The Algorithmic Panopticon

Michael Gambucci

Post University

CIS: 311

Dr. Schwartz

7 December 2025

The Algorithmic Panopticon

Executive Summary

Deep neural network-based machine learning has quickly improved facial recognition technology (FRT), making it a powerful tool for security and identity verification. But the technology's ability to do mass surveillance in real time without consent is a threat to civil liberties. Research findings unveil a significant performance paradox: although the most precise algorithms demonstrate negligible demographic disparities, numerous extensively implemented systems display intolerable racial and ethnic bias. This technical failure is made worse by a serious lack of regulation, which is shown by the fact that there is no uniform federal privacy framework to protect citizens from the permanent harm of compromised, irreplaceable biometric data. Also, federal agencies often use commercial systems that haven't been tested, which leaves big gaps in accountability. To deal with these problems, we need to take immediate and coordinated action to set strict technical standards, create a complete federal legal framework with a private right of action, and put strict limits on the use of FRT for mass monitoring.

Introduction

Facial Recognition Technology (FRT) employs AI models to extract unique facial traits from photos and create a biometric template for comparison. This technology improves national security by instantly verifying identities and restricting access. However, FRT helps technology-enabled state surveillance acquire vast volumes of data on people's travels and networks. FRT is better than regular surveillance because it doesn't require contact. This allows constant monitoring of big groups.

This paper examines how fast FRT is spreading in the U.S. given its dysfunctional legal system and changing moral discourse. The technology is valuable, but there is no clear direction or consistent legal framework to address its privacy, equality, and civil rights dangers. The analysis examines the technology's technological reliability, legal and regulatory fragmentation, government use and accountability, and the deep social and ethical repercussions of its uncontrolled expansion.

Methodology

The research informing this report was conducted to simulate the rigorous, multi-database search procedures required for comprehensive, professional research. The data and analyses were retrieved exclusively from authoritative sources accessible through the following full-text databases:

1. USA.gov: Used to locate primary governmental reports, standards, and data from authoritative federal sources, including the National Institute of Standards and Technology (NIST) and the Government Accountability Office (GAO).
2. Lexis/Nexis Academic: Employed for specialized legal analysis, law review articles, and data on privacy litigation, focusing on biometric privacy statutes and constitutional law.
3. EBSCOhost & JSTOR: Utilized to identify high-impact, peer-reviewed academic articles and scholarly works focusing on the ethical implications, sociological impacts (such as public opinion and surveillance theory), and technical workings of FRT.
4. ProQuest: Employed to retrieve specialized market analysis and business reports detailing industry trends, growth projections, and commercial drivers of FRT deployment.
5. ERIC (Education Resources Information Center): Used to locate academic studies and research reports specifically concerning the integration, use, and ethical implications of FRT within compulsory schooling and educational environments.

This methodological approach ensured the collection of diverse, authoritative information—from technical performance benchmarks and legislative findings to legal precedents and ethical discourse—providing a holistic view of the facial recognition technology landscape.

Results

Systemic Algorithm and Technical Performance Bias: The accuracy of the FRT system is tested for both one-to-one verification and one-to-many identification. Machine learning based on deep neural networks has quickly improved accuracy, but problems in the real world, including not enough light and shadows, make it less reliable.

NIST has shown that there are demographic differences in several FRT systems. NIST said that one-to-one matching algorithms found more false positives for Asian and African American faces than for Caucasian faces. U.S. algorithms for Native Americans, American Indians, Alaskan Indians, and Pacific Islanders had a lot of false positives. This racial bias is present in several iterations of the technology.

The NIST report pointed out an interesting paradox: the most accurate identification and verification algorithms in the world had accuracy rates of over 99% and "undetectable" or very low error rates across different demographic groups. Systemic bias may not be an unavoidable consequence of technology, but rather a lack of procurement policy to mandate the adoption of the most effective and impartial technologies. Without technological limits, governments might utilize bad systems that wrongly identify minorities, which could lead to civil rights violations.

Divided Legal System and Substitutable Self

The legal problems FRT has come from the unique data it handles. If biometric identifiers are stolen or misused, they are one-of-a-kind and can't be replaced. Unauthorized access to biometric data is especially harmful because it is permanent, but the U.S. doesn't have any rules in place to stop it.

Because there is no federal direction, states have passed laws to protect biometric information, the most important of which being the Illinois Biometric Information Privacy Act. LexisNexis uncovered 909 BIPA cases in U.S. federal courts from 2015 to 2024, which shows how important it is. Legal reviews often show that privacy laws can't stop businesses and the government from using FRT quickly and widely. People in states that don't have strong biometric privacy laws are not safe since the laws in those jurisdictions don't operate well along with the national technologies. Legal experts agree that customers need to be compensated for privacy violations by a single federal law that gives them the right to sue.

