

March 16, 2026

Mr. Shantanu Narayen  
Chief Executive Officer  
Adobe  
345 Park Avenue  
San Jose, CA 95110

Dear Mr. Narayen:

Leading technology providers spanning media generation, editing, and distribution have publicly pledged to address the increasing prevalence of maliciously manipulated media. While imperfect and no substitute for comprehensive federal legislation, these voluntary efforts, including the *Coalition for Content Provenance & Authenticity* and the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, complemented by a patchwork of state laws, represent some of the only meaningful interventions to address media manipulation-based threats ahead of the 2026 U.S. midterm elections.

Prior to the 2024 U.S. elections, Russian-attributed actors used media manipulation techniques to denigrate a U.S. Vice-Presidential candidate<sup>1</sup> and a domestic actor utilized voice cloning software for robocalls impersonating President Biden in the New Hampshire primary.<sup>2</sup> While these malicious actions largely failed to meaningfully effect the elections, the capabilities of generative artificial intelligence (AI) products have grown tremendously in the intervening years. Particularly against the backdrop of an abrupt pullback in federal resources, an effective multi-stakeholder approach is needed to ensure that industry, state and local governments, and civil society adequately anticipate – and counteract – media manipulation techniques that cause harm to vulnerable communities, public trust, and democratic institutions.

Policymakers have on a bipartisan basis begun the process of developing measures to ensure that generative AI technologies (and related media modification tools) serve the public interest. But the private sector can – particularly in collaboration with civil society and state and local election officials – dramatically shape the usage and wider impact of these technologies through proactive measures in coming months. As a follow-up to my requests<sup>3</sup> in the wake of the *Munich Tech*

---

<sup>1</sup> Office of the Director of National Intelligence, *Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts*, Press Release (Nov. 1, 2024).

<sup>2</sup> Alex Seitz-Wald and Mike Memoli, *Fake Joe Biden Robocall Tells New Hampshire Voters Not to Vote Tuesday*, NBC News (Jan. 22, 2024).

<sup>3</sup> Senator Mark Warner, *Senate Intel Chairman Pushes Companies to Follow Through on Commitments to Combat Deceptive Use of AI*, Press Release (May 14, 2024).

*Accord*, I strongly encourage you to take the following measures to anticipate, identify, and respond to potential media manipulation efforts targeting the election.

#### Generative AI Model and Media Editing Software Vendors:

- **Attach robust and consensus-based content credentials**, and other relevant provenance or authenticity signals (including metadata and prominent visible watermarks), to any media created using your products.
- To the extent that your product is incorporated in a downstream product offered by a third-party, **adopt license terms that stipulate the adoption of such measures by providers that resell or otherwise repackage your generative AI or media editing tools.**
- **Share detection methodologies or internal classifiers associated with your generative AI or media modification products** through trusted channels with content distributors, other generative AI and media editing software vendors, and trustworthy news organizations.
- Develop and appropriately resource **‘rapid-response’ channels by which verified independent media and civil society organizations can leverage your detection tools to authenticate media** that may have been created with your products.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content**, and consider separate reporting tools for public figures or uniquely vulnerable user groups.
- Maintain **resources to proactively identify impersonation campaigns using your products**, with mechanisms to contact victims promptly.

#### Social Media Platforms and Other Major Content Distributors:

- Establish and enforce **clear Terms of Service regarding generative and manipulated media** and consider policies to **require visual markers of generative or manipulated content for users.**
- Adopt mechanisms to **screen uploaded content for content credentials, watermarks, or other media authenticity signals**, with the goal of ensuring that such content is consistent with your Terms of Service.
- **Develop internal classifiers or enlist third-party detection solutions to detect generative and manipulated media** that lack content credentials, watermarks, or other media authenticity signals – **sharing detection methodologies through trusted channels** with other content distributors.
- Engage independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public.
- **Engage candidates and election officials on effective utilization of content credentialing or other media authentication tools** for their public communications on your distribution platforms.

- Consider **open-sourcing detection tools and methods** to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content.
- **Maintain a publicly-accessible database containing generative or manipulated media that violates your Terms of Service** (particularly with respect to election-related content), enabling civil society and media organizations to track media manipulation campaigns (with appropriate privacy and content-safety features to limit re-victimization).
- Maintain **resources to proactively identify impersonation campaigns conducted on your platforms**, with mechanisms to contact victims promptly.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content violations**, and consider a separate reporting tools for public figures or uniquely-vulnerable user groups.
- Initiate **information-sharing mechanisms between platforms on detecting manipulated content that may be used for malicious ends** (such as election disinformation, voter suppression, non-consensual intimate imagery, online harassment, etc.)

Thank you for your attention to these important matters. I welcome your public commitment to these measures, in addition to concrete commitments you have already made to anticipate, identify, and counteract malicious use of your products ahead of the 2026 U.S. midterm elections.

Sincerely,



---

Mark R. Warner  
United States Senator

March 16, 2026

Mr. Dario Amodei  
Chief Executive Officer  
Anthropic  
500 Howard Street  
San Francisco, CA 94105

Dear Mr. Amodei:

Leading technology providers spanning media generation, editing, and distribution have publicly pledged to address the increasing prevalence of maliciously manipulated media. While imperfect and no substitute for comprehensive federal legislation, these voluntary efforts, including the *Coalition for Content Provenance & Authenticity* and the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, complemented by a patchwork of state laws, represent some of the only meaningful interventions to address media manipulation-based threats ahead of the 2026 U.S. midterm elections.

Prior to the 2024 U.S. elections, Russian-attributed actors used media manipulation techniques to denigrate a U.S. Vice-Presidential candidate<sup>1</sup> and a domestic actor utilized voice cloning software for robocalls impersonating President Biden in the New Hampshire primary.<sup>2</sup> While these malicious actions largely failed to meaningfully effect the elections, the capabilities of generative artificial intelligence (AI) products have grown tremendously in the intervening years. Particularly against the backdrop of an abrupt pullback in federal resources, an effective multi-stakeholder approach is needed to ensure that industry, state and local governments, and civil society adequately anticipate – and counteract – media manipulation techniques that cause harm to vulnerable communities, public trust, and democratic institutions.

Policymakers have on a bipartisan basis begun the process of developing measures to ensure that generative AI technologies (and related media modification tools) serve the public interest. But the private sector can – particularly in collaboration with civil society and state and local election officials – dramatically shape the usage and wider impact of these technologies through proactive measures in coming months. As a follow-up to my requests<sup>3</sup> in the wake of the *Munich Tech*

---

<sup>1</sup> Office of the Director of National Intelligence, *Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts*, Press Release (Nov. 1, 2024).

<sup>2</sup> Alex Seitz-Wald and Mike Memoli, *Fake Joe Biden Robocall Tells New Hampshire Voters Not to Vote Tuesday*, NBC News (Jan. 22, 2024).

<sup>3</sup> Senator Mark Warner, *Senate Intel Chairman Pushes Companies to Follow Through on Commitments to Combat Deceptive Use of AI*, Press Release (May 14, 2024).

*Accord*, I strongly encourage you to take the following measures to anticipate, identify, and respond to potential media manipulation efforts targeting the election.

#### Generative AI Model and Media Editing Software Vendors:

- **Attach robust and consensus-based content credentials**, and other relevant provenance or authenticity signals (including metadata and prominent visible watermarks), to any media created using your products.
- To the extent that your product is incorporated in a downstream product offered by a third-party, **adopt license terms that stipulate the adoption of such measures by providers that resell or otherwise repackage your generative AI or media editing tools.**
- **Share detection methodologies or internal classifiers associated with your generative AI or media modification products** through trusted channels with content distributors, other generative AI and media editing software vendors, and trustworthy news organizations.
- Develop and appropriately resource **‘rapid-response’ channels by which verified independent media and civil society organizations can leverage your detection tools to authenticate media** that may have been created with your products.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content**, and consider separate reporting tools for public figures or uniquely vulnerable user groups.
- Maintain **resources to proactively identify impersonation campaigns using your products**, with mechanisms to contact victims promptly.

#### Social Media Platforms and Other Major Content Distributors:

- Establish and enforce **clear Terms of Service regarding generative and manipulated media** and consider policies to **require visual markers of generative or manipulated content for users.**
- Adopt mechanisms to **screen uploaded content for content credentials, watermarks, or other media authenticity signals**, with the goal of ensuring that such content is consistent with your Terms of Service.
- **Develop internal classifiers or enlist third-party detection solutions to detect generative and manipulated media** that lack content credentials, watermarks, or other media authenticity signals – **sharing detection methodologies through trusted channels** with other content distributors.
- Engage independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public.
- **Engage candidates and election officials on effective utilization of content credentialing or other media authentication tools** for their public communications on your distribution platforms.

- Consider **open-sourcing detection tools and methods** to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content.
- **Maintain a publicly-accessible database containing generative or manipulated media that violates your Terms of Service** (particularly with respect to election-related content), enabling civil society and media organizations to track media manipulation campaigns (with appropriate privacy and content-safety features to limit re-victimization).
- Maintain **resources to proactively identify impersonation campaigns conducted on your platforms**, with mechanisms to contact victims promptly.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content violations**, and consider a separate reporting tools for public figures or uniquely-vulnerable user groups.
- Initiate **information-sharing mechanisms between platforms on detecting manipulated content that may be used for malicious ends** (such as election disinformation, voter suppression, non-consensual intimate imagery, online harassment, etc.)

Thank you for your attention to these important matters. I welcome your public commitment to these measures, in addition to concrete commitments you have already made to anticipate, identify, and counteract malicious use of your products ahead of the 2026 U.S. midterm elections.

Sincerely,



---

Mark R. Warner  
United States Senator

March 16, 2026

Mr. Toni Schneider  
Interim Chief Executive Officer  
Bluesky  
113 Cherry Street, Suite 24821  
Seattle, WA 98104

Dear Mr. Schneider:

Leading technology providers spanning media generation, editing, and distribution have publicly pledged to address the increasing prevalence of maliciously manipulated media. While imperfect and no substitute for comprehensive federal legislation, these voluntary efforts, including the *Coalition for Content Provenance & Authenticity* and the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, complemented by a patchwork of state laws, represent some of the only meaningful interventions to address media manipulation-based threats ahead of the 2026 U.S. midterm elections.

