MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510-4606

May 14, 2024

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

Dear Mr. Narayen,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510-4606

May 14, 2024

Mr. Sundar Pichai
Chief Executive Officer
Alphabet Inc.
1600 Amphitheater Parkway
Mountain View, CA 94043

Dear Mr. Pichai,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510-4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

May 14, 2024

Mr. Andy Jassy
Chief Executive Officer
Amazon.com Inc.
410 Terry Avenue North
Seattle, Washington 98109

Dear Mr. Jassy,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that

can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510–4606

May 14, 2024

Dario Amodei, PhD
Chief Executive Officer
Anthropic PBC
548 Market St.
San Francisco, CA 94104

Dear Dr. Amodei,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that

can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND
URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510-4606

May 14, 2024

Mr. Rene Haas
Chief Executive
ARM Holdings PLC
120 Rose Orchard Way
San Jose, CA 95134

Dear Mr. Haas,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that

can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

May 14, 2024

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

Dear Mr. Staniszewski,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that

can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510–4606

May 14, 2024

Mr. Vincent Pilette
Chief Executive Officer
Gen Digital Inc.
60 East Rio Salado, Parkway Suite 1000
Temple, AZ 85281

Dear Mr. Pilette,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that

can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510-4606

May 14, 2024

Thomas Dohmke, PhD
Chief Executive Officer
GitHub Inc.
88 Colin P Kelly Jr St.
San Francisco, CA 94107

Dear Dr. Dohmke,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that

can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510–4606

May 14, 2024

Arvind Krishna, PhD
Chief Executive Officer
International Business Machines Corp
1 New orchard Road
Armonk, NY 10504

Dear Dr. Krishna,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that

can materially enhance the information ecosystem surrounding this year’s election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company’s willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company’s engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510-4606

May 14, 2024

Sean White, PhD
Chief Executive Officer
Inflection AI Inc.
650 Page Mill Road
Palo Alto, CA 94304

Dear Dr. White,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

May 14, 2024

Mr. Sasan Goodarzi
Chief Executive Officer
Intuit Inc.
2700 Coast Avenue
Mountain View, CA 94043

Dear Mr. Goodarzi,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE

BANKING, HOUSING, AND
URBAN AFFAIRS

BUDGET

INTELLIGENCE

RULES AND ADMINISTRATION

United States Senate

WASHINGTON, DC 20510–4606

May 14, 2024

Kyunghoon Bae, PhD
Chief of LG AI Research
LG AI Research
24 Frank Lloyd Wright Dr. Suite A 3400
Ann Arbor, MI 48105

Dear Dr. Bae,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510–4606

May 14, 2024

Mr. Ryan Roslansky
Chief Executive Officer
LinkedIn Corp.
1000 West Maude Avenue
Sunnyvale, CA 94085

Dear Mr. Roslansky,

Earlier this year, I joined to amplify and applaud your company’s commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India’s elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND
URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510–4606

May 14, 2024

Mr. Greg Johnson
Chief Executive Officer
McAfee Corp.
6220 America Center Drive
San Jose, CA 95002

Dear Mr. Johnson,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510–4606

May 14, 2024

Mr. Mark Zuckerberg
Meta Platforms Inc.
1 Meta Way
Menlo Park, CA 94025

Dear Mr. Zuckerberg,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

May 14, 2024

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

Dear Mr. Nadella,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510-4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

May 14, 2024

Mr. George Kurian
Chief Executive Officer
NetApp Inc.
3060 Olsen Drive
San Jose, CA 95128

Dear Mr. Kurian,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

May 14, 2024

Mr. Myungsu Chae
Chief Executive Officer
Nota AI
440 N. Wolfe Road
Sunnyvale, CA 94085

Dear Mr. Chae,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

May 14, 2024

Mr. Sam Altman
Chief Executive Officer
OpenAI Inc.
3180 18th Street, Suite 100
San Francisco, CA 94110

Dear Mr. Altman,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510-4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

May 14, 2024

Mr. Evan Spiegel
Chief Executive Officer
Snap Inc.
3000 31st Street
Monica, CA 90405

Dear Mr. Spiegel,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

May 14, 2024

Ms. Shan Shan Wong and Mr. Christian Laforte
Interim Co-Chief Executive Officers
Stability AI Ltd.
88 Notting Hill Gate
London, W11 3HT

Dear Ms. Wong and Mr. Laforte,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate

WASHINGTON, DC 20510–4606

May 14, 2024

Mr. Shou Zi Chew
Chief Executive Officer
TikTok Ltd.
5800 Bristol Pkwy
Culver City, CA 90230

Dear Mr. Chew,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?

2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?

3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?

4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?

5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?

6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?

