The Ethics of Biometric Authentication: Balancing Convenience, Consent, and Risk.

CPSC329P25 TUT04 Group2:
Kashfia Karder, Vianne Watson,
Hsuan-Han Liu, and Jaiveer Toor

University of Calgary

Overview

- Introduction
  - What is **Biometric Authentication**?
  - **Ethics** in Biometric Data
- Background & Related Work
- Real-World Case Studies
  - **Clearview AI, Aadhaar, and CBP**
- Main Analysis
- Recommendations
  - Policy, Design Principles, etc.
- Conclusion & the Future

Introduction

Why Biometric Authentication Matters?

- **Biometric authentication verifies identity** using unique physical traits.
  - Ex: fingerprints, facial patterns, or iris scans.

- Its **convenience** and **resistance to forgery** make it a popular authentication tool.

- Due to the **permeance** of biometric data, **strong security** and **ethical safeguards** are **essential** because breaches can lead to **lifelong identity theft or fraud**.

Introduction

Research Scope & Ethical Concerns

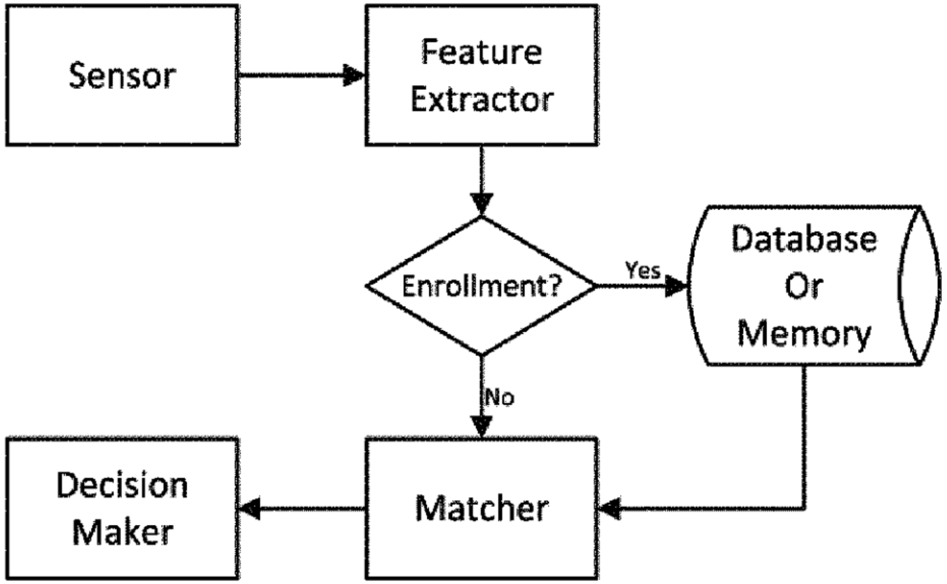
We aim to explore how **ethical transparency**, **user consent**, and **future risks** must be balanced with growing convenience.

- Our project analyzes biometric authentication from an **ethical cybersecurity lens**.
- We examined **real-world cases** involving surveillance, third-party data sharing, consent violations, and lack of transparency.
- Everyday uses include unlocking devices, banking, **airport screening**, and payment apps.

Background & Related Work

Biometric Types & System Architecture

- **Biometric identifiers** fall into two main categories:
  - Physical traits
  - Behavioral traits
- A typical biometric system includes: Sensor → Feature Extractor → Matcher → Decision Module
- These modules transform traits into encrypted **templates** for identity matching.
- While effective for access control, **biometric traits cannot be changed** if compromised, unlike passwords.



Background & Related Work

Security vs Convenience: Trade-offs

- Biometric authentication offers strong **non-repudiation** and **ease of use**, especially in mobile and enterprise contexts.
- However, **usability comes at a cost**: breached biometrics cannot be reset like passwords.
- On-device storage and multimodal systems are recommended to balance risk and convenience.
- Designers must weigh **long-term privacy risks** against user experience.

Background & Related Work

Ethical & Privacy Frameworks

- **Marginalized groups** may face higher error rates and surveillance risks from biased algorithms.
- Facial recognition tech has raised serious **civil rights concerns**, particularly in law enforcement.
- A **privacy-by-design** model was proposed in journal "Ensuring the Privacy and Security of Biometric Data: Ethical Considerations in Focus":
    - o Encrypted templates
    - o Informed consent
    - o Decentralized user control
- Biometrics should be treated as a **digital extension of identity**, not just a convenience layer.

precedented fight over auditors&apos; powers
Former Michigan fire marshal says state ignored mandated insp

