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

Kashfia Karder
Faculty of Science
University of Calgary
Calgary, Alberta, Canada
kashfia.karder@ucalgary.ca

Vianne Watson
Faculty of Science
University of Calgary
Calgary, Alberta, Canada
vianne.watson@ucalgary.ca

Hsuan-Han Liu
Faculty of Science
University of Calgary
Calgary, Alberta, Canada
hsuanhan.liu@ucalgary.ca

Jaiveer Toor
Faculty of Science
University of Calgary
Calgary, Alberta, Canada
jaiveer.toor@ucalgary.ca

***Abstract*—This report explores the ethics of biometric authentication, balancing its benefits against serious concerns such as informed consent and data vulnerability. Through case studies of unethical biometric data usage, we examine the real-world risks and uses of biometric data. We then explore solutions to balance these risks with the convenience and consent of biometric data use. Due to the permanence of biometric data, ethical implementation requires strong security and transparency.**

The cases studied in this report are: Aadhaar program in India; utilizing fingerprint and iris scanning, Clearview AI; collecting publicly posted images to build a facial recognition database, CBP entry-exit program; using biometric facial comparison for identity verification.

These cases outlined a lack of transparency and consent surrounding the usage of biometric data, especially regarding third party usage. They also highlighted the potential for biometric data collection to enable intrusive surveillance practices.

Proposed solutions included improved auditing practices, with transparency measures highlighted to support informed consent. The implementation of hybrid systems is important as quantum computers advance. Using post-quantum encryption techniques helps mitigate real world challenges surrounding 'harvest now, decrypt later' attacks, and ensure proper security of biometric data. Further solutions focused on limiting data retention and the scope of biometric data collection, to reduce surveillance issues. To prevent exploitation of data scraping loopholes and preserve privacy rights, measures such as decentralization, federal oversight, and direct legislation should be implemented.

Overall, these cases were analyzed through an ethical lens, with solutions proposed to enhance the ethical standards of biometric data usage.

I. Introduction

Biometric authentication is the process of using unique measurable physical characteristics associated with an individual to verify access. It has become popular because of the difficulty in forging biometric data, while also being convenient for users. Since biometric data leaks can be detrimental to users' privacy, it is crucial to maintain security when using biometric data. Since this data is permanent and unique to an individual, if biometric data is compromised, it can lead to identity theft and fraud for life. It's essential to properly apply cybersecurity practices to maintain ethical standards and secure biometric data. Ethically, the policies should be transparent, and the users be properly informed prior to consenting to biometric data collection and usage. In our analysis we focused on cases with surveillance concerns, ethical violations, and biometric data being released to 3rd parties without the users' consent. Our research also touched on issues relating to the future of biometric data in cybersecurity. We have become fascinated with how biometric authentication has integrated into our everyday lives: unlocking our cell phones, airport security, online banking access, and paying using applications such as apple pay or google pay. Our research suggests that biometric data will continue to be implemented, and it is important to balance this convenience with ethical risks. This sparked our interest in analysing the ethics surrounding biometric authentication and data usage.

II. Background and Related Work

Biometric data, which includes unique physiological or behavioural traits, has become a cornerstone in modern identification and security systems [11][16]. Its increasing use spans a wide range of applications, such as unlocking smartphones, securing access to physical locations like server rooms, identifying travellers at airports, verifying patient identities in healthcare, and enabling secure financial transactions [11][12].

Biometric identifiers has two main categories: physical identifiers, which are largely immutable and device-independent (e.g., fingerprints, facial patterns, iris/retina scans, hand geometry, palm veins, ear shape, DNA), and behavioral identifiers, which are more recent and generally used in conjunction with other methods (e.g., typing patterns, physical movements, navigation standards, engagement patterns) [11][16]. The inherent uniqueness of these identifiers

allows for the digital identification of individuals to grant access to systems, devices, or data [11][15].

As discussed by Lenildo Morais in "Biometric Data: Increased Security and Risks", biometric systems have become increasingly prevalent in consumer and enterprise security, offering a balance of usability and protection. Morais outlines the widespread adoption of physical biometrics such as fingerprints and facial recognition and notes their benefits in terms of user convenience and enhanced security. However, he also underscores the permanence of biometric identifiers and the implications for privacy breaches, highlighting the fact that unlike passwords, compromised biometrics cannot be revoked or changed [11].

Kumar S, in his article "Biometric Security & Privacy: Balancing Innovation and Protection", provides a comprehensive framework for balancing usability with privacy through principles like on-device storage, template encryption, and informed consent [12]. Kumar also identifies a series of emerging trends such as multimodal biometrics, decentralized identity systems using blockchain, and AI-powered adaptive authentication. These developments suggest that future systems may become more resilient and user-controlled, although concerns about centralization, surveillance, and algorithmic bias remain.

The ethical concerns surrounding biometric surveillance have also been explored by Nicol Turner Lee, who in 2022 examined its implications for communities of colour. Her work, "Police surveillance and facial recognition: Why data privacy is imperative for communities of colour", highlights the civil rights risks and systemic inequalities embedded in the application of these technologies [14]. This critique positions biometric systems within broader societal dynamics, drawing attention to the role of transparency, fairness, and inclusive oversight.

