The Price of Access

Biometrics & Financial Inclusion

The past can't be changed, but the standard can.

Introducing Fine Print Partners

Emalee Postma
Finance ’26

Ashley Fearday
Finance & Econ ’27

Emma Takacs
Accounting ’29

David Goodwin
Finance & International Business ’27

Dario Benes
Finance ’27

Our Client: Access Now Board of Directors

What is Access Now?

- Nonprofit digital rights organization
- Focuses on privacy, surveillance, digital governance

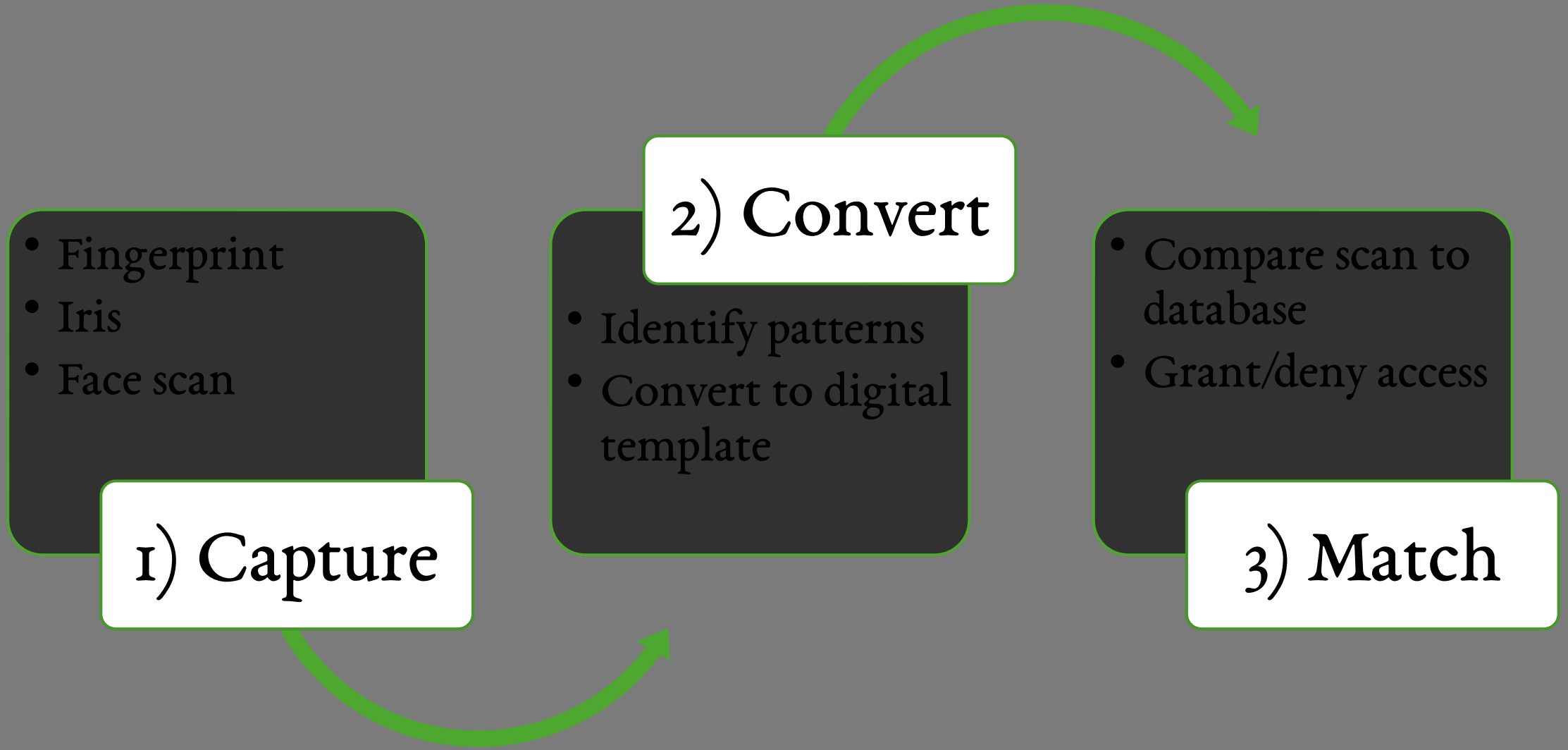
What does Access Now do?

