

ObscureIQ's Guide to Biometric Identifiers - Executive Threat Edition (2025)

Scale	Part	Ico	Biometric Identifier	Block Difficulty	Reveals Sensitive Info	Adversary Value	Description	Venue(s)	Threat Vector(s)	Adversary / Surveillance Use Cases
Potential	BRAIN		Brain Imaging	High	Very High	Medium-High	Uses CT/MRI/PET/EEG scans to analyze brain structures and activity. Promising for medical ID but raises major privacy risks if used outside healthcare.	Healthcare, Research Labs, Espionage	Blackmail, Coercion, Espionage	Extracting subconscious data under coercion; espionage via inferred thoughts; blackmail from mental health or stress patterns.
Growing	BRAIN		Brainwave Signatures (BCI)	Medium	Very High	Medium-High	Captures EEG patterns via brain-computer interfaces for identity verification. Offers strong uniqueness but risks exposing subconscious data.	Healthcare, Research Labs, Espionage	Blackmail, Coercion, Espionage	Extracting subconscious data under coercion; espionage via inferred thoughts; blackmail from mental health or stress patterns.
Common	DNA		DNA Matching	Very High	Very High	High	Uses genetic markers to identify individuals or family relationships. Widely used in forensics and genealogy, but DNA permanence poses privacy risks.	Healthcare, Labs, Borders	Blackmail, Discrimination, Deanonymization	Blackmail using genetic predispositions; targeting minorities or dissidents; building shadow DNA registries; exposing family connections.
Growing	MULTI		Emotional AI	High	High	High	Analyzes facial expressions, voice, and behavior to infer emotions. Useful in marketing and education but criticized for accuracy and bias risks.	Workplace, Interrogation, Public Space	Manipulation, Coercion, Social Scoring	Interrogation and lie detection under duress; workplace micromanagement; manipulation by detecting emotional weakness; political social scoring.
Top	FACE		Facial Recognition	High	Medium	Very High	Analyzes facial features for identification and verification. Widely adopted in law enforcement and devices, but criticized for bias and misuse.	Generic	Tracking	Generic biometric exploitation for tracking, coercion, or blackmail; adaptable to workplace surveillance or authoritarian control.
Rare	FINGER		Fingernail Recognition	Medium	Low	High	Analyzes nail bed patterns for ID. Experimental and supplemental, not widely adopted.	Digital Devices, Law Enforcement, Checkpoints	Evidence Manipulation, Coercion, Tracking	Covert harvesting of prints/geometry from surfaces or devices; forced unlocks in custody; planting fake evidence; integration into state databases for persistent tracking.
Growing	WALK		Gait Recognition	High	Low	High	Identifies individuals by their walking style. Useful in surveillance and forensics, but accuracy drops with injury or disguise.	Public Space, Protests, Smart Cities	Tracking, Deanonymization	Tracking at distance even when masked; identifying disguised persons in crowds; surveilling protesters who obscure faces.
Top	HAND		Hand Vein Recognition	Medium	Low	High	Vein recognition is a type of biometrics that can be used to identify individuals based on the vein patterns in the human finger or palm.	Digital Devices, Law Enforcement, Checkpoints	Evidence Manipulation, Coercion, Tracking	Covert harvesting of prints/geometry from surfaces or devices; forced unlocks in custody; planting fake evidence; integration into state databases for persistent tracking.
Top	EYE		Iris Recognition	High	Low	High	Analyzes iris texture for identity verification. Highly accurate and widely deployed in border control and smartphones, though spoofing risks exist.	Borders/Checkpoints, Secure Facilities	Identification, Discrimination, Tracking	Forced enrollment at checkpoints; covert surveillance of high-security areas; potential exclusion or discrimination via access control systems.
Potential	FACE		Micro-expression Analysis	Medium	Medium	Medium	Captures split-second facial expressions for ID and intent detection. Risk of false positives limits adoption in security.	Workplace, Interrogation, Public Space	Manipulation, Coercion, Social Scoring	Interrogation and lie detection under duress; workplace micromanagement; manipulation by detecting emotional weakness; political social scoring.
Rare	EYE		Retina Recognition	High	Low	High	Maps blood vessel patterns in the retina for ID. Extremely accurate but requires intrusive hardware, limiting mass adoption.	Borders/Checkpoints, Secure Facilities	Identification, Discrimination, Tracking	Forced enrollment at checkpoints; covert surveillance of high-security areas; potential exclusion or discrimination via access control systems.
Top	VOICE		Voice Recognition	Medium	Medium	High	Verifies a claimed identity via voice. Convenient but vulnerable to deepfakes and replay attacks.	Public Space, Online, Telecom	Deanonymization, Impersonation, Fraud, Tracking	Bulk monitoring of calls/VOIP; deanonymizing activists via voiceprints; fraud via AI voice cloning/replay; identifying dissenters in group audio.