Ethics of Facial Recognition: A Comprehensive Analysis

Brandon Keung[1], Jiaheng Dai[1], Jiayi Dong[1], and Pei Tian[1]

[1] *Columbia University, Fu Foundation School of Engineering and Applied Science*

Course:
ENGI E4800 Data Science Capstone & Ethics

Date:
May 19, 2025

Contents

1 Introduction

Facial recognition technology (FRT) stands at the intersection of technological innovation and profound ethical considerations. As these systems have evolved from basic detection algorithms to sophisticated neural network architectures capable of real-time identification across diverse conditions, their deployment across law enforcement, commercial sectors, and government surveillance has raised significant concerns about privacy, consent, algorithmic bias, and democratic freedoms. In this report, we examine the technical foundations of facial recognition, its varied applications, ethical implications, regulatory approaches across jurisdictions, competing stakeholder interests, and governance frameworks—critically exploring the complex landscape in which this powerful technology continues to develop and reshape society.

2 Technical Foundations of Facial Recognition

Facial Recognition Systems Overview

Facial recognition systems typically follow a three-step process: detection, alignment, and matching. Detection involves identifying the presence and location of a face in an image or video stream using deep learning-based detectors such as MTCNN [1] or YOLO. Once detected, facial alignment is performed to normalize the pose and orientation of the face using key landmarks like the eyes and mouth. This step ensures consistency and robustness across images. Finally, the system encodes the aligned face into a feature vector using neural networks such as FaceNet [2] or ArcFace [3], enabling efficient comparison and matching based on vector similarity metrics.

Key Technical Components and Algorithms

Modern facial recognition relies heavily on deep learning. For face detection, algorithms like Haar cascades were traditionally used but have been largely replaced by approaches like RetinaFace

Data Requirements and Processing Methods

Training high-performing facial recognition systems requires large-scale, diverse datasets. Public datasets like LFW, CASIA-WebFace, VGGFace2 [6], and MS-Celeb-1M [7] provide millions of labeled images. Data preprocessing includes image resizing, normalization, and alignment to ensure consistency. Data augmentation techniques such as rotation, cropping, and color changes are employed to improve generalization. Feature vectors extracted from the models are often stored in efficient indexing structures (e.g., FAISS) to enable fast nearest-neighbor searches during recognition.

Accuracy Metrics and Performance Evaluation

Facial recognition systems are evaluated using both verification (1:1 matching) and identification (1:N matching) metrics. Common accuracy metrics include False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER). The ROC

(Receiver Operating Characteristic) curve is widely used to visualize the trade-off between FAR and FRR. Systems strive to minimize EER and maximize overall accuracy across varying conditions, especially in critical use cases such as government identification programs [5].

Capabilities and Limitations

Facial recognition technology has reached impressive levels of performance, especially in controlled environments. It can operate in real time, match across age and expressions, and integrate emotion recognition. However, it also has significant limitations. Biases in training data can lead to reduced accuracy across ethnicities and genders, as highlighted by Buolamwini and Gebru in their study on commercial systems [13]. Privacy concerns are prominent, especially when systems are deployed without user consent. Furthermore, facial recognition is vulnerable to spoofing via photos or masks, though liveness detection techniques are improving resilience. Environmental factors like lighting, occlusion, and camera quality remain challenges.

3 Applications and Use Cases

Law Enforcement and Security Applications

Police agencies increasingly utilize FRT to aid in criminal investigations by matching faces from surveillance footage or witness images against databases of known individuals. A 2023 report from the U.S. Government Accountability Office (GAO) revealed that seven federal law enforcement agencies, including the FBI and U.S. Marshals Service, used facial recognition provided by commercial and non-profit entities. Notably, over 60,000 facial recognition searches were performed without formal training or established policy safeguards, raising concerns about potential false matches and civil rights violations [14]. Without standardized protocols, there's a higher risk of misidentification, leading to severe consequences such as wrongful arrests, highlighting the need for transparency and oversight in deploying FRT.