Faozy Yhang's article, "Ensuring the Privacy and Security of Biometric Data: Ethical Considerations in Focus", adds another dimension to the discussion. Yhang emphasizes the need for privacy-by-design approaches in biometric systems, particularly as use cases expand across healthcare, law enforcement, and finance. Yhang advocates for encrypted storage, multi-factor authentication, and decentralized user control, suggesting that biometric data be treated as a digital extension of personal identity that requires rigorous safeguards [16].

The future risks associated with biometric data are the focus of Iulia-Teodora Stoica's publication "The Future Risk of Biometric Data Theft in Cybersecurity". Stoica provides a technical breakdown of biometric system vulnerabilities, including spoofing attacks, centralized storage risks, and inadequate encryption. She also presents a detailed case study involving the breach of a healthcare company where attackers stole over a million biometric records. Her findings stress the urgency for organizations to implement robust security measures such as encrypted transmission, periodic patching, and continuous monitoring of biometric systems [15].

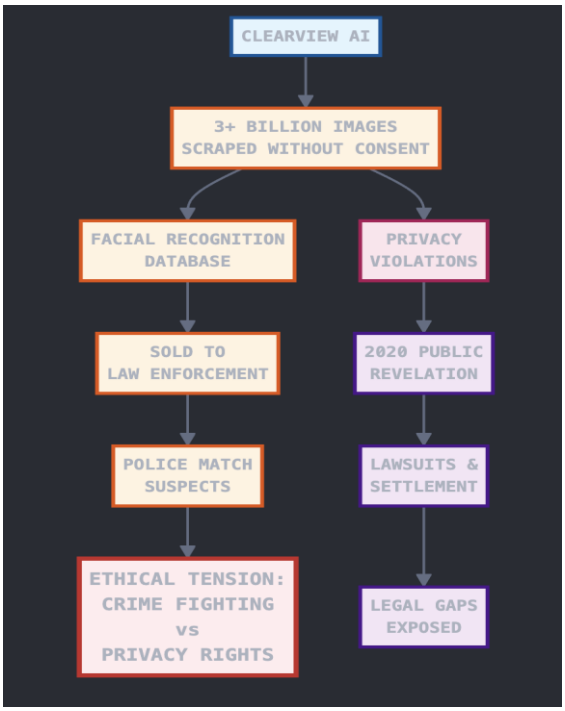
Together, these articles provide a comprehensive backdrop for understanding biometric authentication systems. Our project builds upon these insights by critically examining the ethical implications, technical issues, and privacy challenges of biometric data, particularly as applied in large-scale public systems. We seek to position our analysis in relation to existing literature by proposing a balanced approach that considers both the innovation and responsibility required to implement biometric systems ethically and securely.

III. Case Studies or Real World application

Biometric authentication was supposed to solve our password problems, just scan your fingerprint or face, and you're in. But as these technologies have spread, we've discovered they create new ethical problems we didn't see coming. Every security system involves trade-offs between convenience and privacy, but biometrics feels different because you can't change your face like you can change a password. The three cases below show how even well-designed biometric systems can cause real harm when companies don't handle consent properly, when the technology isn't accurate enough, or when there aren't sufficient safeguards in place.

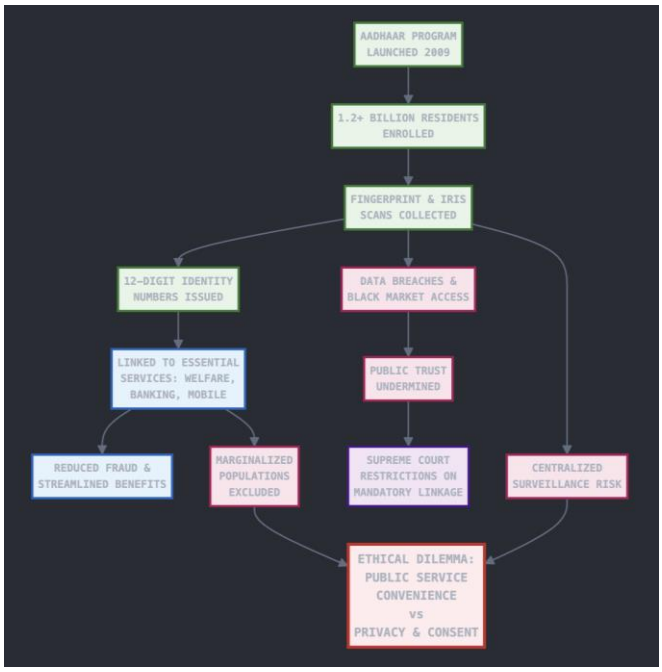
A. Clearview AI's Face-Scraping Controversy

