



PRESIDENT

John Formella

New Hampshire
Attorney General

PRESIDENT-ELECT

William Tong

Connecticut
Attorney General

VICE PRESIDENT

Marty Jackley

South Dakota
Attorney General

IMMEDIATE PAST
PRESIDENT

Letitia A. James

New York
Attorney General

Brian Kane

Executive Director

August 22, 2025

Julie Rottenberg
General Counsel

Visa, Inc.
900 Metro Center Blvd.
Foster City, CA 94404

Laureen Seeger
Chief Legal Officer
American Express Company
200 Vesey Street
New York, NY 10285

Halimah DeLaine Prado
General Counsel
Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

Tiffany Hall
General Counsel
Mastercard, Inc.
2000 Purchase Street
Purchase, NY 10577

Bimal Patel
General Counsel
PayPal, Inc.
2211 North First Street
San Jose, CA 95131

Katherine Adams
General Counsel
Apple Inc.
One Apple Park Way
Cupertino, CA 95014

To the legal representatives of Visa, Mastercard, American Express, PayPal, Google Pay and Apple Pay:

1850 M Street NW
12th Floor
Washington, DC 20036
(202) 326-6000
www.naag.org

We, the undersigned State Attorneys General, write in connection with our concerns about the problem of computer-generated nonconsensual intimate imagery (NCII), commonly known as "deepfake NCII" or "deepfake pornography." The spread of the ability to generate and distribute deepfake NCII poses a significant harm to the public, and to women and girls in particular. We write to call your attention to these harms and to implore each of you to take strong action to stop the spread and use of this technology for nonconsensual purposes.

At the outset, we note that we have the utmost respect for the First Amendment and your rights under it. Rather than potentially implicate those rights, we ask that you assess how you can mitigate the harmful effects of deepfake NCII just as you seek to address other harmful forms of content. Specifically, we respectfully request: 1) a description of how your companies currently work to identify and

remove payment authorization for deepfake NCII tools and content, if at all; and 2) your commitment to take further action to avoid being complicit in the creation and spread of deepfake NCII. In support of this request, below we provide some background on this issue.

I. Deepfake NCII presents a danger to the public.

Deepfake NCII is a growing problem that poses significant harms to the public. It has been used to embarrass, intimidate, and exploit people, including celebrities like Taylor Swift¹ and Bobbi Althoff,² as well as every-day teenagers in New Jersey,³ Florida,⁴ Washington,⁵ Kentucky,⁶ and around the world, including in South Korea⁷ and Spain⁸. As deepfake technology has advanced, the primary effect of its growth has been to expand the reach of deepfake NCII, as a recent report found that 98% of fake videos online are deepfake NCII, with the top 10 dedicated deepfake NCII websites generating more than 300 million video views.⁹ And although deepfake NCII overwhelmingly targets women and girls¹⁰, men and boys have been victimized by this technology as well.¹¹ As this technology becomes more powerful and creates more potential for harm to the public, businesses that help people search for, create, and distribute this content need to be aware of their role in propagating this content and work to prevent its spread.

II. Payment platforms can take stronger action to protect the public from the dangers of deepfake NCII.

Payment platforms provide users with the ability to send and receive money for content and services on the internet, facilitating transactions through credit cards, debit cards, and bank transactions. Payment platforms have demonstrated in the past that they have terms of service and acceptable use policies that prohibit their payment services being used in connection with harmful content. We ask that payment platforms direct their attention to the threat of deepfake NCII and work to ensure that they enforce their policies and avoid playing any role in allowing people to profit from deepfake NCII.

