MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510–4606

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

August 16, 2023

Dr. Dario Amodei
Chief Executive Officer
Anthropic
548 Market St. PMB 90375
San Francisco, CA 94104

Dear Dr. Amodei,

I write to applaud your company's willingness to join the recent Biden Administration initiative to secure voluntary commitments from leading artificial intelligence (AI) vendors related to promoting greater security, safety, and trust through improved development practices. These commitments – in some cases only applicable to your company's largest models – can materially reduce a range of security and safety risks identified by researchers and developers in recent years. In April, I wrote to your company urging the prioritization of security and safety in your company's development, product release, and post-deployment practices relating to AI. Among other things, I asked your company to fully map dependencies and downstream implications of compromise of your systems; focus greater financial, technical and personnel resources on internal security; and improve your company's transparency practices through greater documentation of system capabilities, system limitations, and training data. In many respects, the voluntary commitments by your company last month memorialize many of the commitments sought in my April letter.

These commitments have the potential to shape developer norms and best practices associated with leading-edge AI models. At the same time, less capable models not covered by the commitments are susceptible to misuse, security compromise, and proliferation risks. Moreover, a growing roster of highly-capable open source models have been released to the public – and would benefit from similar pre-deployment commitments contained in a number of the July 21st commitments. As the current commitments stand, leading vendors such as Anthropic do not appear inclined to extend these vital development commitments to the wider range of AI products that your company has released that fall below this threshold or have been released as open source models.

To be sure, responsibility ultimately lies with Congress to develop laws that advance consumer and patient safety, address national security and cyber-crime risks, and promote secure development practices in this burgeoning and highly consequential industry – and in the downstream industries integrating these products. In the interim, the important commitments your company has agreed to can be bolstered in a number of valuable ways.

First, I strongly encourage your company to voluntarily extend all of the July 21st commitments to your company's less capable models that, in part through their wider adoption, can produce the most frequent examples of misuse and compromise.

Second, it is vital to build on these developer- and researcher-facing commitments with a suite of lightweight consumer-facing commitments to prevent the most serious forms of abuse. Most prominent among these should be commitments from your company to adopt development practices, licensing terms, and post-deployment monitoring practices that prevent non-consensual intimate image generation (including child sexual abuse material), social-scoring, real-time facial recognition (in contexts not governed by existing legal protections or due process safeguards), and proliferation activity in the context of malicious cyber activity or the production of biological or chemical agents.

Thank you for your company's engagement in this area. While representing an important improvement upon the status quo, the voluntary commitments announced in July can be bolstered in key ways through additional commitments.

Sincerely,

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

August 16, 2023

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

Dear Mr. Pichai,

I write to applaud your company's willingness to join the recent Biden Administration initiative to secure voluntary commitments from leading artificial intelligence (AI) vendors related to promoting greater security, safety, and trust through improved development practices. These commitments – in some cases only applicable to your company's largest models – can materially reduce a range of security and safety risks identified by researchers and developers in recent years. In April, I wrote to your company urging the prioritization of security and safety in your company's development, product release, and post-deployment practices relating to AI. Among other things, I asked your company to fully map dependencies and downstream implications of compromise of your systems; focus greater financial, technical and personnel resources on internal security; and improve your company's transparency practices through greater documentation of system capabilities, system limitations, and training data. In many respects, the voluntary commitments by your company last month memorialize many of the commitments sought in my April letter.

These commitments have the potential to shape developer norms and best practices associated with leading-edge AI models. At the same time, less capable models not covered by the commitments are susceptible to misuse, security compromise, and proliferation risks. Moreover, a growing roster of highly-capable open source models have been released to the public – and would benefit from similar pre-deployment commitments contained in a number of the July 21st commitments. As the current commitments stand, leading vendors such as Google do not appear inclined to extend these vital development commitments to the wider range of AI products that your company has released that fall below this threshold or have been released as open source models.

To be sure, responsibility ultimately lies with Congress to develop laws that advance consumer and patient safety, address national security and cyber-crime risks, and promote secure development practices in this burgeoning and highly consequential industry – and in the downstream industries integrating these products. In the interim, the important commitments your company has agreed to can be bolstered in a number of valuable ways.

First, I strongly encourage your company to voluntarily extend all of the July 21st commitments to your company's less capable models that, in part through their wider adoption, can produce the most frequent examples of misuse and compromise.

Second, it is vital to build on these developer- and researcher-facing commitments with a suite of lightweight consumer-facing commitments to prevent the most serious forms of abuse. Most prominent among these should be commitments from your company to adopt development practices, licensing terms, and post-deployment monitoring practices that prevent non-consensual intimate image generation (including child sexual abuse material), social-scoring, real-time facial recognition (in contexts not governed by existing legal protections or due process safeguards), and proliferation activity in the context of malicious cyber activity or the production of biological or chemical agents.

