1. Introduction

- Brief overview of facial recognition technology and its growing applications
    - What is facial recognition(FR)? Why is it booming?
- Thesis statement about the ethical challenges it presents
    - Central question: to what extent can corporations ethically use facial recognition technology to monitor and influence consumer behavior, given concerns about consent, bias, and privacy?
        - Facial recognition technology should be used to PROTECT humans
        - Ethical concerns arise the most when influential tactics are being deployed via facial recognition
- Significance of addressing these concerns in today's data-driven society
    - Why it matters

2. Technical Background

- How facial recognition systems work (brief explanation)
    - Buolamwini, J., Ordonez, V., Morgenstern, J., & Learned-Miller, E. (2020). Facial Recognition Technologies: A Primer. Retrieved from https://people.cs.umass.edu/~elm/papers/FRTprimer.pdf
- Evolution of the technology and current capabilities
    - Face matching, face extraction, face recognition
    - https://www.fastcompany.com/91018783/types-of-face-recognition-technology-this-is-what-to-know-about-them-and-your-privacy
    - Why its cheaper, faster, more scalable now
- Different types of facial recognition systems
    - Live recognition, passive recognition, biometric linking

3. Applications and Use Cases Across Sectors

- Commercial: applications (social media, retail, marketing)
    - Retail (smart fridges, personalized ads)
    - Discord age verification
    - Amazon palm scanning
        - Amazon Wants Your Palm and TSA Wants Your Face. What Saying Yes Will Mean." WSJ, 2024 https://www.wsj.com/tech/personal-tech/amazon-wants-your-palm-and-tsa-wants-your-face-what-saying-yes-will-mean-3844a4d8
        - Amazon captures mathematical palm signatures
        - Amazon says it hasn't had a false positive after millions of consumer interactions
        - Could biometric reading in public places be permitted?(solely for public places, where being present is also required)

- Security and law enforcement applications
    - MSG legal tracking
        - Hill, Kashmir. “Which Stores Are Scanning Your Face? No One Knows.” New York Times, 2023, www.nytimes.com/2023/03/10/technology/facial-recognition-stores.html
        - Madison Square Garden uses facial recognition to bar entry to lawyers that are against the owners
        - Security concern - facial recognition should be used to bar individuals who pose a threat to others, not for private corporate reasons
    - Clearview AI
        - As we describe earlier, the private sector is integral to law enforcement operations; companies like Clearview AI often test and develop the facial recognition tools that are available to law enforcement or amass large databases that the government may have access to. Yet, in the absence of a nationwide comprehensive data privacy law, many companies face few legal limitations on how they collect, process, and transfer personal information—allowing Clearview and other companies to gather data from millions of people without clear controls to access or delete their images, and with few safeguards for security, algorithmic bias, and transparency. The Federal Trade Commission (FTC) primarily investigates and enforces data protection on a national level, relying on its authority under Section 5 of the FTC Act to act against entities that engage in “unfair or deceptive acts or practices.” Using this authority, the FTC has entered consent agreements with companies like Sears (2009), Facebook (2011), Snapchat (2014), and Nomi Technologies (2015) for misrepresenting their privacy policies to their users.[64] However, this statute largely emphasizes user transparency, which has led to a system of “notice and choice,” where companies display a lengthy privacy policy and require users to consent to it before accessing their service. Notice-and-choice does not effectively preserve privacy; companies like Clearview or Amazon’s Ring can still set their own privacy policies—choosing what data they collect, store, and share, and for how long—and with the FTC’s more limited authority, the agency has only brought approximately 80 data privacy cases since 2002.
- Identity verification and access control
    - Vallance, Imran Rahman-Jones & Chris. “Discord’s Face Scanning Age Checks ‘Start of a Bigger Shift.’” BBC News, BBC, www.bbc.com/news/articles/cjr75wypg0vo
- Public health applications

4. Ethical Concerns Illustrated Through Case Studies

- **Lack of informed consent**
    - Passive collection → no real choice for users

    - Coerced or manipulative “opt-ins”
    - MSG barring critics; Amazon palm ID
- **Bias and discrimination**
    - Systems show unequal error rates (Gender Shades study)
    - Real-world harm: misidentification, false positives
        - Example: Buolamwini & Gebru; SIA counterpoints
    - Link to fairness frameworks from class
- **Privacy and surveillance risks**
    - Tracking without awareness or control
    - Risk of mission creep (security use → marketing, etc)
    - Clearview AI, Discord
    - Surveillance capitalism, contextual integrity
- **Transparency and accountability features**
    - Corporate policies hidden in fine print
    - Lack of clarity on data sharing, deletion, retention
    - Retail stores failing to disclose FR tech use (NYT)

5. Legal and Regulatory Landscape

- Proposed legislation and policy approaches
- Current U.S. status: FTC enforcement gaps, CCPA, state bans (e.g., SF)
    - “U.S. Commission on Civil Rights Releases Report: The Civil Rights Implications of the Federal Use of Facial Recognition Technology.” U.S. Commission on Civil Rights, www.usccr.gov/news/2024/us-commission-civil-rights-releases-report-civil-rights-implications-federal-use-facial
    - https://executivegov.com/2023/03/lawmakers-reintroduce-facial-recognition-and-biometric-technology-moratorium-act/
- International comparisons / differences in regulation
    - GDPR, China’s shifting posture
    - https://www.nytimes.com/2023/12/08/technology/eu-ai-act-regulation.html
- Regulatory shortcomings: fragmented, reactive, industry-friendly
- Sources: USCCR report, ExecutiveGov, NY

6. Ethical Framework Analysis

Appy class frameworks to the cases above:

- Utilitarianism: net benefit vs collective harm?
- Rights-based approach
    - Bodily autonomy, privacy as a human right
- Fairness & justice considerations
    - Who bears the cost?
    - Equity lens on surveillance
- Cultural and contextual factors
    - Portability and formalism traps

- ○ Selbst et al
  - ○ ML in the wild lecture

7. Proposed Ethical Guidelines

- Concrete prescriptions, both technical and procedural
- Bring up ethical concern cases and also cases where it's being done "right"
- Technical safeguards
  - Fairness audits, accuracy benchmarks, bias mitigation protocols
- Organizational & procedural
  - Human oversight systems, appeals processes, external review boards
- Policy recommendations
  - Require affirmative consent, limit third-party data sharing
  - Establish clear use-case restrictions
- Transparency requirements
  - Public-facing FR usage policies
  - Mandatory disclosure for biometric collection
- Sources: Forbes(2024), Segalla & Rouzies, SCU Tech Ethics Center

8. Future Directions / Conclusion

- Future directions:
  - More empirical research needed on long-term effects (psych, behavioral)
  - Cross-sector coordination for accountability (tech, law, policy, commercial)
  - Ideas for public education and ethical literacy around FR
- Conclusion:
  - Revisit thesis / summary of key findings
  - Emphasize urgency of rethinking ethical boundaries
  - Suggest a vision for responsible innovation
    - Guidelines for development and deployment
    - Respect for dignity and consent