OLOID Unveils Next-Gen Privacy Architecture for Facial Biometric Security

New controls include customer-managed keys for FaceVault™, on-device storage, and AI-synthesized likenesses, ensuring biometric privacy at enterprise scale.

SUNNYVALE, CA, UNITED STATES, July 9, 2025 /EINPresswire.com/ -- OLOID, a leader in passwordless identity and access solutions, today announced its newly enhanced Privacy Architecture for facial-biometric authentication, setting a new benchmark for enterprise-grade privacy and compliance. The FaceVault™ platform design integrates advanced features such as customer-managed encryption (BYOK), on-device template storage, zero-image capture modes, and AI-generated synthetic likenesses that collectively redefine how biometric privacy is implemented at scale.

> We built OLOID FaceVault™ on a simple principle: a facial template should never be a liability. Our architecture lets each customer decide what is stored, who can decrypt it, and when it can be used.”
>
> *Madhu Madhusudhanan, Co-founder & CTO, OLOID*

Unlike credentials that can be rotated or replaced, a person’s face is immutable. This reality demands a fundamentally more rigorous approach to privacy engineering. OLOID has designed this architecture from the ground up to align with the strictest global regulations, including GDPR, CCPA, HIPAA, and BIPA, while maintaining sub-second authentication speeds across cloud, on-prem, and edge environments.

“Privacy is a fundamental human right, and the face is our most personal identifier, so safeguarding facial biometrics must be an absolute priority,” said Madhu Madhusudhanan, Co-founder and CTO of OLOID. “We built OLOID FaceVault™ on a simple principle: a facial template should never become a liability. Our architecture lets each customer decide exactly what is stored, who can decrypt it, and when it can be used. Stripped of context and sealed behind customer-owned keys, a stolen template is worthless to hackers and even to us. That’s privacy by design with zero impact on user convenience.”

Key Components of OLOID’s Privacy Architecture

FaceVault™ with Customer-Managed Keys (BYOK): Biometric templates are generated on the user’s device or in the cloud, irreversibly encoded and encrypted. Customers can manage their own encryption keys, ensuring that OLOID cannot access or decrypt biometric data, delivering

true separation of duties.

Zero Image Capture Mode: Administrators can enable a configuration where raw face images are never stored. Even the image used for feature extraction exists only in RAM for milliseconds before being purged, satisfying GDPR's data minimization and storage limitation principles.

On-Device & On-Premise Processing Options: For air-gapped or classified environments, OLOID offers on-premises biometric vaults and edge-only deployments. Templates and matching can be performed entirely within secure local modules using Trusted Platform Modules (TPMs) or Secure Enclaves, never leaving the device or local network.

Granular Consent & Revocation Controls: OLOID's consent engine supports region-aware workflows with legal-specific opt-in flows, immutable audit logging, and single-click revocation. Users retain continuous control over their biometric data, with real-time deactivation of templates across all endpoints.

Synthetic Likeness Generation: During enrollment, a privacy-preserving synthetic likeness is generated for visual use in ID badges and admin UIs. These AI-generated images resemble the user without being reverse-matchable, removing the need to store actual photos.

Future-Proof Cryptography Roadmap (CY 2025–2026)

OLOID is actively building toward the next frontier in secure biometric computing with cryptographic upgrades that ensure resilience against insider threats and quantum-era vulnerabilities:

* Homomorphic Encryption Matching: OLOID will support fully encrypted biometric matching (CKKS-based FHE), enabling facial comparisons to occur without ever decrypting templates, even in RAM.
* Federated Learning for Templates: Biometric models will update directly on-device, with only anonymized deltas transmitted for global improvements, never face data itself.
* Zero-Knowledge Face Verification: Future updates will include support for cryptographic proofs that verify matches without revealing biometric templates. This is ideal for multi-tenant or third-party environments.
* Differentially Private Analytics: Operational metrics will include noise-injected insights to protect against re-identification while still enabling usage reporting and performance tuning.

Built-In Compliance & Governance

OLOID's platform maps directly to the requirements of leading global regulations:

* GDPR / CPRA: Supports explicit opt-in, the right to be forgotten, and data minimization principles.

* HIPAA & EPCS: Enables local processing and audit trails for electronic protected health information (ePHI) and E-prescriptions for Controlled Substances.
* BIPA & State Laws: Ensures written consent, limited data retention, and irrevocable deletion upon purpose fulfillment.

All administrative actions are secured with multi-factor authentication, logged immutably, and retained for seven years. OLOID undergoes annual SOC 2 Type II certification and independent penetration testing, and follows a Secure SDLC process, including static/dynamic analysis and peer review.

“CISOs have long wanted to adopt facial biometrics without sacrificing data governance,” said Shankar Agarwal, Co-founder and General Manager of OLOID. “With this launch, we’ve eliminated that tradeoff. Enterprises now get sub-second facial authentication and complete control over how biometric data is stored, processed, and protected. This is how modern identity should work: secure, privacy first, and seamless.”

Tailored Deployment Models

From retail and healthcare to manufacturing and defense, OLOID’s flexible deployment options let enterprises align identity verification with their risk posture:

* Cloud with BYOK for scalability and managed compliance
* On-premises deployment for full data residency
* Edge-only mode for offline, high-privacy scenarios

Every customer, whether operating globally or in a single high-security facility, can apply the same core platform in a configuration that meets their privacy, performance, and regulatory needs.

About OLOID

OLOID provides a passwordless identity platform tailored for frontline employees. Fortune 500 companies in manufacturing, retail, healthcare, pharmaceutical, and other frontline industries use OLOID to authenticate workers through physical factors such as facial recognition, NFC, and RFID badges, along with other methods suited to a deskless workforce, while meeting the security and regulatory requirements specific to each industry.

Headquartered in Sunnyvale, California, OLOID is backed by leading investors including Dell Technologies Capital, Yaletown Partners, Honeywell Ventures, Okta Ventures, Unusual Ventures, and Emergent Capital. It is trusted by Fortune 100 companies across manufacturing, healthcare, retail, pharmaceutical, and more.

To learn more, visit www.oloid.com.

Garima Bharti Mehta
OLOID INC.
+1 800-711-9123
email us here