- Leads the #WHYID campaign focused on digital risks
- Engages with governments and international institutions

Where can Access Now Improve?

- Standards are voluntary but not enforceable
- Adoption is inconsistent across jurisdictions

How do Biometric Systems Work?



Why is Biometric Capture an Ethical Problem?

accessnow

There was a promise of inclusion, but it came at the cost of fairness, respect, and duty of care

The Breach

Identity can't be reset
Unlike Passwords, theft is permanent

Fraudulent debt in their name
Legally liable with $2-4 daily income

Redirected Government benefits
Financial, health, and food aid lost

VS

The Consequence

No legal recourse
No bureau or lawyer to call

Exclusion from the system
Locked out of the system made to help them

Physical safety risks
Databases weaponized for targeting

Those with the least resources are those least able to recover from theft

Inclusion vs Rights: Advancing SDG 10 may conflict with SDG 16

Do biometric identity systems expand access, or create structural risks that conflict with fundamental rights?

SDG 10:
Reduce inequality within and among countries.

SDG 16:
Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels.

Why act now?

Biometric financial systems are hitting mass adoption at the exact moment their vulnerabilities are becoming easier to exploit and harder to reverse.

Rapid Scaling

2.3 Billion+

Monthly authentications in India alone. Biometric authentication is no longer experimental tech.

Active Threat

+40% YOY Surge

in real-world cases of fingerprint and iris spoofing bypassing authentication systems.

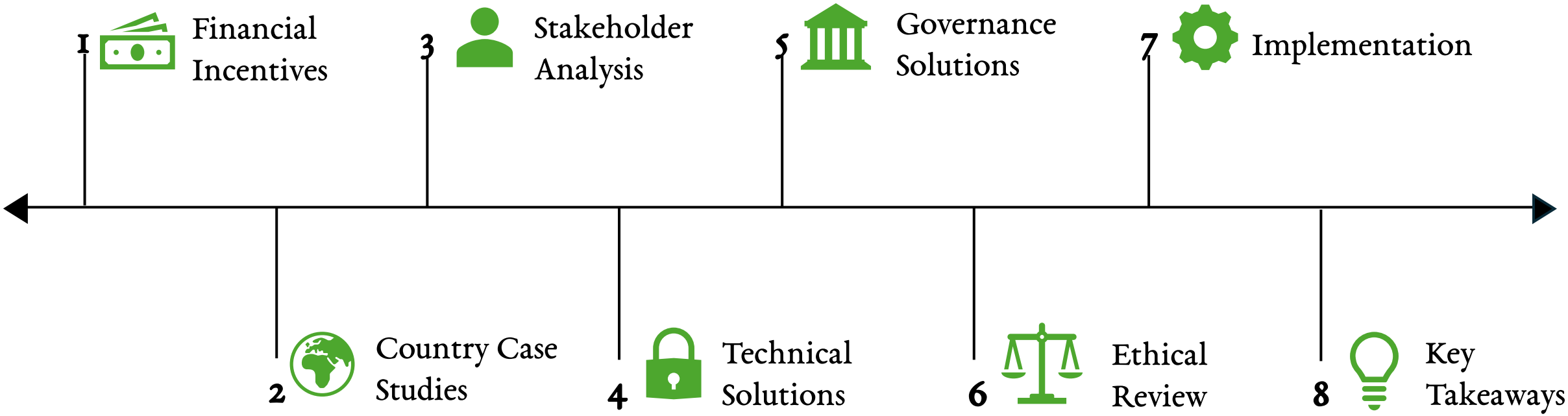
Timing Gap

$11.4B → **$42B**

2026 **2035**

The biometric banking market is expected to nearly quadruple in size over the next decade.

Presentation Timeline



What is the value behind biometric data?

Biometric financial inclusion could unlock ~$3.7 trillion in GDP (McKinsey)

Supply-Side Economics

- Low per-user acquisition cost (~$54 in crypto per iris scan)
- Monetized via identity-as-a-service, data licensing, token economics
- Margin structure incentivizes volume over consent quality

Regulatory Arbitrage

- Deliberate deployment in countries with weak data protection laws
- 22 African nations have zero data protection legislation
- Lower regulatory cost = higher margins

What the User Gets

~$54 in volatile crypto

VS

What the Company Gets

Permanent, irrevocable biometric data + network growth

SDG Tension: Financial incentives are structurally misaligned; companies profit most in the exact environments where users are most vulnerable.