In 2020, it was revealed that Clearview AI had indiscriminately collected over three billion images from social media platforms, including Facebook, YouTube, Twitter, Instagram, and other public websites, without user consent, to build a facial recognition database sold primarily to law enforcement agencies. Those agencies could later upload a probe image and receive matches drawn from this massive, unregulated repository. Moreover, the company's opaque data-sharing agreements were sold as crime-fighting tools, sidestepping any meaningful oversight, raising alarms about mission creep into general surveillance. This large-scale scraping bypassed any meaningful opt-in or notification mechanism, raising serious privacy concerns. Critics argue the practice violated individuals' expectations of privacy and data ownership, while supporters contend that such a comprehensive database can aid criminal investigations by matching suspects' faces against publicly available images. In court, Clearview faced lawsuits under various U.S. privacy statutes and ultimately agreed to a class-action settlement structured around future equity rather than immediate cash compensation, underscoring how existing legal frameworks struggle to address novel biometric data practices. This case talks about the ethical tension of our topic: while biometric matching offers powerful convenience for authorities, it did so here with zero regard for consent and exposed individuals to pervasive privacy risk. Below I added a flowchart representing an overview of the case study.



B. *India's Aadhaar Biometric ID System*

India's Aadhaar program, launched in 2009, enrolled over 1.2 billion residents by collecting fingerprint and iris scans to issue 12-digit identity numbers used for administering subsidies like welfare disbursements, mobile-SIM registration, banking, and other government services. Advocates point to reduced fraud and streamlining benefit delivery, but repeated data breaches, including unauthorized access to personal information on black-market sites, have undercut public trust. While India's Supreme Court upheld Aadhaar's constitutionality, it imposed restrictions on mandatory linkage with services like banking and telecommunications. Nonetheless, critics maintain that requiring biometrics for essential services can exclude marginalized populations who struggle to provide usable scans, and that centralized storage of such sensitive data poses an ongoing risk of large-scale identity theft and state surveillance. This case demonstrates the ethical dilemma we examine, that biometrics here deliver remarkable convenience in public-service access but do so at the price of meaningful consent and against a backdrop of systemic risk from large-scale surveillance. Below I added a flowchart representing an overview of the case study.



C. *U.S. CBP's Biometric Entry-Exit Program*

Since 2018, U.S. Customs and Border Protection has deployed facial-recognition checkpoints at dozens of airports and land crossings, with pilots operating at 32 major U.S. airports by mid-2020 [32]. While CBP emphasizes reduced wait times and strengthened border security, civil-liberties advocates raise concerns over lengthy data retention, for non-U.S. citizens, images may be held for up to 14 days and, in some cases, transferred to long-term systems with retention periods as long as 75 years [31][32], and documented accuracy gaps across demographic groups, which demonstrate algorithmic bias that disproportionately misidentifies people of colour [1]. The program's data-sharing arrangements with law-enforcement and intelligence databases remain opaque [30], and travellers have limited avenues for informed consent or opt-out [31]. Together, these issues underscore the tension between streamlined, touchless processing and the potential for mission creep into pervasive surveillance architectures [19]. Below Kashfia added a flowchart representing an overview of the case study.

IV. MAIN ANALYSIS OF THE CASE STUDIES

Before analyzing each case study, it's important to understand the common ethical and technical dimensions that support all ten cases. In terms of biometric authentication, systems often promise enhanced efficiency and security, yet they simultaneously introduce new vectors for harm, ranging from individual privacy intrusions to systemic biases and governance gaps. The following analysis examines how each case embodies these tensions, highlighting recurring challenges in threat modeling, consent mechanisms, data protection, and oversight.

A. *Analysis of Case Study 1 - Clearview AI's Face Scraping Controversy:*

The Clearview AI case involves the large-scale collection and use of publicly posted images to build a facial recognition database, raising multiple security, privacy, and ethical concerns [20][22]. The system's unrestrained scraping practices and one-to-many matching models have led to wrongful identifications and exposed significant gaps in existing legal frameworks.

1) Threat Types Addressed or Introduced

Clearview AI was designed to enhance law enforcement capabilities by matching faces against a vast repository of images scraped from social media platforms. While intended to identify persons of interest quickly, this approach introduces high false-positive and false-negative rates, resulting in wrongful investigations and undermining trust in biometric authentication [20][21]. Its "collect everything" model ignores the principle of least privilege, enabling adversaries to exploit the dataset for illicit purposes, such as stalking or identity theft [20].

2) Data Security

Although Clearview likely stored biometric templates as hashed representations, weak key management and the absence of advanced template-protection techniques leave these hashes susceptible to reverse engineering or linkage attacks [20]. No robust access controls were in place to restrict scraping bots or internal misuse, resulting in an unvetted dataset that could be exfiltrated or re-identified when combined with other open-source data [20][24].

3) Cryptographic Concerns

Public information about Clearview's encryption practices is limited. It is assumed that biometric templates were hashed, but reliance on reversible or outdated hashing algorithms and inadequate key rotation protocols means that once attackers gained access to encryption keys, they could reconstruct raw images or link hashes back to individuals [20][24]. The absence of template-protection schemes, such as secure multiparty computation or homomorphic encryption, further exacerbates the risk of mass de-anonymization [20].

