Sexual Violence Prevention Association

February 2, 2024

Submitted via regulations.gov

Gina Raimondo
Secretary of Commerce
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

Laurie E. Locascio
Director, NIST
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Re: Written Comment for Request for Information Related to NIST's Assignments Under Sections 4.1, 4.5, and 11 of the Executive Order Concerning Artificial Intelligence, Executive Order 14110, Document Citation 88 FR 88368

To Secretary of Commerce Gina Raimondo and Director of the National Institute of Standards and Technology Laurie E. Locascio:

On behalf of the Sexual Violence Prevention Association (SVPA), a national non-profit dedicated to preventing sexual violence systemically, we would like to thank the Department of Commerce and the National Instute of Standards and Technology for the opportunity to submit a formal comment on the development and use of artificial intelligence (AI). We welcome the Executive Office's efforts to address the use of AI. There are certain aspects of the executive order that we feel need to be addressed through future regulation. Specifically, we believe that the regulations should cover non-consensual deepfake pornography. This issue must be covered comprehensively due to its increasing proliferation in the United States.

A recent analysis found that the United States is ranked 2nd in the world in deepfake pornography. As of 2023, over 98% of deepfakes on the internet were pornography. There were over 500,000 deepfakes shared online in 2023. Further, the number of deepfakes online is doubling every six months.

For good or bad, the internet is forever. As a country, we must move forward with caution. Non-consensual deepfake pornography may be digital but it causes permanent pain to its victims. The SVPA understands the complexity of regulating AI and the need to ensure safe, secure, and trustworthy implementation. We believe that fulfilling the executive order with the following regulations will mitigate substantial risks while promoting responsible usage of AI.

Regulations
Tech companies must be held accountable for hosting and distributing non-consensual deepfake porn. NIST must implement exhaustive regulations requiring platforms to implement comprehensive prevention strategies, effective content moderation policies, and tools to detect and remove deepfake pornography.

Labeling
Labeling is important to help users identify and differentiate between authentic and synthetic media. This can help prevent the spread of misinformation including non-consensual deepfake pornography. NIST should implement regulations that specify that all materials created using AI must be labeled as such. This includes front-end labeling, such as watermarks or a small-text disclaimer. This also includes back-end labeling, such as fragments of code in the metadata that computer programs can screen for and flag when needed. This labeling should be required for tech platforms that create AI materials. It should also be required for platforms that host AI materials, including platforms where users may upload these materials. These platforms should be required to implement automated detection techniques to quickly identify real and synthetic non-consensual pornography.

Consent
In the case of AI-generated images, NIST should implement regulations requiring tech companies to implement consent measures to ensure that consent has been given by the person depicted. This includes ensuring consent for materials that are used in the training of AI programs as well as user-uploads and program outputs. It should include both explicit and non-explicit materials. Most importantly, NIST should require companies to verify the age of the people whose likeness is depicted in training data, user uploads, and materials generated.

Screening
NIST must implement regulations requiring platforms to screen and assess the images users upload, the content the platform creates, and the words/syntax used in the user request. If the platform deems the material to be suspect of pedophilia or non-consensual deepfake pornography, the request should not be completed and should be flagged for human review. Furthermore, user-uploads should be screened to determine the source of the materials. If a user is uploading material that was obtained using a web-scraper, the request should not be completed and should be flagged for human review. Further, if a user is uploading a significant amount of materials that were attained via screenshots or social media downloads, they should be flagged for a consent review.

Marketing
NIST should implement regulations regarding the marketing of AI programs and AI-generated materials. AI-generating platforms should not market their services or programs for use in the creation of pornography. Platforms that host AI-generated content, including user-uploaded content, should not market themselves as a platform for finding, uploading, selling, or soliciting deepfake pornography.

Data & Research
NIST should work with other offices and agencies to implement a system of reporting and tracking that is required for tech companies. Further, NIST should support research on the proliferation and effect of non-consensual deepfake pornography. This includes supporting

surveys and other systems of data collection. Lastly, NIST should form and/or join a task force as a means of ongoing monitoring of this issue.

Research & Development
NIST should complete research and development for technological tools and institutional strategies to aid in the prevention of non-consensual deepfake pornography. This includes strategies for screening, consent verification, and labeling, as discussed in this comment.

Please feel free to contact Omny Miranda Martone, the Founder and CEO of the Sexual Violence Prevention Association (SVPA), with any questions at info@s-v-p-a.org.

Thank you,

Sexual Violence Prevention Association (SVPA)