Kenya: Worldcoin (East Africa)

Iris Scans for Cryptocurrency - Consent or Coercion?

~$54
Paid per iris scan

18+
Orb scan venues in Nairobi

2026
Data finally deleted

Source: National Media Group

Sam Altman. Source: CNBC

- **2022–23**
  Nairobi public launch; government suspension
- **Aug 2023**
  Kenya's Ministry of Interior suspension; High Court agreed
- **Sept 2023**
  ODPC cancels Worldcoin's registration certificates
- **Jan 2026**
  Data deleted, prior exposure unclear

West Africa: Mastercard/GAVI "Wellness Pass"

accessnow

When Vaccine Access Becomes a Gateway to Biometric Enrollment

2020
Program launched

8+
African countries targeted

30M
People to be onboarded

"More aimed at promoting the health of markets for vaccines, not the health of individuals."
- Privacy International

Gavi's Wellness Pass
Health data fused with payments

Trust Stamp's "Evergreen Hash"
Technology built for surveillance repurposed for "aid"

Vulnerable Countries Targeted
No legal framework before rollout

Santoshi Kumari: The Human Cost

Santoshi Kumari • 2006–2017

"She spent her final days begging for a bowl of rice."

In 2017, 11-year-old Santoshi died in Jharkhand, India. Not from famine, but because a digital database failed to recognize her family. While the government fought fraud, a real child starved.

A Family Blocked

No match, no food; for months.

A System That Couldn't See Her

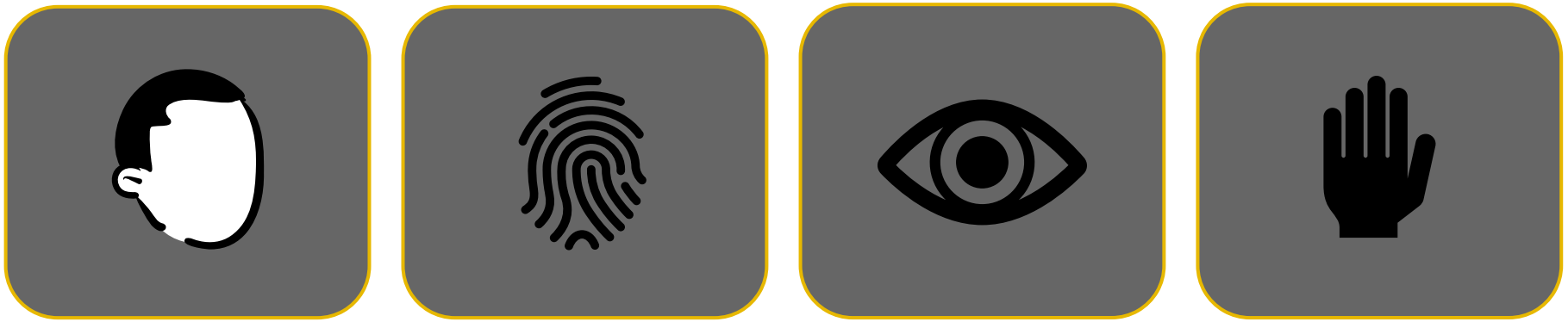
The database saw errors, not a starving child.

A Life Reduced to a Data Point

Efficiency over people.

When systems see data points instead of people, the most vulnerable pay the price.

India: Authentication with Aadhaar



Why?