4) Legal/Policy Gaps

Clearview exploited the lack of explicit prohibitions against scraping publicly available images for biometric purposes. At the time of its operations, no comprehensive biometric-privacy statute prevented the collection of social-media photos at scale, demonstrating that existing laws were not equipped to address emergent AI-powered scraping techniques [22]. Even after class-action lawsuits and regulatory scrutiny, cross-jurisdictional frameworks to govern large-scale image scraping and biometric profiling remain fragmented or nonexistent [22][23].

5) Ethical and Legal Considerations

Ethically, Clearview fails to uphold principles of fairness, accountability, transparency, and explainability. Individuals have no means to verify whether their images are included in the database or to correct misidentifications. The one-to-many matching model compounds bias issues, as error rates vary across demographic groups, undermining due process [20][21]. Legally, while some settlements impose restrictions on Clearview's practices, there is still no clear pathway for affected individuals to seek remediation or exercise data-subject rights under existing privacy laws [23].

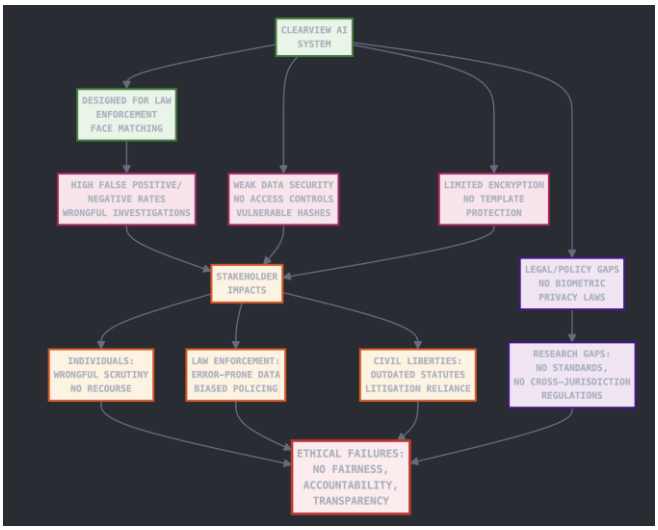
6) Impact on Key Stakeholders

- Individuals: Face wrongful scrutiny, reputational harm, and loss of anonymity; lack recourse to challenge or correct false matches [20][21].
- Law Enforcement: Gains rapid identification capabilities but risks relying on error-prone data, potentially leading to biased policing and civil-liberties violations [20][21].
- Technology Partners: Airlines and third-party integrators may inadvertently facilitate mass surveillance without sufficient audits or compliance mechanisms [24].
- Civil Liberties Groups: Struggle to hold Clearview accountable under outdated statutes, forcing reliance on litigation to enforce basic privacy rights [22].

7) Research Gaps or Unresolved Challenges

- No standardized methodology exists to measure false-match and false-non-match rates in operational, real-world image sets [20][21].
- Cross-jurisdictional regulations explicitly addressing large-scale image scraping for biometric databases remain undeveloped [22].
- Accountability and transparency metrics for one-to-many facial recognition systems have yet to be defined [20].
- Cryptographic schemes that protect massive biometric repositories against reverse engineering while maintaining matching accuracy are still lacking [20][24].
- Longitudinal studies quantifying privacy implications of mass aggregation and re-identification through linkage attacks are urgently needed [24].

Below, Kashfia added a flowchart representing an overview of the case study analysis.



B. *Analysis of Case Study 2 - India's Aadhaar Biometric ID System:*

The Aadhaar program in India centralizes fingerprint and iris scans for over a billion residents to provide unique identity verification for access to services [25][26]. While aiming to streamline welfare distribution, its scale introduces significant security, privacy, and ethical challenges that remain underexplored.

1) Threat Types Addressed or Introduced

Aadhaar was implemented to prevent identity fraud and improve service delivery by using biometric-based authentication. However, frequent scan failures, particularly among elderly or labor-intensive workers, lead to exclusion errors that deny legitimate beneficiaries access to essential services [27][28]. The large, centralized repository becomes a high-value target for both external attackers and insider misuse, enabling unauthorized API access and reconstruction of hashed templates once encryption keys are exposed [26][29].

2) Data Security

Despite employing encryption to protect biometric templates, Aadhaar's reliance on reversible encryption and inconsistent key management practices have led to multiple data breaches [29]. Insecure API endpoints and lack of continuous monitoring allowed unauthorized entities to access profile data, resulting in the reconstruction of hashed templates and potential identity theft [26][29]. Fine-grained access controls are absent, permitting service providers to request more data than necessary, violating the principle of least privilege [26][28].

3) Cryptographic Concerns

Aadhaar's initial use of reversible encryption, rather than irreversible biometric-tokenization techniques, exposed raw biometric templates when encryption keys were compromised [29]. The absence of robust cryptographic safeguards like bloom filters or secure sketch mechanisms makes it easier to reconstruct or link biometric data. Continuous key rotation strategies and hardware-based key storage are not universally enforced, leaving vast segments of the database vulnerable [26].

4) Legal/Policy Gaps

Although Indian courts have limited mandatory Aadhaar linkage for banking and telecom, there are no enforceable data-minimization or retention limits, causing templates and metadata to remain stored indefinitely [27][29]. Privacy laws lack specific provisions for large-scale biometric collection, leaving Aadhaar data subject to broad retention without clear deletion protocols [29]. Regulatory oversight is fragmented, with no unified framework to audit nor impose sanctions on misuse [26].