Thank you for your company's engagement in this area. While representing an important improvement upon the status quo, the voluntary commitments announced in July can be bolstered in key ways through additional commitments.

Sincerely,

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

August 16, 2023

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

Dear Mr. Zuckerberg,

I write to applaud your company's willingness to join the recent Biden Administration initiative to secure voluntary commitments from leading artificial intelligence (AI) vendors related to promoting greater security, safety, and trust through improved development practices. These commitments – in some cases only applicable to your company's largest models – can materially reduce a range of security and safety risks identified by researchers and developers in recent years. In April, I wrote to your company urging the prioritization of security and safety in your company's development, product release, and post-deployment practices relating to AI. Among other things, I asked your company to fully map dependencies and downstream implications of compromise of your systems; focus greater financial, technical and personnel resources on internal security; and improve your company's transparency practices through greater documentation of system capabilities, system limitations, and training data. In many respects, the voluntary commitments by your company last month memorialize many of the commitments sought in my April letter.

These commitments have the potential to shape developer norms and best practices associated with leading-edge AI models. At the same time, less capable models not covered by the commitments are susceptible to misuse, security compromise, and proliferation risks. Moreover, a growing roster of highly-capable open source models have been released to the public – and would benefit from similar pre-deployment commitments contained in a number of the July 21st commitments. As the current commitments stand, leading vendors such as Meta do not appear inclined to extend these vital development commitments to the wider range of AI products that your company has released that fall below this threshold or have been released as open source models.

To be sure, responsibility ultimately lies with Congress to develop laws that advance consumer and patient safety, address national security and cyber-crime risks, and promote secure development practices in this burgeoning and highly consequential industry – and in the downstream industries integrating these products. In the interim, the important commitments your company has agreed to can be bolstered in a number of valuable ways.

First, I strongly encourage your company to voluntarily extend all of the July 21st commitments to your company's less capable models that, in part through their wider adoption, can produce the most frequent examples of misuse and compromise.

Second, it is vital to build on these developer- and researcher-facing commitments with a suite of lightweight consumer-facing commitments to prevent the most serious forms of abuse. Most prominent among these should be commitments from your company to adopt development practices, licensing terms, and post-deployment monitoring practices that prevent non-consensual intimate image generation (including child sexual abuse material), social-scoring, real-time facial recognition (in contexts not governed by existing legal protections or due process safeguards), and proliferation activity in the context of malicious cyber activity or the production of biological or chemical agents.

Thank you for your company's engagement in this area. While representing an important improvement upon the status quo, the voluntary commitments announced in July can be bolstered in key ways through additional commitments.

Sincerely,

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

August 16, 2023

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

Dear Mr. Nadella,

I write to applaud your company's willingness to join the recent Biden Administration initiative to secure voluntary commitments from leading artificial intelligence (AI) vendors related to promoting greater security, safety, and trust through improved development practices. These commitments – in some cases only applicable to your company's largest models – can materially reduce a range of security and safety risks identified by researchers and developers in recent years. In April, I wrote to your company urging the prioritization of security and safety in your company's development, product release, and post-deployment practices relating to AI. Among other things, I asked your company to fully map dependencies and downstream implications of compromise of your systems; focus greater financial, technical and personnel resources on internal security; and improve your company's transparency practices through greater documentation of system capabilities, system limitations, and training data. In many respects, the voluntary commitments by your company last month memorialize many of the commitments sought in my April letter.

These commitments have the potential to shape developer norms and best practices associated with leading-edge AI models. At the same time, less capable models not covered by the commitments are susceptible to misuse, security compromise, and proliferation risks. Moreover, a growing roster of highly-capable open source models have been released to the public – and would benefit from similar pre-deployment commitments contained in a number of the July 21st commitments. As the current commitments stand, leading vendors such as Microsoft do not appear inclined to extend these vital development commitments to the wider range of AI products that your company has released that fall below this threshold or have been released as open source models.

To be sure, responsibility ultimately lies with Congress to develop laws that advance consumer and patient safety, address national security and cyber-crime risks, and promote secure development practices in this burgeoning and highly consequential industry – and in the downstream industries integrating these products. In the interim, the important commitments your company has agreed to can be bolstered in a number of valuable ways.

First, I strongly encourage your company to voluntarily extend all of the July 21st commitments to your company's less capable models that, in part through their wider adoption, can produce the most frequent examples of misuse and compromise.

Second, it is vital to build on these developer- and researcher-facing commitments with a suite of lightweight consumer-facing commitments to prevent the most serious forms of abuse. Most prominent among these should be commitments from your company to adopt development practices, licensing terms, and post-deployment monitoring practices that prevent non-consensual intimate image generation (including child sexual abuse material), social-scoring, real-time facial recognition (in contexts not governed by existing legal protections or due process safeguards), and proliferation activity in the context of malicious cyber activity or the production of biological or chemical agents.