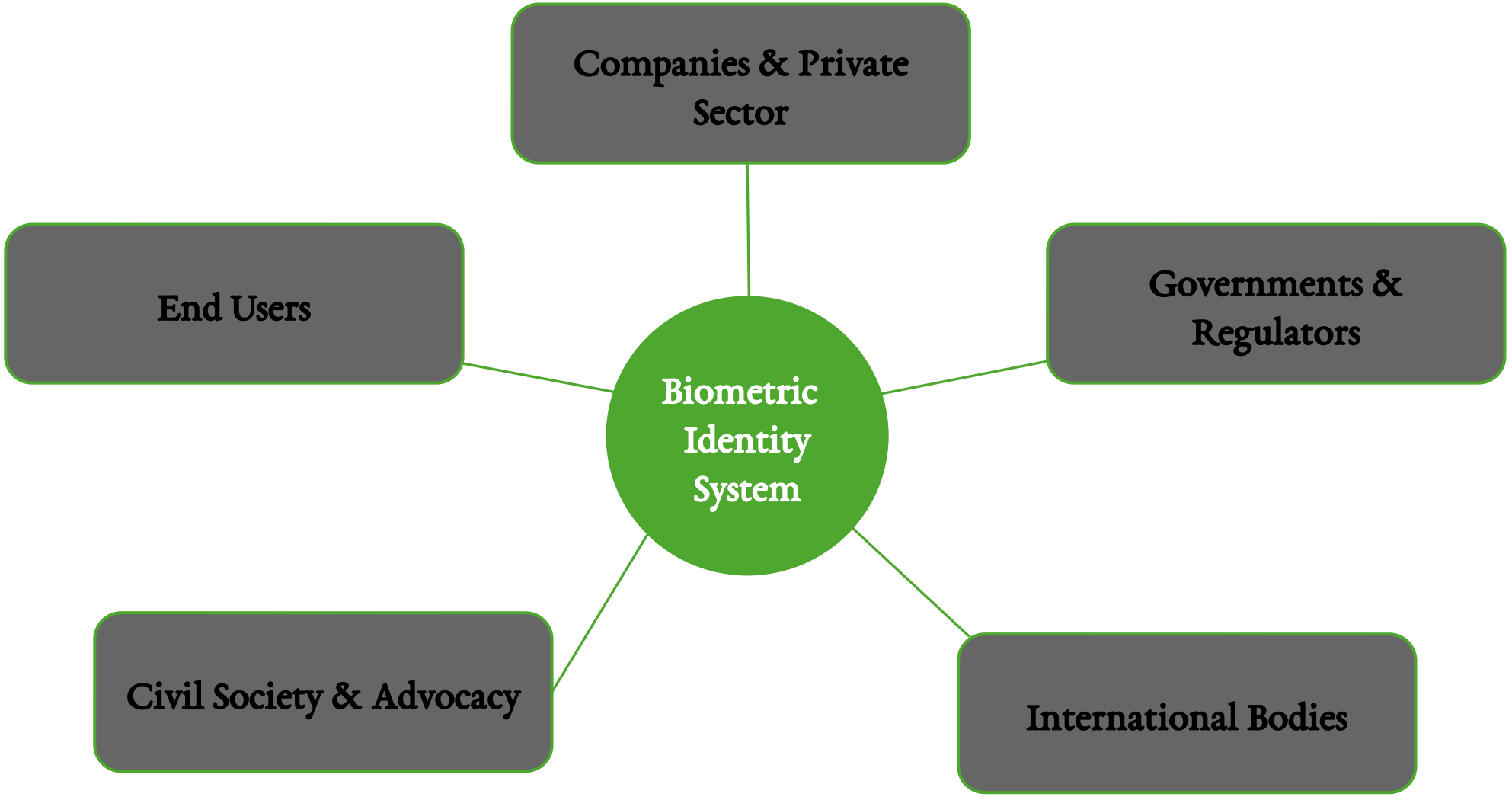
- Paperless authentications
- Complies ID documents to one number
- Easy Access and faster onboarding

Benefits

- No duplicates
- Body is legal document
- Government pays social benefits into biometric-linked accounts

AADHAAR

Who is impacted?



End Users

Those who see biometric capture as a ticket to financial inclusion

1.3B unbanked (Global South)

