

UCLA

Recent Work

Title

Facial Recognition and Surveillance Capitalism: Challenging Legal Frameworks of Privacy, Consent, and Citizenship

Permalink

<https://escholarship.org/uc/item/6qv0k280>

Author

Cavanagh, Payton

Publication Date

2026-03-16

Facial Recognition and Surveillance Capitalism: Challenging Legal Frameworks of Privacy, Consent, and Citizenship

Payton Cavanagh¹

¹Affiliation (e.g., Department of Computer Science, University of California, Los Angeles)

pcavanagh34@g.ucla.edu

Abstract: Facial recognition technologies have become popular due to AI and have been utilized through different surveillance systems. This paper looks into how these systems impact human privacy, consent, and the law. Using Hegemonic narratives, this paper will analyze how surveillance technology disproportionately impacts marginalized communities.

INTRODUCTION

Thanks to AI, facial recognition technology has become very popular for modern surveillance systems. Using AI to help analyze people's facial parts (biometrics), these systems are able to identify people through different photos or videos. Governments, corporations, and law enforcement agencies have begun to implement facial recognition technologies into tracking criminals, identity verification, and general surveillance. However, the use of facial recognition has raised concerns regarding privacy, consent, and civil liberties/rights.

The increasing popularity of facial recognition technology has led to something called surveillance capitalism, which is a system where corporations collect and monetize personal data on a large scale (Zuboff, 2019). Within this system, biometric information such as facial images become a very valuable resource for tech companies and government agencies. As AI becomes more and more popular, the difference between public observation and illegal data collection becomes hard to differentiate.

Even before the big boom of AI in 2020, the company by the name of Clearview AI was in the news for using facial recognition surveillance illegally. They created a facial recognition database by searching through different social media pages and obtaining billions of images of people's faces and then selling it to their customers (American Civil Liberties Union, 2020). They sold this data to law enforcement agencies and we were told that it was used for security purposes in identifying individuals through biometric matching. This led to the company getting sued because the people they stole the data from did not consent to their data being used this way and it resulted in numerous investigations (Hart, 2024). This demonstrates one of the many legal problems that come from these AI surveillance systems.

This paper examines how facial recognition technologies challenge existing legal frameworks surrounding privacy, consent, and citizenship through the concept of hegemonic narratives. Hegemonic narratives are essentially storylines that the dominant group creates to convince the public that what they are doing is okay. Governments and tech companies often argue that the facial recognition tools that they are using are for security reasons which simultaneously downplay the impacts on civil liberties and privacy. Using this framework, the paper will analyze how these narratives can unknowingly impact civilians' privacy and consent. **This work is in partial fulfillment of the ENGR184 course using the blueprint curriculum in Ref [1,2] and captured in a collection [3].**

METHODS

This paper uses hegemonic narratives to analyze the rapid growth of facial recognition surveillance technologies. Hegemonic narratives describe how dominant institutions such as tech companies or government agencies provide misleading reasons as to why public surveillance is good for them. Using this idea, the paper will analyze how facial recognition systems are justified by making the public “safer” and downplaying any concerns about privacy, consent, and laws.

We will analyze two different scenarios where facial recognition was used, one being by Clearview AI and the other being the police in Detroit, Michigan. Using this framework for these case studies, the paper will analyze how the dominant narrative shapes the public and legal view of these facial recognition systems. To be more specific, the paper will study how hegemonic narratives influence privacy, consent, and legal regulation. The paper will investigate how tech companies and governments justify the use of these facial recognition systems. These hegemonic narratives will help us understand how the dominant companies/governments can avoid public scrutiny because they control what the public believes

RESULTS AND INTERPRETATION

Clearview AI provides one of the most obvious examples of surveillance capitalism because they took advantage of people’s data in exchange for money. The problem with this was that the individuals whose faces were included in the data could not opt out or limit how they wanted their data to be used. Clearview was able to argue that they didn’t infringe on the people’s privacy because the photos were technically public, however the users did not consent to their data being used. This means that although their privacy was not taken from them, their consent was not given and Clearview took their data and used it how they pleased anyways.

Hegemonic narratives are what allowed Clearview AI to make it seem like the data they were collecting was only being used for finding criminals and helping law enforcement, but what they failed to realize is that you need consent to use people’s data. How much data did they collect before getting caught? Why did no one question it at first? These are all very important questions and they seemed to be overlooked because people assumed it was okay because the data was being used for something “good.” If you use this argument then you need to ask yourself, where do we draw the line? Clearview AI’s narrative emphasized the benefits of surveillance and hid the concerns of mass surveillance underneath it.

Another example of the dangers of facial recognition technology can be seen from the Detroit Police Department, which used a software to identify criminals. This quickly became an issue because multiple different people were wrongfully arrested after these facial recognition systems incorrectly matched them to the people that were seen on the surveillance footage. Robert Williams was someone who was wrongfully arrested because the facial recognition system incorrectly identified him as the person who was being charged for theft (American Civil Liberties Union, 2020). The police’s only evidence was that the AI surveillance system had a match on Robert so they ended up arresting him without a proper investigation. He was detained and interrogated even though there was no clear evidence against him other than the security footage.