5) Ethical and Legal Considerations

Mandating Aadhaar for essential services raises severe surveillance and concerns about consent. Many rural or older populations with worn fingerprints frequently experience scan failures, effectively excluding them from welfare programs, which infringes upon their fundamental rights [27][28]. Ethically, the aggregation of biometric data without granular consent mechanisms violates individual autonomy, while the potential for linkage attacks with other government databases amplifies privacy risks [26][29].

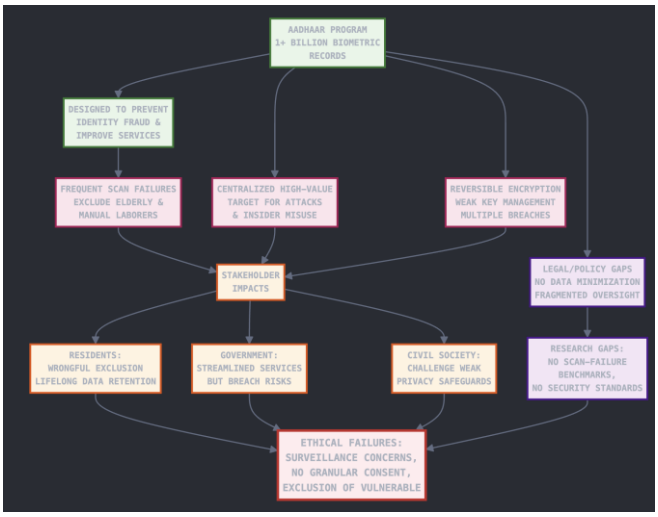
6) Impact on Key Stakeholders

- Residents: Vulnerable to wrongful exclusion from services due to unreliable authentication; face lifelong retention of biometric data without recourse [27][28].
- Service Providers: Lack clarity on necessary data scope, leading to over-collection and misuse; potential legal liability if systems fail [26].
- Government Agencies: Benefit from streamlined beneficiary verification but risk massive breaches and reputational damage; unclear accountability frameworks hamper oversight [26][29].
- Civil Society and Advocacy Groups: Challenge absence of enforceable privacy safeguards and push for robust data protection laws; struggle against entrenched institutional inertia [27][29].

7) Research Gaps or Unresolved Challenges

- No standardized benchmarks exist to quantify real-world scan-failure rates across diverse demographic groups, leading to unreliable authentication metrics [27][28].
- Formal API security benchmarks for large-scale biometric systems, including continuous monitoring for unauthorized access, have yet to be defined [26][29].
- Legal definitions and enforcement mechanisms for biometric data minimization and retention remain absent, leaving long-term data exposure unregulated [29].
- Anonymization and de-identification techniques that balance authentication accuracy with reduced re-identification risk are underexplored [26][29].
- Comprehensive socio-economic studies measuring the impact of biometric exclusion on vulnerable populations have not been conducted [28][29].
- The evolution of linkage-attack methodologies when Aadhaar data is fused with other public datasets remains poorly understood, leaving cumulative privacy exposure unquantified [29].

Below, Kashfia added a flowchart representing an overview of the case study analysis.



C. *Analysis of Case Study 3 - U.S. CBP's Biometric Entry-Exit Program:*

The CBP Biometric Entry-Exit Program uses biometric facial comparison technology for identity verification of travellers entering and exiting the United States [31]. The conversation history notes that CBP has rolled out facial-recognition checkpoints at 32 major U.S. airports for arriving and departing travellers. While CBP asserts this system enhances border security, civil-liberties groups raise concerns about lengthy data retention and algorithmic bias.

1) Threat Types Addressed or Introduced

The CBP Biometric Entry-Exit Program was developed to enhance national security and enforce immigration law by using biometric facial comparison technology to verify travellers entering and leaving the United States. This system aims to streamline travel while identifying individuals who may pose a security threat by matching their facial images against law enforcement databases [2]. The program includes successful cases like identifying travellers with criminal histories attempting to leave under false identities [19]. However, it introduces the risk of false positives, which can allow someone using a false identity to pass through, and false negatives, which may delay or flag legitimate travellers. Although false negatives typically lead to manual review, false positives can undermine the integrity of security measures [2].

2) Data Security

CBP's facial recognition system is hosted in a secure cloud-based environment [31]. For U.S. citizens, images are retained for no more than 12 hours and are deleted after the identity check. For non-U.S. citizens, images are stored for 14 days in the Automated Targeting System Unified Passenger Module (UPAX) and later transferred to the IDENT system where they may be retained for up to 75 years [2]. The Traveler Verification Service (TVS), a public-private partnership, operates this infrastructure, relying on private airlines and cruise lines. While CBP audits some air partners for compliance with privacy rules, as of 2022 only five audits had been conducted with three more underway, and no comprehensive audit plan exists for other partners such as those at land and seaports [1]. Concerns have also been raised following a data breach involving a CBP subcontractor, questioning the security practices of third-party partners [2].