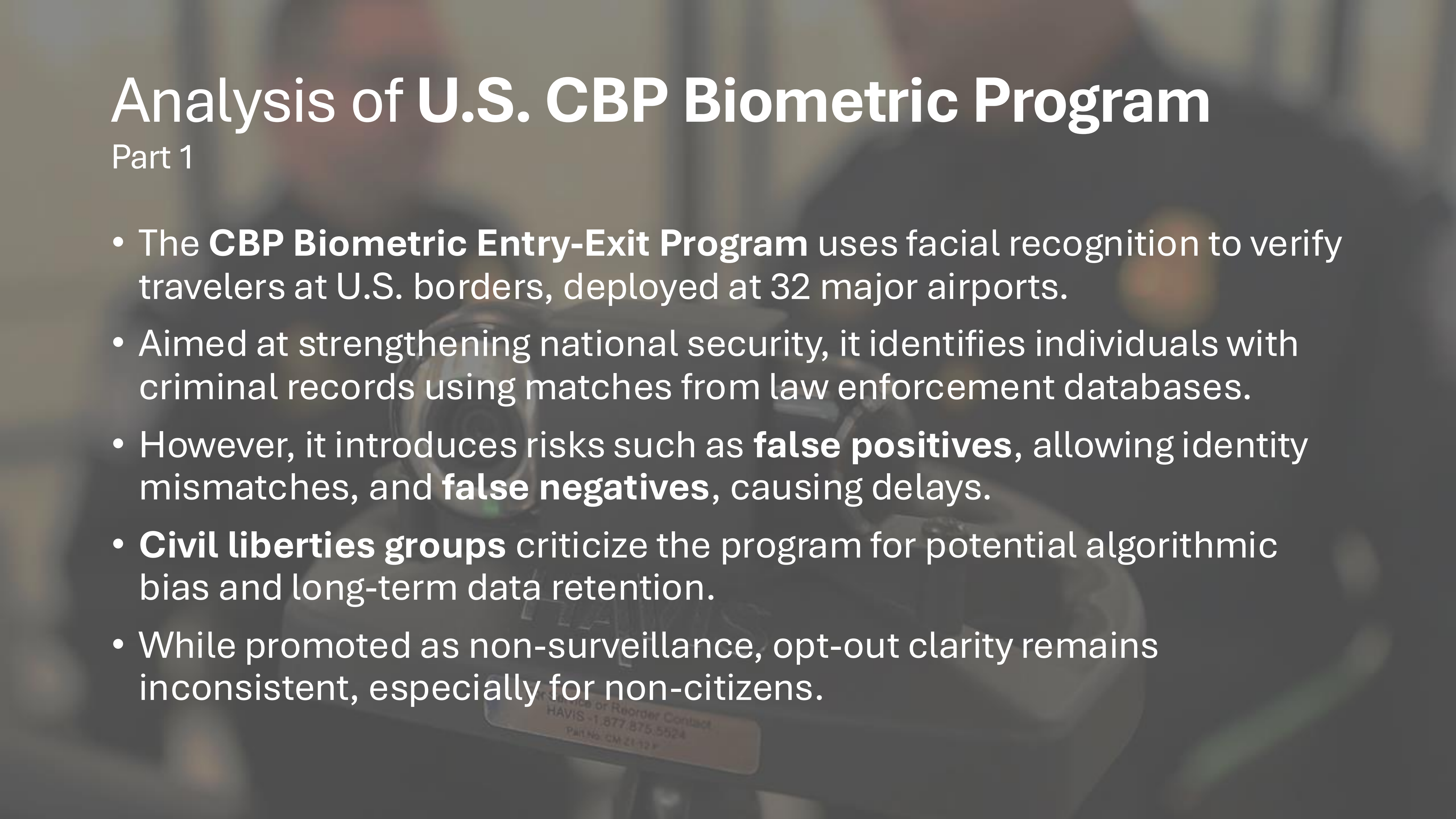
Background & Related Work

Emerging Trends & Future Threats

- Future directions for Biometric Security & Privacy:
  - AI-powered authentication
  - Blockchain-based identity
  - Multimodal biometrics
- Stoica, in "The Future Risk of Biometric Data Theft in Cybersecurity", warns of threats like **spoofing**, **database breaches**, and **re-identification attacks**.
- A 2020 case study showed that healthcare biometrics were stolen due to outdated security.
- Stronger encryption, patching, and **system-level audits** are essential for future resilience.

Case Study 1: U.S. CBP Biometric Program

- Launched in 2018, facial-recognition checkpoints at airports and land crossings for non-U.S. traveler identity verification
- Expanded to 32 airports by mid-2020 to automate and expedite border processing
- CBP claims benefits: reduced wait times and enhanced border security
- Criticized for long data retention, non-citizen photos held for 14 days, and in some cases up to 75 years
- Documented accuracy gaps reveal algorithmic bias, with higher misidentification rates for people of color
- Opaque data sharing with law enforcement databases raises privacy concerns
- Minimal traveler consent mechanisms, risking function creep into mass surveillance systems
- Highlights the tension between streamlined, touchless travel and potential civil liberties infringements



Analysis of **U.S. CBP Biometric Program**

Part 1

- The **CBP Biometric Entry-Exit Program** uses facial recognition to verify travelers at U.S. borders, deployed at 32 major airports.
- Aimed at strengthening national security, it identifies individuals with criminal records using matches from law enforcement databases.
- However, it introduces risks such as **false positives**, allowing identity mismatches, and **false negatives**, causing delays.
- **Civil liberties groups** criticize the program for potential algorithmic bias and long-term data retention.
- While promoted as non-surveillance, opt-out clarity remains inconsistent, especially for non-citizens.