Thank you for your company's engagement in this area. While representing an important improvement upon the status quo, the voluntary commitments announced in July can be bolstered in key ways through additional commitments.

Sincerely,

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

August 16, 2023

Mr. Sam Altman
Chief Executive Officer
OpenAI
1960 Bryant Street
San Francisco, CA 94110

Dear Mr. Altman,

I write to applaud your company's willingness to join the recent Biden Administration initiative to secure voluntary commitments from leading artificial intelligence (AI) vendors related to promoting greater security, safety, and trust through improved development practices. These commitments – in some cases only applicable to your company's largest models – can materially reduce a range of security and safety risks identified by researchers and developers in recent years. In April, I wrote to your company urging the prioritization of security and safety in your company's development, product release, and post-deployment practices relating to AI. Among other things, I asked your company to fully map dependencies and downstream implications of compromise of your systems; focus greater financial, technical and personnel resources on internal security; and improve your company's transparency practices through greater documentation of system capabilities, system limitations, and training data. In many respects, the voluntary commitments by your company last month memorialize many of the commitments sought in my April letter.

These commitments have the potential to shape developer norms and best practices associated with leading-edge AI models. At the same time, less capable models not covered by the commitments are susceptible to misuse, security compromise, and proliferation risks. Moreover, a growing roster of highly-capable open source models have been released to the public – and would benefit from similar pre-deployment commitments contained in a number of the July 21st commitments. As the current commitments stand, leading vendors such as OpenAI do not appear inclined to extend these vital development commitments to the wider range of AI products that your company has released that fall below this threshold or have been released as open source models.

To be sure, responsibility ultimately lies with Congress to develop laws that advance consumer and patient safety, address national security and cyber-crime risks, and promote secure development practices in this burgeoning and highly consequential industry – and in the downstream industries integrating these products. In the interim, the important commitments your company has agreed to can be bolstered in a number of valuable ways.

First, I strongly encourage your company to voluntarily extend all of the July 21st commitments to your company's less capable models that, in part through their wider adoption, can produce the most frequent examples of misuse and compromise.

Second, it is vital to build on these developer- and researcher-facing commitments with a suite of lightweight consumer-facing commitments to prevent the most serious forms of abuse. Most prominent among these should be commitments from your company to adopt development practices, licensing terms, and post-deployment monitoring practices that prevent non-consensual intimate image generation (including child sexual abuse material), social-scoring, real-time facial recognition (in contexts not governed by existing legal protections or due process safeguards), and proliferation activity in the context of malicious cyber activity or the production of biological or chemical agents.

Thank you for your company's engagement in this area. While representing an important improvement upon the status quo, the voluntary commitments announced in July can be bolstered in key ways through additional commitments.

Sincerely,

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

August 16, 2023

Mr. Andy Jassy
Chief Executive Officer
Amazon
410 Terry Ave N
Seattle, WA 98109

Dear Mr. Jassy,

I write to applaud your company's willingness to join the recent Biden Administration initiative to secure voluntary commitments from leading artificial intelligence (AI) vendors related to promoting greater security, safety, and trust through improved development practices. These commitments – in some cases only applicable to your company's largest models – can materially reduce a range of security and safety risks identified by researchers and developers in recent years. In April, I wrote to several AI companies urging the prioritization of security and safety in the development, product release, and post-deployment practices relating to AI. Among other things, I asked these companies to fully map dependencies and downstream implications of compromise of systems; focus greater financial, technical and personnel resources on internal security; and improve transparency practices through greater documentation of system capabilities, system limitations, and training data. In many respects, the voluntary commitments by your company last month memorialize many of the commitments sought in my April letter.

These commitments have the potential to shape developer norms and best practices associated with leading-edge AI models. At the same time, less capable models not covered by the commitments are susceptible to misuse, security compromise, and proliferation risks. Moreover, a growing roster of highly-capable open source models have been released to the public – and would benefit from similar pre-deployment commitments contained in a number of the July 21st commitments. As the current commitments stand, leading vendors such as Amazon do not appear inclined to extend these vital development commitments to the wider range of AI products that your company has released that fall below this threshold or have been released as open source models.

To be sure, responsibility ultimately lies with Congress to develop laws that advance consumer and patient safety, address national security and cyber-crime risks, and promote secure development practices in this burgeoning and highly consequential industry – and in the downstream industries integrating these products. In the interim, the important commitments your company has agreed to can be bolstered in a number of valuable ways.

First, I strongly encourage your company to voluntarily extend all of the July 21st commitments to your company's less capable models that, in part through their wider adoption, can produce the most frequent examples of misuse and compromise.