At international borders, FRT is employed to verify the identities of travelers and detect flagged individuals. U.S. Customs and Border Protection (CBP) has implemented biometric facial comparison systems at all international arrival airports, numerous seaports, and land crossings. These systems match live photos against government databases, facilitating the detection of imposters and improving customs procedure efficiency. As of 2022, CBP reported processing over 200 million travelers using facial recognition, achieving match rates exceeding 98% [15]. To address privacy concerns, CBP has instituted measures such as deleting biometric data of U.S. citizens within 12 hours of collection and providing opt-out options at most locations.

Government agencies also deploy facial recognition in public areas to monitor large crowds and identify persons of interest in real time. This is often integrated with CCTV systems in locations such as airports, stadiums, and major city intersections. In early 2024, the London Metropolitan Police significantly expanded its deployment of live facial recognition (LFR) technology to enhance public safety, leading to over 500 arrests for offenses ranging from shoplifting to serious crimes like rape [17]. However, the widespread use of LFR raises concerns about mass surveillance and the disproportionate impact on marginalized communities [18]. Facial recognition technology is frequently combined with

tools like license plate readers, crowd analytics, and video management software (VMS) to create comprehensive surveillance networks. Solutions from companies like Milestone Systems demonstrate how FRT can be incorporated into broader smart city or enterprise security systems, offering analytics, real-time monitoring, and access control [19].

Commercial and Consumer Uses

Facial recognition is increasingly adopted to secure access to personal devices and digital services. Smartphones commonly feature face authentication for unlocking screens and approving payments. In the financial sector, banks and fintech platforms utilize FRT to verify user identities during sensitive transactions, enhancing fraud prevention and user convenience. Applications such as Face ID enable customers to authenticate by scanning their face, eliminating the need for passwords or physical cards and reducing the risk of unauthorized access.

Private companies across technology, retail, banking, and marketing sectors see lucrative opportunities in facial recognition. Tech firms such as Amazon, Microsoft, and Clearview AI have developed or deployed FRT platforms for access control, targeted advertising, and customer analytics. The market for facial recognition technologies is projected to grow significantly, with estimates surpassing $12 billion globally by 2026 [10]. However, commercial entities often prioritize trade secrecy and proprietary algorithms, resisting transparency that could expose systems to critique or regulation [11], creating tension between innovation and accountability.

Businesses are increasingly adopting FRT to streamline employee attendance and access control. These technologies automate check-ins, reduce timekeeping errors, and help prevent practices like "buddy punching." For example, Timeero offers a facial recognition time clock that uses advanced AI to verify employee identities during clock-ins and alerts managers in case of mismatches [16]. While effective, these tools also raise concerns about workplace surveillance and data privacy.

Competing Stakeholder Perspectives on FRT

Governments and law enforcement agencies view facial recognition as a tool to enhance public safety and operational efficiency. It enables quicker suspect identification, real-time surveillance, and streamlined border security, critical in responding to crimes and preventing terrorist threats. The FBI, for instance, has integrated facial recognition into its biometric database for investigative support [8], while cities like New York and London have piloted or deployed FRT for crowd monitoring and event security. Advocates within this sector argue that the benefits outweigh privacy concerns, particularly when the technology is used with appropriate oversight [9].

Conversely, civil rights organizations express deep concern over the social implications of facial recognition, especially regarding racial bias, surveillance, and due process violations. Studies, including those by MIT and the ACLU, have shown higher error rates for people of color and women, raising alarm about systemic discrimination in law enforcement use [13, 12]. These groups advocate for strict regulation, greater transparency, and—in many cases—moratoria or outright bans on facial recognition technologies. Their stance is grounded in protecting individual freedoms, privacy, and democratic accountability.