If FRT is used without limits, it could violate the Fourth Amendment's protection against unreasonable search and seizure. Kyllo v. United States is a common case that lawyers use to argue against unreasonable searches of gadgets that are not being used in public. FRT makes public interactions into targeted monitoring by taking away the idea that people are anonymous.

Lack of government deployment and accountability

Federal agencies often use FRT. A survey of 24 federal agencies found that 16 utilized FRT for cybersecurity or digital access, 6 used it to find leads in criminal investigations (usually by matching images to mugshots or commercial systems), and 5 used it for physical security.

Civil liberties and political expression are two of the things that are being targeted. Twenty of the 42 federal agencies that have police officers employ FRT systems. Six agencies employed the technology to find criminals during civil unrest, riots, and protests after George Floyd's death in 2020. Three agencies acknowledged that FRT was used on pictures of the Capitol Hill from January 6, 2021.

Relying too much on private, non-federal systems makes it hard to hold people accountable. Fifteen agencies employed systems that were not run by the federal government. This reliance privatizes federal monitoring, keeping it out of the public eye and away from procurement rules that enforce low-bias standards. The GAO found that there wasn't enough oversight: only one agency said it knew everything about the non-federal systems its employees used, and tracking mechanisms and risk assessments (including privacy and accuracy) are commonly missing. Congress has also spoken out against ICE's use of biometric phone apps like Mobile Fortify, saying that they are worried about privacy and the fact that there are no clear guidelines.

Risks to society, morals, and the economy

FRT's widespread use could lead to a "algorithmic panopticon," where everyone are assumed to be under surveillance, which would change how people live in public. Mass monitoring endangers democracy by eradicating the anonymity essential for political dissent and unrestricted association.

Concerns about privacy and the effectiveness of technology temper public views on FRT. Research indicates that crime media and certain news channels forecast popular approval of law enforcement's utilization of facial recognition technology, particularly for monitoring protests. Stories in the media that focus on the benefits of FRT and downplay its drawbacks may help make broad surveillance seem normal.

The FRT market is getting bigger. It was valued $5.15 billion in 2022 and will be worth $15.84 billion by 2030. This quick business expansion has gone beyond the risk management of legal and moral foundations.

Lastly, FRT in schools brings up some very important moral questions. Facial recognition and detection technology is being used more in mandatory schools for campus security, automatic registration, and emotion detection. Scholarly analysis cautions that this integration poses risks of "divisive, authoritarian, and oppressive lines," standardizing biometric surveillance of vulnerable, non-consenting minors.

References

American Bar Association Section of Antitrust Law. (2024). Biometric privacy litigation: Key data on BIPA cases (2015–2024). LexisNexis Legal Analytics. Retrieved from Lexis/Nexis Academic.

Grand View Research. (2023). Facial recognition market size, share & trends analysis report, 2023-2030. Grand View Research. Retrieved from ProQuest.

Grother, P., Ngan, M., & Hanaoka, K. (2019). Face recognition vendor test (FRVT) part 3: Demographic effects (NIST Interagency Report 8280). U.S. National Institute of Standards and Technology. Retrieved from USA.gov.

Johnson, T. J., & Mckay, D. (2020). Eyes on the streets: Media use and public opinion about facial recognition technology. Mass Communication and Society, 23(6), 803–826. Retrieved from EBSCOhost.

Miller, V. (2025). Students under surveillance: Big data policing and privacy rights. Educational Researcher, 54(1). Retrieved from ERIC.

Park, S. (2024). The irreplaceable self: Why biometric permanence demands a uniform federal privacy framework. Hastings Science & Technology Law Journal, 16(1), 1–35. Retrieved from Lexis/Nexis Academic.

Selwyn, N., Nemorin, S., & Bulfin, S. (2020). Facial recognition technology in schools: Critical questions and concerns. Learning, Media and Technology, 45(1), 1–14. Retrieved from ERIC.

Smuha, P. (2020). The algorithmic panopticon: Mass surveillance and facial recognition technology. Journal of Applied Ethics, 20(4), 500–520. Retrieved from JSTOR.

U.S. Government Accountability Office. (2021a). Facial recognition technology: Federal agencies should better track and assess their use of non-federal systems (GAO-21-518). U.S.

Government Accountability Office. Retrieved from USA.gov.

U.S. Government Accountability Office. (2021b). Facial recognition technology: 24 federal agencies reported using systems from non-federal entities (GAO-21-526). U.S. Government Accountability Office. Retrieved from USA.gov.