Payment platforms typically have terms of service and acceptable use policies that prohibit the use of their services in connection with harmful content. At times, payment platforms have taken action to remove the ability for sellers to accept payment for other

¹ <https://www.washingtonpost.com/technology/2024/01/26/taylor-swift-fans-deepfakes-ai-porn/>

² <https://www.washingtonpost.com/technology/2024/02/22/x-twitter-bobbi-althoff-deepfake-porn-viral/>

³ <https://www.cbsnews.com/newyork/news/westfield-high-school-ai-pornographic-images-students/>

⁴ <https://www.nbcmiami.com/news/local/ai-app-misused-by-miami-dade-students-to-make-inappropriate-images-of-classmates-police/3184692/>

⁵ <https://www.theguardian.com/technology/2024/mar/12/family-takes-fight-against-deepfake-nudes-to-washington>

⁶ <https://www.cbsnews.com/news/sextortion-generative-ai-scam-elijah-heacock-take-it-down-act/>

⁷ <https://www.nytimes.com/2024/09/03/world/asia/south-korean-teens-deepfake-sex-images.html>

⁸ <https://www.theguardian.com/world/2023/sep/25/spanish-prosecutor-investigates-if-shared-ai-images-of-naked-girls-constitute-a>

⁹ <https://www.securityhero.io/state-of-deepfakes/assets/pdf/state-of-deepfake-infographic-2023.pdf>

¹⁰ *Id.*, stating that 99% of all deepfake pornography is of women.

¹¹ <https://www.gq-magazine.co.uk/article/sextortion-scams-deepfake-porn-men>

services related to harmful content.¹² The same principles that have led payment processors to withdraw their services from sellers who engaged in other harmful activities should also apply to sellers that are distributing deepfake NCII tools and content.

Payment platforms must be more aggressive in identifying and removing payment authorization for deepfake NCII tools and content. Sellers of deepfake NCII tools and content have made their services available in exchange for fees paid via payment platforms including Visa, Mastercard, American Express, PayPal, Google Pay, and Apple Pay, even including the logos of those companies on their webpages. Payment platforms should not only deny sellers the ability to use their services when they are on notice of these connections but should be actively working to identify and remove any such sellers from their network. Active, aggressive enforcement of payment platforms' terms of service and acceptable use policies is essential to slowing the proliferation of deepfake NCII tools and content. We are glad to see that some payment platforms have taken action in this area,¹³ and we hope to continue to see more action in this area from the payment platforms going forward.

III. Protecting the Public

We look forward to learning more about what steps you have taken so far to combat this problem, and to discussing with you how you plan to address it in the future. We urge you to treat the problem of deepfake NCII seriously and to work to better prevent your own complicity in the creating and sharing of this content. We would welcome an opportunity to speak with you further regarding our concerns.

Sincerely,



Russell Coleman
Kentucky Attorney General



Andrea Joy Campbell
Massachusetts Attorney General

¹² See, e.g., <https://www.theverge.com/2020/12/10/22168240/mastercard-ending-pornhub-payment-processing-unlawful-videos>.

¹³ See, e.g., <https://www.bellingcat.com/news/2024/02/23/behind-a-secretive-global-network-of-non-consensual-deepfake-pornography/>, <https://www.404media.co/civitai-site-used-to-generate-ai-porn-cut-off-by-credit-card-processor/>, and <https://indicator.media/p/ai-nudifiers-continue-to-reach-millions-and-make-millions>.



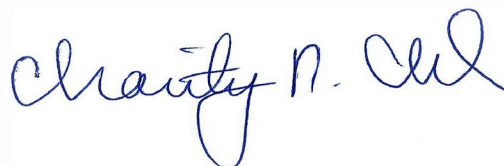
Matthew J. Platkin
New Jersey Attorney General



Dave Sunday
Pennsylvania Attorney General



Derek Brown
Utah Attorney General



Charity Clark
Vermont Attorney General



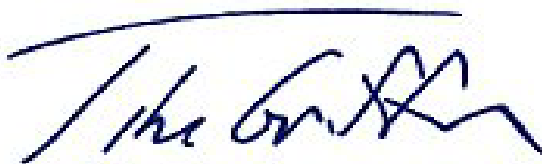
Treg R. Taylor
Alaska Attorney General



Gwen Tauiliili-Langkilde
American Samoa Attorney General



Kris Mayes
Arizona Attorney General



Tim Griffin
Arkansas Attorney General



Rob Bonta
California Attorney General



Phil Weiser
Colorado Attorney General



William Tong
Connecticut Attorney General



Kathleen Jennings
Delaware Attorney General



Christopher M. Carr
Georgia Attorney General



Anne E. Lopez
Hawaii Attorney General



Raúl Labrador
Idaho Attorney General



Kwame Raoul
Illinois Attorney General



Brenna Bird
Iowa Attorney General



Liz Murrill
Louisiana Attorney General



Aaron M. Frey
Maine Attorney General



Anthony G. Brown
Maryland Attorney General



Dana Nessel
Michigan Attorney General



Keith Ellison
Minnesota Attorney General

A cursive signature in black ink that reads "Lynn Fitch".

