# Trust Without Biometric Custody

### The core security problem

*A password can be reset. A face, fingerprint, iris or voice cannot.* When a password database is breached, credentials can be revoked and replaced. When a persistent biometric template or repository is compromised, the underlying human characteristic is effectively exposed for life. The individual cannot issue themselves a new face, fingerprint or iris. That makes unnecessary biometric custody a uniquely durable security and privacy risk**.**

### The CypherEye proposition

**CypherEye separates verification from biometric custody.** Authorized multimodal biological, behavioral, device and environmental signals can be evaluated by the Human Factor Authentication (HFA) layer. The relying service receives a real-time Trust Score or signed trust assertion—not the underlying biometric repository it would otherwise need to collect, retain, protect and eventually delete.

| LIVE HUMAN | → | CYPHEREYE HFA | → | RELYING SERVICE |
|---|---|---|---|---|
| Authorized human signals | | Continuous multimodal verification Trust Score generated | | Consumes trust Minimizes biometric custody |

## The architectural shift

| | CONVENTIONAL BIOMETRIC MODEL | CYPHEREYE TRUST-LAYER MODEL |
|---|---|---|
| **Service receives** | Biometric image/template + result | Trust Score / signed trust assertion |
| **Service retains** | Potential biometric repository or template | Potentially no new raw-biometric repository |
| **Breach consequence** | Potentially persistent identity exposure | Trust credential can be rotated/reissued |
| **User experience** | Enrollment + repeated point checks | Seamless, continuous, passive assurance |

***Why store the biometric when all a service needs is the trust?***

## Biometric custody is already a global reality

The risk is not limited to raw photographs. Templates, embeddings and face vectors can remain persistent biometric representations and may themselves be sensitive or regulated.

## Representative commercial examples

| SERVICE | BIOMETRIC APPROACH | USE |
|---|---|---|
| **CLEAR** | Face and other biometric identifiers used for enrollment and verification. | Airport/access identity |
| **Jumio / Veriff / AU10TIX** | Facial images and derived biometric data used for remote identity verification and authentication. | KYC, onboarding, fraud |
| **Amazon Rekognition / Azure AI Face** | Cloud services can persist mathematical face vectors or extracted face features for later matching. | Enterprise identity systems |

## Representative governmental system examples

| SYSTEM | BIOMETRICS | PURPOSE |
|---|---|---|
| **U.S. DHS / FBI** | Fingerprints, facial images, iris and related identity data | Borders, immigration, law enforcement and authorized civil uses |
| **U.S. CBP** | Facial comparison using government-held traveler images | Airport, seaport, land-borders |
| **Russia EBS** | Face and voice | Government and commercial authentication |
| **China public-security programs** | Multiple biometric modalities in documented programs | Identification, public security and surveillance |

## Regulation is moving towards data custody minimization

| JURISDICTION | DIRECTION OF TRAVEL |
|---|---|
| **Illinois BIPA** | Notice, written release, public retention/destruction policy, restrictions on disclosure/sale and destruction |
| **Colorado** | Consent plus written biometric policies covering retention, deletion and security-incident response. |
| **California CCPA/CPRA** | Biometric information used to uniquely identify a consumer is sensitive personal information. |
| **European Union GDPR** | Biometric data used for uniquely identifying a person is special-category personal data and receives heightened protection. |

### Privacy by architecture—not merely by policy

*The strongest privacy architecture is not simply a better-protected biometric database.* It is an architecture that asks whether the database needs to exist at the relying service in the first place. CypherEye can reduce the amount of sensitive information a retailer, bank, airport, building operator or government checkpoint needs to receive and retain.

World ID provides a useful adjacent example of this direction. Its current documentation says Orb images and iris codes are sent to the user's phone and deleted from the Orb, while anonymized multi-party computation is used for uniqueness checks; relying parties do not receive the underlying face/eye images or iris code.

***The Design Principle: Do not send the biometric when the service only needs the answer***

## CypherEye – a more defensible security and privacy architecture

- CypherEye is designed to control the collection, transmission and retention of biometric data at the source
- CypherEye can allow a service to consume a real-time Trust Score or signed trust assertion rather than maintaining its own biometric repository.
- Reducing biometric custody reduces the number of repositories, copies, integrations and retention obligations that can become targets for attack.
- A Trust Score is revocable and replaceable; the underlying human biometric is not.

| TRUST SCORE | LIVE HUMAN | AUTHORIZED HUMAN | CONTINUITY |
|---|---|---|---|
| e.g., 97/100 confidence | present / not present | matched to authorized relationship | confidence that the same human remains behind the session |

***Verify the person, relay the trust and maintain user custody of the biometric data***

## Selected source basis

- CLEAR Privacy Policy and Member Terms (2026): biometric data includes faceprints, fingerprints, iris scans and related images/video; terms address collection and storage.
- Jumio Online Services Privacy Notice (Aug. 4, 2026) and Jumio Authentication materials: collection/retention of facial and biometric data and template-based authentication.
- Veriff Privacy Notice and Biometric Authentication service description (2026): face-scan information and saved biometric sets for ongoing authentication.
- Amazon Rekognition documentation: server-side Collections store mathematical face vectors/user vectors for search and identity verification.
- Microsoft Azure AI Face documentation: persisted face features/templates in PersonGroup/LargePersonGroup/PersonDirectory structures.
- AU10TIX Privacy Notice (Aug. 19, 2026): biometric ID/selfie verification and age-assurance services.
- Facephi product/compliance materials: facial, fingerprint, voice and behavioral biometric identity/authentication capabilities across international deployments.
- World / Tools for Humanity privacy materials (2026): personal custody, on-device processing and anonymized multi-party computation as an example of minimizing biometric exposure to relying parties.
- Illinois BIPA §15; Colorado HB24-1130; California CCPA/CPRA; EU GDPR Article 9.