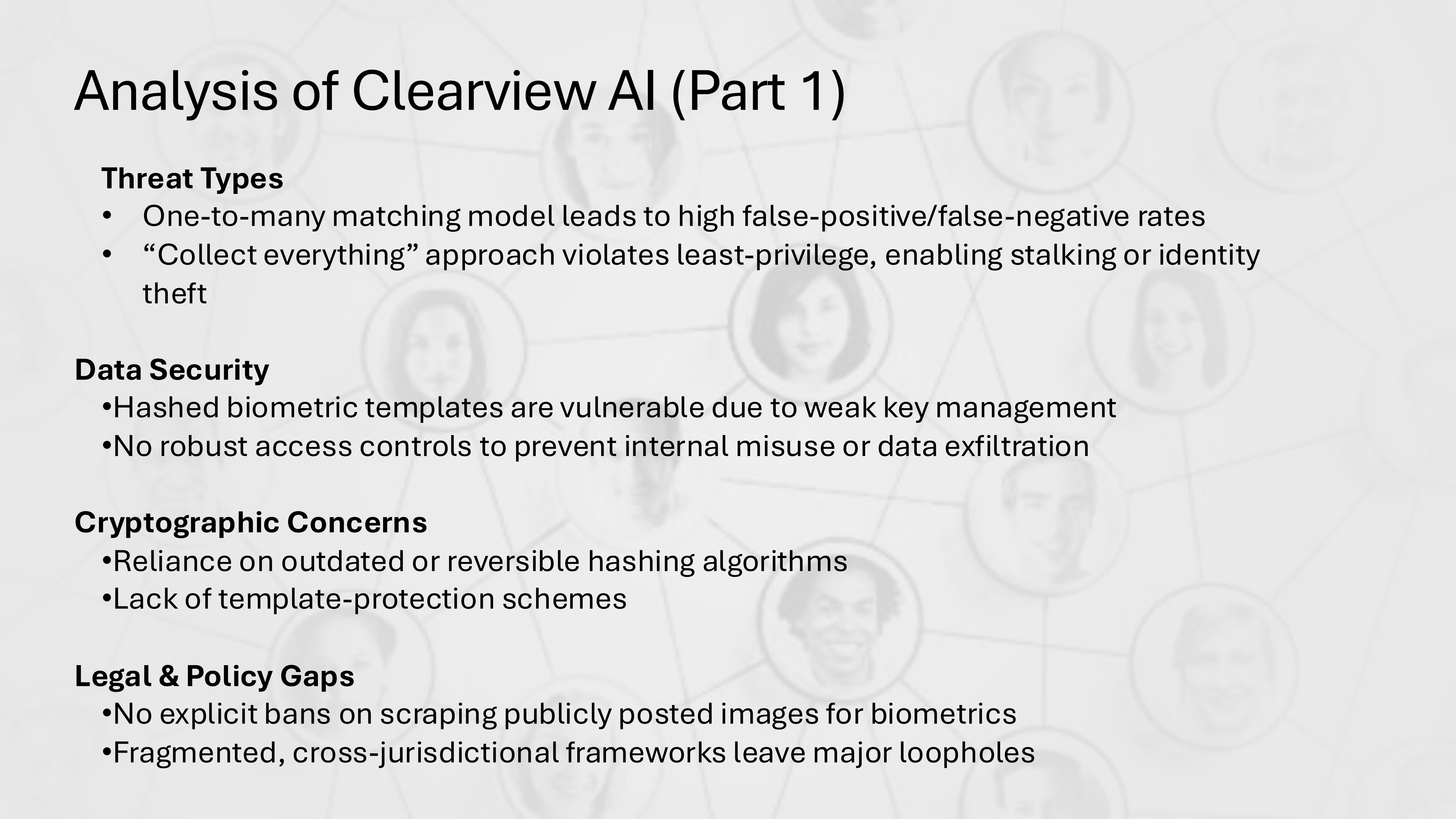
Analysis of **U.S. CBP Biometric Program**

Part 2

- CBP stores **U.S. citizen data for 12 hours**, while **non-citizen data** may be held up to 75 years.
- Cryptographic practices are **not publicly disclosed**, raising transparency and security concerns.
- Despite legal mandates since 1996, the **biometric exit system** remains incomplete due to planning and staffing issues.
- **Audit gaps** exist for commercial partners; only five airline audits were done by 2022, with no consistent checks at land/sea ports.
- Ongoing challenges include incomplete signage, weak opt-out messaging, and limited operational metrics on false matches.

Case Study 2: Clearview AI

- In 2020, Clearview AI scraped over three billion images from public platforms without user consent
- Built a facial recognition database, sold mainly to law enforcement agencies
- Agencies could upload a probe image and receive matches from this unregulated repository
- Data-sharing agreements were opaque, with minimal oversight and potential mission creep into general surveillance
- No opt-in or notification mechanisms, users had no chance to consent or opt out
- Raised serious privacy concerns: violated expectations of data ownership and individual privacy
- Supporters argue the database aids criminal investigations by matching suspects’ faces to public images
- Clearview faced lawsuits under various U.S. privacy statutes and settled a class-action suit with future equity rather than cash
- Highlights ethical tension: biometric matching’s convenience for authorities vs. zero regard for user consent and pervasive privacy risk



Analysis of Clearview AI (Part 1)

Threat Types

- One-to-many matching model leads to high false-positive/false-negative rates
- “Collect everything” approach violates least-privilege, enabling stalking or identity theft

Data Security

- Hashed biometric templates are vulnerable due to weak key management
- No robust access controls to prevent internal misuse or data exfiltration

Cryptographic Concerns

- Reliance on outdated or reversible hashing algorithms
- Lack of template-protection schemes

Legal & Policy Gaps

- No explicit bans on scraping publicly posted images for biometrics
- Fragmented, cross-jurisdictional frameworks leave major loopholes

Analysis of Clearview AI (Part 2)

Ethical & Legal Considerations

- Absence of transparency: individuals can’t verify or correct inclusion/misidentifications
- Biased error rates across demographics undermine fairness and due process

Impact on Key Stakeholders

- Individuals: Risk wrongful scrutiny, reputational harm, no recourse
- Law Enforcement: Faster IDs but potential biased policing and civil liberties violations
- Technology Partners: Unwittingly enable mass surveillance without audit mechanisms
- Civil Liberties Groups: Forced into litigation amid outdated statutes