7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510–4606

May 14, 2024

Ms. Eva Chen
Chief Executive Officer
Trend Micro Inc.
225 E. John Carpenter Freeway, Suite 1500
Irving, TX 75062

Dear Ms. Chen,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510–4606

May 14, 2024

Dr. Oren Etzioni
Founder
TrueMedia.org

Dear Dr. Etzioni,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510-4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

May 14, 2024

Mr. Jeffrey McGregor
Chief Executive Officer
Truepic Inc.
369 Mesa Way
San Diego, CA 92037

Dear Mr. McGregor,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that

can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510-4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

May 14, 2024

Ms. Linda Yaccarino
Chief Executive Officer
X Corp.
1355 Market Street
San Francisco, CA 94103

Dear Ms. Yaccarino,

Earlier this year, I joined to amplify and applaud your company's commitment to advance election integrity worldwide through the *Tech Accord to Combat Deceptive Use of AI in 2024 Elections.* As generative artificial intelligence (AI) products proliferate for both commercial and general users, a multi-stakeholder approach is needed to ensure that industry, governments, and civil society adequately anticipate – and counteract – misuse of these products in ways that cause harm to vulnerable communities, public trust, and democratic institutions. The release of a range of powerful new AI tools – many enabled or directly offered by your company coincides with an unprecedented number of elections worldwide. As memorialized during the Munich Summit, elections have occurred – or will occur – in over 40 countries worldwide, with more than four billion global citizens exercising their franchise. Since the signing of the Tech Accord on February 16th, the first round of India's elections have already concluded. European Parliament elections will take place in early June and– as primary contests are already well underway – the U.S. general election will take place on November 5th.

While policymakers worldwide have begun the process of developing measures to ensure that generative AI technologies (and related media manipulation tools) serve the public interest, the private sector can – particularly in collaboration with civil society – dramatically shape the usage and wider impact of these technologies through proactive measures. Against the backdrop of worldwide proliferation of malign influence activity globally – with an ever-growing range of malign actors embracing social media and wider digital communications technologies to undermine trust in public institutions, markets, democratic systems, and the free press – generative AI (and related media-manipulation) tools can impact the volume, velocity, and believability of deceptive election information.

While high-level, the commitments your company announced in conjunction with the Tech Accord offer a clear roadmap for a variety of new initiatives, investments, and interventions that can materially enhance the information ecosystem surrounding this year's election contests. To that end, I am interested in learning more about the specific measures your company is taking to implement the Tech Accord. While the public pledge demonstrated your company's willingness to constructively engage on this front, ultimately the impact of the Tech Accord will be measured in the efficacy – and durability – of the initiatives and protection measures you adopt. Indeed, many of these measures will be vital in addressing adjacent misuses of generative AI products, such as the creation of non-consensual intimate imagery, child sexual abuse material, or content generated for online harassment and bullying campaigns. I request that you provide answers to the following questions no later than May 24, 2024.

1. What steps is your company taking to attach content credentials, and other relevant provenance signals, to any media created using your products? To the extent that your product is incorporated in a downstream product offered by a third-party, do license terms or other terms of use stipulate the adoption of such measures? To the extent you distribute content generated by others, does your company attach labels when you assess – based on either internal classifiers or credible third-party reports – to be machine-generated or machine-manipulated?
2. What specific public engagement and education initiatives have you initiated in countries holding elections this year? What has the engagement rate been thus far and what proactive steps are you undertaking to raise user awareness on the availability of new tools hosted by your platform?
3. What specific resources has your company provided for independent media and civil society organizations to assist in their efforts to verify media, generate authenticated media, and educate the public?
4. What has been your company's engagement with candidates and election officials with respect to anticipating misuse of your products, as well as the effective utilization of content credentialing or other media authentication tools for their public communications?
5. Has your company worked to develop widely-available detection tools and methods to identify, catalogue, and/or continuously track the distribution of machine-generated or machine-manipulated content?
6. (To the extent your company offers social media or other content distribution platforms) What kinds of internal classifiers and detection measures are you developing to identify machine-generated or machine-manipulated content? To what extent to these measures depend on collaboration or contributions from generative AI vendors?
7. (To the extent your company offers social media or other content distribution platforms) What mechanisms has your platform implemented to enable victims of impersonation campaigns to report content that may violate your Terms of Service? Do you maintain separate reporting tools for public figures?

8. (To the extent your company offers generative AI products) What mechanisms has your platform implemented to enable victims of impersonation campaigns that may have relied on your models to report activity that may violate your Terms of Service?
9. (To the extent your company offers social media or other content distribution platforms) What is the current status of information sharing between platforms on detecting machine-generated or machine-manipulated content that may be used for malicious ends (such as election disinformation, non-consensual intimate imagery, online harassment, etc.)? Will your company commit to participation in a common database of violative content?

Thank you for your attention to these important matters and I look forward to your response.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator