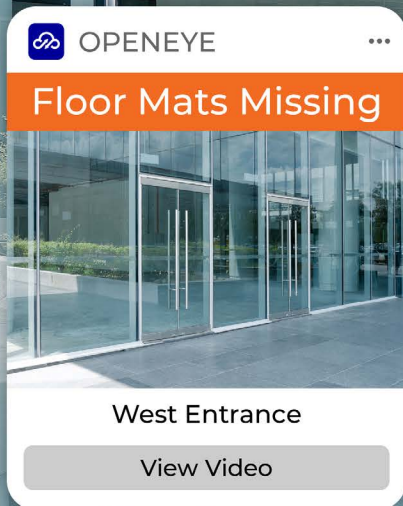


Are the floor mats in place?



TECHNICAL RESOURCE

AI Feature Governance and Moderation Overview

openeye.net



Overview

OpenEye employs AI to help users make video-informed work faster, easier, and more useful. Features such as AI Visual Search and AI Visual Check are designed to reduce manual review, surface relevant information, and help teams respond to operational, safety, and security conditions more efficiently.

This overview explains how OpenEye moderates and safeguards AI-powered video features that use natural-language prompts, visual summaries, thumbnails, alerts, or AI-generated results. It is intended to help customers understand what these features are designed to do, how moderation may affect prompts or configurations, how customer data is protected, and why users should review source video or images before taking action.

AI-Powered Features Covered by This Overview

[AI Visual Search](#) helps users search retained video by describing what they are looking for in natural language. To support search, video-derived visual information may be processed and summarized before a user submits a query. When a user searches, the natural-language prompt is used to find relevant results from that prepared search context.

[AI Visual Check](#) helps users automatically evaluate camera snapshots against predefined or user-defined prompts. Depending on the configured check, the feature may send a thumbnail, prompt, and related context to approved AI infrastructure so the system can determine whether a visual condition appears to be present, not present, or indeterminate.

How OpenEye Moderates and Safeguards AI Use

OpenEye designs, hosts, governs, and moderates its AI-powered features to support responsible customer use in real workflows. For example, AI may help a user search for a delivery vehicle, check whether a shelf appears low on inventory, or flag a visual condition for review, but the user remains responsible for confirming the result and deciding what action to take.

- **Assistive by design:** OpenEye AI features are positioned as decision-support tools. They help users find, interpret, or monitor information more efficiently, while users remain responsible for reviewing results and deciding what action to take.



- **Moderated by design:** OpenEye applies automated, layered controls across AI features to help prevent restricted, prohibited, abusive, or out-of-scope use. User-defined prompts are reviewed by OpenEye safeguards and may be blocked or require revision if they use abusive language, fall outside the feature's intended purpose, or seek to identify a person by name or determine race, ethnicity, religion, disability status, sexual orientation, political beliefs, attractiveness, wealth, age, or other protected or sensitive characteristics.
- **Privacy-conscious by design:** Customer video, images, prompts, and related data are handled under OpenEye's privacy, security, contractual, and compliance practices, including OpenEye's [Privacy Policy](#). OpenEye AI features are designed to work without using customer data to train AI models unless the customer explicitly gives permission.
- **Enterprise-hosted and governed by design:** OpenEye uses commercially supported AI infrastructure designed for **enterprise** use, governance, and operational reliability, rather than public consumer AI services.
- **Verification-oriented by design:** OpenEye communicates limitations and encourages users to verify AI results before relying on them, especially when decisions may have legal, safety, employment, disciplinary, or operational impact.

OpenEye also maintains internal governance processes for AI model use, including vendor and configuration review, access controls, auditing, logging, monitoring, rate limiting, usage tracking, and model lifecycle review where applicable.

Regulatory alignment: OpenEye designs its AI features with awareness of applicable privacy and data protection frameworks, including regulations governing biometric data, video surveillance, and automated decision-making in the regions where its products are used. OpenEye evaluates platform-level regional and compliance considerations as AI features expand. Customers operating in regulated industries or jurisdictions - including those subject to GDPR, CCPA, BIPA, or similar frameworks - should review their own obligations and consult legal counsel as needed. OpenEye's [Privacy Policy](#) provides additional detail on data handling practices.





Accuracy, Limitations, and Human Review

OpenEye AI features are designed to help users find, interpret, or monitor visual information more efficiently, but they do not guarantee that every relevant condition will be detected or that every result is correct. These features are designed to assist with visual review and monitoring - not to serve as facial recognition systems, life-safety alarms, legal evidence tools, or a replacement for human judgment. For decisions with serious consequences, always verify results and follow your organization's established procedures.

- Users should review the underlying video, image, alert, or search result before taking action.
- Single-image checks cannot reliably determine duration, sequence, motion, or what happened before or after the captured moment.
- Overly complex, vague, or multi-condition prompts may produce weaker results. Prompts such as "check whether the fire exit appears blocked" are more useful than broad requests such as "tell me if anything looks wrong."
- AI features should not be relied on as dedicated weapon-detection, threat-detection, emergency-response, or life-safety systems unless expressly documented for that purpose.

Common Questions

Why does OpenEye use AI in video features?

OpenEye uses AI to help customers reduce manual review, identify relevant video faster, automate routine visual checks, and focus attention on conditions that may need follow-up. AI is intended to assist users, not replace human judgment.

What kinds of prompts work best?

Prompts work best when they are objective, specific, and visually observable. Strong prompts describe what the user wants to find or verify, such as a person near an entrance, a delivery vehicle in a parking lot, a blocked exit, a low shelf, or an unattended post. Vague or overly broad prompts may return less useful results.

Can OpenEye AI features identify a specific person?

Results returned are based on similarity confidence and should not be treated as factual determinations. AI Visual Search and AI Visual Check are not intended to identify specific individuals by name or determine a person's private identity. Users should use objective visual descriptions rather than names or identity-based requests.



Can OpenEye AI features detect weapons, emergencies, or life-safety conditions?

OpenEye AI features should not be relied on as dedicated weapon-detection, threat-detection, emergency-response, or life-safety systems. AI outputs may help surface information for review, but users should follow their organization's established safety and emergency procedures.

Can OpenEye AI features read text, logos, license plates, or numbers?

Some AI features may return useful results when text, logos, markings, or numbers are large and clearly visible, but these features are not a substitute for dedicated optical character recognition or license plate recognition unless specifically documented. Users should verify important details directly from the source image or video.

What happens if a prompt is blocked by moderation?

If a prompt is flagged by OpenEye safeguards, the request may not be completed as entered, the configuration may not be saved, or the user may be asked to revise it. Users should rephrase prompts using objective, respectful, visually observable language that stays within the feature's intended purpose.

Can users provide feedback on AI results?

OpenEye provides feedback tools that allow users to report whether AI results were accurate, inaccurate, inappropriate, or otherwise not useful. This feedback helps OpenEye evaluate feature quality, identify false positives and false negatives, improve prompts and safeguards, and prioritize future product improvements. Submitting feedback does not, by itself, give OpenEye permission to use customer video or customer data for model training unless the customer explicitly agrees to that use.

Will OpenEye use my video or data to train AI models?

No, unless the customer explicitly gives OpenEye permission to do so. OpenEye AI features are designed to function without using customer video, images, prompts, or related data to train AI models, and customers do not need to permit model training to use these features. If OpenEye ever requests customer feedback or data for model training or product improvement, OpenEye will explain what is being requested, how it will be used, and how the customer can choose whether to participate.

Who is responsible for ensuring AI features are used in compliance with applicable laws?

OpenEye designs its AI features to support responsible use and applies moderation, safeguards,



and governance practices as described in this overview. However, customers are responsible for determining whether their use of OpenEye AI features complies with the laws, regulations, and internal policies that apply to their organization.

This is especially important for organizations operating in industries or contexts where AI-assisted video analysis may be subject to additional legal requirements, including but not limited to:

- **Workplace monitoring:** employment law, labor agreements, or employee notification requirements
- **Biometric or facial data:** state or regional laws governing the collection or processing of biometric information
- **Law enforcement or investigative use:** evidentiary standards, chain of custody, or civil liberties considerations
- **Healthcare or education environments:** HIPAA, FERPA, or similar sector-specific privacy obligations
- **Public or semi-public spaces:** local surveillance ordinances or consent requirements

If you are unsure whether your intended use of OpenEye AI features is permissible under applicable law, OpenEye recommends consulting your legal counsel before deploying or configuring these features. OpenEye support and account teams can help clarify how features work but cannot provide legal advice.

Are AI results always accurate?

No. AI can help users evaluate information more efficiently, but results may be inaccurate, incomplete, inappropriate, or indeterminate. Users should review the underlying video, image, or alert context before taking action, especially for decisions with legal, safety, employment, disciplinary, or operational impact.

OpenEye will continue updating safeguards as AI capabilities, customer needs, and regulatory expectations evolve.



For more information, visit openeye.net
or experience a demo at openeye.net/demo