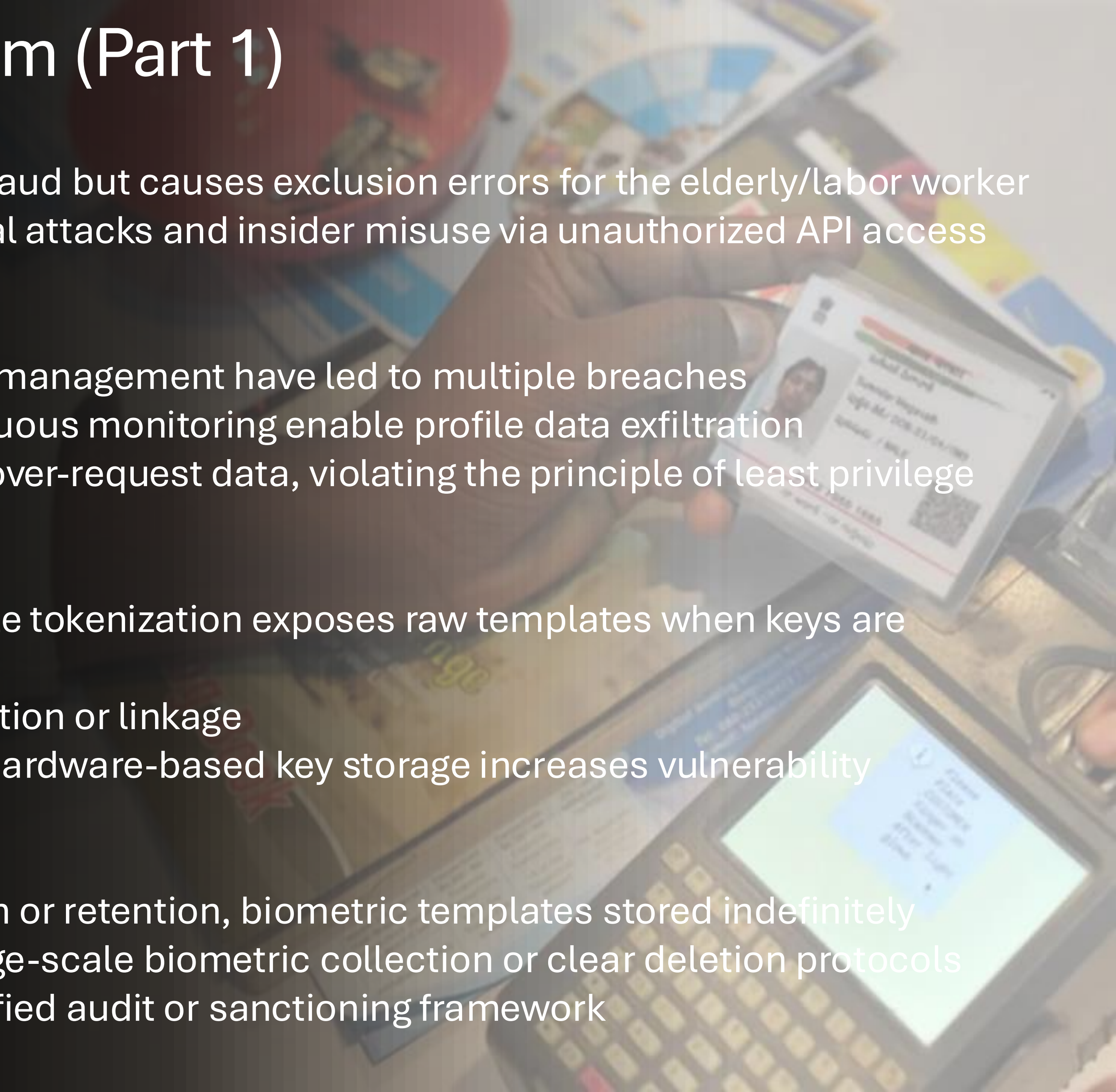
Research Gaps & Unresolved Challenges

- No standard metrics for false-match/non-match rates in real-world deployments
- Lack of defined accountability/transparency metrics for one-to-many systems
- Need cryptographic schemes that balance large-scale matching accuracy and privacy
- Urgent longitudinal studies on re-identification risks via data linkage

Case Study 3: Aadhaar Biometric ID System

- Launched in 2009, enrolled over 1.2 billion residents using fingerprint and iris scans to issue 12-digit IDs
- IDs used for welfare subsidies, mobile-SIM registration, banking, and other government services
- Advocates cite reduced fraud and streamlined benefit delivery
- Repeated data breaches exposed personal information on black-market sites, undermining public trust
- India’s Supreme Court upheld Aadhaar’s constitutionality but restricted mandatory linkage with banking and telecom
- Critics argue that biometrics requirements can exclude marginalized populations unable to provide usable scans
- Centralized storage of sensitive data poses ongoing risks of large-scale identity theft and state surveillance
- Demonstrates ethical dilemma: exceptional convenience versus lack of meaningful consent and systemic surveillance risks

Analysis of Aadhaar Program (Part 1)



Threat Types

•Biometric authentication reduces identity fraud but causes exclusion errors for the elderly/labor worker

•Centralized repository is a target for external attacks and insider misuse via unauthorized API access

Data Security

•Reversible encryption and inconsistent key management have led to multiple breaches

•Insecure API endpoints and a lack of continuous monitoring enable profile data exfiltration

•Absence of access controls lets providers over-request data, violating the principle of least privilege

Cryptographic Concerns

•Reversible encryption rather than irreversible tokenization exposes raw templates when keys are compromised