Prior to the 2024 U.S. elections, Russian-attributed actors used media manipulation techniques to denigrate a U.S. Vice-Presidential candidate<sup>1</sup> and a domestic actor utilized voice cloning software for robocalls impersonating President Biden in the New Hampshire primary.<sup>2</sup> While these malicious actions largely failed to meaningfully effect the elections, the capabilities of generative artificial intelligence (AI) products have grown tremendously in the intervening years. Particularly against the backdrop of an abrupt pullback in federal resources, an effective multi-stakeholder approach is needed to ensure that industry, state and local governments, and civil society adequately anticipate – and counteract – media manipulation techniques that cause harm to vulnerable communities, public trust, and democratic institutions.

Policymakers have on a bipartisan basis begun the process of developing measures to ensure that generative AI technologies (and related media modification tools) serve the public interest. But the private sector can – particularly in collaboration with civil society and state and local election officials – dramatically shape the usage and wider impact of these technologies through proactive measures in coming months. As a follow-up to my requests<sup>3</sup> in the wake of the *Munich Tech*

---

<sup>1</sup> Office of the Director of National Intelligence, *Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts*, Press Release (Nov. 1, 2024).

<sup>2</sup> Alex Seitz-Wald and Mike Memoli, *Fake Joe Biden Robocall Tells New Hampshire Voters Not to Vote Tuesday*, NBC News (Jan. 22, 2024).

<sup>3</sup> Senator Mark Warner, *Senate Intel Chairman Pushes Companies to Follow Through on Commitments to Combat Deceptive Use of AI*, Press Release (May 14, 2024).

*Accord*, I strongly encourage you to take the following measures to anticipate, identify, and respond to potential media manipulation efforts targeting the election.

#### Generative AI Model and Media Editing Software Vendors:

- **Attach robust and consensus-based content credentials**, and other relevant provenance or authenticity signals (including metadata and prominent visible watermarks), to any media created using your products.
- To the extent that your product is incorporated in a downstream product offered by a third-party, **adopt license terms that stipulate the adoption of such measures by providers that resell or otherwise repackage your generative AI or media editing tools.**
- **Share detection methodologies or internal classifiers associated with your generative AI or media modification products** through trusted channels with content distributors, other generative AI and media editing software vendors, and trustworthy news organizations.
- Develop and appropriately resource **‘rapid-response’ channels by which verified independent media and civil society organizations can leverage your detection tools to authenticate media** that may have been created with your products.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content**, and consider separate reporting tools for public figures or uniquely vulnerable user groups.
- Maintain **resources to proactively identify impersonation campaigns using your products**, with mechanisms to contact victims promptly.

#### Social Media Platforms and Other Major Content Distributors:

- Establish and enforce **clear Terms of Service regarding generative and manipulated media** and consider policies to **require visual markers of generative or manipulated content for users.**
- Adopt mechanisms to **screen uploaded content for content credentials, watermarks, or other media authenticity signals**, with the goal of ensuring that such content is consistent with your Terms of Service.
- **Develop internal classifiers or enlist third-party detection solutions to detect generative and manipulated media** that lack content credentials, watermarks, or other media authenticity signals – **sharing detection methodologies through trusted channels** with other content distributors.
- Engage independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public.
- **Engage candidates and election officials on effective utilization of content credentialing or other media authentication tools** for their public communications on your distribution platforms.

- Consider **open-sourcing detection tools and methods** to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content.
- **Maintain a publicly-accessible database containing generative or manipulated media that violates your Terms of Service** (particularly with respect to election-related content), enabling civil society and media organizations to track media manipulation campaigns (with appropriate privacy and content-safety features to limit re-victimization).
- Maintain **resources to proactively identify impersonation campaigns conducted on your platforms**, with mechanisms to contact victims promptly.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content violations**, and consider a separate reporting tools for public figures or uniquely-vulnerable user groups.
- Initiate **information-sharing mechanisms between platforms on detecting manipulated content that may be used for malicious ends** (such as election disinformation, voter suppression, non-consensual intimate imagery, online harassment, etc.)

Thank you for your attention to these important matters. I welcome your public commitment to these measures, in addition to concrete commitments you have already made to anticipate, identify, and counteract malicious use of your products ahead of the 2026 U.S. midterm elections.

Sincerely,



---

Mark R. Warner  
United States Senator

# United States Senate

WASHINGTON, DC 20510-4606

March 16, 2026

Ms. Melanie Perkins  
Chief Executive Officer  
Canva  
3212 E. Cesar Chavez Street, Suite 1300  
Austin, TX 78702

Dear Ms. Perkins:

Leading technology providers spanning media generation, editing, and distribution have publicly pledged to address the increasing prevalence of maliciously manipulated media. While imperfect and no substitute for comprehensive federal legislation, these voluntary efforts, including the *Coalition for Content Provenance & Authenticity* and the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, complemented by a patchwork of state laws, represent some of the only meaningful interventions to address media manipulation-based threats ahead of the 2026 U.S. midterm elections.

Prior to the 2024 U.S. elections, Russian-attributed actors used media manipulation techniques to denigrate a U.S. Vice-Presidential candidate<sup>1</sup> and a domestic actor utilized voice cloning software for robocalls impersonating President Biden in the New Hampshire primary.<sup>2</sup> While these malicious actions largely failed to meaningfully effect the elections, the capabilities of generative artificial intelligence (AI) products have grown tremendously in the intervening years. Particularly against the backdrop of an abrupt pullback in federal resources, an effective multi-stakeholder approach is needed to ensure that industry, state and local governments, and civil society adequately anticipate – and counteract – media manipulation techniques that cause harm to vulnerable communities, public trust, and democratic institutions.

Policymakers have on a bipartisan basis begun the process of developing measures to ensure that generative AI technologies (and related media modification tools) serve the public interest. But the private sector can – particularly in collaboration with civil society and state and local election officials – dramatically shape the usage and wider impact of these technologies through proactive measures in coming months. As a follow-up to my requests<sup>3</sup> in the wake of the *Munich Tech*

---

<sup>1</sup> Office of the Director of National Intelligence, *Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts*, Press Release (Nov. 1, 2024).

<sup>2</sup> Alex Seitz-Wald and Mike Memoli, *Fake Joe Biden Robocall Tells New Hampshire Voters Not to Vote Tuesday*, NBC News (Jan. 22, 2024).

<sup>3</sup> Senator Mark Warner, *Senate Intel Chairman Pushes Companies to Follow Through on Commitments to Combat Deceptive Use of AI*, Press Release (May 14, 2024).

*Accord*, I strongly encourage you to take the following measures to anticipate, identify, and respond to potential media manipulation efforts targeting the election.

#### Generative AI Model and Media Editing Software Vendors:

- **Attach robust and consensus-based content credentials**, and other relevant provenance or authenticity signals (including metadata and prominent visible watermarks), to any media created using your products.
- To the extent that your product is incorporated in a downstream product offered by a third-party, **adopt license terms that stipulate the adoption of such measures by providers that resell or otherwise repackage your generative AI or media editing tools.**
- **Share detection methodologies or internal classifiers associated with your generative AI or media modification products** through trusted channels with content distributors, other generative AI and media editing software vendors, and trustworthy news organizations.
- Develop and appropriately resource **‘rapid-response’ channels by which verified independent media and civil society organizations can leverage your detection tools to authenticate media** that may have been created with your products.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content**, and consider separate reporting tools for public figures or uniquely vulnerable user groups.
- Maintain **resources to proactively identify impersonation campaigns using your products**, with mechanisms to contact victims promptly.

#### Social Media Platforms and Other Major Content Distributors:

- Establish and enforce **clear Terms of Service regarding generative and manipulated media** and consider policies to **require visual markers of generative or manipulated content for users.**
- Adopt mechanisms to **screen uploaded content for content credentials, watermarks, or other media authenticity signals**, with the goal of ensuring that such content is consistent with your Terms of Service.
- **Develop internal classifiers or enlist third-party detection solutions to detect generative and manipulated media** that lack content credentials, watermarks, or other media authenticity signals – **sharing detection methodologies through trusted channels** with other content distributors.
- Engage independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public.
- **Engage candidates and election officials on effective utilization of content credentialing or other media authentication tools** for their public communications on your distribution platforms.

- Consider **open-sourcing detection tools and methods** to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content.
- **Maintain a publicly-accessible database containing generative or manipulated media that violates your Terms of Service** (particularly with respect to election-related content), enabling civil society and media organizations to track media manipulation campaigns (with appropriate privacy and content-safety features to limit re-victimization).
- Maintain **resources to proactively identify impersonation campaigns conducted on your platforms**, with mechanisms to contact victims promptly.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content violations**, and consider a separate reporting tools for public figures or uniquely-vulnerable user groups.
- Initiate **information-sharing mechanisms between platforms on detecting manipulated content that may be used for malicious ends** (such as election disinformation, voter suppression, non-consensual intimate imagery, online harassment, etc.)

Thank you for your attention to these important matters. I welcome your public commitment to these measures, in addition to concrete commitments you have already made to anticipate, identify, and counteract malicious use of your products ahead of the 2026 U.S. midterm elections.

Sincerely,



---

Mark R. Warner  
United States Senator

March 16, 2026

Mr. Aidan Gomez  
Chief Executive Officer  
Cohere  
171 John Street, Suite 200  
Toronto, ON M5T1X3

Dear Mr. Gomez:

Leading technology providers spanning media generation, editing, and distribution have publicly pledged to address the increasing prevalence of maliciously manipulated media. While imperfect and no substitute for comprehensive federal legislation, these voluntary efforts, including the *Coalition for Content Provenance & Authenticity* and the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, complemented by a patchwork of state laws, represent some of the only meaningful interventions to address media manipulation-based threats ahead of the 2026 U.S. midterm elections.

Prior to the 2024 U.S. elections, Russian-attributed actors used media manipulation techniques to denigrate a U.S. Vice-Presidential candidate<sup>1</sup> and a domestic actor utilized voice cloning software for robocalls impersonating President Biden in the New Hampshire primary.<sup>2</sup> While these malicious actions largely failed to meaningfully effect the elections, the capabilities of generative artificial intelligence (AI) products have grown tremendously in the intervening years. Particularly against the backdrop of an abrupt pullback in federal resources, an effective multi-stakeholder approach is needed to ensure that industry, state and local governments, and civil society adequately anticipate – and counteract – media manipulation techniques that cause harm to vulnerable communities, public trust, and democratic institutions.