3) Cryptographic Concerns

Public documents do not provide detailed information on the cryptographic protections or encryption practices used within the CBP's biometric systems. The lack of transparency on cryptographic measures constitutes a gap in understanding the full security posture of the system [2].

4) Legal/Policy Gaps

The development of the biometric entry-exit system has been mandated by Congress through a series of acts since 1996, including updates after 9/11 to incorporate biometric features and law enforcement interoperability [2]. Despite this statutory basis, the biometric exit portion remains only partially operational due to infrastructure, staffing, and planning issues [2]. Furthermore, GAO reports indicate that CBP has not fully implemented required actions such as ensuring complete and visible privacy signage, developing a thorough audit plan for all commercial partners, and ensuring consistent photo capture across all sites [1]. These gaps suggest challenges in meeting both legislative intent and operational effectiveness.

5) Ethical and Legal Considerations

CBP maintains that its facial recognition program is not a surveillance initiative, emphasizing that travelers are informed through signs and public announcements [31]. U.S. citizens are allowed to opt out of biometric checks in favor of manual document inspection [31]. Nonetheless, civil liberties groups have expressed concerns over the clarity and consistency of opt-out signage and notices, particularly given that non-U.S. citizens do not have the same opt-out rights [1][2]. Additionally, accuracy disparities remain a concern. Although CBP claims minimal demographic bias based on internal analyses, independent studies suggest that facial recognition technologies generally exhibit variable accuracy across age, gender, and racial lines [2].

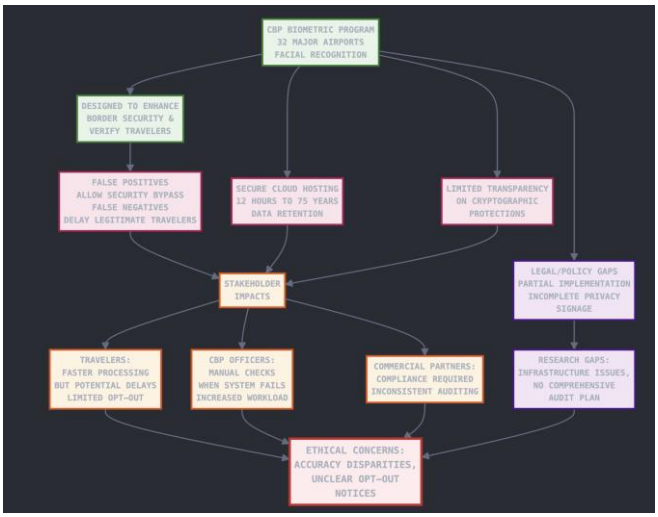
6) Impact on Key Stakeholders

For travelers, the program offers potential benefits such as reduced processing time and a smoother travel experience. However, false matches can delay or inconvenience legitimate travelers, and non-U.S. citizens lack opt-out rights that U.S. citizens have [2][31]. Commercial partners, including airlines and cruise lines, must comply with CBP's privacy rules, but lack of consistent auditing undermines assurance of compliance [1]. CBP officers must perform manual checks when biometric verification fails or travelers opt out, which could increase workload and reduce efficiency goals [2].

7) Research Gaps or Unresolved Challenges

The biometric exit program still faces multiple unresolved challenges. CBP must address infrastructure and staffing gaps that have slowed the rollout of the system [2]. Additionally, comprehensive audit procedures for all commercial partners remain undeveloped, and CBP continues to rely on voluntary participation by airlines, making consistent data collection difficult [1]. There is also concern about the adequacy of traveler notifications and opt-out explanations, particularly for U.S. citizens [1][2]. More transparency is needed regarding the cryptographic methods employed to secure biometric data. Further research should assess whether the system achieves its stated goals without compromising individual rights and explore the full operational implications of errors such as false matches and non-matches on the travel process [2].

Below, Kashfia added a flowchart representing an overview of the case study analysis.



V. Policy Recommendations or Strategic Insights

A. *Policy Recommendations or Strategic Insights of Case Study 1 - Clearview AI's Face-Scraping Controversy:*

In response to the ethical and legal concerns raised by Clearview AI's facial recognition practices, several policy actions are necessary. First, governments should establish clear consent laws that prohibit companies from collecting biometric data without explicit, informed opt-in from users, even when that data is publicly available. The fact that Clearview scraped billions of photos from social media without user permission highlights the urgent need for this kind of regulation [10]. Alongside this, legislation should directly address and restrict the mass scraping of biometric data from public websites, preventing companies from exploiting loopholes around "publicly posted" content [10]. To improve transparency and oversight, companies like Clearview must be required to publish regular reports that disclose how their data is collected, what it's used for, who it's shared with, and how often errors occur [10]. Their systems should also be subject to independent audits that test for bias, accuracy, and misuse, especially since one-to-many facial matching is prone to false positives [13]. Another important step would be to move away from centralized biometric databases and instead adopt decentralized or federated systems that limit the damage caused by a single breach. Finally, people affected by wrongful matches or unauthorized use of their data should have a clear legal pathway to dispute and correct their biometric records, as well as seek compensation if harm is caused.