4 Privacy and Ethical Concerns

Fundamental Privacy Issues

One of the primary concerns with facial recognition is privacy. To construct an advanced facial recognition system, developers need a large high-quality datasets. To develop such a dataset, data could be pulled from public cameras, commercial systems, and social media. Although some of these can be considered public developers are not getting explicit consent from individuals who are being captured. On top of this, ethic questions such as who can access these, can facial data be sold, shared, or even hacked arise. [20]

Assuming all data is acquired ethically (with permission from individuals), biases in facial recognition systems are very common. A likely cause of this could be how the data was collected. Many studies show facial recognition systems perform worse on color and non-male individuals. This can be a major issue, especially if these facial recognition systems are used for government systems. One use case could be at airports to verify individuals at security points. If a facial recognition system were developed with a bias for white males, the airport facial recognition system could flag minority groups for due to technical problems, which would be unethical. [20]

Uniqueness of facial data as identifiers

The existence of hackers causes another layer of problems. If facial data were collected with consent, hackers could hack and access this data, much like passwords or credit cards. Passwords and credit cards can cause major problems for individuals. However, passwords and credit cards can be changed or cancelled. Facial data can not. A faceprint is permanent and is an intrinsic link to one's identity. Once leaked or hacked, there are no clear "fixes". [27]

Algorithmic Bias and Discrimination

Continuing off this idea, numerous evaluations have shown that government and commercial facial recognition algorithms perform unfairly across different demographics. In particular, error rates tend to be significantly higher for matching women and people with darker skin tones. These examples across different organizations (government and commercial) originate from biases in training data and model design. [26]

Impact on marginalized communities

These accuracy gaps do not exist in a vacuum—they exacerbate longstanding social inequities. The U.S. Commission on Civil Rights warns that unregulated deployment of facial recognition poses "significant risks to civil rights, especially for marginalized groups who have historically borne the brunt of discriminatory practices," from wrongful stops and arrests to exclusion from services and public spaces. Addressing these disparities requires rigorous testing, transparent reporting, and the ability to suspend systems that fail to meet fairness thresholds. [27]

Impact on free expression and association

The constant use of facial surveillance can indirectly lead to a restriction on freedom of speech and assembly. With unchecked usage, governments can utilize facial recognition systems at protests or community gatherings, causing many individuals to be less likely to express their opinions freely. [26]

Implications for democratic freedoms

Currently, facial recognition usage varies across different nations. Some nations call for an all out ban while others push for transparency and consent when it comes to facial recognition. The European Union classifies facial recognition as a high risk, requiring strict oversight on such systems. However, the United States of America is much more fragmented in regulations. Some states and cities have varying policies. Regardless, policy makers, engineers, and the general public must work together to define a boundary for what is considered "acceptable" usage of facial recognition systems. [29]

5 Future Ethical Implementation of FRT

While the challenges of facial recognition technology are significant, they are not insurmountable. The ethical concerns outlined above have prompted researchers, policymakers, and industry stakeholders to develop frameworks and practices that could enable more responsible implementation of FRT systems. By addressing fundamental issues of privacy, consent, transparency, and fairness through deliberate design choices and regulatory oversight, it may be possible to harness the benefits of facial recognition while mitigating its most harmful potential impacts.

Ethical Design Principles

Achieving an ethical implementation of FRT requires a responsible technology development process. Privacy by Design (PbD) and privacy by default is one way. This approach means to integrate privacy protections into the fundamental architecture of facial recognition systems rather than adding them later. Implementing PbD includes minimizing data collection, encrypting facial templates, automatically deleting images after processing, and preventing unauthorized use through system architecture. Some regulatory entity like EU's General Data Protection Regulation (GDPR) has already started to require "systems to be implemented where 'privacy by design' (PbD) and 'privacy by default' are inbuilt for any personal data processing" [23].