Policymakers have on a bipartisan basis begun the process of developing measures to ensure that generative AI technologies (and related media modification tools) serve the public interest. But the private sector can – particularly in collaboration with civil society and state and local election officials – dramatically shape the usage and wider impact of these technologies through proactive measures in coming months. As a follow-up to my requests<sup>3</sup> in the wake of the *Munich Tech*

---

<sup>1</sup> Office of the Director of National Intelligence, *Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts*, Press Release (Nov. 1, 2024).

<sup>2</sup> Alex Seitz-Wald and Mike Memoli, *Fake Joe Biden Robocall Tells New Hampshire Voters Not to Vote Tuesday*, NBC News (Jan. 22, 2024).

<sup>3</sup> Senator Mark Warner, *Senate Intel Chairman Pushes Companies to Follow Through on Commitments to Combat Deceptive Use of AI*, Press Release (May 14, 2024).

*Accord*, I strongly encourage you to take the following measures to anticipate, identify, and respond to potential media manipulation efforts targeting the election.

#### Generative AI Model and Media Editing Software Vendors:

- **Attach robust and consensus-based content credentials**, and other relevant provenance or authenticity signals (including metadata and prominent visible watermarks), to any media created using your products.
- To the extent that your product is incorporated in a downstream product offered by a third-party, **adopt license terms that stipulate the adoption of such measures by providers that resell or otherwise repackage your generative AI or media editing tools.**
- **Share detection methodologies or internal classifiers associated with your generative AI or media modification products** through trusted channels with content distributors, other generative AI and media editing software vendors, and trustworthy news organizations.
- Develop and appropriately resource **‘rapid-response’ channels by which verified independent media and civil society organizations can leverage your detection tools to authenticate media** that may have been created with your products.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content**, and consider separate reporting tools for public figures or uniquely vulnerable user groups.
- Maintain **resources to proactively identify impersonation campaigns using your products**, with mechanisms to contact victims promptly.

#### Social Media Platforms and Other Major Content Distributors:

- Establish and enforce **clear Terms of Service regarding generative and manipulated media** and consider policies to **require visual markers of generative or manipulated content for users.**
- Adopt mechanisms to **screen uploaded content for content credentials, watermarks, or other media authenticity signals**, with the goal of ensuring that such content is consistent with your Terms of Service.
- **Develop internal classifiers or enlist third-party detection solutions to detect generative and manipulated media** that lack content credentials, watermarks, or other media authenticity signals – **sharing detection methodologies through trusted channels** with other content distributors.
- Engage independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public.
- **Engage candidates and election officials on effective utilization of content credentialing or other media authentication tools** for their public communications on your distribution platforms.

- Consider **open-sourcing detection tools and methods** to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content.
- **Maintain a publicly-accessible database containing generative or manipulated media that violates your Terms of Service** (particularly with respect to election-related content), enabling civil society and media organizations to track media manipulation campaigns (with appropriate privacy and content-safety features to limit re-victimization).
- Maintain **resources to proactively identify impersonation campaigns conducted on your platforms**, with mechanisms to contact victims promptly.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content violations**, and consider a separate reporting tools for public figures or uniquely-vulnerable user groups.
- Initiate **information-sharing mechanisms between platforms on detecting manipulated content that may be used for malicious ends** (such as election disinformation, voter suppression, non-consensual intimate imagery, online harassment, etc.)

Thank you for your attention to these important matters. I welcome your public commitment to these measures, in addition to concrete commitments you have already made to anticipate, identify, and counteract malicious use of your products ahead of the 2026 U.S. midterm elections.

Sincerely,



---

Mark R. Warner  
United States Senator

March 16, 2026

Mr. Mati Staniszewski  
Chief Executive Officer  
ElevenLabs  
169 Madison Avenue #2484  
New York, NY 10016

Dear Mr. Staniszewski:

Leading technology providers spanning media generation, editing, and distribution have publicly pledged to address the increasing prevalence of maliciously manipulated media. While imperfect and no substitute for comprehensive federal legislation, these voluntary efforts, including the *Coalition for Content Provenance & Authenticity* and the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, complemented by a patchwork of state laws, represent some of the only meaningful interventions to address media manipulation-based threats ahead of the 2026 U.S. midterm elections.

Prior to the 2024 U.S. elections, Russian-attributed actors used media manipulation techniques to denigrate a U.S. Vice-Presidential candidate<sup>1</sup> and a domestic actor utilized voice cloning software for robocalls impersonating President Biden in the New Hampshire primary.<sup>2</sup> While these malicious actions largely failed to meaningfully effect the elections, the capabilities of generative artificial intelligence (AI) products have grown tremendously in the intervening years. Particularly against the backdrop of an abrupt pullback in federal resources, an effective multi-stakeholder approach is needed to ensure that industry, state and local governments, and civil society adequately anticipate – and counteract – media manipulation techniques that cause harm to vulnerable communities, public trust, and democratic institutions.

Policymakers have on a bipartisan basis begun the process of developing measures to ensure that generative AI technologies (and related media modification tools) serve the public interest. But the private sector can – particularly in collaboration with civil society and state and local election officials – dramatically shape the usage and wider impact of these technologies through proactive measures in coming months. As a follow-up to my requests<sup>3</sup> in the wake of the *Munich Tech*

---

<sup>1</sup> Office of the Director of National Intelligence, *Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts*, Press Release (Nov. 1, 2024).

<sup>2</sup> Alex Seitz-Wald and Mike Memoli, *Fake Joe Biden Robocall Tells New Hampshire Voters Not to Vote Tuesday*, NBC News (Jan. 22, 2024).

<sup>3</sup> Senator Mark Warner, *Senate Intel Chairman Pushes Companies to Follow Through on Commitments to Combat Deceptive Use of AI*, Press Release (May 14, 2024).

*Accord*, I strongly encourage you to take the following measures to anticipate, identify, and respond to potential media manipulation efforts targeting the election.

#### Generative AI Model and Media Editing Software Vendors:

- **Attach robust and consensus-based content credentials**, and other relevant provenance or authenticity signals (including metadata and prominent visible watermarks), to any media created using your products.
- To the extent that your product is incorporated in a downstream product offered by a third-party, **adopt license terms that stipulate the adoption of such measures by providers that resell or otherwise repackage your generative AI or media editing tools.**
- **Share detection methodologies or internal classifiers associated with your generative AI or media modification products** through trusted channels with content distributors, other generative AI and media editing software vendors, and trustworthy news organizations.
- Develop and appropriately resource **‘rapid-response’ channels by which verified independent media and civil society organizations can leverage your detection tools to authenticate media** that may have been created with your products.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content**, and consider separate reporting tools for public figures or uniquely vulnerable user groups.
- Maintain **resources to proactively identify impersonation campaigns using your products**, with mechanisms to contact victims promptly.

#### Social Media Platforms and Other Major Content Distributors:

- Establish and enforce **clear Terms of Service regarding generative and manipulated media** and consider policies to **require visual markers of generative or manipulated content for users.**
- Adopt mechanisms to **screen uploaded content for content credentials, watermarks, or other media authenticity signals**, with the goal of ensuring that such content is consistent with your Terms of Service.
- **Develop internal classifiers or enlist third-party detection solutions to detect generative and manipulated media** that lack content credentials, watermarks, or other media authenticity signals – **sharing detection methodologies through trusted channels** with other content distributors.
- Engage independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public.
- **Engage candidates and election officials on effective utilization of content credentialing or other media authentication tools** for their public communications on your distribution platforms.

- Consider **open-sourcing detection tools and methods** to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content.
- **Maintain a publicly-accessible database containing generative or manipulated media that violates your Terms of Service** (particularly with respect to election-related content), enabling civil society and media organizations to track media manipulation campaigns (with appropriate privacy and content-safety features to limit re-victimization).
- Maintain **resources to proactively identify impersonation campaigns conducted on your platforms**, with mechanisms to contact victims promptly.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content violations**, and consider a separate reporting tools for public figures or uniquely-vulnerable user groups.
- Initiate **information-sharing mechanisms between platforms on detecting manipulated content that may be used for malicious ends** (such as election disinformation, voter suppression, non-consensual intimate imagery, online harassment, etc.)

Thank you for your attention to these important matters. I welcome your public commitment to these measures, in addition to concrete commitments you have already made to anticipate, identify, and counteract malicious use of your products ahead of the 2026 U.S. midterm elections.

Sincerely,



---

Mark R. Warner  
United States Senator

March 16, 2026

Mr. Sundar Pichai  
Chief Executive Officer  
Google  
1600 Amphitheatre Parkway  
Mountain View, CA 94043

Dear Mr. Pichai:

Leading technology providers spanning media generation, editing, and distribution have publicly pledged to address the increasing prevalence of maliciously manipulated media. While imperfect and no substitute for comprehensive federal legislation, these voluntary efforts, including the *Coalition for Content Provenance & Authenticity* and the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, complemented by a patchwork of state laws, represent some of the only meaningful interventions to address media manipulation-based threats ahead of the 2026 U.S. midterm elections.

Prior to the 2024 U.S. elections, Russian-attributed actors used media manipulation techniques to denigrate a U.S. Vice-Presidential candidate<sup>1</sup> and a domestic actor utilized voice cloning software for robocalls impersonating President Biden in the New Hampshire primary.<sup>2</sup> While these malicious actions largely failed to meaningfully effect the elections, the capabilities of generative artificial intelligence (AI) products have grown tremendously in the intervening years. Particularly against the backdrop of an abrupt pullback in federal resources, an effective multi-stakeholder approach is needed to ensure that industry, state and local governments, and civil society adequately anticipate – and counteract – media manipulation techniques that cause harm to vulnerable communities, public trust, and democratic institutions.

Policymakers have on a bipartisan basis begun the process of developing measures to ensure that generative AI technologies (and related media modification tools) serve the public interest. But the private sector can – particularly in collaboration with civil society and state and local election officials – dramatically shape the usage and wider impact of these technologies through proactive measures in coming months. As a follow-up to my requests<sup>3</sup> in the wake of the *Munich Tech*

---

<sup>1</sup> Office of the Director of National Intelligence, *Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts*, Press Release (Nov. 1, 2024).

<sup>2</sup> Alex Seitz-Wald and Mike Memoli, *Fake Joe Biden Robocall Tells New Hampshire Voters Not to Vote Tuesday*, NBC News (Jan. 22, 2024).