Second, it is vital to build on these developer- and researcher-facing commitments with a suite of lightweight consumer-facing commitments to prevent the most serious forms of abuse. Most prominent among these should be commitments from your company to adopt development practices, licensing terms, and post-deployment monitoring practices that prevent non-consensual intimate image generation (including child sexual abuse material), social-scoring, real-time facial recognition (in contexts not governed by existing legal protections or due process safeguards), and proliferation activity in the context of malicious cyber activity or the production of biological or chemical agents.

Thank you for your company's engagement in this area. While representing an important improvement upon the status quo, the voluntary commitments announced in July can be bolstered in key ways through additional commitments.

Sincerely,

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

August 16, 2023

Mr. Mustafa Suleyman
Chief Executive Officer
Inflection AI
650 Page Mill Road
Palo Alto, CA 94304

Dear Mr. Suleyman,

I write to applaud your company's willingness to join the recent Biden Administration initiative to secure voluntary commitments from leading artificial intelligence (AI) vendors related to promoting greater security, safety, and trust through improved development practices. These commitments – in some cases only applicable to your company's largest models – can materially reduce a range of security and safety risks identified by researchers and developers in recent years. In April, I wrote to several AI companies urging the prioritization of security and safety in the development, product release, and post-deployment practices relating to AI. Among other things, I asked these companies to fully map dependencies and downstream implications of compromise of systems; focus greater financial, technical and personnel resources on internal security; and improve transparency practices through greater documentation of system capabilities, system limitations, and training data. In many respects, the voluntary commitments by your company last month memorialize many of the commitments sought in my April letter.

These commitments have the potential to shape developer norms and best practices associated with leading-edge AI models. At the same time, less capable models not covered by the commitments are susceptible to misuse, security compromise, and proliferation risks. Moreover, a growing roster of highly-capable open source models have been released to the public – and would benefit from similar pre-deployment commitments contained in a number of the July 21st commitments. As the current commitments stand, leading vendors such as Inflection AI do not appear inclined to extend these vital development commitments to the wider range of AI products that your company has released that fall below this threshold or have been released as open source models.

To be sure, responsibility ultimately lies with Congress to develop laws that advance consumer and patient safety, address national security and cyber-crime risks, and promote secure development practices in this burgeoning and highly consequential industry – and in the downstream industries integrating these products. In the interim, the important commitments your company has agreed to can be bolstered in a number of valuable ways.

First, I strongly encourage your company to voluntarily extend all of the July 21st commitments to your company's less capable models that, in part through their wider adoption, can produce the most frequent examples of misuse and compromise.

Second, it is vital to build on these developer- and researcher-facing commitments with a suite of lightweight consumer-facing commitments to prevent the most serious forms of abuse. Most prominent among these should be commitments from your company to adopt development practices, licensing terms, and post-deployment monitoring practices that prevent non-consensual intimate image generation (including child sexual abuse material), social-scoring, real-time facial recognition (in contexts not governed by existing legal protections or due process safeguards), and proliferation activity in the context of malicious cyber activity or the production of biological or chemical agents.

Thank you for your company's engagement in this area. While representing an important improvement upon the status quo, the voluntary commitments announced in July can be bolstered in key ways through additional commitments.

Sincerely,

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

August 16, 2023

Mr. Alexandr Wang
Chief Executive Officer
Scale AI
155 5th St
San Francisco, CA 94103

Dear Mr. Wang,

I write today regarding the voluntary commitments on artificial intelligence (AI) safety, security, and trust that the Biden-Harris Administration recently announced.[1] While I applaud the Administration's efforts to secure these commitments, I was hoping to see your company included as one of the participants. As I wrote in my last letter to you in April, I see an urgent need to emphasize security at the forefront of your work and I believe that, as a leading company in AI technology, you have a responsibility to ensure that your products and systems are secure.[2]

In addition to my April letter urging your company and a number of others to prioritize security and safety in the development, release, and post-deployment practices of AI technologies, in July, I wrote to the Administration with a number of suggestions to bolster their existing voluntary commitments.[3]

First, I strongly encouraged the Administration to continue engaging with industry to extend these commitments to less capable models that are susceptible to misuse and compromise. Second, I highlighted the importance of building on these developer- and researcher-facing commitments with specific consumer-facing commitments, such as licensing terms and post-deployment monitoring practices. Finally, I suggested that the Administration complement their existing work with a deeper engagement strategy to better engage vendors, downstream commercial users, and researchers on the security risks posed by, or directed at, AI systems.