We also need a proper risk assessment framework that provide methodologies for identifying and mitigating ethical concerns before deployment. The International Compliance Association emphasizes that assessments must evaluate potential harms across multiple dimensions, including privacy violations, discriminatory outcomes, function creep, and security vulnerabilities[25]. These evaluations should occur during design, before deployment, and regularly during operation, involving diverse stakeholders to ensure comprehensive impact analysis.

Consent and Transparency Measures

While the technology needs to be inherently ethical, organizations also need to implement explicit opt-in processes that clearly communicate what facial data will be collected, how it will be used, and who will have access to it. Effective practices include plain and concise language explanations of capabilities, realistic risk assessments, and accessible consent mechanisms that allow individuals to withdraw consent easily, which is very important[26]. The technology should only collect information necessary for stated purposes and these collected facial data should not be repurposed for other uses without explicit consent. One more critical but very challenging component of ethical implementation, which was mentioned in class, is requiring organizations to establish transparent data retention policies with automated deletion protocols, while developing comprehensive governance frameworks that document data flows and establish clear accountability mechanisms. Even though it seems to be very hard to achieve in short term, we hope to see it in a risk free world some days in the future.

Addressing Algorithmic Bias

Now we will go into to a more technical side. To address the algorithmic bias issue, testing must occur throughout the development pipeline—from pre-training data analysis to post-deployment monitoring—utilizing both synthetic validation sets and real-world deployment scenarios. These evaluation protocols should employ stratified sampling techniques across demographic subgroups, calculating disaggregated performance metrics including false positive rates (FPR), false negative rates (FNR), and area under receiver operating characteristic curves (AUC-ROC)[32].

6 National-Level Regulatory Landscape

With these ethical implementation frameworks and regulatory approaches in mind, we would like to explore the existing policies being enforced in different countries. In this section, we will examine the current global landscape of facial recognition governance.

International policies

Internationally, under international human rights laws, countries have the obligation to protect individuals by regulating against AI systems such as facial recognition. This means that countries are required to implement legal frameworks to govern FRT's use, ensuring that it aligns with general principles of legality. Such regulations could be on the purpose of FRT, design, circumstance of deployment, etc. [29]

To ensure the deployment of FRT meet regulatory standards, it is essential to mandate formal impact assessments. Data protection Impact Assessments and Human Rights Impact Assessments can evaluate fairness, and privacy risks protecting the general public from privacy violations as well as discriminatory FRT. These assessments should be made publicly available allowing anyone to test existing and used FRT. Through this, a transparent and fair basis can be made, creating a stable baseline for legal challenges and future policy adjustments [23]

United States Approach

The U.S. has no comprehensive federal law specifically regulating facial recognition technology, with federal agencies following mainly advisory guidelines. This regulatory gap has prompted states and localities to create their own rules. Illinois led the way with its 2008 Biometric Information Privacy Act (BIPA), which uniquely allows individuals to sue companies directly for collecting facial data without written consent, resulting in major settlements with tech companies like Facebook[26]. Texas and Washington have passed similar but weaker laws without this private right to sue. Meanwhile, several cities including San Francisco, Boston, and Portland have completely banned government use of facial recognition, reflecting growing public concern about surveillance and civil liberties issues[30][31].

European Regulatory Frameworks

The EU regulates facial recognition within its broader data protection framework, particularly General Data Protection Regulation (GDPR). The GDPR classifies facial recognition data as biometric information requiring special protection and require facial recognition systems "to be implemented with 'privacy by design' (PbD) and 'privacy by default"'[23]. PbD requires privacy safeguards be built into technology from the earliest development stages, including data minimization, automatic deletion, and privacy-preserving processing methods. European courts have also established important legal boundaries through landmark cases. In Ed Bridges v. South Wales Police, the UK Court of Appeal found that police use of automated facial recognition violated legal standards, highlighting issues with transparency, data protection, and equality [29]. These rulings establish that facial recognition technology must be deployed with proportionality, necessity, and strong safeguards.