<sup>3</sup> Senator Mark Warner, *Senate Intel Chairman Pushes Companies to Follow Through on Commitments to Combat Deceptive Use of AI*, Press Release (May 14, 2024).

*Accord*, I strongly encourage you to take the following measures to anticipate, identify, and respond to potential media manipulation efforts targeting the election.

#### Generative AI Model and Media Editing Software Vendors:

- **Attach robust and consensus-based content credentials**, and other relevant provenance or authenticity signals (including metadata and prominent visible watermarks), to any media created using your products.
- To the extent that your product is incorporated in a downstream product offered by a third-party, **adopt license terms that stipulate the adoption of such measures by providers that resell or otherwise repackage your generative AI or media editing tools.**
- **Share detection methodologies or internal classifiers associated with your generative AI or media modification products** through trusted channels with content distributors, other generative AI and media editing software vendors, and trustworthy news organizations.
- Develop and appropriately resource **‘rapid-response’ channels by which verified independent media and civil society organizations can leverage your detection tools to authenticate media** that may have been created with your products.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content**, and consider separate reporting tools for public figures or uniquely vulnerable user groups.
- Maintain **resources to proactively identify impersonation campaigns using your products**, with mechanisms to contact victims promptly.

#### Social Media Platforms and Other Major Content Distributors:

- Establish and enforce **clear Terms of Service regarding generative and manipulated media** and consider policies to **require visual markers of generative or manipulated content for users.**
- Adopt mechanisms to **screen uploaded content for content credentials, watermarks, or other media authenticity signals**, with the goal of ensuring that such content is consistent with your Terms of Service.
- **Develop internal classifiers or enlist third-party detection solutions to detect generative and manipulated media** that lack content credentials, watermarks, or other media authenticity signals – **sharing detection methodologies through trusted channels** with other content distributors.
- Engage independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public.
- **Engage candidates and election officials on effective utilization of content credentialing or other media authentication tools** for their public communications on your distribution platforms.

- Consider **open-sourcing detection tools and methods** to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content.
- **Maintain a publicly-accessible database containing generative or manipulated media that violates your Terms of Service** (particularly with respect to election-related content), enabling civil society and media organizations to track media manipulation campaigns (with appropriate privacy and content-safety features to limit re-victimization).
- Maintain **resources to proactively identify impersonation campaigns conducted on your platforms**, with mechanisms to contact victims promptly.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content violations**, and consider a separate reporting tools for public figures or uniquely-vulnerable user groups.
- Initiate **information-sharing mechanisms between platforms on detecting manipulated content that may be used for malicious ends** (such as election disinformation, voter suppression, non-consensual intimate imagery, online harassment, etc.)

Thank you for your attention to these important matters. I welcome your public commitment to these measures, in addition to concrete commitments you have already made to anticipate, identify, and counteract malicious use of your products ahead of the 2026 U.S. midterm elections.

Sincerely,



---

Mark R. Warner  
United States Senator

# United States Senate

WASHINGTON, DC 20510-4606

March 16, 2026

Mr. Mark Zuckerberg  
Chief Executive Officer  
Meta  
1 Meta Way  
Menlo Park, CA 94025

Dear Mr. Zuckerberg:

Leading technology providers spanning media generation, editing, and distribution have publicly pledged to address the increasing prevalence of maliciously manipulated media. While imperfect and no substitute for comprehensive federal legislation, these voluntary efforts, including the *Coalition for Content Provenance & Authenticity* and the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, complemented by a patchwork of state laws, represent some of the only meaningful interventions to address media manipulation-based threats ahead of the 2026 U.S. midterm elections.

Prior to the 2024 U.S. elections, Russian-attributed actors used media manipulation techniques to denigrate a U.S. Vice-Presidential candidate<sup>1</sup> and a domestic actor utilized voice cloning software for robocalls impersonating President Biden in the New Hampshire primary.<sup>2</sup> While these malicious actions largely failed to meaningfully effect the elections, the capabilities of generative artificial intelligence (AI) products have grown tremendously in the intervening years. Particularly against the backdrop of an abrupt pullback in federal resources, an effective multi-stakeholder approach is needed to ensure that industry, state and local governments, and civil society adequately anticipate – and counteract – media manipulation techniques that cause harm to vulnerable communities, public trust, and democratic institutions.

Policymakers have on a bipartisan basis begun the process of developing measures to ensure that generative AI technologies (and related media modification tools) serve the public interest. But the private sector can – particularly in collaboration with civil society and state and local election officials – dramatically shape the usage and wider impact of these technologies through proactive measures in coming months. As a follow-up to my requests<sup>3</sup> in the wake of the *Munich Tech*

---

<sup>1</sup> Office of the Director of National Intelligence, *Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts*, Press Release (Nov. 1, 2024).

<sup>2</sup> Alex Seitz-Wald and Mike Memoli, *Fake Joe Biden Robocall Tells New Hampshire Voters Not to Vote Tuesday*, NBC News (Jan. 22, 2024).

<sup>3</sup> Senator Mark Warner, *Senate Intel Chairman Pushes Companies to Follow Through on Commitments to Combat Deceptive Use of AI*, Press Release (May 14, 2024).

*Accord*, I strongly encourage you to take the following measures to anticipate, identify, and respond to potential media manipulation efforts targeting the election.

#### Generative AI Model and Media Editing Software Vendors:

- **Attach robust and consensus-based content credentials**, and other relevant provenance or authenticity signals (including metadata and prominent visible watermarks), to any media created using your products.
- To the extent that your product is incorporated in a downstream product offered by a third-party, **adopt license terms that stipulate the adoption of such measures by providers that resell or otherwise repackage your generative AI or media editing tools.**
- **Share detection methodologies or internal classifiers associated with your generative AI or media modification products** through trusted channels with content distributors, other generative AI and media editing software vendors, and trustworthy news organizations.
- Develop and appropriately resource **‘rapid-response’ channels by which verified independent media and civil society organizations can leverage your detection tools to authenticate media** that may have been created with your products.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content**, and consider separate reporting tools for public figures or uniquely vulnerable user groups.
- Maintain **resources to proactively identify impersonation campaigns using your products**, with mechanisms to contact victims promptly.

#### Social Media Platforms and Other Major Content Distributors:

- Establish and enforce **clear Terms of Service regarding generative and manipulated media** and consider policies to **require visual markers of generative or manipulated content for users.**
- Adopt mechanisms to **screen uploaded content for content credentials, watermarks, or other media authenticity signals**, with the goal of ensuring that such content is consistent with your Terms of Service.
- **Develop internal classifiers or enlist third-party detection solutions to detect generative and manipulated media** that lack content credentials, watermarks, or other media authenticity signals – **sharing detection methodologies through trusted channels** with other content distributors.
- Engage independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public.
- **Engage candidates and election officials on effective utilization of content credentialing or other media authentication tools** for their public communications on your distribution platforms.

- Consider **open-sourcing detection tools and methods** to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content.
- **Maintain a publicly-accessible database containing generative or manipulated media that violates your Terms of Service** (particularly with respect to election-related content), enabling civil society and media organizations to track media manipulation campaigns (with appropriate privacy and content-safety features to limit re-victimization).
- Maintain **resources to proactively identify impersonation campaigns conducted on your platforms**, with mechanisms to contact victims promptly.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content violations**, and consider a separate reporting tools for public figures or uniquely-vulnerable user groups.
- Initiate **information-sharing mechanisms between platforms on detecting manipulated content that may be used for malicious ends** (such as election disinformation, voter suppression, non-consensual intimate imagery, online harassment, etc.)

Thank you for your attention to these important matters. I welcome your public commitment to these measures, in addition to concrete commitments you have already made to anticipate, identify, and counteract malicious use of your products ahead of the 2026 U.S. midterm elections.

Sincerely,



---

Mark R. Warner  
United States Senator

March 16, 2026

Mr. Satya Nadella  
Chief Executive Officer  
Microsoft  
1 Microsoft Way  
Redmond, WA 98052

Dear Mr. Nadella:

Leading technology providers spanning media generation, editing, and distribution have publicly pledged to address the increasing prevalence of maliciously manipulated media. While imperfect and no substitute for comprehensive federal legislation, these voluntary efforts, including the *Coalition for Content Provenance & Authenticity* and the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, complemented by a patchwork of state laws, represent some of the only meaningful interventions to address media manipulation-based threats ahead of the 2026 U.S. midterm elections.

Prior to the 2024 U.S. elections, Russian-attributed actors used media manipulation techniques to denigrate a U.S. Vice-Presidential candidate<sup>1</sup> and a domestic actor utilized voice cloning software for robocalls impersonating President Biden in the New Hampshire primary.<sup>2</sup> While these malicious actions largely failed to meaningfully effect the elections, the capabilities of generative artificial intelligence (AI) products have grown tremendously in the intervening years. Particularly against the backdrop of an abrupt pullback in federal resources, an effective multi-stakeholder approach is needed to ensure that industry, state and local governments, and civil society adequately anticipate – and counteract – media manipulation techniques that cause harm to vulnerable communities, public trust, and democratic institutions.

Policymakers have on a bipartisan basis begun the process of developing measures to ensure that generative AI technologies (and related media modification tools) serve the public interest. But the private sector can – particularly in collaboration with civil society and state and local election officials – dramatically shape the usage and wider impact of these technologies through proactive measures in coming months. As a follow-up to my requests<sup>3</sup> in the wake of the *Munich Tech*

---

<sup>1</sup> Office of the Director of National Intelligence, *Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts*, Press Release (Nov. 1, 2024).

<sup>2</sup> Alex Seitz-Wald and Mike Memoli, *Fake Joe Biden Robocall Tells New Hampshire Voters Not to Vote Tuesday*, NBC News (Jan. 22, 2024).

<sup>3</sup> Senator Mark Warner, *Senate Intel Chairman Pushes Companies to Follow Through on Commitments to Combat Deceptive Use of AI*, Press Release (May 14, 2024).

*Accord*, I strongly encourage you to take the following measures to anticipate, identify, and respond to potential media manipulation efforts targeting the election.