Lynn Fitch
Mississippi Attorney General

A stylized signature in blue ink, consisting of a series of loops and a long horizontal stroke.

Andrew Bailey
Missouri Attorney General

A signature in blue ink that reads "Mike Hilgers" in a cursive style.

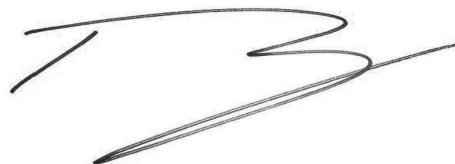
Mike Hilgers
Nebraska Attorney General

A signature in blue ink that reads "Aaron D. Ford" in a cursive style.

Aaron D. Ford
Nevada Attorney General

A signature in black ink that reads "John M. Formella" in a cursive style.

John M. Formella
New Hampshire Attorney General

A signature in black ink that reads "Raúl Torrez" in a cursive style.

Raúl Torrez
New Mexico Attorney General

A signature in blue ink that reads "Letitia James" in a cursive style.

Letitia James
New York Attorney General

A signature in blue ink that reads "Jeff Jackson" in a cursive style.

Jeff Jackson
North Carolina Attorney General

A signature in black ink that reads "Drew H. Wrigley" in a cursive style.

Drew H. Wrigley
North Dakota Attorney General

A signature in blue ink that reads "Dave Yost" in a cursive style.

Dave Yost
Ohio Attorney General

A signature in blue ink that reads "Gentner Drummond" in a cursive style.

Gentner Drummond
Oklahoma Attorney General

A signature in black ink that reads "Dan Rayfield" in a cursive style.

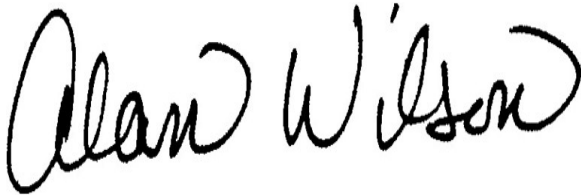
Dan Rayfield
Oregon Attorney General



Lourdes Lynnette Gómez Torres
Puerto Rico Attorney General



Peter F. Neronha
Rhode Island Attorney General



Alan Wilson
South Carolina Attorney General



Marty Jackley
South Dakota Attorney General



Jonathan Skrmetti
Tennessee Attorney General



Gordon C. Rhea
U.S. Virgin Islands Attorney General



Jason S. Miyares
Virginia Attorney General



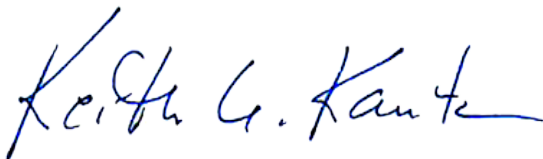
Nick Brown
Washington Attorney General



John "JB" McCuskey
West Virginia Attorney General



Joshua L. Kaul
Wisconsin Attorney General



Keith Kautz
Wyoming Attorney General



NATIONAL
ASSOCIATION OF
ATTORNEYS GENERAL

PRESIDENT

John Formella
New Hampshire
Attorney General

PRESIDENT-ELECT

William Tong
Connecticut
Attorney General

VICE PRESIDENT

Marty Jackley
South Dakota
Attorney General

IMMEDIATE PAST
PRESIDENT

Letitia A. James
New York
Attorney General

Brian Kane
Executive Director

1850 M Street NW
12th Floor
Washington, DC 20036
(202) 326-6000
www.naag.org

August 22, 2025

Halimah DeLaine Prado
General Counsel
Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