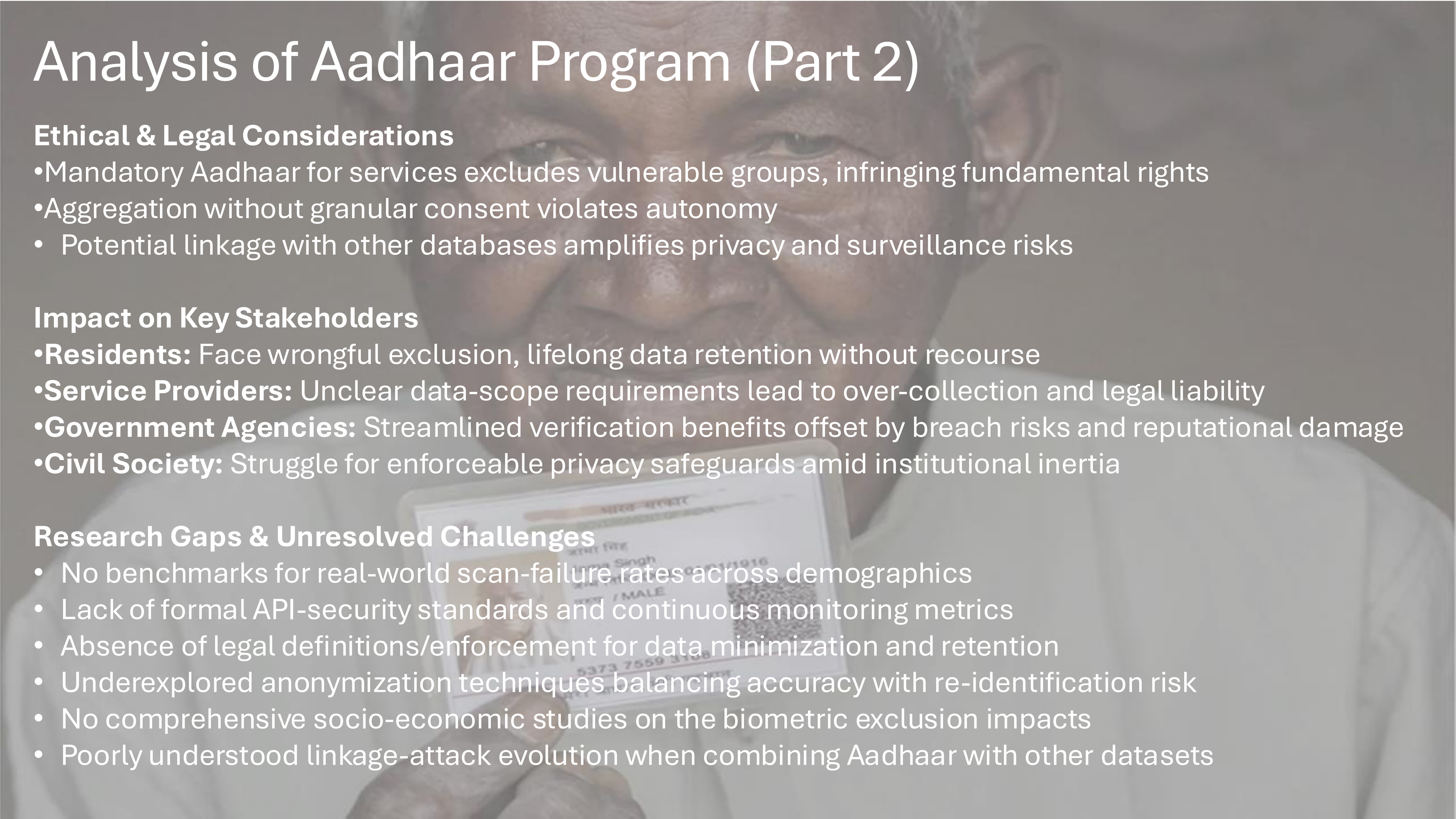
•No robust safeguards to prevent reconstruction or linkage

•Lack of universal key-rotation policies and hardware-based key storage increases vulnerability

Legal & Policy Gaps

- No enforceable limits on data minimization or retention, biometric templates stored indefinitely
- Privacy laws don’t specifically address large-scale biometric collection or clear deletion protocols
- Regulatory oversight is fragmented; no unified audit or sanctioning framework

Analysis of Aadhaar Program (Part 2)



Ethical & Legal Considerations

- Mandatory Aadhaar for services excludes vulnerable groups, infringing fundamental rights
- Aggregation without granular consent violates autonomy
- Potential linkage with other databases amplifies privacy and surveillance risks

Impact on Key Stakeholders

- **Residents:** Face wrongful exclusion, lifelong data retention without recourse
- **Service Providers:** Unclear data-scope requirements lead to over-collection and legal liability
- **Government Agencies:** Streamlined verification benefits offset by breach risks and reputational damage
- **Civil Society:** Struggle for enforceable privacy safeguards amid institutional inertia