B. *Policy Recommendations or Strategic Insights of Case Study 2 - India's Aadhaar Biometric ID System:*

Similarly, the Aadhaar biometric ID system in India presents significant privacy and security risks, particularly due to its scale and centralized nature. To address these issues, the program should implement strong data minimization policies that only collect what is necessary and enforce strict limits on how long biometric data is stored [18]. Data that is no longer needed should be securely deleted. Technical improvements are also essential as biometric data must be encrypted using strong, modern encryption standards, and the keys used to protect this data must be managed in a secure and auditable way [17]. There also needs to be tighter access control; service providers using Aadhaar data should only be allowed to request the minimum information required for a given task, and all data requests should be logged and reviewed through regular audits [18]. To make Aadhaar more inclusive, especially for people whose fingerprints or iris scans don't work reliably (like elderly citizens or manual laborers), alternative verification methods such as mobile OTPs or assisted verification should be supported [17]. Decentralizing the matching process, so that it can be done on secure local devices rather than in centralized databases, would reduce the risk of mass surveillance and make Aadhaar more privacy friendly. Lastly, citizens should have enforceable rights when it comes to how their biometric data is used. This includes the right to view their stored data, opt out of certain uses, and appeal when services are unfairly denied due to biometric issues—all under the guidance of an independent regulatory body [17].

C. *Policy Recommendations or Strategic Insights of Case Study 3 - U.S. CBP's Biometric Entry-Exit Program:*

The biggest security concerns regarding the U.S. Customs and border Protection's (CBP) use of biometric authentication include a lack of regular auditing [1], lack of transparency in data collection and security, insufficient communication of individuals' rights [1], and gaps in infrastructure and staffing [2]. A critical concern highlighted is the third party's compliance with CBP's privacy regulations. These concerns arise due to the inconsistent system standards and inadequate auditing practices [1].

To address transparency concerns, there needs to be improved disclosure of cryptographic methods used and ensuring all individuals subject to biometric screening are clearly informed regarding biometric data collection, retention, and their rights.

The Global Entry kiosks demonstrate effective transparency by providing language options and clear consent prompts, ensuring individuals are adequately informed [3]. This model should be adopted as the standard for biometric facial scanning systems used in U.S. CBP.

Providing information about biometric data collection and retention in advance is essential for promoting ethical and transparent border security practices when implementing this new safety standard. This information should be included in flight information emailed to passengers, giving individuals sufficient time to understand the process and consider options regarding their participation. For non-citizens, who are not granted opt-out rights, early notification is especially critical. It ensures they are aware of compulsory biometric authentication and allows them to make informed decisions about whether they wish to proceed with travel. Then their proceeding with travel would be implied consent, where they have been given proper information prior to. Given the stress of air travel and limited time at border crossings, advanced transparency is essential to maintain ethical standards and ensure informed consent.

The CBP currently has standards for practices surrounding this biometric authentication system, but due to lack of auditing it is unclear if these practices are being followed by third-party participants. [1] A regular auditing schedule must be implemented across all participating border control points to ensure consistent compliance with data protection and privacy requirements. Auditing should: verify secure data storage practices, identify any gaps in staffing or infrastructure and adherence to transparency measures. These transparency measures would be signage, notification, and consent

surrounding biometric data collection and retention. Additionally, standards for participating in border patrols prior to application of this new security system are needed.

Prior to the implementation of this biometric authentication system, participating border patrols need to meet defined operational and compliance criteria. This would include adequate staffing, appropriate infrastructure, sufficient budget allocation, designated space for accessible and multilingual signage, and robust security measures in line with federal privacy and data protection standards. These requirements should align with CBP Privacy Impact Assessments (PIAs) [8], NIST [6] cybersecurity guidelines, and DHS Fair Information Practice Principles (FIPPs) [9]. Establishing these standards will ensure transparent, ethical, and secure operations prior to the implementation of this new system.

Due to limited transparency around current cryptographic methods, these mitigations may be redundant since it is unclear whether some advanced protections are already in place. However, it is essential that raw biometric data is never stored. Instead, enclave-based storage and end-to-end encryption must be implemented. The U.S. Customs and Border Protection (CBP) has begun exploring post-quantum cryptography (PQC) to strengthen the security of biometric and sensitive personal data. [4] Current code-based encryption systems are increasingly vulnerable as quantum computers advance. 'Harvest now, decrypt later' [4] attacks are rising. This is when encrypted data is collected to be decrypted later by more advanced quantum computers. To ensure smooth transition and mitigation against these new attacks, a hybrid cryptographic system needs to be adopted. Which implements a layer of pre-quantum security measures and then another layer of post-quantum security measures. [5] This system will ensure dual-layer protection against attacks or in the event of failures and ensure a smooth transition to quantum-resilient infrastructure.