Jonathan Palmer
General Counsel
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Darin Bassin
Chief Legal Officer
Yahoo! Inc.
770 Broadway, 9th Floor
New York, NY 10003

To the legal representatives of Google Search, Microsoft Bing, and
Yahoo! Search:

We, the undersigned State Attorneys General, write in connection with our concerns about the problem of computer-generated nonconsensual intimate imagery (NCII), commonly known as “deepfake NCII” or “deepfake pornography.” The spread of the ability to generate and distribute deepfake NCII poses a significant harm to the public, and to women and girls in particular. We write to call your attention to these harms and to implore each of you to take strong action to stop the spread and use of this technology for nonconsensual purposes.

At the outset, we note that we have the utmost respect for the First Amendment and your rights under it. Rather than potentially implicate those rights, we ask that you assess how you can mitigate the harmful effects of deepfake NCII just as you seek to address other harmful forms of content. Specifically, we respectfully request: 1) a description of how your companies currently work to de-prioritize, restrict, and/or block deepfake NCII content and creation tools from your services, if at all; and 2) your commitment to take further action to avoid being complicit in the creation and spread of deepfake NCII. In support of this request, below we provide some background on this issue.

I. Deepfake NCII presents a danger to the public.

Deepfake NCII is a growing problem that poses significant harms to the public. It has been used to embarrass, intimidate, and exploit people, including celebrities like Taylor Swift¹ and Bobbi Althoff,² as well as every-day teenagers in New Jersey,³ Florida,⁴ Washington,⁵ Kentucky,⁶ and around the world, including in South Korea⁷ and Spain.⁸ As deepfake technology has advanced, the primary effect of its growth has been to expand the reach of deepfake NCII, as a recent report found that 98% of fake videos online are deepfake NCII, with the top 10 dedicated deepfake NCII websites generating more than 300 million video views.⁹ And although deepfake NCII overwhelmingly targets women and girls,¹⁰ men and boys have been victimized by this technology as well.¹¹ As this technology becomes more powerful and creates more potential for harm to the public, businesses that help people search for, create, and distribute this content need to be aware of their role in propagating this content and work to prevent its spread.

II. Search platforms can take stronger action to protect the public from the dangers of deepfake NCII.

Search platforms can and do limit the reach of harmful content on the internet. Search results for “how to build a bomb” generally link to government resources, encyclopedia articles, and responsible scientific articles, all sources that seem unlikely to connect a searcher to actionable information about how to make a bomb. Searches for “how to kill yourself” are even more tightly limited, highlighting suicide prevention phone numbers and emergency resources and linking to various mental health treatment options, rightly recognizing the risk of harm of the information being searched for and steering the user towards appropriate resources to discourage and redirect them. These limitations reflect that these platforms, when appropriately aware and motivated, can take action to protect the public from dangerous and harmful content, even when users are actively searching for such content.

The same limitations do not appear to be in place on these platforms when it comes to searches relating to deepfake NCII. Searches on major search engines for “how to make deepfake pornography,” “undress apps,” “nudify apps,” or simply “deepfake porn” do not lead

¹ <https://www.washingtonpost.com/technology/2024/01/26/taylor-swift-fans-deepfakes-ai-porn/>

² <https://www.washingtonpost.com/technology/2024/02/22/x-twitter-bobbi-althoff-deepfake-porn-viral/>

³ <https://www.cbsnews.com/newyork/news/westfield-high-school-ai-pornographic-images-students/>

⁴ <https://www.nbcmiami.com/news/local/ai-app-misused-by-miami-dade-students-to-make-inappropriate-images-of-classmates-police/3184692/>

⁵ <https://www.theguardian.com/technology/2024/mar/12/family-takes-fight-against-deepfake-nudes-to-washington>

⁶ <https://www.cbsnews.com/news/sextortion-generative-ai-scam-elijah-heacock-take-it-down-act/>

⁷ <https://www.nytimes.com/2024/09/03/world/asia/south-korean-teens-deepfake-sex-images.html>

⁸ <https://www.theguardian.com/world/2023/sep/25/spanish-prosecutor-investigates-if-shared-ai-images-of-naked-girls-constitute-a>

⁹ <https://www.securityhero.io/state-of-deepfakes/assets/pdf/state-of-deepfake-infographic-2023.pdf>

¹⁰ *Id.*, stating that 99% of all deepfake pornography is of women.