I have continued to be vocal that the responsibility ultimately lies with Congress to develop laws that advance consumer and patient safety, address national security and cyber-crime risks, and

[1] The White House. "FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI." *The White House*, 21 July 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/.
[2] Senator Mark R. Warner. *Warner Calls on AI Companies to Prioritize Security and Prevent Malicious Misuse*. 26 Apr. 2023, https://www.warner.senate.gov/public/index.cfm/2023/4/warner-calls-on-ai-companies-to-prioritize-security-and-prevent-malicious-misuse.
[3] Senator Mark R. Warner. *Warner Calls on Biden Administration to Remain Engaged in AI Regulation*. 24 July 2023, https://www.warner.senate.gov/public/index.cfm/2023/7/warner-calls-on-biden-administration-to-remain-engaged-in-ai-regulation.

promote secure development practices in this industry – and the downstream industries integrating these products. However, as we continue to work together to better understand and protect against potential risks, private sector commitments, like those announced by the Administration, have the potential to inform best practices and impact development of AI models. Still, I believe that there are, and will continue to be, opportunities for companies like yours to make additional commitments to users around safety and security of your technologies as well as commitments around trustworthiness and bias.

I am interested in learning more about your commitment to safety, security, and transparency and to learn about the measures that your company is taking, and would be willing to take, in order to prioritize these principles in your AI technologies. I ask that you provide answers to the following questions:

1. Are you engaging with the Administration on participation in their voluntary commitments?
2. Are you already engaging in some or all of the specific processes outlined in the Administration's voluntary AI commitments?
3. If not, are you willing to make these commitments to promote safety, security, and transparency in the development and use of your AI technologies?
4. Are you willing to make any additional commitments beyond what is included by the Administration? Most notably, are you willing to make commitments to prevent your model or models misuse for the creation of non-consensual intimate image generation (including child sexual abuse material), social-scoring, real-time facial recognition (in contexts not governed by existing legal protections or due process safeguards), and proliferation activity in the context of malicious cyber activity or the production of biological or chemical agents?
5. Are there other commitments that you believe to be imperative for the safety, security, and transparency of AI technology that should be included in additional voluntary AI commitments?

Thank you for your continued engagement as we work together to address these important matters.

Sincerely,

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

August 16, 2023

Mr. Tim Cook
Chief Executive Officer
Apple
One Apple Park Way
Cupertino, CA 95014

Dear Mr. Cook,

I write today regarding the voluntary commitments on artificial intelligence (AI) safety, security, and trust that the Biden-Harris Administration recently announced.[4] While I applaud the Administration's efforts to secure these commitments, I was hoping to see your company included as one of the participants. As I wrote in my last letter to you in April, I see an urgent need to emphasize security at the forefront of your work and I believe that, as a leading company in AI technology, you have a responsibility to ensure that your products and systems are secure.[5]

In addition to my April letter urging your company and a number of others to prioritize security and safety in the development, release, and post-deployment practices of AI technologies, in July, I wrote to the Administration with a number of suggestions to bolster their existing voluntary commitments.[6]

First, I strongly encouraged the Administration to continue engaging with industry to extend these commitments to less capable models that are susceptible to misuse and compromise. Second, I highlighted the importance of building on these developer- and researcher-facing commitments with specific consumer-facing commitments, such as licensing terms and post-deployment monitoring practices. Finally, I suggested that the Administration complement their existing work with a deeper engagement strategy to better engage vendors, downstream commercial users, and researchers on the security risks posed by, or directed at, AI systems.

I have continued to be vocal that the responsibility ultimately lies with Congress to develop laws that advance consumer and patient safety, address national security and cyber-crime risks, and

[4] The White House. "FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI." *The White House*, 21 July 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/.
[5] Senator Mark R. Warner. *Warner Calls on AI Companies to Prioritize Security and Prevent Malicious Misuse*. 26 Apr. 2023, https://www.warner.senate.gov/public/index.cfm/2023/4/warner-calls-on-ai-companies-to-prioritize-security-and-prevent-malicious-misuse.
[6] Senator Mark R. Warner. *Warner Calls on Biden Administration to Remain Engaged in AI Regulation*. 24 July 2023, https://www.warner.senate.gov/public/index.cfm/2023/7/warner-calls-on-biden-administration-to-remain-engaged-in-ai-regulation.

promote secure development practices in this industry – and the downstream industries integrating these products. However, as we continue to work together to better understand and protect against potential risks, private sector commitments, like those announced by the Administration, have the potential to inform best practices and impact development of AI models. Still, I believe that there are, and will continue to be, opportunities for companies like yours to make additional commitments to users around safety and security of your technologies as well as commitments around trustworthiness and bias.

I am interested in learning more about your commitment to safety, security, and transparency and to learn about the measures that your company is taking, and would be willing to take, in order to prioritize these principles in your AI technologies. I ask that you provide answers to the following questions:

1. Are you engaging with the Administration on participation in their voluntary commitments?
2. Are you already engaging in some or all of the specific processes outlined in the Administration's voluntary AI commitments?
3. If not, are you willing to make these commitments to promote safety, security, and transparency in the development and use of your AI technologies?
4. Are you willing to make any additional commitments beyond what is included by the Administration? Most notably, are you willing to make commitments to prevent your model or models misuse for the creation of non-consensual intimate image generation (including child sexual abuse material), social-scoring, real-time facial recognition (in contexts not governed by existing legal protections or due process safeguards), and proliferation activity in the context of malicious cyber activity or the production of biological or chemical agents?
5. Are there other commitments that you believe to be imperative for the safety, security, and transparency of AI technology that should be included in additional voluntary AI commitments?

