Privacy Governance and Revocation for Biological Identity

by Nick Clark | Published March 27, 2026 | PDF

Biological identity systems handle the most sensitive personal data that exists: the features of a person's body. Privacy governance defines the complete framework for how this data is collected, processed, retained, and revoked. Every operation is subject to explicit policy, every processing step minimizes data exposure, and every individual retains the right to revoke their biological identity participation.

What It Is

Privacy governance for biological identity encompasses the full set of policies governing biological data handling: collection consent, processing limitations, retention rules, access controls, audit requirements, and revocation rights. These policies are enforced structurally through the governance framework rather than through organizational processes.

Revocation mechanisms enable individuals to withdraw from biological identity participation, triggering the governed deletion of their trust slope data while maintaining audit records of the revocation itself.

Why It Matters

Biological data is irrevocable in a way that passwords and tokens are not. A compromised password can be changed. A compromised biometric template cannot. This makes privacy governance for biological identity not merely desirable but essential. The consequences of privacy failure are permanent.

Regulatory frameworks worldwide increasingly mandate specific protections for biometric data. The governance framework provides the structural mechanisms to demonstrate compliance with these requirements.

How It Works

Every biological observation is processed under a data minimization principle: only the information needed for the specific identity operation is retained, and it is retained only as long as necessary. Raw biological signals are processed and discarded. Only derived hashes and trust slope metadata persist.

Revocation triggers a governed deletion process that removes all trust slope data associated with the revoking individual while preserving audit records. The deletion is verified and the verification is recorded. Post-revocation, the individual's biological observations produce no matches in the system.

What It Enables

Privacy governance enables biological identity systems that comply with regulations such as GDPR, BIPA, and emerging biometric privacy laws worldwide. It ensures that individuals retain meaningful control over their biological data even within systems designed for persistent identity. This governance is not an add-on but a structural component of the architecture.

Biological Identity All 21 steps →

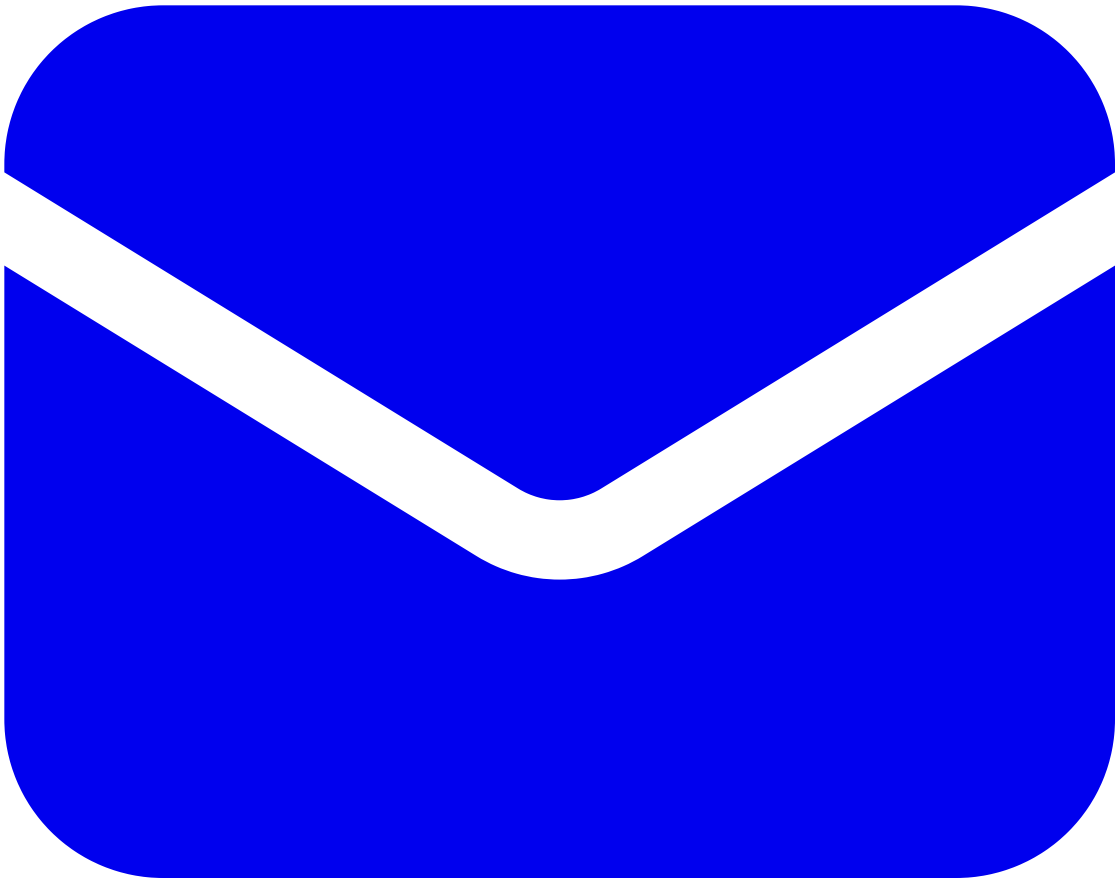
Identity from behavioral continuity. No stored templates. No keys.