Global Variations in Approach

Different countries approach facial recognition regulation according to their unique social and political contexts. China has deployed facial recognition extensively for security, governance, and commercial purposes. While China has introduced some regulations requiring consent for facial recognition use, these rules typically exempt security applications and allow broad government deployment. Canada takes a contrasting approach centered on privacy protection. Canadian regulators emphasize obtaining consent, maintaining transparency, and limiting the purpose of facial recognition systems. The country's Privacy Commissioner has investigated both public and private facial recognition deployments, establishing expectations that include clear notification, meaningful consent options, and strict limitations on how the technology can be used[26].

7 Industry Regulatory Frameworks

While government regulations establish foundational legal frameworks for facial recognition technology, they face significant limitations when applied to multinational corporations operating across diverse jurisdictions. These global entities can navigate regulatory inconsistencies or locate operations in regions with minimal oversight, creating enforcement challenges. Consequently, industry-led initiatives and self-regulatory frameworks

have become essential complements to formal legislation, potentially establishing consistent ethical standards that transcend national boundaries.

Transparency requirements for vendors

In addition to formal impact assessments, FRT vendors can be required to publish extensive technical documentations on algorithmic development methodologies, training data sources, model performance metrics, and limitations. Model performance metrics can include impact assessments described earlier to ensure fair deployment of FRT. [28]

Self-regulatory practices

In addition to external (third-party and government) regulations, organizations are encouraged to have self-regulatory practices regarding facial recognition systems. Ethical codes of conduct, disciplinary review boards, mandatory risk and ethics trainings can promote self-regulations within companies and development teams. These self-regulatory measures can help to bridge gaps from formal regulations still emerging and the safeguarding the public needs from potentially dangerous AI technology. [25]

Industry privacy principles

Sector-wide privacy frameworks establish clear standards for consent and data collections. Organizations should follow privacy frameworks allowing for further transparency and privacy. Baking privacy design into FRTs before development can encourage and decrease the amount of regulatory violations from development teams. By following such sector-wide privacy frameworks, a genuine commitment to protecting individual rights can help shape industry practices. [28]

8 Conclusion and Recommendations

Throughout this report, we highlight the ethical risks of using facial recognition technology. These risks include privacy issues, biometric data, and discrimination within the models. To ensure these risks are minimized, it is important to enforce both self imposed regulations as well as third party regulations, ensuring the security of individuals and fair usage of FRT.

There must be a clear-cut legal framework that strikes a balance between protecting individual rights as well as fostering an innovative environment for FRT to grow. Impact assessments and transparency requirements (documentation and metrics) can help to promote innovation and protection of civil liberties. Although facial recognition systems are not new, ongoing research is needed to evaluate long-term impacts of such systems. Efforts to standardize benchmarks for fairness, privacy, and accuracy anre necessary to develop countermeasures to malicious FRT attacks such as deepfakes. In order to utilize FRT to its potential while maintaining a safe environment for individuals, policymakers and engineers need to collaborate to foster an innovative but safe environment for FRT.

References

[1] Kaipeng Zhang et al. *Joint face detection and alignment using multitask cascaded convolutional networks*. IEEE Signal Processing Letters, 2016.

[2] Florian Schroff, Dmitry Kalenichenko, and James Philbin. *FaceNet: A unified embedding for face recognition and clustering*. In Proceedings of the IEEE conference on computer vision and pattern recognition (CVPR), 2015.

[3] Jiankang Deng et al. *ArcFace: Additive angular margin loss for deep face recognition*. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2019.

[4] Jiankang Deng et al. *RetinaFace: Single-shot multi-level face localisation in the wild*. In CVPR, 2020.

[5] Patrick Grother et al. *Ongoing face recognition vendor test (FRVT) part 2: Identification*. NIST, 2018.

[6] Qiong Cao et al. *VGGFace2: A dataset for recognising faces across pose and age*. In FG 2018.