¹¹ <https://www.gq-magazine.co.uk/article/sextortion-scams-deepfake-porn-men>.

to any warnings and, on many platforms, do not demonstrate any apparent effort to limit or redirect the results of these searches. Results for these searches present users with an array of options of deepfake pornography creation tools and content, with no warnings other than SafeSearch features sometimes blurring image thumbnails. Searches for this content quickly present users with direct links to deepfake NCII, to listicles rating the top apps for creating deepfake NCII, and to apps that enable the creation of naked and/or sexual images and videos of any person in any photo. Just as search platforms appear to recognize that it would be irresponsible to connect users with a top 10 list of the best instruction sets for creating an improvised explosive device from household items, or a step-by-step guide to an effective method of suicide, these platforms must understand that searches seeking to find or create deepfake NCII are similarly harmful to the public, particularly children, and demand a response other than an unfiltered list of the most popular content.

We recognize that search platforms have taken some action on this topic,¹² and that platforms are likely to provide additional tools to victims of deepfake NCII in response to the passage of the Take It Down Act. We are encouraged to see these steps and are hopeful that more such steps have been taken or are in the works. However, the results of currently available searches indicate to our offices that there needs to be quicker and more decisive action against this content. Search platforms should work to implement new policies that appreciate the threat of deepfake NCII by steering users away from harmful content and providing appropriate warnings.

III. Protecting the Public

We look forward to learning more about what steps you have taken so far to combat this problem, and to discussing with you how you plan to address it in the future. We urge you to treat the problem of deepfake NCII seriously and to work to better prevent your own complicity in the creating and sharing of this harmful content. We would welcome an opportunity to speak with you further regarding our concerns.

Sincerely,



Russell Coleman
Kentucky Attorney General



Andrea Joy Campbell
Massachusetts Attorney General

¹² See, e.g., <https://support.google.com/websearch/answer/9116649>, <https://www.pcmag.com/news/microsoft-to-help-users-remove-deepfake-nudes-from-bing-image-search>, and <https://indicator.media/p/ai-nudifiers-continue-to-reach-millions-and-make-millions>.

A blue ink signature of Matthew J. Platkin, featuring a stylized 'M' and 'P'.

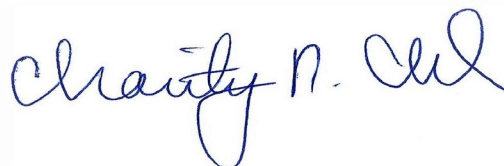
Matthew J. Platkin
New Jersey Attorney General

A blue ink signature of Dave Sunday, featuring a large, flowing 'D' and 'S'.

Dave Sunday
Pennsylvania Attorney General

A blue ink signature of Derek Brown, featuring a large, stylized 'D' and 'B'.

Derek Brown
Utah Attorney General

A blue ink signature of Charity Clark, featuring a stylized 'C' and 'C'.

Charity Clark
Vermont Attorney General

A blue ink signature of Treg R. Taylor, featuring a stylized 'T' and 'T'.

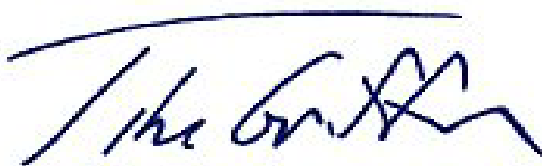
Treg R. Taylor
Alaska Attorney General

A blue ink signature of Gwen Tauiliili-Langkilde, featuring a stylized 'G' and 'T'.

Gwen Tauiliili-Langkilde
American Samoa Attorney General

A blue ink signature of Kris Mayes, featuring a stylized 'K' and 'M'.