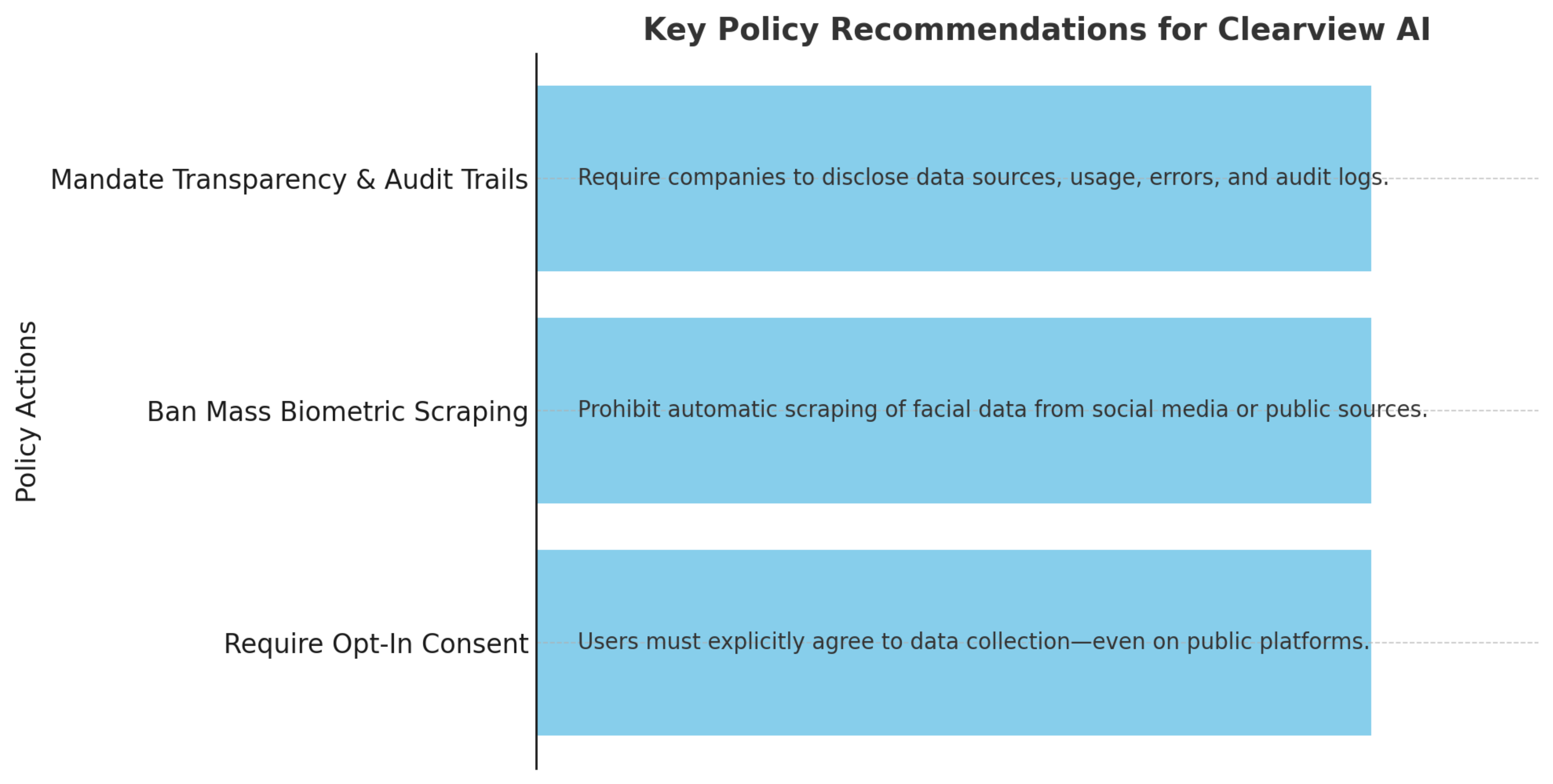
Research Gaps & Unresolved Challenges

- No benchmarks for real-world scan-failure rates across demographics
- Lack of formal API-security standards and continuous monitoring metrics
- Absence of legal definitions/enforcement for data minimization and retention
- Underexplored anonymization techniques balancing accuracy with re-identification risk
- No comprehensive socio-economic studies on the biometric exclusion impacts
- Poorly understood linkage-attack evolution when combining Aadhaar with other datasets

Policy Recommendations: Clearview AI

- Require **opt-in consent** before scraping biometric data
  - Ensure individuals explicitly agree to data collection, even from public platforms, aligning with global privacy laws.
- **Ban mass biometric scraping** from social media
  - Close legal **loopholes** that allow unchecked scraping of facial data from public posts.
- Mandate **transparency reports** and **audit** trails
  - Companies must **disclose** data sources, error rates, and law enforcement partnerships in regular public reports.
- Enforce independent **audits** for bias and accuracy
  - Require **external assessments** of system fairness, especially in one-to-many matching contexts.
- **Promote federated/decentralized** storage
  - Reduce central points of failure by storing biometric data across secure, distributed systems.
- Offer **legal recourse** for victims of false matches
  - Give individuals the **right to dispute** matches and seek redress in cases of harm or misidentification.

Policy Recommendations: Clearview AI



Key Policy Recommendations for Clearview AI

Mandate Transparency & Audit Trails: Require companies to disclose data sources, usage, errors, and audit logs.

Ban Mass Biometric Scraping: Prohibit automatic scraping of facial data from social media or public sources.

Require Opt-In Consent: Users must explicitly agree to data collection—even on public platforms.

Policy Recommendations: Aadhaar System

- Enforce data minimization and retention limits
    - Only collect what is strictly necessary and delete outdated biometric data promptly.
- Secure biometric templates with encryption & key controls
    - Use strong encryption and safe key management to prevent unauthorized access.
- Require fine-grained access control and logging
    - Limit data access to what’s needed and log all usage for accountability.
- Support alternative verification (mobile OTPs, assisted auth)
    - Provide fallback methods for people who struggle with fingerprints or iris scans.

Policy Recommendations: CBP Biometric Program

- Implementation of **hybrid systems** to move towards post-quantum cryptography, as quantum computers advance.
  - Aids in protection against **'harvest now, decrypt later'** attacks
  - Complying with **NIST standards**
- Standardize systems that **enable transparency** regarding biometric data collection and **opt-out rights**.
  - **Global Entry kiosks**
  - **Notice** of biometric data collection **prior to travel**
- Regulated **auditing** practices
  - Monitors compliance with standards
  - Identifies gaps in staffing or infrastructure
  - Adherence to transparency measures

Conclusion

- Biometric systems **offer convenience—but carry risks**
    - **Without ethical** safeguards, they can lead to **surveillance, exclusion, and privacy violations**.
- Consent and transparency are essential
    - Clearview, Aadhaar, and CBP show how **failing to inform** or empower users **erodes trust**.
- Technology must be guided by human values
    - Ethical design, legal protections, and inclusive alternatives must shape biometric systems.
- Trust must be earned, not assumed
    - Future systems should prioritize transparency, decentralization, and accountability.