This example shows how these AI facial recognition systems can easily fail, especially when identifying people of color. A perfect example of this was done in a study proving that facial recognition algorithms display significant racial and gender biases. In the Gender Shades study, researchers found that women with a darker skin tone were misgendered as high as 34.7% of the time, while men with lighter skin tones were misgendered less than 1% (Buolamwini & Gebru, 2018). This happened because the data being

used in this experiment disproportionately included much more lighter skinned males when compared to darker skins. These disparities raise critical questions about the groups responsible for developing and training these AI models. When these models are trained by members of the hegemonic groups, the AI will display biases that support those groups rather than reflecting a more neutral perspective. If the non-dominant group was able to provide their input, then the results would have been much more accurate and wouldn't have favored light skinned individuals.

This study highlights the concerns with these facial recognition systems and shows that there are still tons of flaws in them still and cannot be fully trusted. This wrongful arrest is a clearcut example of someone's legal rights being violated and shows how the dominant group's narrative will be on full display for the output of the system. This demonstrates how hegemonic narratives allow companies to get away with doing things that should be illegal but because they have the dominant perspective everyone just lets them do what they want without considering the consequences. That's why it's important to consider all perspectives when utilizing these technologies and make sure that people's rights are not violated. Law enforcement will often argue that facial recognition is just another tool to identify criminals, but the consequences of misidentifying someone because of a mistake on the system's behalf can threaten civil liberties.

CONCLUSIONS

Facial recognition technologies have grown dramatically over the last 10 years due to the growing popularity of AI and in the process, raising lots of ethical and legal concerns. Through the Clearview AI and Detroit Police department examples, this paper demonstrates how these technologies could be dangerous and why we need to be more careful as a society. In a defense against themselves, Clearview AI tried to argue that since the images they were scraping were public, they were free to do whatever they wanted with them. This led to them getting into tons of lawsuits forcing them to restrict some of their technology (Hart, 2024). The Detroit Police Department had a similar situation and also faced legal consequences after wrongfully arresting someone because of their facial software incorrectly identifying suspects. These examples demonstrate how important it is to be wary of these new technologies because they can negatively impact individuals' privacy and civil liberties.

Using hegemonic narratives helps to explain how these companies/governments were able to keep these systems running for such a long period of time until there was legal intervention. These tech companies and government agencies are able to promote these facial recognition systems because they have so much power in controlling what people believe. If someone told you there are security cameras in an area and they are able to catch bad guys with it you would probably have no problem with it right? It all depends on how they frame it but what if someone said that they are gathering biometric data on you to sell to other companies or the government? You might not be as comfortable with them surveilling you. This is a perfect example of hegemonic narratives. The companies are able to determine what people think they are doing and most people don't think to question it. In the example with Clearview AI they framed their data collection as a tool to fight crime which helped to convince people that their data was being used for good. Detroit law enforcement did the same thing.

These examples highlight a serious issue with our legal system. Lots of these AI surveillance systems are very new and have only been getting much more advanced recently. This could lead to lawmakers having a difficult time creating regulations for these companies as quickly as the technology is evolving. If there is no clear law, then a gray area will appear and companies/governments can experiment with surveillance technologies without the proper consequences being applied to them. A perfect example of

this would be the Clearview AI company where they had already gathered tons of data and sold it before any legal action was taken.

The Detroit police case further proves how poor legal oversight can lead to some horrible consequences. The fact that the police department was able to just use their surveillance system as the sole evidence against Robert Williams proves that there was a problem with the laws surrounding the AI recognition system. Eventually, the settlement led to the police department changing its policing regarding the role of the facial recognition system in their investigations. However, the fact that these changes occurred only after a wrongful arrest speaks volumes to the lack of legal protection and laws against AI surveillance.

Ultimately, the fast growth of these facial recognition technologies brings up some important questions about how we as a society should balance technological advancements with our rights as people. Quicker and more effective laws need to be in place to regulate the collection of our data, the use of our data, and they need to make the companies more transparent about what they are using our data for. They should need our consent before using our data! Without these protections, hegemonic narratives regarding security could lead to other institutions trying to justify their surveillance while leaving citizens vulnerable to privacy violations and incorrect arrests.

REFERENCES

American Civil Liberties Union. (2020). Clearview AI and the threat to personal privacy.

<https://www.aclu.org/cases/aclu-v-clearview-ai>

American Civil Liberties Union. (2020). Williams v. City of Detroit: Facial recognition false arrest case.

<https://www.aclu.org/cases/williams-v-city-of-detroit-face-recognition-false-arrest>

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, 81, 1–15.

Hart, R. (2024). Clearview AI fined for illegal facial recognition database. *Forbes*.

<https://www.forbes.com/sites/roberthart/2024/09/03/clearview-ai-controversial-facial-recognition-firm-fined-33-million-for-illegal-database/>

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.