocalls through the Industry Traceback Group. We appreciate the cooperation from this group, which facilitates information sharing from wireline, wireless, VoIP and cable companies to track and help stop illegal robocalls. Going forward we know that this work will be even more critical. To further assist us at the FCC to keep illegal robocalls, and especially those using AI-generated voices, off of our networks we request you respond to the questions below regarding your efforts to stop these calls from reaching consumers.

- (1) Please describe the steps your company takes to authenticate calls, in line with the FCC’s STIR/SHAKEN rules and policies.

- (2) Please describe your Know Your Customer Practices. Include in your response:
 - a. How do you verify the identity of your customer—both the company and individual point of contact?
 - b. How do you verify your customer’s phone, email, and address information?
- (3) Does your company have dedicated resources to respond to FCC requests for information related to suspected illegal robocall campaigns?
- (4) Does your company have dedicated resources—human and/or technological—capable of identifying generative AI voice?
- (5) What is your company’s involvement/contribution to the Industry Traceback Group?
- (6) What other steps has your company taken to address the threat of unauthorized AI-generated messaging campaigns during elections?

Please send your response to Priscilla Delgado Argeris via email (priscilla.argeris@fcc.gov) by July 15, 2024.

Sincerely,

A handwritten signature in black ink, appearing to read "James Ramm", with a long horizontal flourish extending to the right.

cc: Edward Smith



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

June 26, 2024

Hans Vestberg
Chairman and Chief Executive Officer
Verizon
One Verizon Way
Basking Ridge, NJ 07920

Dear Mr. Vestberg:

As you know, the use of Artificial Intelligence-generated voice cloning to mimic the voices of politicians, celebrities, or even family members, can be used to sow confusion, scam consumers and spread misinformation.

We already see it happening here in the United States. Just two days before a primary election in January, a fraudulent robocalling campaign that used AI to clone the voice of President Biden targeted voters in New Hampshire. When this happened, we acted swiftly. The Federal Communications Commission issued a Declaratory Ruling that made clear that “artificial or prerecorded voice” robocalls using AI voice cloning technology violate the Telephone Consumer Protection Act. We partnered in this effort with State Attorneys General, including the New Hampshire Attorney General, who is one of 49 State Attorneys General who have signed on to a Memorandum of Understanding to work with this agency on junk robocalls. This ruling gives our state colleagues the authority to go after bad actors behind these calls and seek damages under the law.

When we identified the carrier behind this scam, we immediately sent a cease-and-desist letter and allowed all other carriers to stop carrying this traffic. And in May, we took two enforcement actions. First, we adopted a \$6 million fine for the party responsible for the scam calls. Second, we adopted a \$2 million fine for the carrier that put these junk calls on the line and apparently failed to follow our call authentication rules.

This is just the beginning. We know that AI technologies will make it cheap and easy to flood our networks with deepfakes used to mislead and betray trust. It is especially chilling to see AI voice cloning used to impersonate candidates during elections. As AI tools become more accessible to bad actors and scammers, we need to do everything we can to keep this junk off our networks.

At the FCC, with this call and others, we have worked with the telecommunications industry to combat robocalls through the Industry Traceback Group. We appreciate the cooperation from this group, which facilitates information sharing from wireline, wireless, VoIP and cable companies to track and help stop illegal robocalls. Going forward we know that this work will be even more critical. To further assist us at the FCC to keep illegal robocalls, and especially those using AI-generated voices, off of our networks we request you respond to the questions below regarding your efforts to stop these calls from reaching consumers.

- (1) Please describe the steps your company takes to authenticate calls, in line with the FCC’s STIR/SHAKEN rules and policies.

- (2) Please describe your Know Your Customer Practices. Include in your response:
 - a. How do you verify the identity of your customer—both the company and individual point of contact?
 - b. How do you verify your customer's phone, email, and address information?
- (3) Does your company have dedicated resources to respond to FCC requests for information related to suspected illegal robocall campaigns?
- (4) Does your company have dedicated resources—human and/or technological—capable of identifying generative AI voice?
- (5) What is your company's involvement/contribution to the Industry Traceback Group?
- (6) What other steps has your company taken to address the threat of unauthorized AI-generated messaging campaigns during elections?

Please send your response to Priscilla Delgado Argeris via email (priscilla.argeris@fcc.gov) by July 15, 2024.

Sincerely,

A handwritten signature in black ink, appearing to read "Priscilla Argeris", with a long horizontal flourish extending to the right.

cc: Kathleen Grillo