MARSHA BLACKBURN
TENNESSEE
http://www.blackburn.senate.gov/

357 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224–3344
FAX: (202) 228–0566

United States Senate

COMMITTEES:
COMMERCE, SCIENCE, AND TRANSPORTATION
FINANCE
JUDICIARY
VETERANS' AFFAIRS

September 17, 2025

VIA ELECTRONIC TRANSMISSION

Mr. Giorgi Gobronidze
Owner & CEO
PimEyes

Dear Mr. Gobronidze:

I write to express my deep concern with PimEyes's artificial intelligence facial recognition technology and the harm it poses to individuals' safety and privacy. Specifically, I write regarding reporting from *Politico* that Dominick Skinner and a group of individuals have undertaken an activism project using your facial search engine to identify a list of at least 20 U.S. Immigration and Customs Enforcement (ICE) officers' names and photos.[1] According to Mr. Skinner, if 35 percent or more of a face is visible, your technology can reveal the covered faces of individuals. Although this "ICE List" does not publish addresses, Mr. Skinner has confirmed the fact that an individual's name is sufficient to find personal information about them online.[2]

Online foreign activists should not be weaponizing generative AI to threaten and endanger our federal officers and their families. Reverse image search systems like PimEyes can be used by gangs like MS-13 and Tren De Aragua to target ICE agents and their loved ones. According to the Department of Homeland Security, as of July 2025, ICE agents have experienced a nearly ***700 percent increase*** in assaults.[3] Our law enforcement officers devote their lives to protecting our communities. They willingly and courageously stand in the face of danger to keep us safe. Nashville Mayor Freddie O'Connell even went so far as to publicly release the names of several ICE agents—placing those tasked with protecting us and their families directly in harm's way.[4] That disgusting act against the brave men and women of law enforcement is precisely why I introduced the Protecting Law Enforcement from Doxxing Act, which creates a criminal prohibition on the public release of the name of a federal law enforcement officer with the intent to obstruct a criminal investigation or immigration enforcement operation.

In addition to threatening the safety of law enforcement officers, this use of your technology also presents ethical concerns regarding the storing of biometric data, as well as the exploitation of children. Your website urges visitors to "protect your privacy," which implies that your technology

[1] Alfred Ng, *AI Is Unmasking ICE Officers. Can Washington Do Anything About It?*, POLITICO (Aug. 29, 2025), https://www.politico.com/news/2025/08/29/ai-unmasking-ice-officers-00519478.
[2] *Id.*
[3] Dep't of Homeland Sec., *Anarchists and Rioters in Portland Illegally Dox ICE Officers and Federal Law Enforcement* (July 11, 2025), https://www.dhs.gov/news/2025/07/11/anarchists-and-rioters-portland-illegally-dox-ice-officers-and-federal-law.
[4] Alec Schemmel, *Nashville Mayor Freddie O'Connell Stands Behind Doxing ICE Agents Even After Officials Said His Actions Put Them in Danger*, N.Y. POST (June 21, 2025), https://nypost.com/2025/06/21/us-news/nashville-mayor-freddie-oconnell-stands-behind-doxing-ice-agents-even-after-officials-said-his-actions-put-them-in-danger/.

empowers users to reclaim their own identities and reputations by locating photos of themselves.[5] This is a false reality to abolish anonymity under the guise of autonomy. This ethical honor system also fails to account for the abuses possible through the search engine, including doxxing, stalking, revenge pornography, and child harm.

Further, PimEyes has purported that this technology can assist in public safety by locating dangerous offenders. This, in the carefully trained hands of law enforcement, is true. However, a publicly accessible digital library of individuals' lives and likenesses in the wrong hands poses unthinkable risks. As the Chairman of the Senate Judiciary Subcommittee on Privacy, Technology, and the Law, I am dedicated to ensuring that Americans' data, privacy, and likeness protections are not abandoned in the digital space. I urge you to take immediate action in transparency and accountability.

To that end, please respond to the following questions by **5:00 PM on September 24, 2025**:

1. Are you aware of groups, including Mr. Skinner's organization, who utilize PimEyes to, in his words, "publicly shame"[6] and publish the names and photos of United States federal officers, endangering them and their relatives?

2. Your terms of service state: "PimEyes is intended solely for personal use. Pursuant to our Terms of Service, any search pertaining to other individuals is strictly prohibited. We take all necessary measures to ensure the privacy and protection of our users. We consider non-compliance with our policies to be a grave matter, tantamount to violating the law." What are these "necessary measures" and how are you monitoring and enforcing this rule?

3. Mr. Skinner acknowledged that name and image alone are sufficient to locate additional personal and private information about an individual online.[7] What do you say to individuals who can use the images found through your software to locate addresses, communities, and even workplaces of U.S. Immigration and Customs Enforcement (ICE) officers and their children?

4. What safeguards do individuals have regarding their biometric data being uploaded into or returned from PimEyes by third parties?

5. What safeguards do you have to ensure that this software is defending individuals from scams, identity theft, stalking, trafficking, blackmail, and other threats rather than making them more vulnerable and accessible to them?

6. According to the "Opt-Out" option, individuals must upload government-issued identity proof, requiring that individuals provide your system with sensitive information to ask for protection for that sensitive information in return.[8] Additionally, the subscription based

[5] PimEyes Home Page, https://pimeyes.com/en [https://perma.cc/EWQ9-6JAS] (last visited Sep. 11, 2025).
[6] Ng, *supra*.
[7] *Id.*
[8] Opt-Out Request Form, https://pimeyes.com/en/opt-out-request-form (last visited Sep. 11, 2025).

"PROtect plans" to request the removal of photos have not been entirely successful.[9] If identity verification is required to "Opt-Out" of search results, what steps is PimEyes taking to ensure that individuals are searching for their own identities when opting into utilizing the system?

7. PimEyes uses a paid feature to locate the sources, or locations of images. With PimEyes's Open Plus plan, individuals can even be notified when a new photo is located.[10] This means that a stalker or trafficker could receive a notification of a new photo uploaded in their back pocket. In absence of mandatory identity verification, how can individuals be assured that their photos, whereabouts, and other information are not being alerted and delivered directly to harmful individuals?

Thank you for your attention to this urgent matter.

Sincerely,

Marsha Blackburn
United States Senator

[9] Rachel Metz, *She Thought a Dark Moment in Her Past Was Forgotten. Then She Scanned Her Face Online*, CNN Business (May 24, 2022, at 12:18 ET), https://edition.cnn.com/2022/05/24/tech/cher-scarlett-facial-recognition-trauma/index.html.
[10] PimEyes Pricing Plans, https://pimeyes.com/en/premium (last visited Sep. 11, 2025).