Thank you for your continued engagement as we work together to address these important matters.

Sincerely,

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

August 16, 2023

Mr. Emad Mostaque
Chief Executive Officer
Stability AI
88 Notting Hill Gate
London, England, W11 3HP

Dear Mr. Mostaque,

I write today regarding the voluntary commitments on artificial intelligence (AI) safety, security, and trust that the Biden-Harris Administration recently announced.[7] While I applaud the Administration's efforts to secure these commitments, I was hoping to see your company included as one of the participants. As I wrote in my last letter to you in April, I see an urgent need to emphasize security at the forefront of your work and I believe that, as a leading company in AI technology, you have a responsibility to ensure that your products and systems are secure.[8]

In addition to my April letter urging your company and a number of others to prioritize security and safety in the development, release, and post-deployment practices of AI technologies, in July, I wrote to the Administration with a number of suggestions to bolster their existing voluntary commitments.[9]

First, I strongly encouraged the Administration to continue engaging with industry to extend these commitments to less capable models that are susceptible to misuse and compromise. Second, I highlighted the importance of building on these developer- and researcher-facing commitments with specific consumer-facing commitments, such as licensing terms and post-deployment monitoring practices. Finally, I suggested that the Administration complement their existing work with a deeper engagement strategy to better engage vendors, downstream commercial users, and researchers on the security risks posed by, or directed at, AI systems.

I have continued to be vocal that the responsibility ultimately lies with Congress to develop laws that advance consumer and patient safety, address national security and cyber-crime risks, and

[7] The White House. "FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI." *The White House*, 21 July 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/.
[8] Senator Mark R. Warner. *Warner Calls on AI Companies to Prioritize Security and Prevent Malicious Misuse*. 26 Apr. 2023, https://www.warner.senate.gov/public/index.cfm/2023/4/warner-calls-on-ai-companies-to-prioritize-security-and-prevent-malicious-misuse.
[9] Senator Mark R. Warner. *Warner Calls on Biden Administration to Remain Engaged in AI Regulation*. 24 July 2023, https://www.warner.senate.gov/public/index.cfm/2023/7/warner-calls-on-biden-administration-to-remain-engaged-in-ai-regulation.

promote secure development practices in this industry – and the downstream industries integrating these products. However, as we continue to work together to better understand and protect against potential risks, private sector commitments, like those announced by the Administration, have the potential to inform best practices and impact development of AI models. Still, I believe that there are, and will continue to be, opportunities for companies like yours to make additional commitments to users around safety and security of your technologies as well as commitments around trustworthiness and bias.

I am interested in learning more about your commitment to safety, security, and transparency and to learn about the measures that your company is taking, and would be willing to take, in order to prioritize these principles in your AI technologies. I ask that you provide answers to the following questions:

1. Are you engaging with the Administration on participation in their voluntary commitments?
2. Are you already engaging in some or all of the specific processes outlined in the Administration's voluntary AI commitments?
3. If not, are you willing to make these commitments to promote safety, security, and transparency in the development and use of your AI technologies?
4. Are you willing to make any additional commitments beyond what is included by the Administration? Most notably, are you willing to make commitments to prevent your model or models misuse for the creation of non-consensual intimate image generation (including child sexual abuse material), social-scoring, real-time facial recognition (in contexts not governed by existing legal protections or due process safeguards), and proliferation activity in the context of malicious cyber activity or the production of biological or chemical agents?
5. Are there other commitments that you believe to be imperative for the safety, security, and transparency of AI technology that should be included in additional voluntary AI commitments?

Thank you for your continued engagement as we work together to address these important matters.

Sincerely,

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

August 16, 2023

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

Dear Mr. Holz,

I write today regarding the voluntary commitments on artificial intelligence (AI) safety, security, and trust that the Biden-Harris Administration recently announced.[10] While I applaud the Administration's efforts to secure these commitments, I was hoping to see your company included as one of the participants. As I wrote in my last letter to you in April, I see an urgent need to emphasize security at the forefront of your work and I believe that, as a leading company in AI technology, you have a responsibility to ensure that your products and systems are secure.[11]

In addition to my April letter urging your company and a number of others to prioritize security and safety in the development, release, and post-deployment practices of AI technologies, in July, I wrote to the Administration with a number of suggestions to bolster their existing voluntary commitments.[12]

First, I strongly encouraged the Administration to continue engaging with industry to extend these commitments to less capable models that are susceptible to misuse and compromise. Second, I highlighted the importance of building on these developer- and researcher-facing commitments with specific consumer-facing commitments, such as licensing terms and post-deployment monitoring practices. Finally, I suggested that the Administration complement their existing work with a deeper engagement strategy to better engage vendors, downstream commercial users, and researchers on the security risks posed by, or directed at, AI systems.