[7] Yandong Guo et al. *MS-Celeb-1M: Challenge of recognizing one million celebrities in the real world*. arXiv preprint arXiv:1607.08221, 2016.

[8] U.S. Government Accountability Office. *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, GAO-16-267, 2016.

[9] New York City Police Department. *Facial recognition: Impact and use policy*. `https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/facial-recognition-nypd-impact-and-use-policy_10.26.23.pdf`

[10] MarketsandMarkets. *Facial Recognition Market by Technology, Application, Vertical, and Region - Global Forecast to 2026*, 2022.

[11] Hill, Kashmir. *The Secretive Company That Might End Privacy as We Know It*, The New York Times, 2021.

[12] The perpetual line-up. *Perpetual Line Up*. `https://www.perpetuallineup.org/`

[13] Joy Buolamwini and Timnit Gebru. *Gender shades: Intersectional accuracy disparities in commercial gender classification*. In Conference on Fairness, Accountability and Transparency, 2018.

[14] U.S. Government Accountability Office. *Facial Recognition Services: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, GAO-23-105607, 2023.

[15] U.S. Customs and Border Protection. *Statement for the Record on Assessing CBP's Use of Facial Recognition Technology*, 2022. `https://www.cbp.gov/about/congressional-resources/testimony/statement-record-assessing-cbps-use-facial-recognition-technology`.

[16] Timeero. *7 Best Facial Recognition Attendance Systems in 2024*, 2024.

[17] France 24. *London police make 500 arrests using facial recognition tech*, 2024. https://www.france24.com/en/live-news/20241206-london-police-make-500-arrests-using-facial-recognition-tech.

[18] Hardesty, L. *Study finds gender and skin-type bias in commercial artificial-intelligence systems*, MIT News, 2018. https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.

[19] Milestone Systems. *Integrating Facial Recognition with VMS (Video Management Software)*, 2024.

[20] Tuhin, M.. *What is facial recognition technology? how it works and why it matters in 2025. Science News Today*, 2025. https://www.sciencenewstoday.org/what-is-facial-recognition-technology-how-it-works-and-why-it-matters-in-2025

[21] National Academies of Sciences, Engineering, and Medicine. *Advances in Facial Recognition Technology Have Outpaced Laws, Regulations*, 2024. https://www.nationalacademies.org/news/2024/01/advances-in-facial-recognition-technology-have-outpaced-laws-regulations-new-repo

[22] The Regulatory Review. *Facial Recognition Technologies.*, 2024. https://www.theregreview.org/2024/12/28/seminar-facial-recognition-technologies/

[23] Slack, D., Friedman, B., Givens, E. et al. *The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks.* AI & Ethics, 2, 377–387, 2020.

[24] PMC. *Beyond surveillance: privacy, ethics, and regulations in face recognition technology.*, 2024. https://pmc.ncbi.nlm.nih.gov/articles/PMC11256005/

[25] International Compliance Association. *Ethical compliance for facial recognition technology.*, 2024.

[26] IEEE Public Safety Technology Initiative. "Ethical Considerations in the Use of Facial Recognition for Public Safety.", 2024.

[27] Security Management Magazine. "Facial Recognition in the US: Privacy Concerns and Legal Developments.", 2021. https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2021/december/facial-recognition-in-the-us-privacy-concerns-and-legal-developments/

[28] Strategian: Science Magazine. "Facial recognition: technology and privacy.", 2025. https://www.strategian.com/2025/04/04/facial-recognition-technology-and-privacy-2/

[29] Qandeel, M. *Facial Recognition Technology: Regulations, rights and the rule of law.* Frontiers, 2025. https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1354659/full

[30] San Francisco bans facial recognition technology. (n.d.), 2019. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

[31] Wray, S. *Portland bans private companies from using facial recognition technology.* Cities Today, 2020.

[32] Buolamwini, J., & Gebru, T. *Gender shades: Intersectional accuracy disparities in commercial gender classification.* PMLR, 2018.