#### Generative AI Model and Media Editing Software Vendors:

- **Attach robust and consensus-based content credentials**, and other relevant provenance or authenticity signals (including metadata and prominent visible watermarks), to any media created using your products.
- To the extent that your product is incorporated in a downstream product offered by a third-party, **adopt license terms that stipulate the adoption of such measures by providers that resell or otherwise repackage your generative AI or media editing tools.**
- **Share detection methodologies or internal classifiers associated with your generative AI or media modification products** through trusted channels with content distributors, other generative AI and media editing software vendors, and trustworthy news organizations.
- Develop and appropriately resource **‘rapid-response’ channels by which verified independent media and civil society organizations can leverage your detection tools to authenticate media** that may have been created with your products.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content**, and consider separate reporting tools for public figures or uniquely vulnerable user groups.
- Maintain **resources to proactively identify impersonation campaigns using your products**, with mechanisms to contact victims promptly.

#### Social Media Platforms and Other Major Content Distributors:

- Establish and enforce **clear Terms of Service regarding generative and manipulated media** and consider policies to **require visual markers of generative or manipulated content for users.**
- Adopt mechanisms to **screen uploaded content for content credentials, watermarks, or other media authenticity signals**, with the goal of ensuring that such content is consistent with your Terms of Service.
- **Develop internal classifiers or enlist third-party detection solutions to detect generative and manipulated media** that lack content credentials, watermarks, or other media authenticity signals – **sharing detection methodologies through trusted channels** with other content distributors.
- Engage independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public.
- **Engage candidates and election officials on effective utilization of content credentialing or other media authentication tools** for their public communications on your distribution platforms.

- Consider **open-sourcing detection tools and methods** to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content.
- **Maintain a publicly-accessible database containing generative or manipulated media that violates your Terms of Service** (particularly with respect to election-related content), enabling civil society and media organizations to track media manipulation campaigns (with appropriate privacy and content-safety features to limit re-victimization).
- Maintain **resources to proactively identify impersonation campaigns conducted on your platforms**, with mechanisms to contact victims promptly.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content violations**, and consider a separate reporting tools for public figures or uniquely-vulnerable user groups.
- Initiate **information-sharing mechanisms between platforms on detecting manipulated content that may be used for malicious ends** (such as election disinformation, voter suppression, non-consensual intimate imagery, online harassment, etc.)

Thank you for your attention to these important matters. I welcome your public commitment to these measures, in addition to concrete commitments you have already made to anticipate, identify, and counteract malicious use of your products ahead of the 2026 U.S. midterm elections.

Sincerely,



---

Mark R. Warner  
United States Senator

March 16, 2026

Mr. David Holz  
Chief Executive Officer  
Midjourney  
611 Gateway Boulevard, Suite 120  
South San Francisco, CA 94080

Dear Mr. Holz:

Leading technology providers spanning media generation, editing, and distribution have publicly pledged to address the increasing prevalence of maliciously manipulated media. While imperfect and no substitute for comprehensive federal legislation, these voluntary efforts, including the *Coalition for Content Provenance & Authenticity* and the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, complemented by a patchwork of state laws, represent some of the only meaningful interventions to address media manipulation-based threats ahead of the 2026 U.S. midterm elections.

Prior to the 2024 U.S. elections, Russian-attributed actors used media manipulation techniques to denigrate a U.S. Vice-Presidential candidate<sup>1</sup> and a domestic actor utilized voice cloning software for robocalls impersonating President Biden in the New Hampshire primary.<sup>2</sup> While these malicious actions largely failed to meaningfully effect the elections, the capabilities of generative artificial intelligence (AI) products have grown tremendously in the intervening years. Particularly against the backdrop of an abrupt pullback in federal resources, an effective multi-stakeholder approach is needed to ensure that industry, state and local governments, and civil society adequately anticipate – and counteract – media manipulation techniques that cause harm to vulnerable communities, public trust, and democratic institutions.

Policymakers have on a bipartisan basis begun the process of developing measures to ensure that generative AI technologies (and related media modification tools) serve the public interest. But the private sector can – particularly in collaboration with civil society and state and local election officials – dramatically shape the usage and wider impact of these technologies through proactive measures in coming months. As a follow-up to my requests<sup>3</sup> in the wake of the *Munich Tech*

---

<sup>1</sup> Office of the Director of National Intelligence, *Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts*, Press Release (Nov. 1, 2024).

<sup>2</sup> Alex Seitz-Wald and Mike Memoli, *Fake Joe Biden Robocall Tells New Hampshire Voters Not to Vote Tuesday*, NBC News (Jan. 22, 2024).

<sup>3</sup> Senator Mark Warner, *Senate Intel Chairman Pushes Companies to Follow Through on Commitments to Combat Deceptive Use of AI*, Press Release (May 14, 2024).

*Accord*, I strongly encourage you to take the following measures to anticipate, identify, and respond to potential media manipulation efforts targeting the election.

#### Generative AI Model and Media Editing Software Vendors:

- **Attach robust and consensus-based content credentials**, and other relevant provenance or authenticity signals (including metadata and prominent visible watermarks), to any media created using your products.
- To the extent that your product is incorporated in a downstream product offered by a third-party, **adopt license terms that stipulate the adoption of such measures by providers that resell or otherwise repackage your generative AI or media editing tools.**
- **Share detection methodologies or internal classifiers associated with your generative AI or media modification products** through trusted channels with content distributors, other generative AI and media editing software vendors, and trustworthy news organizations.
- Develop and appropriately resource **‘rapid-response’ channels by which verified independent media and civil society organizations can leverage your detection tools to authenticate media** that may have been created with your products.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content**, and consider separate reporting tools for public figures or uniquely vulnerable user groups.
- Maintain **resources to proactively identify impersonation campaigns using your products**, with mechanisms to contact victims promptly.

#### Social Media Platforms and Other Major Content Distributors:

- Establish and enforce **clear Terms of Service regarding generative and manipulated media** and consider policies to **require visual markers of generative or manipulated content for users.**
- Adopt mechanisms to **screen uploaded content for content credentials, watermarks, or other media authenticity signals**, with the goal of ensuring that such content is consistent with your Terms of Service.
- **Develop internal classifiers or enlist third-party detection solutions to detect generative and manipulated media** that lack content credentials, watermarks, or other media authenticity signals – **sharing detection methodologies through trusted channels** with other content distributors.
- Engage independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public.
- **Engage candidates and election officials on effective utilization of content credentialing or other media authentication tools** for their public communications on your distribution platforms.

- Consider **open-sourcing detection tools and methods** to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content.
- **Maintain a publicly-accessible database containing generative or manipulated media that violates your Terms of Service** (particularly with respect to election-related content), enabling civil society and media organizations to track media manipulation campaigns (with appropriate privacy and content-safety features to limit re-victimization).
- Maintain **resources to proactively identify impersonation campaigns conducted on your platforms**, with mechanisms to contact victims promptly.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content violations**, and consider a separate reporting tools for public figures or uniquely-vulnerable user groups.
- Initiate **information-sharing mechanisms between platforms on detecting manipulated content that may be used for malicious ends** (such as election disinformation, voter suppression, non-consensual intimate imagery, online harassment, etc.)

Thank you for your attention to these important matters. I welcome your public commitment to these measures, in addition to concrete commitments you have already made to anticipate, identify, and counteract malicious use of your products ahead of the 2026 U.S. midterm elections.

Sincerely,



---

Mark R. Warner  
United States Senator

March 16, 2026

Mr. Sam Altman  
Chief Executive Officer  
OpenAI  
1455 3<sup>rd</sup> Street  
San Francisco, CA 94158

Dear Mr. Altman:

Leading technology providers spanning media generation, editing, and distribution have publicly pledged to address the increasing prevalence of maliciously manipulated media. While imperfect and no substitute for comprehensive federal legislation, these voluntary efforts, including the *Coalition for Content Provenance & Authenticity* and the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, complemented by a patchwork of state laws, represent some of the only meaningful interventions to address media manipulation-based threats ahead of the 2026 U.S. midterm elections.

Prior to the 2024 U.S. elections, Russian-attributed actors used media manipulation techniques to denigrate a U.S. Vice-Presidential candidate<sup>1</sup> and a domestic actor utilized voice cloning software for robocalls impersonating President Biden in the New Hampshire primary.<sup>2</sup> While these malicious actions largely failed to meaningfully effect the elections, the capabilities of generative artificial intelligence (AI) products have grown tremendously in the intervening years. Particularly against the backdrop of an abrupt pullback in federal resources, an effective multi-stakeholder approach is needed to ensure that industry, state and local governments, and civil society adequately anticipate – and counteract – media manipulation techniques that cause harm to vulnerable communities, public trust, and democratic institutions.

Policymakers have on a bipartisan basis begun the process of developing measures to ensure that generative AI technologies (and related media modification tools) serve the public interest. But the private sector can – particularly in collaboration with civil society and state and local election officials – dramatically shape the usage and wider impact of these technologies through proactive measures in coming months. As a follow-up to my requests<sup>3</sup> in the wake of the *Munich Tech*

---

<sup>1</sup> Office of the Director of National Intelligence, *Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts*, Press Release (Nov. 1, 2024).

<sup>2</sup> Alex Seitz-Wald and Mike Memoli, *Fake Joe Biden Robocall Tells New Hampshire Voters Not to Vote Tuesday*, NBC News (Jan. 22, 2024).

<sup>3</sup> Senator Mark Warner, *Senate Intel Chairman Pushes Companies to Follow Through on Commitments to Combat Deceptive Use of AI*, Press Release (May 14, 2024).

*Accord*, I strongly encourage you to take the following measures to anticipate, identify, and respond to potential media manipulation efforts targeting the election.

#### Generative AI Model and Media Editing Software Vendors:

- **Attach robust and consensus-based content credentials**, and other relevant provenance or authenticity signals (including metadata and prominent visible watermarks), to any media created using your products.
- To the extent that your product is incorporated in a downstream product offered by a third-party, **adopt license terms that stipulate the adoption of such measures by providers that resell or otherwise repackage your generative AI or media editing tools.**
- **Share detection methodologies or internal classifiers associated with your generative AI or media modification products** through trusted channels with content distributors, other generative AI and media editing software vendors, and trustworthy news organizations.
- Develop and appropriately resource **‘rapid-response’ channels by which verified independent media and civil society organizations can leverage your detection tools to authenticate media** that may have been created with your products.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content**, and consider separate reporting tools for public figures or uniquely vulnerable user groups.
- Maintain **resources to proactively identify impersonation campaigns using your products**, with mechanisms to contact victims promptly.

#### Social Media Platforms and Other Major Content Distributors:

- Establish and enforce **clear Terms of Service regarding generative and manipulated media** and consider policies to **require visual markers of generative or manipulated content for users.**
- Adopt mechanisms to **screen uploaded content for content credentials, watermarks, or other media authenticity signals**, with the goal of ensuring that such content is consistent with your Terms of Service.
- **Develop internal classifiers or enlist third-party detection solutions to detect generative and manipulated media** that lack content credentials, watermarks, or other media authenticity signals – **sharing detection methodologies through trusted channels** with other content distributors.
- Engage independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public.
- **Engage candidates and election officials on effective utilization of content credentialing or other media authentication tools** for their public communications on your distribution platforms.

- Consider **open-sourcing detection tools and methods** to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content.
- **Maintain a publicly-accessible database containing generative or manipulated media that violates your Terms of Service** (particularly with respect to election-related content), enabling civil society and media organizations to track media manipulation campaigns (with appropriate privacy and content-safety features to limit re-victimization).
- Maintain **resources to proactively identify impersonation campaigns conducted on your platforms**, with mechanisms to contact victims promptly.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content violations**, and consider a separate reporting tools for public figures or uniquely-vulnerable user groups.
- Initiate **information-sharing mechanisms between platforms on detecting manipulated content that may be used for malicious ends** (such as election disinformation, voter suppression, non-consensual intimate imagery, online harassment, etc.)

Thank you for your attention to these important matters. I welcome your public commitment to these measures, in addition to concrete commitments you have already made to anticipate, identify, and counteract malicious use of your products ahead of the 2026 U.S. midterm elections.

Sincerely,



---

Mark R. Warner  
United States Senator

March 16, 2026

Mr. Bill Ready  
Chief Executive Officer  
Pinterest  
651 Brannan Street  
San Francisco, CA 94107

Dear Mr. Ready:

Leading technology providers spanning media generation, editing, and distribution have publicly pledged to address the increasing prevalence of maliciously manipulated media. While imperfect and no substitute for comprehensive federal legislation, these voluntary efforts, including the *Coalition for Content Provenance & Authenticity* and the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, complemented by a patchwork of state laws, represent some of the only meaningful interventions to address media manipulation-based threats ahead of the 2026 U.S. midterm elections.

Prior to the 2024 U.S. elections, Russian-attributed actors used media manipulation techniques to denigrate a U.S. Vice-Presidential candidate<sup>1</sup> and a domestic actor utilized voice cloning software for robocalls impersonating President Biden in the New Hampshire primary.<sup>2</sup> While these malicious actions largely failed to meaningfully effect the elections, the capabilities of generative artificial intelligence (AI) products have grown tremendously in the intervening years. Particularly against the backdrop of an abrupt pullback in federal resources, an effective multi-stakeholder approach is needed to ensure that industry, state and local governments, and civil society adequately anticipate – and counteract – media manipulation techniques that cause harm to vulnerable communities, public trust, and democratic institutions.

Policymakers have on a bipartisan basis begun the process of developing measures to ensure that generative AI technologies (and related media modification tools) serve the public interest. But the private sector can – particularly in collaboration with civil society and state and local election officials – dramatically shape the usage and wider impact of these technologies through proactive measures in coming months. As a follow-up to my requests<sup>3</sup> in the wake of the *Munich Tech*

---

<sup>1</sup> Office of the Director of National Intelligence, *Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts*, Press Release (Nov. 1, 2024).

<sup>2</sup> Alex Seitz-Wald and Mike Memoli, *Fake Joe Biden Robocall Tells New Hampshire Voters Not to Vote Tuesday*, NBC News (Jan. 22, 2024).

<sup>3</sup> Senator Mark Warner, *Senate Intel Chairman Pushes Companies to Follow Through on Commitments to Combat Deceptive Use of AI*, Press Release (May 14, 2024).

*Accord*, I strongly encourage you to take the following measures to anticipate, identify, and respond to potential media manipulation efforts targeting the election.

#### Generative AI Model and Media Editing Software Vendors:

- **Attach robust and consensus-based content credentials**, and other relevant provenance or authenticity signals (including metadata and prominent visible watermarks), to any media created using your products.
- To the extent that your product is incorporated in a downstream product offered by a third-party, **adopt license terms that stipulate the adoption of such measures by providers that resell or otherwise repackage your generative AI or media editing tools.**
- **Share detection methodologies or internal classifiers associated with your generative AI or media modification products** through trusted channels with content distributors, other generative AI and media editing software vendors, and trustworthy news organizations.
- Develop and appropriately resource **‘rapid-response’ channels by which verified independent media and civil society organizations can leverage your detection tools to authenticate media** that may have been created with your products.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content**, and consider separate reporting tools for public figures or uniquely vulnerable user groups.
- Maintain **resources to proactively identify impersonation campaigns using your products**, with mechanisms to contact victims promptly.

#### Social Media Platforms and Other Major Content Distributors:

- Establish and enforce **clear Terms of Service regarding generative and manipulated media** and consider policies to **require visual markers of generative or manipulated content for users.**
- Adopt mechanisms to **screen uploaded content for content credentials, watermarks, or other media authenticity signals**, with the goal of ensuring that such content is consistent with your Terms of Service.
- **Develop internal classifiers or enlist third-party detection solutions to detect generative and manipulated media** that lack content credentials, watermarks, or other media authenticity signals – **sharing detection methodologies through trusted channels** with other content distributors.
- Engage independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public.
- **Engage candidates and election officials on effective utilization of content credentialing or other media authentication tools** for their public communications on your distribution platforms.

- Consider **open-sourcing detection tools and methods** to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content.
- **Maintain a publicly-accessible database containing generative or manipulated media that violates your Terms of Service** (particularly with respect to election-related content), enabling civil society and media organizations to track media manipulation campaigns (with appropriate privacy and content-safety features to limit re-victimization).
- Maintain **resources to proactively identify impersonation campaigns conducted on your platforms**, with mechanisms to contact victims promptly.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content violations**, and consider a separate reporting tools for public figures or uniquely-vulnerable user groups.
- Initiate **information-sharing mechanisms between platforms on detecting manipulated content that may be used for malicious ends** (such as election disinformation, voter suppression, non-consensual intimate imagery, online harassment, etc.)

Thank you for your attention to these important matters. I welcome your public commitment to these measures, in addition to concrete commitments you have already made to anticipate, identify, and counteract malicious use of your products ahead of the 2026 U.S. midterm elections.

Sincerely,



---

Mark R. Warner  
United States Senator

March 16, 2026

Mr. Evan Spiegel  
Chief Executive Officer  
Snap Inc.  
3000 31<sup>st</sup> Street  
Santa Monica, CA 90405

Dear Mr. Spiegel:

Leading technology providers spanning media generation, editing, and distribution have publicly pledged to address the increasing prevalence of maliciously manipulated media. While imperfect and no substitute for comprehensive federal legislation, these voluntary efforts, including the *Coalition for Content Provenance & Authenticity* and the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, complemented by a patchwork of state laws, represent some of the only meaningful interventions to address media manipulation-based threats ahead of the 2026 U.S. midterm elections.

Prior to the 2024 U.S. elections, Russian-attributed actors used media manipulation techniques to denigrate a U.S. Vice-Presidential candidate<sup>1</sup> and a domestic actor utilized voice cloning software for robocalls impersonating President Biden in the New Hampshire primary.<sup>2</sup> While these malicious actions largely failed to meaningfully effect the elections, the capabilities of generative artificial intelligence (AI) products have grown tremendously in the intervening years. Particularly against the backdrop of an abrupt pullback in federal resources, an effective multi-stakeholder approach is needed to ensure that industry, state and local governments, and civil society adequately anticipate – and counteract – media manipulation techniques that cause harm to vulnerable communities, public trust, and democratic institutions.

Policymakers have on a bipartisan basis begun the process of developing measures to ensure that generative AI technologies (and related media modification tools) serve the public interest. But the private sector can – particularly in collaboration with civil society and state and local election officials – dramatically shape the usage and wider impact of these technologies through proactive measures in coming months. As a follow-up to my requests<sup>3</sup> in the wake of the *Munich Tech*

---

<sup>1</sup> Office of the Director of National Intelligence, *Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts*, Press Release (Nov. 1, 2024).

<sup>2</sup> Alex Seitz-Wald and Mike Memoli, *Fake Joe Biden Robocall Tells New Hampshire Voters Not to Vote Tuesday*, NBC News (Jan. 22, 2024).

<sup>3</sup> Senator Mark Warner, *Senate Intel Chairman Pushes Companies to Follow Through on Commitments to Combat Deceptive Use of AI*, Press Release (May 14, 2024).

*Accord*, I strongly encourage you to take the following measures to anticipate, identify, and respond to potential media manipulation efforts targeting the election.

#### Generative AI Model and Media Editing Software Vendors:

- **Attach robust and consensus-based content credentials**, and other relevant provenance or authenticity signals (including metadata and prominent visible watermarks), to any media created using your products.
- To the extent that your product is incorporated in a downstream product offered by a third-party, **adopt license terms that stipulate the adoption of such measures by providers that resell or otherwise repackage your generative AI or media editing tools.**
- **Share detection methodologies or internal classifiers associated with your generative AI or media modification products** through trusted channels with content distributors, other generative AI and media editing software vendors, and trustworthy news organizations.
- Develop and appropriately resource **‘rapid-response’ channels by which verified independent media and civil society organizations can leverage your detection tools to authenticate media** that may have been created with your products.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content**, and consider separate reporting tools for public figures or uniquely vulnerable user groups.
- Maintain **resources to proactively identify impersonation campaigns using your products**, with mechanisms to contact victims promptly.

#### Social Media Platforms and Other Major Content Distributors:

- Establish and enforce **clear Terms of Service regarding generative and manipulated media** and consider policies to **require visual markers of generative or manipulated content for users.**
- Adopt mechanisms to **screen uploaded content for content credentials, watermarks, or other media authenticity signals**, with the goal of ensuring that such content is consistent with your Terms of Service.
- **Develop internal classifiers or enlist third-party detection solutions to detect generative and manipulated media** that lack content credentials, watermarks, or other media authenticity signals – **sharing detection methodologies through trusted channels** with other content distributors.
- Engage independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public.
- **Engage candidates and election officials on effective utilization of content credentialing or other media authentication tools** for their public communications on your distribution platforms.

- Consider **open-sourcing detection tools and methods** to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content.
- **Maintain a publicly-accessible database containing generative or manipulated media that violates your Terms of Service** (particularly with respect to election-related content), enabling civil society and media organizations to track media manipulation campaigns (with appropriate privacy and content-safety features to limit re-victimization).
- Maintain **resources to proactively identify impersonation campaigns conducted on your platforms**, with mechanisms to contact victims promptly.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content violations**, and consider a separate reporting tools for public figures or uniquely-vulnerable user groups.
- Initiate **information-sharing mechanisms between platforms on detecting manipulated content that may be used for malicious ends** (such as election disinformation, voter suppression, non-consensual intimate imagery, online harassment, etc.)

Thank you for your attention to these important matters. I welcome your public commitment to these measures, in addition to concrete commitments you have already made to anticipate, identify, and counteract malicious use of your products ahead of the 2026 U.S. midterm elections.

Sincerely,



---

Mark R. Warner  
United States Senator

March 16, 2026

Mr. Victor Riparbelli  
Chief Executive Officer  
Synthesia  
20 Triton Street, Regent's Place, 3<sup>rd</sup> Floor  
London NW1 3BF, United Kingdom

Dear Mr. Riparbelli:

Leading technology providers spanning media generation, editing, and distribution have publicly pledged to address the increasing prevalence of maliciously manipulated media. While imperfect and no substitute for comprehensive federal legislation, these voluntary efforts, including the *Coalition for Content Provenance & Authenticity* and the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, complemented by a patchwork of state laws, represent some of the only meaningful interventions to address media manipulation-based threats ahead of the 2026 U.S. midterm elections.

Prior to the 2024 U.S. elections, Russian-attributed actors used media manipulation techniques to denigrate a U.S. Vice-Presidential candidate<sup>1</sup> and a domestic actor utilized voice cloning software for robocalls impersonating President Biden in the New Hampshire primary.<sup>2</sup> While these malicious actions largely failed to meaningfully effect the elections, the capabilities of generative artificial intelligence (AI) products have grown tremendously in the intervening years. Particularly against the backdrop of an abrupt pullback in federal resources, an effective multi-stakeholder approach is needed to ensure that industry, state and local governments, and civil society adequately anticipate – and counteract – media manipulation techniques that cause harm to vulnerable communities, public trust, and democratic institutions.

Policymakers have on a bipartisan basis begun the process of developing measures to ensure that generative AI technologies (and related media modification tools) serve the public interest. But the private sector can – particularly in collaboration with civil society and state and local election officials – dramatically shape the usage and wider impact of these technologies through proactive measures in coming months. As a follow-up to my requests<sup>3</sup> in the wake of the *Munich Tech*

---

<sup>1</sup> Office of the Director of National Intelligence, *Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts*, Press Release (Nov. 1, 2024).

<sup>2</sup> Alex Seitz-Wald and Mike Memoli, *Fake Joe Biden Robocall Tells New Hampshire Voters Not to Vote Tuesday*, NBC News (Jan. 22, 2024).

<sup>3</sup> Senator Mark Warner, *Senate Intel Chairman Pushes Companies to Follow Through on Commitments to Combat Deceptive Use of AI*, Press Release (May 14, 2024).

*Accord*, I strongly encourage you to take the following measures to anticipate, identify, and respond to potential media manipulation efforts targeting the election.

#### Generative AI Model and Media Editing Software Vendors:

- **Attach robust and consensus-based content credentials**, and other relevant provenance or authenticity signals (including metadata and prominent visible watermarks), to any media created using your products.
- To the extent that your product is incorporated in a downstream product offered by a third-party, **adopt license terms that stipulate the adoption of such measures by providers that resell or otherwise repackage your generative AI or media editing tools.**
- **Share detection methodologies or internal classifiers associated with your generative AI or media modification products** through trusted channels with content distributors, other generative AI and media editing software vendors, and trustworthy news organizations.
- Develop and appropriately resource **‘rapid-response’ channels by which verified independent media and civil society organizations can leverage your detection tools to authenticate media** that may have been created with your products.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content**, and consider separate reporting tools for public figures or uniquely vulnerable user groups.
- Maintain **resources to proactively identify impersonation campaigns using your products**, with mechanisms to contact victims promptly.

#### Social Media Platforms and Other Major Content Distributors:

- Establish and enforce **clear Terms of Service regarding generative and manipulated media** and consider policies to **require visual markers of generative or manipulated content for users.**
- Adopt mechanisms to **screen uploaded content for content credentials, watermarks, or other media authenticity signals**, with the goal of ensuring that such content is consistent with your Terms of Service.
- **Develop internal classifiers or enlist third-party detection solutions to detect generative and manipulated media** that lack content credentials, watermarks, or other media authenticity signals – **sharing detection methodologies through trusted channels** with other content distributors.
- Engage independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public.
- **Engage candidates and election officials on effective utilization of content credentialing or other media authentication tools** for their public communications on your distribution platforms.

- Consider **open-sourcing detection tools and methods** to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content.
- **Maintain a publicly-accessible database containing generative or manipulated media that violates your Terms of Service** (particularly with respect to election-related content), enabling civil society and media organizations to track media manipulation campaigns (with appropriate privacy and content-safety features to limit re-victimization).
- Maintain **resources to proactively identify impersonation campaigns conducted on your platforms**, with mechanisms to contact victims promptly.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content violations**, and consider a separate reporting tools for public figures or uniquely-vulnerable user groups.
- Initiate **information-sharing mechanisms between platforms on detecting manipulated content that may be used for malicious ends** (such as election disinformation, voter suppression, non-consensual intimate imagery, online harassment, etc.)

Thank you for your attention to these important matters. I welcome your public commitment to these measures, in addition to concrete commitments you have already made to anticipate, identify, and counteract malicious use of your products ahead of the 2026 U.S. midterm elections.

Sincerely,



---

Mark R. Warner  
United States Senator

March 16, 2026

Mr. Adam Presser  
Chief Executive Officer  
TikTok USDS JV  
5800 Bristol Parkway  
Culver City, CA 90230

Dear Mr. Presser:

Leading technology providers spanning media generation, editing, and distribution have publicly pledged to address the increasing prevalence of maliciously manipulated media. While imperfect and no substitute for comprehensive federal legislation, these voluntary efforts, including the *Coalition for Content Provenance & Authenticity* and the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, complemented by a patchwork of state laws, represent some of the only meaningful interventions to address media manipulation-based threats ahead of the 2026 U.S. midterm elections.

Prior to the 2024 U.S. elections, Russian-attributed actors used media manipulation techniques to denigrate a U.S. Vice-Presidential candidate<sup>1</sup> and a domestic actor utilized voice cloning software for robocalls impersonating President Biden in the New Hampshire primary.<sup>2</sup> While these malicious actions largely failed to meaningfully effect the elections, the capabilities of generative artificial intelligence (AI) products have grown tremendously in the intervening years. Particularly against the backdrop of an abrupt pullback in federal resources, an effective multi-stakeholder approach is needed to ensure that industry, state and local governments, and civil society adequately anticipate – and counteract – media manipulation techniques that cause harm to vulnerable communities, public trust, and democratic institutions.

Policymakers have on a bipartisan basis begun the process of developing measures to ensure that generative AI technologies (and related media modification tools) serve the public interest. But the private sector can – particularly in collaboration with civil society and state and local election officials – dramatically shape the usage and wider impact of these technologies through proactive measures in coming months. As a follow-up to my requests<sup>3</sup> in the wake of the *Munich Tech*

---

<sup>1</sup> Office of the Director of National Intelligence, *Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts*, Press Release (Nov. 1, 2024).

<sup>2</sup> Alex Seitz-Wald and Mike Memoli, *Fake Joe Biden Robocall Tells New Hampshire Voters Not to Vote Tuesday*, NBC News (Jan. 22, 2024).

<sup>3</sup> Senator Mark Warner, *Senate Intel Chairman Pushes Companies to Follow Through on Commitments to Combat Deceptive Use of AI*, Press Release (May 14, 2024).

*Accord*, I strongly encourage you to take the following measures to anticipate, identify, and respond to potential media manipulation efforts targeting the election.

#### Generative AI Model and Media Editing Software Vendors:

- **Attach robust and consensus-based content credentials**, and other relevant provenance or authenticity signals (including metadata and prominent visible watermarks), to any media created using your products.
- To the extent that your product is incorporated in a downstream product offered by a third-party, **adopt license terms that stipulate the adoption of such measures by providers that resell or otherwise repackage your generative AI or media editing tools.**
- **Share detection methodologies or internal classifiers associated with your generative AI or media modification products** through trusted channels with content distributors, other generative AI and media editing software vendors, and trustworthy news organizations.
- Develop and appropriately resource **‘rapid-response’ channels by which verified independent media and civil society organizations can leverage your detection tools to authenticate media** that may have been created with your products.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content**, and consider separate reporting tools for public figures or uniquely vulnerable user groups.
- Maintain **resources to proactively identify impersonation campaigns using your products**, with mechanisms to contact victims promptly.

#### Social Media Platforms and Other Major Content Distributors:

- Establish and enforce **clear Terms of Service regarding generative and manipulated media** and consider policies to **require visual markers of generative or manipulated content for users.**
- Adopt mechanisms to **screen uploaded content for content credentials, watermarks, or other media authenticity signals**, with the goal of ensuring that such content is consistent with your Terms of Service.
- **Develop internal classifiers or enlist third-party detection solutions to detect generative and manipulated media** that lack content credentials, watermarks, or other media authenticity signals – **sharing detection methodologies through trusted channels** with other content distributors.
- Engage independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public.
- **Engage candidates and election officials on effective utilization of content credentialing or other media authentication tools** for their public communications on your distribution platforms.

- Consider **open-sourcing detection tools and methods** to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content.
- **Maintain a publicly-accessible database containing generative or manipulated media that violates your Terms of Service** (particularly with respect to election-related content), enabling civil society and media organizations to track media manipulation campaigns (with appropriate privacy and content-safety features to limit re-victimization).
- Maintain **resources to proactively identify impersonation campaigns conducted on your platforms**, with mechanisms to contact victims promptly.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content violations**, and consider a separate reporting tools for public figures or uniquely-vulnerable user groups.
- Initiate **information-sharing mechanisms between platforms on detecting manipulated content that may be used for malicious ends** (such as election disinformation, voter suppression, non-consensual intimate imagery, online harassment, etc.)

