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

October 31, 2025

VIA ELECTRONIC TRANSMISSION

Mr. Giorgi Gobronidze
Owner & CEO
PimEyes

Dear Mr. Gobronidze:

Thank you for your response acknowledging the severity of the privacy and safety concerns posed by your platform. Your response sidesteps the role that your platform specifically plays in perpetuating and broadening the range of these harms. As technology continues to outpace lawmaking, your overreliance on regulatory compliance is an insufficient defense. Additionally, I disagree that this platform empowers the reclaiming of identities more than it compromises them. I am following up in writing to reiterate these concerns.

Your claim that, "[f]ollowing full cooperation, authorities identified **no violations** of applicable data protection law,"[1] places too little emphasis on ethical responsibility and too much on regulatory compliance. Current regulatory frameworks lack sufficient data protection, and mere compliance is not a strict enough threshold in comparison to the possible harms.

Second, you rely heavily on the distinction between biometric identifiers and photographic analysis, which is a semantic rather than substantive distinction. A photo of an individual's face is perhaps one of the best likeness and identity matches, regardless of whether it is arrived at through pixel comparison or biometric data. You have stated in your response that the larger risk to officer safety is already public information that is not generated by PimEyes.[2] Despite the fact that PimEyes does not text search, Mr. Skinner—who used image recognition software such as yours to dox federal officers—has publicly acknowledged that name alone is sufficient to find other personal data regarding an individual or their family online.[3]

Both statements are factual realities: Searching names alone can easily generate corresponding facial matches and searching faces alone can easily lead to names. Therefore, platforms like PimEyes are vital links in the chain of potential harm and are not vindicated by the absence of name identifiers. Even if the software is not technically assigning an identity *during* the search, there is certainly no debate that the process itself is used for the *very purpose* of identification. Lastly, just because no biometric data is stored, the transient processing of facial geometry alone—even temporarily or afterwards deleted—undeniably steps into privacy-regulated territory.

[1] *See* Response to Senator Blackburn.pdf
[2] *Id.*
[3] 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.

Further, you write that, as a necessary measure to enforce "personal-use only" on your platform, "[u]sers agree to self-search only and legitimate personal use."[4] This response shifts responsibility and accountability from the software itself to the users' self-protection. In an age where fine print is small, an agreement to only self-search—if not met with clear enforcement—will result in meaningful consent surrendered and wrongful third-party abuse bypassed.

Finally, although PimEyes does not create the content it indexes and that content is already publicly accessible, your platform amplifies the already available content. Downplaying this reality as a symptom of the open web refuses to take ownership over PimEyes's part in discovering, recovering, concentrating, and linking information once scattered. Accordingly, regardless of the self-characterizations, any legislative or regulatory efforts to combat doxxing, protect law enforcement, or protect personal likeness and data should consider platforms similar to but not exclusive to PimEyes within its scope.

To that end, please respond to the following questions by **5:00 PM on November 7, 2025**:

1. You mention "layered controls" to combat malicious actors. From those controls, please answer the following: How many accounts have been suspended or terminated due to officer targeting? What proportion of misuse is internally detected versus externally reported? Please provide a comprehensive data profile of enforcement and oversight over the past 12 months, categorized by abuse type, enforcement action taken, and any cooperation with U.S. or relevant authorities.

2. You state that users must agree to "self-search only." How does PimEyes verify or audit this claim?

3. You mention child recognition and protection features. Regarding officer safety, are there similar review processes in place for images including uniforms, badges, or public service insignia and can this same scrutiny feature be applied for high-risk roles like law enforcement or federal immigration officers?

Thank you for your attention to this urgent matter.

Sincerely,

Marsha Blackburn
United States Senator

[4] *See* Response to Senator Blackburn.pdf