Existing Users

Targeted Communities

Companies & Private Sector

Those who benefit

Players

e-world

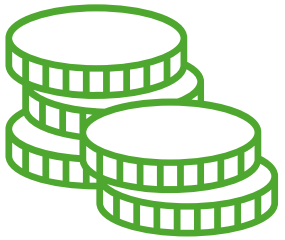
AADHAAR

mastercard

TrustStamp

Gavi The Vaccine Alliance

Incentives



Biometric involvement data has commercial value

Biometric Fintech
Banks using KYC
Data Brokers

Selling Data
First Mover Advantage
Financial Leverage

Governments & Regulators

accessnow

Those who set the rules

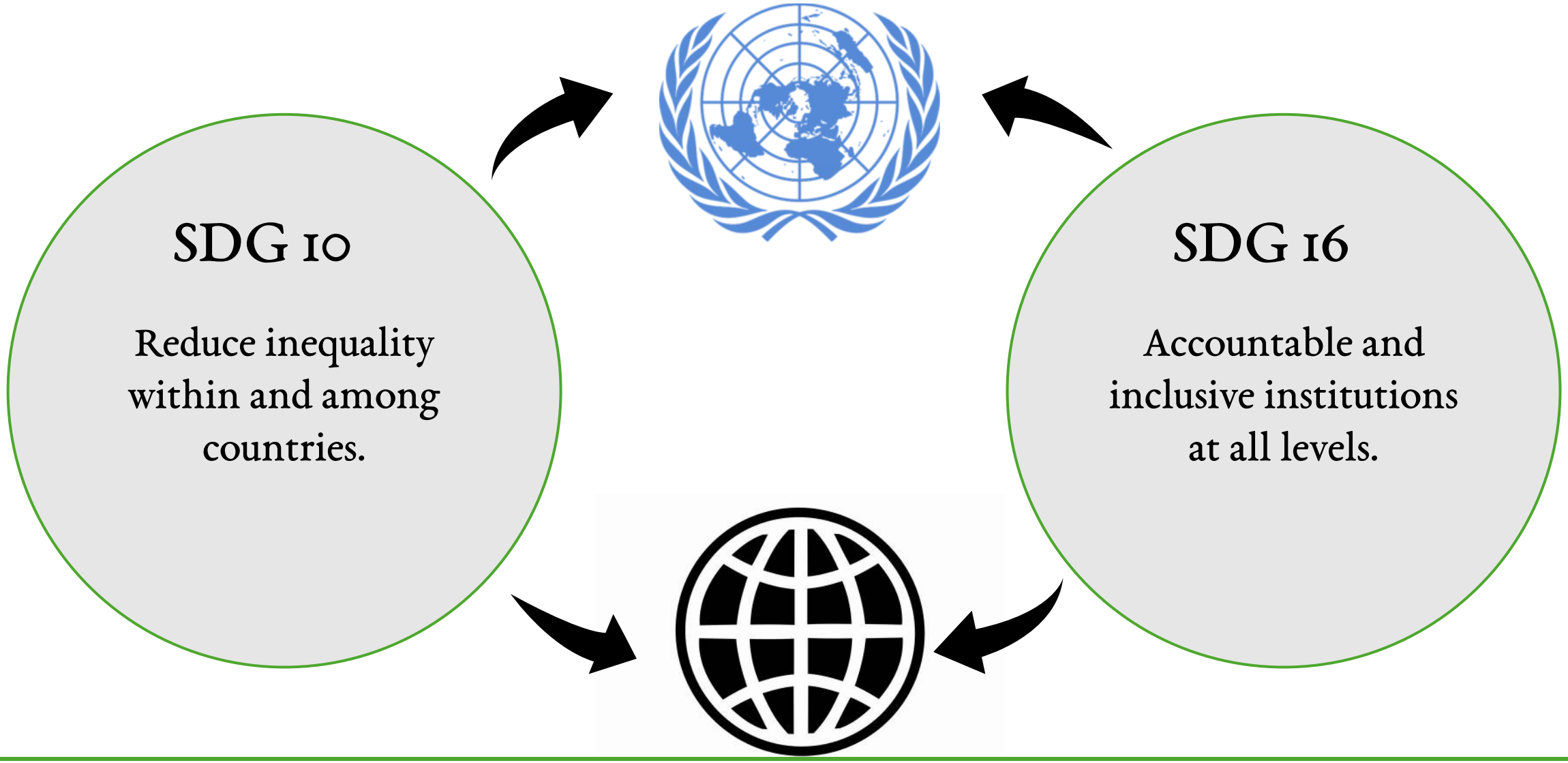
Current Legal Bodies

- Kenya's ODPC
- India's UIDAI
- EU's GDPR

Vulnerabilities

- 22 African states don't have a framework
- Another reason for them to be a target

International Bodies



Civil Societies

accessnow

Don't make the rules or enforce them; the voice of the people

Non-Profits

Mission driven groups that invest resources into their causes

NGO's

Separate entities than governments that deliver support, aid, services.