Thank you for your attention to these important matters. I welcome your public commitment to these measures, in addition to concrete commitments you have already made to anticipate, identify, and counteract malicious use of your products ahead of the 2026 U.S. midterm elections.

Sincerely,



---

Mark R. Warner  
United States Senator

# United States Senate

WASHINGTON, DC 20510-4606

March 16, 2026

Mr. Elon Musk  
Chief Executive Officer  
xAI  
1450 Page Mill Road  
Palo Alto, CA 94304

Dear Mr. Musk:

Leading technology providers spanning media generation, editing, and distribution have publicly pledged to address the increasing prevalence of maliciously manipulated media. While imperfect and no substitute for comprehensive federal legislation, these voluntary efforts, including the *Coalition for Content Provenance & Authenticity* and the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, complemented by a patchwork of state laws, represent some of the only meaningful interventions to address media manipulation-based threats ahead of the 2026 U.S. midterm elections.

Prior to the 2024 U.S. elections, Russian-attributed actors used media manipulation techniques to denigrate a U.S. Vice-Presidential candidate<sup>1</sup> and a domestic actor utilized voice cloning software for robocalls impersonating President Biden in the New Hampshire primary.<sup>2</sup> While these malicious actions largely failed to meaningfully effect the elections, the capabilities of generative artificial intelligence (AI) products have grown tremendously in the intervening years. Particularly against the backdrop of an abrupt pullback in federal resources, an effective multi-stakeholder approach is needed to ensure that industry, state and local governments, and civil society adequately anticipate – and counteract – media manipulation techniques that cause harm to vulnerable communities, public trust, and democratic institutions.

Policymakers have on a bipartisan basis begun the process of developing measures to ensure that generative AI technologies (and related media modification tools) serve the public interest. But the private sector can – particularly in collaboration with civil society and state and local election officials – dramatically shape the usage and wider impact of these technologies through proactive measures in coming months. As a follow-up to my requests<sup>3</sup> in the wake of the *Munich Tech*

---

<sup>1</sup> Office of the Director of National Intelligence, *Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts*, Press Release (Nov. 1, 2024).

<sup>2</sup> Alex Seitz-Wald and Mike Memoli, *Fake Joe Biden Robocall Tells New Hampshire Voters Not to Vote Tuesday*, NBC News (Jan. 22, 2024).

<sup>3</sup> Senator Mark Warner, *Senate Intel Chairman Pushes Companies to Follow Through on Commitments to Combat Deceptive Use of AI*, Press Release (May 14, 2024).

*Accord*, I strongly encourage you to take the following measures to anticipate, identify, and respond to potential media manipulation efforts targeting the election.

#### Generative AI Model and Media Editing Software Vendors:

- **Attach robust and consensus-based content credentials**, and other relevant provenance or authenticity signals (including metadata and prominent visible watermarks), to any media created using your products.
- To the extent that your product is incorporated in a downstream product offered by a third-party, **adopt license terms that stipulate the adoption of such measures by providers that resell or otherwise repackage your generative AI or media editing tools.**
- **Share detection methodologies or internal classifiers associated with your generative AI or media modification products** through trusted channels with content distributors, other generative AI and media editing software vendors, and trustworthy news organizations.
- Develop and appropriately resource **‘rapid-response’ channels by which verified independent media and civil society organizations can leverage your detection tools to authenticate media** that may have been created with your products.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content**, and consider separate reporting tools for public figures or uniquely vulnerable user groups.
- Maintain **resources to proactively identify impersonation campaigns using your products**, with mechanisms to contact victims promptly.

#### Social Media Platforms and Other Major Content Distributors:

- Establish and enforce **clear Terms of Service regarding generative and manipulated media** and consider policies to **require visual markers of generative or manipulated content for users.**
- Adopt mechanisms to **screen uploaded content for content credentials, watermarks, or other media authenticity signals**, with the goal of ensuring that such content is consistent with your Terms of Service.
- **Develop internal classifiers or enlist third-party detection solutions to detect generative and manipulated media** that lack content credentials, watermarks, or other media authenticity signals – **sharing detection methodologies through trusted channels** with other content distributors.
- Engage independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public.
- **Engage candidates and election officials on effective utilization of content credentialing or other media authentication tools** for their public communications on your distribution platforms.

- Consider **open-sourcing detection tools and methods** to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content.
- **Maintain a publicly-accessible database containing generative or manipulated media that violates your Terms of Service** (particularly with respect to election-related content), enabling civil society and media organizations to track media manipulation campaigns (with appropriate privacy and content-safety features to limit re-victimization).
- Maintain **resources to proactively identify impersonation campaigns conducted on your platforms**, with mechanisms to contact victims promptly.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content violations**, and consider a separate reporting tools for public figures or uniquely-vulnerable user groups.
- Initiate **information-sharing mechanisms between platforms on detecting manipulated content that may be used for malicious ends** (such as election disinformation, voter suppression, non-consensual intimate imagery, online harassment, etc.)

Thank you for your attention to these important matters. I welcome your public commitment to these measures, in addition to concrete commitments you have already made to anticipate, identify, and counteract malicious use of your products ahead of the 2026 U.S. midterm elections.

Sincerely,



---

Mark R. Warner  
United States Senator

# United States Senate

WASHINGTON, DC 20510-4606

March 16, 2026

Mr. Steve Huffman  
Chief Executive Officer  
Reddit, Inc.  
303 2nd Street  
South Tower, 5th Floor  
San Francisco, CA 94107

Dear Mr. Musk:

Leading technology providers spanning media generation, editing, and distribution have publicly pledged to address the increasing prevalence of maliciously manipulated media. While imperfect and no substitute for comprehensive federal legislation, these voluntary efforts, including the *Coalition for Content Provenance & Authenticity* and the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, complemented by a patchwork of state laws, represent some of the only meaningful interventions to address media manipulation-based threats ahead of the 2026 U.S. midterm elections.

Prior to the 2024 U.S. elections, Russian-attributed actors used media manipulation techniques to denigrate a U.S. Vice-Presidential candidate<sup>1</sup> and a domestic actor utilized voice cloning software for robocalls impersonating President Biden in the New Hampshire primary.<sup>2</sup> While these malicious actions largely failed to meaningfully effect the elections, the capabilities of generative artificial intelligence (AI) products have grown tremendously in the intervening years. Particularly against the backdrop of an abrupt pullback in federal resources, an effective multi-stakeholder approach is needed to ensure that industry, state and local governments, and civil society adequately anticipate – and counteract – media manipulation techniques that cause harm to vulnerable communities, public trust, and democratic institutions.

Policymakers have on a bipartisan basis begun the process of developing measures to ensure that generative AI technologies (and related media modification tools) serve the public interest. But the private sector can – particularly in collaboration with civil society and state and local election officials – dramatically shape the usage and wider impact of these technologies through proactive measures in coming months. As a follow-up to my requests<sup>3</sup> in the wake of the *Munich Tech*

---

<sup>1</sup> Office of the Director of National Intelligence, *Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts*, Press Release (Nov. 1, 2024).

<sup>2</sup> Alex Seitz-Wald and Mike Memoli, *Fake Joe Biden Robocall Tells New Hampshire Voters Not to Vote Tuesday*, NBC News (Jan. 22, 2024).

<sup>3</sup> Senator Mark Warner, *Senate Intel Chairman Pushes Companies to Follow Through on Commitments to Combat Deceptive Use of AI*, Press Release (May 14, 2024).

*Accord*, I strongly encourage you to take the following measures to anticipate, identify, and respond to potential media manipulation efforts targeting the election.

#### Generative AI Model and Media Editing Software Vendors:

- **Attach robust and consensus-based content credentials**, and other relevant provenance or authenticity signals (including metadata and prominent visible watermarks), to any media created using your products.
- To the extent that your product is incorporated in a downstream product offered by a third-party, **adopt license terms that stipulate the adoption of such measures by providers that resell or otherwise repackage your generative AI or media editing tools.**
- **Share detection methodologies or internal classifiers associated with your generative AI or media modification products** through trusted channels with content distributors, other generative AI and media editing software vendors, and trustworthy news organizations.
- Develop and appropriately resource **‘rapid-response’ channels by which verified independent media and civil society organizations can leverage your detection tools to authenticate media** that may have been created with your products.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content**, and consider separate reporting tools for public figures or uniquely vulnerable user groups.
- Maintain **resources to proactively identify impersonation campaigns using your products**, with mechanisms to contact victims promptly.

#### Social Media Platforms and Other Major Content Distributors:

- Establish and enforce **clear Terms of Service regarding generative and manipulated media** and consider policies to **require visual markers of generative or manipulated content for users.**
- Adopt mechanisms to **screen uploaded content for content credentials, watermarks, or other media authenticity signals**, with the goal of ensuring that such content is consistent with your Terms of Service.
- **Develop internal classifiers or enlist third-party detection solutions to detect generative and manipulated media** that lack content credentials, watermarks, or other media authenticity signals – **sharing detection methodologies through trusted channels** with other content distributors.
- Engage independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public.
- **Engage candidates and election officials on effective utilization of content credentialing or other media authentication tools** for their public communications on your distribution platforms.

- Consider **open-sourcing detection tools and methods** to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content.
- **Maintain a publicly-accessible database containing generative or manipulated media that violates your Terms of Service** (particularly with respect to election-related content), enabling civil society and media organizations to track media manipulation campaigns (with appropriate privacy and content-safety features to limit re-victimization).
- Maintain **resources to proactively identify impersonation campaigns conducted on your platforms**, with mechanisms to contact victims promptly.
- Develop **clear policies and mechanisms by which victims of impersonation campaigns may report content violations**, and consider a separate reporting tools for public figures or uniquely-vulnerable user groups.
- Initiate **information-sharing mechanisms between platforms on detecting manipulated content that may be used for malicious ends** (such as election disinformation, voter suppression, non-consensual intimate imagery, online harassment, etc.)

Thank you for your attention to these important matters. I welcome your public commitment to these measures, in addition to concrete commitments you have already made to anticipate, identify, and counteract malicious use of your products ahead of the 2026 U.S. midterm elections.

Sincerely,



---

Mark R. Warner  
United States Senator