The CBP is starting to align its cryptographic practices with a framework from the National Institute of Standards and Technology (NIST) [6][7], to create encryption algorithms that can withstand quantum attacks. This will be one of the standards that third parties must adopt to deploy these biometric authentication systems. The post-quantum algorithms adopted from the NIST framework [6] that will be applied are CRYSTALS-Kyber, CRYSTALS dilithium, and SPHINCS+. CRYSTALS-Kyber is used to encrypt biometric templates, providing quantum-resistant confidentiality. [6] CRYSTALS dilithium will be applied to authenticate biometric data signing, to ensure tamper resistance, and enable breach detection [6]. SPHINCS+ is a hashed-based signature that will be applied for long term storage of biometric data in CBP systems [6]. These algorithms all selected by NIST for standardization bust be baseline requirements for securing CBP's biometric authentication systems [6]. As quantum computing evolves, adopting and enforcing these encryption standards will be essential to maintain privacy, integrity, and trustworthiness of biometric authentication.

VI. Conclusion

The case studies of Clearview AI, India's Aadhaar system, and CBP entry exit system highlight the complex trade-offs involved in deploying biometric authentication technologies. While these systems offer significant convenience and operational efficiency, they also raise critical ethical concerns, particularly around user's consent, privacy, and fairness. Clearview's mass scraping of facial images without consent, combined with opaque law enforcement use, demonstrates how biometric systems can quickly outpace regulatory safeguards and infringe on individual rights [10][11]. Similarly, Aadhaar's centralized collection of sensitive biometric data has led to exclusion, technical failures, and privacy risks, especially for vulnerable populations [12][13].

These cases underscore a core message: the success of biometric systems depends not just on technological robustness, but on ethical design, legal accountability, and transparent consent mechanisms. Systems that prioritize control over users instead of empowering them risk becoming tools of surveillance and inequality. True trust in biometric authentication must be earned through policies that embed ethics into design, give users agency over their data, and minimize harm.

As biometric technologies continue to expand globally, future work must focus on developing universal transparency standards, secure and decentralized storage solutions, and mechanisms to prevent demographic exclusion. The promise of convenience must never come at the expense of human dignity and informed choice.

VII. References

[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.

[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?
[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.

VIII. APPENDIX

CONTRIBUTION STATEMENTS

A. Kashfia Karder’s Contribution

I took the lead on identifying and researching three real-world case studies about our topic. I drafted the comprehensive case-study narratives for all three case studies (No. 5 from the requirements outline). I wrote the in-depth analysis (No. 6 from the requirements outline), including threat modeling, access-control, and cryptographic considerations, legal/policy gaps, and ethical impacts, for the first two case studies: Clearview AI and Aadhaar Biometric ID System. In the report, in addition to writing, I also drew all the flowcharts. I created the slides according to my part of the work. Through this process, I deepened my understanding of how large-scale biometric deployments can both streamline services and erode individual privacy and gained knowledge about the unresolved challenges that must be addressed in future work. Our group maintained close communication through frequent online calls/messages, and we used Microsoft Word/PowerPoint’s co-authoring features to edit, ensuring a cohesive and well-coordinated final report.

B. Vianne Watson’s Contribution

For this project, I was responsible for writing the introduction, abstract, and mitigation strategies related to the third case study, the CBP Entry/Exit system. Through my research, I gained valuable insight into NIST guidelines, hybrid encryption systems, and post-quantum cryptography (PQC). Given my recent travel experiences, it was especially interesting to learn about the encryption methods and logistical frameworks behind biometric authentication at the border. I also deepened my understanding of ethical considerations surrounding data collection and retention. Additionally, I developed my skills in writing a scientific research paper, which will be a very valuable skill as I progress in my academic career. Our group collaborated by dividing tasks based on availability, strengths, and preferences. With members who were available earlier, taking on time-sensitive sections like initial research. We stayed connected through regular check-ins during tutorials, group chats, and group calls to stay on track with our goals. I used Microsoft Word and PowerPoint’s co-authoring tools alongside Grammarly’s AI editing features to enhance grammatical accuracy, spelling, and ensuring a professional tone in my writing.

C. Hsuan-Han Liu’s Contribution

For this project, I was responsible for writing the full Background and Related Work section, which involved reviewing and synthesizing multiple scholarly and industry sources to provide a strong conceptual foundation for our topic. I also contributed to the main analysis by writing the technical and ethical evaluation of the U.S. CBP facial recognition program. In addition to content writing, I took the initiative to design the title slide for our presentation, led the creation of the initial PowerPoint structure, and finalized the citation and reference list to ensure consistency and proper formatting across the report. This experience sharpened my skills in academic research synthesis, critical

analysis of biometric infrastructure, and professional presentation design. Our team collaborated through regular updates, shared editing tools, and clear task division, which allowed us to complete a successful final submission.

D. Jaiveer Toor's Contribution

For this project, I was responsible for writing policy recommendations and strategic insights for Clearview AI and Aadhaar case studies, which were originally researched and analyzed by another group member. I also wrote the conclusion section of the report, using insights from those two case studies to summarize the ethical, legal, and technical challenges associated with biometric authentication. Through this work, I learned how important consent, transparency, and inclusive access are when it comes to deploying biometric systems responsibly. Our group collaborated by clearly dividing sections, sharing slides and notes over group chat, and checking in regularly to ensure each person stayed on track.