Advocacy Groups

Groups that campaign for policy change on behalf of the at-risk

Journalists

Investigators that expose how systems affect people bringing stories to light.

Our Two-Part Solution: Infrastructure & Oversight

Privacy-Preserving Infrastructure

How we protect data

- Cryptographic Verification
- User Controlled Identity
- Revocable Biometrics

Governance Standards

How we enforce accountability

- Transparency Standards
- Consent Standards
- Data Protection
- Oversight & Accountability

Privacy-Preserving Infrastructure

accessnow

Cryptographic Verification

Mathematic algorithms confirm identity without exposing biometric data

Ex: Zero-Knowledge Proofs (ZKPs)

User-Controlled Identity

Gives individuals ownership over what data is shared

Ex: Self-Sovereign Identity (SSI)

Revocable Biometrics

Systems store a transformed version of the raw biometric

Ex: Cancelable Biometrics

Financial Cost to Implement Privacy-Preserving Technologies

accessnow

⚠ Cost of Inaction

Average Data Breach
$4.4M global / $10.2M in U.S.

Biometric-Specific Fines
Meta: $1.4B / Clearview AI: €30.5M

Regulatory Precedents
GDPR: €5.8B in fines since 2018

Cost of Action

Zero-Knowledge Proofs
$7.59B market by 2033 (22.1% CAGR)

Self-Sovereign Identity
Per-credential cost: fractions of a cent

Cancelable Biometrics
Software-layer; near-zero marginal cost per user

Prevention is cheaper than the penalty. Privacy-preserving infrastructure is not just ethically sound, it is financially rational.

Governance Standards

accessnow

Transparency Requirements

Consent Standards

Data Protection

Oversight & Accountability

- Disclose how biometric data is collected, used and stored
- Clarify data ownership and third-party sharing
- Communicate policies in clear and accessible language

Governance Standards

Transparency Requirements | **Consent Standards** | **Data Protection** | **Oversight & Accountability**

- Require explicit, opt-in consent for all data collection
- Prohibit coercive incentives or conditional access to services
- Guarantee opt-out with equivalent non-biometric alternatives

Governance Standards

accessnow

Transparency Requirements

Consent Standards

Data Protection

Oversight & Accountability

- Limit data collection to what is strictly necessary
- Enforce defined retention periods and secure deletion
- Align with frameworks like the General Data Protection Regulation (GDPR)

Governance Standards

Transparency Requirements

Consent Standards

Data Protection

Oversight & Accountability

- Mandate independent audits and compliance reviews
- Establish enforceable regulatory standards and penalties
- Require organizations to demonstrate ongoing risk mitigation

Regional Regulations

U.S.
Gramm-Leach-Bliley Act (GLBA)

- Only Financial Institutions
- Privacy Rule (telling you how your info is shared)
- Safeguards Rule (requiring a written security plan)
- Requires "opt-out"

Illinois
Biometric Information Privacy Act (BIPA)

- All organizations (Excluding Financial Institutions)
- Requires deletion once purpose for collection is fulfilled
- Requires consent

Europe
General Data Protection Regulation (GDPR)

- All Institutions handling personal data
- Requires "opt-in"

What are the Tangible Harms & Goods?

accessnow

STAKEHOLDER	Current System	→	Proposed Solution	NET CHANGE
End User	Permanent harm		Protected access	↑ Major gain
Companies & Private Sector	Profits from data		Constrained profit	— Neutral
Governments & Regulators	Limited capacity		Enforceable tools	↑ Gain
International Bodies	SDG gap widens		SDG goals served	↑ Gain
Civil Societies	Bears the fallout		Mission advanced	↑ Major gain

Are the Actions Defensible?

accessnow

Current – Not Defensible

Known risk, ignored

The harm was foreseeable and unregulated execution was deliberate

Good intent isn't a defense

Exposing people to known permanent harm while trying to help is contradictory

Not a fair system

No reasonable designer of this system would accept the current security systems

Proposed – Defensible

Preserves the good

Maintained financial access ready to scale safely

Fairly redistributes risk

Those who profit now carry the liability

Brings honesty to the business model

It doesn't kill the incentive but aligns it with the mission

What Ethical Value Does the Solution Advance?

