

# The Ethics of Digital Surveillance: A Case Study on Clearview AI

## Thesis Statement

Clearview AI's facial recognition technology involves scraping billions of images from social media without consent, which presents significant ethical, legal, and societal challenges. These challenges highlight the need for comprehensive regulations and ethical guidelines to balance public safety with individual privacy rights.

---

## Introduction

Clearview AI, founded in 2017, has been at the center of numerous legal and ethical debates since its practices were publicly exposed in early 2020. The company's business model relies on scraping publicly available images from social media and other websites to build a vast database, which it then sells to law enforcement agencies and private companies. This case study examines the ethical and legal implications of Clearview AI's practices, the potential for misuse and abuse, and the broader societal impact of digital surveillance technologies.

# Background of Clearview AI

## Company Overview

Clearview AI specializes in facial recognition technology. Without user consent, it has created a massive database containing over 3 billion images by scraping social media platforms such as Facebook, Instagram, and LinkedIn.

## Use Cases

The company's technology is marketed primarily to law enforcement agencies to aid in identifying suspects in criminal investigations, including cases of child exploitation and human trafficking.

## Controversies

The company's practices have led to significant public backlash and legal scrutiny, with concerns centering around privacy violations, ethical issues, and potential technological biases.

## Ethical Issues

### Privacy Violations

#### ❖ Data Collection without Consent

- Clearview AI's method of scraping images without users' explicit consent raises severe ethical concerns about privacy rights. Most users are

unaware that their pictures are being collected and used for purposes they did not agree to.

#### ❖ **Public Perception**

- The company's actions challenge traditional norms and expectations about privacy, leading to widespread public criticism and resistance.

### Potential for Abuse

#### ❖ **Misuse by Law Enforcement**

- Law enforcement agencies' use of facial recognition technology without sufficient oversight or accountability can lead to potential abuses, such as unauthorized surveillance and targeting of individuals without probable cause.

#### ❖ **Commercial Exploitation**

- Clearview AI's database could be exploited commercially, raising concerns about commodifying personal data without individual consent.

### Bias and Discrimination

#### ❖ **Accuracy Concerns**

- Studies have shown that facial recognition technologies often have higher error rates when identifying individuals with darker skin tones, potentially leading to racial profiling and wrongful arrests.

#### ❖ **Impact on Marginalized Communities**

- The deployment of such technologies disproportionately affects minority communities, who may already face biases in law enforcement practices.

# Legal Implications

## Violations of Privacy Laws

### ❖ **Biometric Information Privacy Act (BIPA)**

- Clearview AI faces multiple lawsuits under BIPA, which protects biometric data, including facial recognition information. These lawsuits allege that the company collects and stores biometric data without obtaining informed consent, violating privacy rights.

### ❖ **Regulatory Scrutiny**

- Clearview AI has faced regulatory challenges in the United States and other countries, some of which have banned the company's technology.

## Need for Regulatory Frameworks

### ❖ **Lack of Clear Guidelines**

- The legal landscape regarding biometric data and surveillance technologies is still evolving. There is a pressing need for clear, enforceable regulations that protect individual privacy while allowing responsible technology use.

### ❖ **Calls for Reform**

- Advocacy groups and legal experts have called for stricter regulations on facial recognition technology, emphasizing the importance of transparency, accountability, and consent in data collection practices.

# Societal Impact

## Changing Notions of Privacy

The widespread use of facial recognition technology by companies like Clearview AI challenges traditional notions of privacy and anonymity. As surveillance technologies become more pervasive, society must reevaluate what privacy means in the digital age.

## Trust in Law Enforcement

Law enforcement agencies can erode public trust using facial recognition technology, mainly if the technology is used without appropriate safeguards and oversight.

## Public Debate and Advocacy

The controversies surrounding Clearview AI have sparked public debates on the ethical use of surveillance technologies. Privacy advocates, legal scholars, and civil rights organizations continue to push for more robust protections and ethical standards.

## Balancing Security and Privacy

### Responsible Use of Technology

Implementing transparent and accountable surveillance practices that respect individual rights is crucial. This includes requiring consent for data collection, limiting access to authorized personnel, and establishing clear guidelines for technology usage.

## Ethical Standards

Law enforcement and private companies using facial recognition technology should adhere to ethical standards, prioritizing privacy and minimizing the risk of bias and discrimination.

## Regulatory Oversight

Regular audits and oversight mechanisms should be in place to ensure that facial recognition technologies are not misused and that individuals' rights are protected.

## Conclusion

The case of Clearview AI underscores the urgent need for ethical guidelines, legal regulations, and societal awareness regarding the use of facial recognition technology. As digital surveillance becomes increasingly prevalent, striking a balance between security and privacy will be critical to ensuring that technology serves the public interest without infringing individual rights. Ongoing public and academic debate is essential to shape the future of digital surveillance and privacy protection in the 21st century.

---

## Works Cited

Hill, Kashmir. "The Secretive Company That Might End Privacy as We Know It." *The New York Times*, January 18, 2020.

Simonite, Tom. "This is how AI bias really happens—and why it's so hard to fix." *MIT Technology Review*, February 4, 2020.

Selinger, Evan, and Woodrow Hartzog. "The Inconsentability of Facial Surveillance." *Loyola Law Review*, Vol. 66, 2019.

Koepke, Logan, and Harlan Yu. "The Perpetual Line-Up: Unregulated Police Face Recognition in America." *Georgetown Law, Center on Privacy & Technology*, October 18, 2016.