[10] The White House. "FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI." *The White House*, 21 July 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/.
[11] Senator Mark R. Warner. *Warner Calls on AI Companies to Prioritize Security and Prevent Malicious Misuse*. 26 Apr. 2023, https://www.warner.senate.gov/public/index.cfm/2023/4/warner-calls-on-ai-companies-to-prioritize-security-and-prevent-malicious-misuse.
[12] Senator Mark R. Warner. *Warner Calls on Biden Administration to Remain Engaged in AI Regulation*. 24 July 2023, https://www.warner.senate.gov/public/index.cfm/2023/7/warner-calls-on-biden-administration-to-remain-engaged-in-ai-regulation.

I have continued to be vocal that the responsibility ultimately lies with Congress to develop laws that advance consumer and patient safety, address national security and cyber-crime risks, and promote secure development practices in this industry – and the downstream industries integrating these products. However, as we continue to work together to better understand and protect against potential risks, private sector commitments, like those announced by the Administration, have the potential to inform best practices and impact development of AI models. Still, I believe that there are, and will continue to be, opportunities for companies like yours to make additional commitments to users around safety and security of your technologies as well as commitments around trustworthiness and bias.

I am interested in learning more about your commitment to safety, security, and transparency and to learn about the measures that your company is taking, and would be willing to take, in order to prioritize these principles in your AI technologies. I ask that you provide answers to the following questions:

1. Are you engaging with the Administration on participation in their voluntary commitments?
2. Are you already engaging in some or all of the specific processes outlined in the Administration's voluntary AI commitments?
3. If not, are you willing to make these commitments to promote safety, security, and transparency in the development and use of your AI technologies?
4. Are you willing to make any additional commitments beyond what is included by the Administration? Most notably, are you willing to make commitments to prevent your model or models misuse for the creation of non-consensual intimate image generation (including child sexual abuse material), social-scoring, real-time facial recognition (in contexts not governed by existing legal protections or due process safeguards), and proliferation activity in the context of malicious cyber activity or the production of biological or chemical agents?
5. Are there other commitments that you believe to be imperative for the safety, security, and transparency of AI technology that should be included in additional voluntary AI commitments?

Thank you for your continued engagement as we work together to address these important matters.

Sincerely,

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

August 16, 2023

Dr. Ali Ghodsi
Chief Executive Officer
Databricks
160 Spear Street 13th Floor
San Francisco, CA 94105

Dear Dr. Ghodsi,

I write today regarding the voluntary commitments on artificial intelligence (AI) safety, security, and trust that the Biden-Harris Administration recently announced.[1] While I applaud the Administration's efforts to secure these commitments, I was hoping to see your company included as one of the participants. As I wrote in a letter to several AI companies in April, I see an urgent need to emphasize security at the forefront of AI technology development and I believe that, as a leading company in this space, you have a responsibility to ensure that your products and systems are secure.[2]

In addition to my April letter urging a number of companies to prioritize security and safety in the development, release, and post-deployment practices of AI technologies, in July, I wrote to the Administration with a number of suggestions to bolster their existing voluntary commitments.[3]

First, I strongly encouraged the Administration to continue engaging with industry to extend these commitments to less capable models that are susceptible to misuse and compromise. Second, I highlighted the importance of building on these developer- and researcher-facing commitments with specific consumer-facing commitments, such as licensing terms and post-deployment monitoring practices. Finally, I suggested that the Administration complement their existing work with a deeper engagement strategy to better engage vendors, downstream commercial users, and researchers on the security risks posed by, or directed at, AI systems.

[1] The White House. "FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI." *The White House*, 21 July 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/.
[2] Senator Mark R. Warner. *Warner Calls on AI Companies to Prioritize Security and Prevent Malicious Misuse*. 26 Apr. 2023, https://www.warner.senate.gov/public/index.cfm/2023/4/warner-calls-on-ai-companies-to-prioritize-security-and-prevent-malicious-misuse.
[3] Senator Mark R. Warner. *Warner Calls on Biden Administration to Remain Engaged in AI Regulation*. 24 July 2023, https://www.warner.senate.gov/public/index.cfm/2023/7/warner-calls-on-biden-administration-to-remain-engaged-in-ai-regulation.

I have continued to be vocal that the responsibility ultimately lies with Congress to develop laws that advance consumer and patient safety, address national security and cyber-crime risks, and promote secure development practices in this industry – and the downstream industries integrating these products. However, as we continue to work together to better understand and protect against potential risks, private sector commitments, like those announced by the Administration, have the potential to inform best practices and impact development of AI models. Still, I believe that there are, and will continue to be, opportunities for companies like yours to make additional commitments to users around safety and security of your technologies as well as commitments around trustworthiness and bias.