Each maps to a failure in the current system and a concrete repair in the proposed solution

01

Dignity

Individuals gain back control over their identity

Your body isn't a data point, it's your personhood

02

Equity

Security protections are equal for every user

Firs-world protections are the baseline for all

03

Genuine Inclusion

Access that isn't forced through necessity

A system with few guardrails is more of a trap than an opportunity

04

Accountability

Responsibility is shifted to the ones who collect and hold the data

Enforced standards and audits make accountability structural

Is the Solution Ethically Defensible?

A Clear Rationale for Ethicality

1. **Financial Inclusion at Scale** – It preserves the good aspect of the technology
2. **Risk Redistribution** – Redistributes risk to those most able to handle it
3. **Prevents Harm Before it Happens** – Stronger regulations mean fewer possibilities of misuse and theft
4. **Tangible Accountability** – With public reporting and auditing the accountability is structural, not aspirational
5. **It Treats the Harm as What it is** – The harm with stolen biometric data is its permanence, the solution treats it as such

Access Now's Timeline of Action

accessnow

1

Audit & Awareness
(0 - 3 months)

- Publish biometric risk report via #WHYID
- Launch stakeholder awareness campaigns
- Provide immediate privacy guidance

2

Privacy Infrastructure
(3 - 9 months)

- Test infrastructure
- Release technical frameworks for implementation
- Collaborate with NGOs, universities, and policy bodies

3

Governance Standards
(9-18 months)

- Push for mandatory global guidelines
- Monitor and report compliance
- Share best practices as adoption scales

Access Now's Timeline of Action

accessnow

1

Audit & Awareness
(0 - 3 months)

- Publish biometric risk report via #WHYID
- Launch stakeholder awareness campaigns
- Provide immediate privacy guidance

2

Privacy Infrastructure
(3 - 9 months)

- Test infrastructure
- Release technical frameworks for implementation
- Collaborate with NGOs, universities, and policy bodies

3

Governance Standards
(9-18 months)

- Push for mandatory global guidelines
- Monitor and report compliance
- Share best practices as adoption scales

Access Now's Timeline of Action

accessnow

1

Audit & Awareness
(0 - 3 months)

- Publish biometric risk report via #WHYID
- Launch stakeholder awareness campaigns
- Provide immediate privacy guidance

2

Privacy Infrastructure
(3 - 9 months)

- Test infrastructure
- Release technical frameworks for implementation
- Collaborate with NGOs, universities, and policy bodies

3

Governance Standards
(9-18 months)

- Push for mandatory global guidelines
- Monitor and report compliance
- Share best practices as adoption scales

Access Now's Timeline of Action

accessnow

1

Audit & Awareness
(0 - 3 months)

- Publish biometric risk report via #WHYID
- Launch stakeholder awareness campaigns
- Provide immediate privacy guidance

2

Privacy Infrastructure
(3 - 9 months)

- Test infrastructure
- Release technical frameworks for implementation
- Collaborate with NGOs, universities, and policy bodies

3

Governance Standards
(9-18 months)

- Push for mandatory global guidelines
- Monitor and report compliance
- Share best practices as adoption scales

Call to Action

The past can't be changed, but the standard can.

The Problem is Evident

- 1.3 billion being onboarded into biometric systems **today**
- 22 African countries with **no data protection laws**
- Once biometric data is leaked, it **can't ever be recovered**
- Those with **fewer resources** carry the **most risk**

