

United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

February 11, 2025

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

Dear Mr. Zuckerberg:

I write regarding troubling reports that advertisements on Instagram and other Meta platforms are generating a significant amount of traffic for Crushmate or Crush AI (“Crush”), an app that allows—and, in fact, encourages—users to create nonconsensual deepfake intimate imagery. Because Meta has allowed Crush to run advertisements on mainstream platforms like Instagram, a significant number of Meta users have now accessed a highly problematic, otherwise little used app. I want to know how Meta allowed this to happen and what Meta is doing to address this dangerous trend.

A recent article published by 404 Media revealed that most of Crush’s traffic originates from Meta platforms, where Crush is buying thousands of explicit ads featuring nonconsensual nudity of celebrities and influencers.¹ According to the article, Crush has purchased ads on Facebook, Instagram, and other Meta platforms since at least early September 2024. And the ads have been effective. An analysis of four Crush domains revealed that in December 2024, the domains had a combined 263,119 visits. Of these visits, 237,420 were referrals from either Facebook or Instagram. That is 90 percent of the company’s traffic that originates from Meta platforms.²

Each ad for Crush violates Meta’s Advertising Standards, including its prohibitions on ads that feature Adult Nudity and Sexual Activity and ads that include certain forms of Bullying and Harassment. Yet, the ads are prevalent on Meta’s platforms. In the first two weeks of this year alone, Meta ran at least 8,010 ads for Crush.

It appears that Crush is evading Meta’s enforcement efforts through a simple strategy. The company creates dozens of fake advertiser profiles on Meta, often with AI-generated profile pictures. It then employs multiple domains that redirect to Crush to evade detection. Once caught, the company repeats the process.

Because of apps like Crush, no special expertise is needed to create deepfakes. Research has identified more than 290 deepfake pornography apps, 80 percent of which have launched in the

¹ Emanuel Maiberg, *Instagram Ads Send This Nudify Site 90 Percent of Its Traffic*, 404 Media (Jan. 15, 2025), available at https://www.404media.co/instagram-ads-send-this-nudify-site-90-percent-of-its-traffic/?utm_campaign=wp_the_technology_202&utm_medium=email&utm_source=newsletter.

² Alexios, *AI Nudifier Makes a Mockery Of Meta’s Moderation*, FakedUp Newsletter (Jan. 15, 2025), available at <https://fakedup.substack.com/p/ai-nudifiers-make-a-mockery-of-metas-moderation?ref=404media.com>.

past year.³ Because this easily used software is now so readily accessible through platforms like Facebook, Instagram, and Threads, middle schools and high schools around the country are grappling with shocking acts of image-based abuse committed by students on other students.

The generation and dissemination of nonconsensual, deepfake intimate imagery are acts of abuse and violations of privacy that inflict lasting harm on victims. Victims can feel destabilized when they lose control over their likeness and identity and can feel powerless to remove the illicit content or to prevent it from being produced again. They may experience depression, anxiety, and a fear of being in public. This can have the effect of silencing victims, causing them to withdraw from online spaces and public discourse as a protective measure. These images may be used to harass victims and damage their employment, education, or reputation, or to further criminal activity such as extortion and stalking. In the worst cases, they drive victims to suicide.

Tech companies should not assist malevolent actors who seek to take advantage of women and children. I am gravely concerned with Meta's failure to prevent this perverse abuse of its platforms and I refuse to accept Meta's facilitation of these crimes. I therefore urge Meta to join us in combatting this threat.

To that end, please respond to the following questions, no later than March 11, 2025:

1. What safeguards has Meta put in place to prevent advertisements on its platforms for Crush and similar apps that encourage users to create nonconsensual deepfake intimate imagery?
2. How does Meta ensure that advertiser profiles are legitimate?
3. What safeguards does Meta have in place to identify and remove fake advertiser profiles on its platforms?
4. What steps does Meta take to ensure advertisements on its platforms do not redirect users to otherwise prohibited products or advertisers?
5. What is Meta doing to educate the public, and youth in particular, about the harms of nonconsensual deepfake intimate imagery?

I look forward to your prompt response.

Sincerely,



Richard J. Durbin
Ranking Member

³ Lorena O'Neil, *Fake Photos, Real Harm: AOC and the Fight Against AI Porn*, ROLLING STONE (Apr. 8, 2024), available at <https://www.rollingstone.com/culture/culture-features/aoc-deepfake-ai-porn-personal-experience-defiance-act-1234998491/>.