Kris Mayes
Arizona Attorney General

A blue ink signature of Tim Griffin, featuring a stylized 'T' and 'G'.

Tim Griffin
Arkansas Attorney General

A blue ink signature of Rob Bonta, featuring a stylized 'R' and 'B'.

Rob Bonta
California Attorney General

A blue ink signature of Phil Weiser, featuring a stylized 'P' and 'W'.

Phil Weiser
Colorado Attorney General



William Tong
Connecticut Attorney General



Kathleen Jennings
Delaware Attorney General



Christopher M. Carr
Georgia Attorney General



Anne E. Lopez
Hawaii Attorney General



Raúl Labrador
Idaho Attorney General



Kwame Raoul
Illinois Attorney General



Brenna Bird
Iowa Attorney General



Liz Murrill
Louisiana Attorney General



Aaron M. Frey
Maine Attorney General



Anthony G. Brown
Maryland Attorney General



Dana Nessel
Michigan Attorney General



Keith Ellison
Minnesota Attorney General

A cursive signature in black ink that reads "Lynn Fitch".

Lynn Fitch
Mississippi Attorney General

A stylized signature in blue ink, consisting of a series of loops and a long horizontal stroke.

Andrew Bailey
Missouri Attorney General

A signature in blue ink that reads "Mike Hilgers".

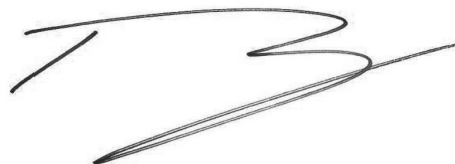
Mike Hilgers
Nebraska Attorney General

A signature in blue ink that reads "Aaron D. Ford".

Aaron D. Ford
Nevada Attorney General

A signature in black ink that reads "John M. Formella".

John M. Formella
New Hampshire Attorney General

A signature in black ink that reads "Raúl Torrez".

Raúl Torrez
New Mexico Attorney General

A signature in blue ink that reads "Letitia James".

Letitia James
New York Attorney General

A signature in blue ink that reads "Jeff Jackson".

Jeff Jackson
North Carolina Attorney General

A signature in black ink that reads "Drew H. Wrigley".

Drew H. Wrigley
North Dakota Attorney General

A signature in blue ink that reads "Dave Yost".

Dave Yost
Ohio Attorney General

A signature in blue ink that reads "Gentner Drummond".

Gentner Drummond
Oklahoma Attorney General

A signature in black ink that reads "Dan Rayfield".

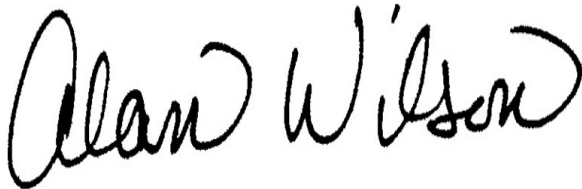
Dan Rayfield
Oregon Attorney General



Lourdes Lynnette Gómez Torres
Puerto Rico Attorney General



Peter F. Neronha
Rhode Island Attorney General



Alan Wilson
South Carolina Attorney General



Marty Jackley
South Dakota Attorney General



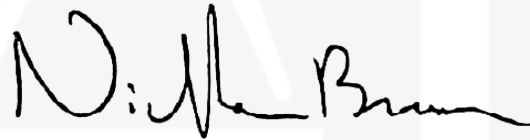
Jonathan Skrmetti
Tennessee Attorney General



Gordon C. Rhea
U.S. Virgin Islands Attorney General



Jason S. Miyares
Virginia Attorney General



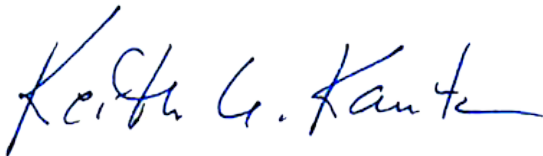
Nick Brown
Washington Attorney General



John "JB" McCuskey
West Virginia Attorney General



Joshua L. Kaul
Wisconsin Attorney General



Keith Kautz
Wyoming Attorney General