Master Citation List (Slides)

- **Slide 3:** https://www.bing.com/images/searchview=detailV2&insightstoken=bcid_s13Jnq7XiowIrNSF0z6kdCU3dQVa.....4w*ccid_XcmerteK&form=ANCMS1&iss=VSI&selectedindex=0&id=D0286E5A77E3F2ADD617EABDA70C626DFFFF1A29&ccid=1uWYgcsu&exph=250&expw=400&vt=2&sim=11&simid=608018803022377971&ck=18DE1D5F71AFF65CA5F8A486FA3EED3C&thid=OIP.1uWYgcsuS4Z7vTxTaiUsPAAAAA&mediaurl=https%3A%2F%2Fwww.acalvio.com%2Fwp-content%2Fuploads%2F2020%2F03%2FSCA.png&cdnurl=https%3A%2F%2Fth.bing.com%2Fth%2Fid%2FR.d6e59881cb2e4b867bbd3c536a252c3c%3Frik%3DKRr%252f%252f21iDKe96g%26pid%3DImgRaw%26r%3D0&pivotparams=insightsToken%3Dbcid_s13Jnq7XiowIrNSF0z6kdCU3dQVa.....4w*ccid_XcmerteK%26%26cal%3D0%26cat%3D0%26car%3D1%26cab%3D1%26ann%3D%26hotspot%3D
- **Slide 4:** https://www.bing.com/images/searchview=detailV2&ccid=ikvxwFfp&id=33340E1FDCD869F1AFC86312E63AB86E7E4A069C&thid=OIP.ikvxwFfpu5nAS6BBixfFfgAAAA&mediaurl=https%3A%2F%2Fsmallimg.pngkey.com%2Fpng%2Fsmall%2F503-5038951_the-impact-of-third-party-data-changes-on.png&cdnurl=https%3A%2F%2Fth.bing.com%2Fth%2Fid%2FR.8a4bf1c057e9bb99c04ba0418b17c57e%3Frik%3DnAZKfm64OuYSYw%26pid%3DImgRaw%26r%3D0&exph=333&expw=320&q=third+party+data+sharing+icons&simid=607990138446485709&FORM=IRPRST&ck=FD3C84DEED89AC24061867271BE5F93F&selectedIndex=12&itb=0&cw=1212&ch=578&ajaxhist=0&ajaxserp=0
- **Slide 5:** https://heinonline.org/HOL/Pagecollection=journals&handle=hein.journals/ijisc13&id=50&men_tab=srchresults
- **Slide 6:** https://www.securitymagazine.com/articles/92319-biometric-data-increased-security-and-risks)
- **Slide 7:** https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/
- **Slide 8:** https://www.cpomagazine.com/cyber-security/breach-of-biometrics-database-exposes-28-million-records-containing-fingerprint-and-facial-recognition-data/

Master Citation List (Slides) cont…

- **Slide 9:** https://www.nytimes.com/2022/02/26/travel/facial-recognition-airports-customs.html
- **Slide 10:** https://www.theverge.com/policy/664433/cbp-photos-facial-recognition-travelers-leaving-us
- **Slide 11**: https://www.gao.gov/products/gao-22-106154
- **Slide 12:** https://blog.avast.com/facing-facts-clearview-ai-cases-impact-on-consumers
- **Slide 13:** https://www.iotworldtoday.com/iiot/clearview-ai-fined-9-4m-over-facial-data-scraping
- **Slide 14:** https://www.reuters.com/technology/clearview-ais-facial-recognition-tool-coming-apps-schools-2022-05-24/
- **Slide 15:** https://www.bbc.com/news/world-asia-india-44777787 and https://cacm.acm.org/opinion/biometric-identity/
- **Slide 16:** https://spectrum.ieee.org/aadhaar-indias-biometric-id-system-gets-its-day-in-court
- **Slide 17:** https://www.bbc.com/news/world-asia-india-43207964
- **Slide 19:** Drawn by Jaiveer
- **Slide 20:** https://en.wikipedia.org/wiki/Aadhaar
- **Slide 21:** https://www.cbp.gov/newsroom/local-media-release/cbp-lawa-expand-biometric-traveler-experience-lax

Master Citation List Research

- [1] “Facial Recognition Technology: CBP Traveler Identity Verification and Efforts to Address Privacy Issues.” U.S. GAO, www.gao.gov/products/gao-22-106154.
- [2] “Biometric Entry-Exit System: legislative history and status.” CRS Reports, 27 Aug. 2020, sgp.fas.org/crs/misc/IF11634.pdf.
- [3] “CBP, LAWA Expand Biometric Traveler Experience at LAX.” U.S. Customs and Border Protection, www.cbp.gov/newsroom/local-media-release/cbp-lawa-expand-biometric-traveler-experience-lax.
- [4] Kimery, Anthony. “CBP Exploring Post-quantum Cryptography to Protect Sensitive Data.” Biometric Update | Biometrics News, Companies and Explainers, 1 Apr. 2025, www.biometricupdate.com/202411/cbp-exploring-post-quantum-cryptography-to-protect-sensitive-data.
- [5] “Post-Quantum Cryptography in Identity Management | IDEMIA.” IDEMIA, 16 Oct. 2024, www.idemia.com/insights/post-quantum-cryptography-identity-managementthe-time-act-now.
- [6] Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. Post-Quantum Cryptography | CSRC | CSRC. csrc.nist.gov/projects/post-quantum-cryptography.
- [7] “SandboxAQ Quantum-resistant Encryption Algorithm Approved by NIST.” Biometric Update | Biometrics News, Companies and Explainers, 1 Apr. 2025, www.biometricupdate.com/202504/sandboxaq-quantum-resistant-encryption-algorithm-approved-by-nist?.com
- [8] “Privacy Impact Assessments | Homeland Security.” U.S. Department of Homeland Security, www.dhs.gov/privacy-impact-assessments.
- [9] “The Fair Information Practice Principles | Homeland Security.” U.S. Department of Homeland Security, www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles.
- [10] ACLU. "Clearview AI’s Face-Scraping Technology Violates Privacy Rights." https://www.aclu.org/news/privacy-technology/clearview-ai-scraping-of-faces-has-violated-the-rights-of-millions.