Show the risk
#WHYID needs to show the harm with real cases

Implement the solution
A security standard that can't be ignored

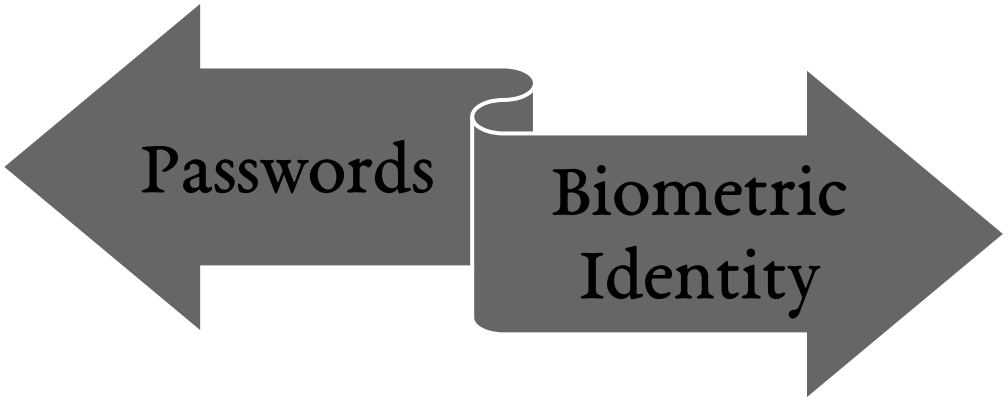
Shift the liability
Redistributes risk to those able to handle loss

Set the standard before the harm becomes permanent

Appendix

The Irreversibility Problem

- Can be reset
- User retains control
- Breaches are typically recoverable
- Identity is based on knowledge

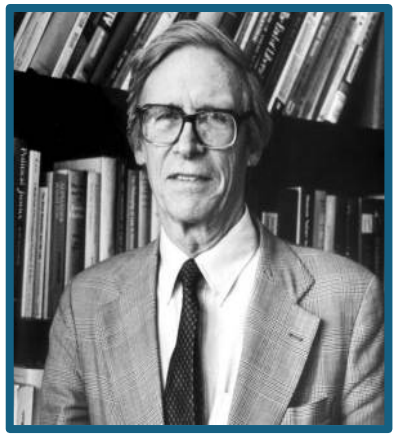


- Cannot be reset
- User cannot change it
- Breaches are permanent
- Identity is based on physical traits

John Rawls – The Original Position

What rules would you set for biometric data if you might be the one handing it over?

Rawlsian Approach to Ethics



- Philosopher John Rawls (1921-2002) focused primarily on how a just society should be run.
- His philosophy was centered on the concept of justice as fairness, which is the idea that a society's rules should be ones that free and equal people would rationally agree to under fair conditions.
- Rawls's most famous thought experiment is the original position, which uses the idea of a veil of ignorance.

Biometrics Through the Veil of Ignorance

- Behind the veil of ignorance, one would not choose to have their biometric data collected.
- Inequalities are permitted under Rawlsian ethics if they benefit the least advantaged without exposing them to disproportionate risk.
- If there are fewer invasive alternatives for the same outcome (Banking), they should be used.

Is the Solution Ethically Acceptable?

accessnow

Preserves Genuine Good

Redistributes Risk

Restores User Agency

Aligns Practice with Values

It preserves genuine good, redistributes risk to those best positioned to manage it, restores user agency, and aligns practice with stated values.

Tie-Back to SDGs

- **SDG 1** (No Poverty) & **SDG 10** (Reduced Inequalities); served only if the system is trustworthy
- **SDG 16** (Peace, Justice, Strong Institutions); responsible data governance is what strong institutions look like

Capabilities Approach – True Freedom

Capabilities approach – What are people able to do and be?

Capabilities Approach

- Developed by economist/philosopher Amartya Sen and further developed by philosopher Martha Nussbaum ~1980s.
- This approach looks at "true freedom," not just the formal choice.
- It was developed to highlight the idea that equal resources do not equate to equal opportunities.

Biometrics Through the Capabilities Approach

- Choices of vulnerable individuals may be coerced due to circumstance, and if so, is their choice truly based in freedom?
- Banking services enhances capabilities like saving money and credit, but it poses risks of data breaches, surveillance, and loss of control over identity.
- Wealthier individuals often don't need to provide biometric as a condition of inclusion.

Are the Actions Defensible?

CURRENT – NOT DEFENSIBLE

Known risk, ignored
The harm was foreseeable and unregulated execution was deliberate

Good intent isn't a defense
Exposing people to known permanent harm while trying to help is contradictory

Not a fair system
No reasonable designer of this system would accept the current security systems

Solution

PROPOSED - DEFENSIBLE

Preserves the good
Maintained financial access ready to scale safely

Fairly redistributes risk
Those who profit now carry the liability

Brings honesty to the business model
It doesn't kill the incentive but aligns it with the mission