22101627_cse422_sec13

by MOLLA SAZIDUR RAHMAN

Submission date: 09-Jan-2026 10:29PM (UTC+0530)

Submission ID: 2854457701

File name: 22101627-CSE-422_Final_Case_Study.pdf (123.15K)

Word count: 799

Character count: 4774

22101627-CSE-422 Final Case Study

Molla Sazidur Rahman

Case 1: Data Appropriation – Clearview AI

1. Description of the Application

Clearview AI is a US-based company that develops AI-powered facial recognition software, mostly used by the US Army, rapidly integrating artificial intelligence across its operations. This system works by collecting facial images from the publicly available online sources such as Facebook, Instagram, LinkedIn, and sometimes live streams (YouTube-Twitch). From here, these pictures are trained or processed into deep learning based computer vision models, from there it extract facial features and convert them into biological images. So, whenever a user uploads a picture on any social media or government CCTV, from there, it searches the whole dataset to match the person's face and location, and provides a live location, and links to the images.

So what makes this case more powerful is the scale and manner of data collection. Clearview AI holds more than **ten billion** facial images, and with local information and classification information to expand this database further. These images are collected without a person's knowledge and consent. Most of the people in this data are simple and ordinary citizens with no connection to law enforcement. This practice distinguishes Clearview AI from conventional facial recognition that relies on consent-based or legally regulated image databases.

Technically, Clearview AI's system is similar to facial recognition methods described in academic literature, such as deep neural networks-based face recognition, enabling large-scale matching of people's data. However, such as this technology, when it comes to concerns about people's safety, personal images raise serious ethical and legal concern realted to data appropriation.

2. Ethical Implications: Data Appropriation

Data appropriation, which is defined as the unlawful, unjust, or unauthorized capture and use of personal data without meaningful consent or remuneration, is exemplified by this case.

Lack of Consent and Privacy Violations

Facial images constitute biometric data, which is highly sensitive because they uniquely identify individuals. Clearview AI violated the ethical precepts of autonomy and privacy by collecting and processing this data without notifying users or getting their consent. The corporation was determined by European regulators to have no legal basis for processing biometric data and to have disregarded people's rights to view or remove their data. From an ethical perspective, but also as part of law enforcement, no one wants to be a part of it. This mismatch between user intent and actual data use is central to data privacy.

Power Imbalance and Surveillance Capitalism

Appropriated data helps Clearview AI strategically and commercially, but data subjects are not compensated or given any influence. This echoes more general worries about AI ethics with reference to surveillance capitalism, in which businesses profit greatly from personal data while externalizing privacy and societal costs to individuals. These actions exacerbate the power disparities that exist between citizens, governments, and corporations.

Risk of Bias and Harm

According to research, facial recognition software may display demographic biases that disproportionately impact women and racial minorities. These biases might result in negative effects, such as misidentification and disproportionate surveillance, when such systems are trained or run with an appropriate dataset. Even assessing facial recognition systems presents ethical issues, according to Raji et al., because biased technologies can be harmful even when they have great overall accuracy.

3. Long-Term Societal Impact

If systems like Clearview AI were deployed globally without strict regulation, the long-term impact on society could be profound.

First, anonymity in public places would be practically eliminated by pervasive facial recognition technology. People might be constantly recognized and monitored, which would result in self-censorship and less freedom of speech and gathering. Participation in democracy is directly threatened by this stifling impact.

Second, widespread biometric monitoring runs the risk of normalizing and allowing for function creep. Technologies that were first developed for specific uses, like investigating major crimes, might eventually be used to routinely monitor citizens, activists, journalists, or political rivals.

Third, these concerns are increased by the irreversible nature of biometric data. Facial data cannot be altered, in contrast to passwords. Misuse or violations can cause irreversible harm once appropriated and circulated. Abuse and social control are more likely when such authority is concentrated in state institutions or private corporations.

While limited facial recognition use under strict legal safeguards may offer some benefits, the Clearview AI case demonstrates that **unregulated data appropriation fundamentally undermines trust, privacy, and human rights**.

References

[1] I. D. Raji et al., “Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing,” *Proc. AAAI/ACM Conf. on AI, Ethics, and Society (AIES)*, 2020.

[2] J. Buolamwini and T. Gebru, “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,” *Proc. ACM Conf. on Fairness, Accountability, and Transparency (FAT*)*, 2018.

[3] M. Smith and S. Miller, “The Ethical Application of Biometric Facial Recognition Technology,” *AI & Society*, vol. 36, no. 1, pp. 209–221, 2021.

22101627_cse422_sec13

ORIGINALITY REPORT

0%	0%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		