Master Citation List (Research) cont…

- [11] Morais, Lenildo. “Biometric Data: Increased Security and Risks.” 2020-05-06 | Security Magazine, 5 May 2020, www.securitymagazine.com/articles/92319-biometric-data-increased-security-and-risks.
- [12] S, Kumar. “Biometric Security &Amp; Privacy: Balancing Innovation and Protection.” Cyber Tech Journals, 29 Apr. 2025, cybertechjournals.com/biometric-security-privacy-balancing-innovation-and-protection/#The_Future_of_Biometrics_Trends_to_Watch.
- [13] The New York Times. "The Secretive Company That Might End Privacy as We Know It." https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
- [14] Chin-Rothmann, Caitlin, and Nicol Turner Lee. “Police Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color.” Brookings, 7 Apr. 2022, www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color.
- [15] “The Future Risk of Biometric Data Theft in Cybersecurity.” International Journal of Information Security and Cybercrime, uploaded by University of Calgary Library, vol. 13, no. 1, June 2024, pp. 49–58.
- [16] Yhang, Faozy. “Ensuring the Privacy and Security of Biometric Data: Ethical Considerations in Focus.” Journal of Biometrics & Biostatistics, by University of Texas, vol. 15–06, Journal Article, 26 Dec. 2024, https://doi.org/10.37421/2155-6180.2024.15.249.
- [17] Scroll.in, "UIDAI admits Aadhaar system failed to recognize biometric data of many users". https://scroll.in/latest/1006184/uidai-admits-aadhaar-system-failed-to-recognise-biometric-data-of-many-users
- [18] Access Now. "India’s Aadhaar data breaches continue to threaten user privacy". https://www.accessnow.org/india-aadhaar-data-breach-privacy/
- [19] Del Valle, Gaby. “Border Agents Are Going to Photograph Everyone Leaving the US by Car.” The Verge, 9 May 2025, www.theverge.com/policy/664433/cbp-photos-facial-recognition-travelers-leaving-us.
- [20] Allyn, Bobby. “‘The Computer Got It Wrong’: How Facial Recognition Led to False Arrest of Black Man.” NPR, 24 June 2020, www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig?

Master Citation List (Research) cont…

- [21] "Williams V. City of Detroit | American Civil Liberties Union." American Civil Liberties Union, 2 July 2024, www.aclu.org/cases/williams-v-city-of-detroit-face-recognition-false-arrest?
- [22] Merken, Sara. "Clearview AI strikes 'unique' deal to end privacy class action." 13 June 2024. https://www.reuters.com/legal/litigation/clearview-ai-strikes-unique-deal-end-privacy-class-action-2024-06-13/
- [23] Scarcella, Mike. "US judge approves 'novel' Clearview AI class action settlement" 21 March 2025. https://www.reuters.com/legal/litigation/us-judge-approves-novel-clearview-ai-class-action-settlement-2025-03-21/
- [24] Taylor, Josh. "Privacy Regulator Drops Pursuit of Clearview AI as Greens Call for More Scrutiny on Use of Australians' Images." The Guardian, 21 Aug. 2024, www.theguardian.com/technology/article/2024/aug/21/privacy-regulator-drops-pursuit-of-clearview-ai-over-use-of-australians-images-in-facial-recognition-tech-ntwnfb.
- [25] Wikipedia contributors. "Aadhaar." Wikipedia, 9 June 2025, en.wikipedia.org/wiki/Aadhaar.
- [26] "ID Systems Analysed: Aadhaar." Privacy International, privacyinternational.org/case-study/4698/id-systems-analysed-aadhaar.
- [27] BBC News. Aadhaar: "Leak" in World's Biggest Database Worries Indians. 5 Jan. 2018, www.bbc.com/news/world-asia-india-42575443.
- [28] ---. Seven Important Questions on Aadhaar Answered. 27 Mar. 2018, www.bbc.com/news/world-asia-india-43426158.
- [29] BBC News. Aadhaar: India Top Court Upholds World's Largest Biometric Scheme. 26 Sept. 2018, www.bbc.com/news/world-asia-india-44777787.
- [30] DEPARTMENT OF HOMELAND SECURITY. "COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER to U.S. CUSTOMS AND BORDER PROTECTION" October 28, 2024. https://epic.org/documents/epic-comments-to-cbp-on-biometric-identity/.
- [31] "Biometrics: Privacy Policy." U.S. Customs And Border Protection, www.cbp.gov/travel/biometrics/privacy-policy.
- [32] "Biometrics." U.S. Customs And Border Protection, www.cbp.gov/travel/biometrics.
- [33] Kolker, Abigail F. Immigration: The U.S. Entry-Exit System. 2 May 2023. https://www.congress.gov/crs-product/R47541.

THANK YOU FOR LISTENING

Any Questions?