Primary Technical Disclosure
○ Continuity-Based Biological Identity Using Trust-Slope Validation
Secondary Technical
○ Biological Trust Slope Construction: Identity Through Behavioral Continuity○ Contact, Non-Contact, and Passive Resolution Modes for Biological Identity○ Biological Hash Generation With Domain Separation○ Biological State Inference From Continuity Baseline○ Cross-Modal Biological Hash Fusion○ Biological Continuity as Handoff Verification○ Relational Trust Trajectories: Trust as Temporal Relationship○ Identity as Behavioral Continuity: Beyond Single-Point Capture○ Biological-Device-Agent Identity Layering○ Biological Signal Acquisition Tiers○ Noise-Tolerant Feature Normalization for Biological Signals○ Stable Sketching and Helper Data for Biological Features○ Predictive Identity Trajectory: Forecasting Biological Identity Evolution○ Population-Scale Collision Resistance for Biological Hashes○ Adaptive Indexing of Biological Trust Slopes○ Delayed and Sparse Validation for Disconnected Environments○ Policy-Governed Capability Binding for Biological Identity○ Multi-Identity Delegation Without Biological Data Disclosure○ External Credential Integration With Trust-Slope Integrity○ Anti-Spoofing Through Continuity Validation○ Identity Lifecycle Management and Phase-Based Reseeding○ Quorum-Based Biological Identity Recovery● Privacy Governance and Revocation for Biological Identity○ Human-Agent Primitive Integration for Biological Identity
Applications (General)
○ Airport Security Without Biometric Databases○ Estate Verification Through Behavioral Continuity○ Biological Identity for Elder Care Continuity○ Biological Identity for Child Development Tracking○ Biological Identity for Addiction Recovery Monitoring○ Biological Identity for Workplace Safety Monitoring○ Biological Identity for Athletic Performance○ Biological Identity for Immigration Processing
Applications (Specific)
○ TSA PreCheck Matches Templates, Not Continuity○ Global Entry Verifies Documents, Not Biological Continuity○ Face ID Matches a Stored Model, Not a Living Trajectory○ Samsung Knox Guards the Container, Not the Identity○ ID.me Verifies Documents, Not Biological Continuity○ Socure Scores Risk at a Single Point in Time○ Plaid Identity Verifies Financial Accounts, Not Biological Persons○ Onfido Detects Document Fraud, Not Identity Drift○ Veriff Captures Sessions, Not Trajectories○ Trulioo Queries Databases, Not Biological Trajectories
Biological Identity overview →
AQ
deterministic
autonomy

Legal

Subject to one or more pending U.S. and international patent applications, see Patents for the current list and status. No license, express or implied, is granted. Any use requires a separate written agreement—see Licensing. Patent applications referenced on this site are pending. Claim scope, if any, is subject to examination and may issue in altered form or not at all. See Legal for terms and conditions.

Last updated: 2026-03-03



-
- nick@qu3ry.net
- 72 28 14 36 01

Invented by Nick Clark | Founding Investors: Devin Wilkie