I am interested in learning more about your commitment to safety, security, and transparency and to learn about the measures that your company is taking, and would be willing to take, in order to prioritize these principles in your AI technologies. I ask that you provide answers to the following questions:

1. Are you engaging with the Administration on participation in their voluntary commitments?
2. Are you already engaging in some or all of the specific processes outlined in the Administration's voluntary AI commitments?
3. If not, are you willing to make these commitments to promote safety, security, and transparency in the development and use of your AI technologies?
4. Are you willing to make any additional commitments beyond what is included by the Administration? Most notably, are you willing to make commitments to prevent your model or models misuse for the creation of non-consensual intimate image generation (including child sexual abuse imagery), social-scoring, real-time facial recognition (in contexts not governed by existing legal protections or due process safeguards), and proliferation activity in the context of malicious cyber activity or the production of biological or chemical agents?
5. Are there other commitments that you believe to be imperative for the safety, security, and transparency of AI technology that should be included in additional voluntary AI commitments?

Thank you for your engagement as we work together to address these important matters.

Sincerely,

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

August 16, 2023

Dr. Arthur Mensch
Chief Executive Officer
Mistral AI
21 Rue Tandou
75019 Paris, France

Dear Dr. Mensch,

I write today regarding the voluntary commitments on artificial intelligence (AI) safety, security, and trust that the Biden-Harris Administration recently announced.[4] While I applaud the Administration's efforts to secure these commitments, I was hoping to see your company included as one of the participants. As I wrote in a letter to several AI companies in April, I see an urgent need to emphasize security at the forefront of AI technology development and I believe that, as a leading company in this space, you have a responsibility to ensure that your products and systems are secure.[5]

In addition to my April letter urging a number of companies to prioritize security and safety in the development, release, and post-deployment practices of AI technologies, in July, I wrote to the Administration with a number of suggestions to bolster their existing voluntary commitments.[6]

First, I strongly encouraged the Administration to continue engaging with industry to extend these commitments to less capable models that are susceptible to misuse and compromise. Second, I highlighted the importance of building on these developer- and researcher-facing commitments with specific consumer-facing commitments, such as licensing terms and post-deployment monitoring practices. Finally, I suggested that the Administration complement their existing work with a deeper engagement strategy to better engage vendors, downstream commercial users, and researchers on the security risks posed by, or directed at, AI systems.

[4] The White House. "FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI." *The White House*, 21 July 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/.
[5] Senator Mark R. Warner. *Warner Calls on AI Companies to Prioritize Security and Prevent Malicious Misuse*. 26 Apr. 2023, https://www.warner.senate.gov/public/index.cfm/2023/4/warner-calls-on-ai-companies-to-prioritize-security-and-prevent-malicious-misuse.
[6] Senator Mark R. Warner. *Warner Calls on Biden Administration to Remain Engaged in AI Regulation*. 24 July 2023, https://www.warner.senate.gov/public/index.cfm/2023/7/warner-calls-on-biden-administration-to-remain-engaged-in-ai-regulation.

I have continued to be vocal that the responsibility ultimately lies with Congress to develop laws that advance consumer and patient safety, address national security and cyber-crime risks, and promote secure development practices in this industry – and the downstream industries integrating these products. However, as we continue to work together to better understand and protect against potential risks, private sector commitments, like those announced by the Administration, have the potential to inform best practices and impact development of AI models. Still, I believe that there are, and will continue to be, opportunities for companies like yours to make additional commitments to users around safety and security of your technologies as well as commitments around trustworthiness and bias.

I am interested in learning more about your commitment to safety, security, and transparency and to learn about the measures that your company is taking, and would be willing to take, in order to prioritize these principles in your AI technologies. I ask that you provide answers to the following questions:

1. Are you engaging with the Administration on participation in their voluntary commitments?
2. Are you already engaging in some or all of the specific processes outlined in the Administration's voluntary AI commitments?
3. If not, are you willing to make these commitments to promote safety, security, and transparency in the development and use of your AI technologies?
4. Are you willing to make any additional commitments beyond what is included by the Administration? Most notably, are you willing to make commitments to prevent your model or models misuse for the creation of non-consensual intimate image generation (including child sexual abuse imagery), social-scoring, real-time facial recognition (in contexts not governed by existing legal protections or due process safeguards), and proliferation activity in the context of malicious cyber activity or the production of biological or chemical agents?
5. Are there other commitments that you believe to be imperative for the safety, security, and transparency of AI technology that should be included in additional voluntary AI commitments?

Thank you for your engagement as we work together to address these important matters.

Sincerely,

Mark R. Warner
United States Senator