Biometric Surveillance and the Erosion of Rights: A Human Rights Analysis of Facial Recognition Technology in the United States

Perla Khattar*

ABSTRACT

This article examines the growing deployment of facial recognition technology ("FRT") in the United States and its implications for core human rights, including privacy, freedom of expression, and freedom from discrimination. As both government agencies and private companies increasingly use FRT to track individuals, identify faces in public spaces, and profile consumers, the potential for abuse grows exponentially. Drawing on international human rights law, U.S. constitutional principles, and recent case studies, this article argues that unregulated facial recognition threatens to normalize mass biometric surveillance and disproportionately burdens marginalized communities through algorithmic bias and chilling effects on dissent. The current U.S. legal framework—lacking a comprehensive federal privacy law—fails to provide sufficient protections, leaving much of the regulatory burden to a patchwork of state and local measures like Illinois' BIPA and city-level bans.

In response, this article proposes a rights-based approach to facial recognition governance. It recommends enacting a federal (biometric) privacy statute modeled on the Illinois Biometric Information Privacy Act ("BIPA"), requiring consent, transparency, and algorithmic fairness. It further advocates for warrant requirements and strict limits on law enforcement use, bans on persistent public surveillance, and corporate accountability grounded in human rights due diligence. This article concludes that preserving civil liberties in the age of facial recognition will

*J.S.D. Candidate, Notre Dame Law School; Research Fellow, Notre Dame-IBM Technology Ethics Lab; Fellow, Kellogg Institute for International Studies; LL.M., Loyola University-New Orleans (2021); LL.B., La Sagesse University (2020).

require deliberate legal reforms that prioritize individual autonomy and dignity over surveillance convenience and commercial interest.

Table of Contents

I. INTRODUCTION

In recent years, facial recognition technology has moved from the realm of science fiction into a pervasive reality of modern life. Private corporations use it to monitor retail customers and "enhance" security, while law enforcement agencies deploy it to identify suspects in crowds and public spaces. These developments have sparked intense debate over the impact of facial recognition on fundamental human rights. Critics warn that ubiquitous face surveillance imperils the right to privacy, chills freedom of speech and association, and can facilitate discriminatory practices.

In the United States—often considered a champion of civil liberties—this issue poses unique challenges. How can American legal frameworks reconcile emerging biometric surveillance with the nation's commitments to privacy and freedom? This article explores that question by examining the intersection of consumer privacy, facial recognition, and human rights in the U.S. context. It analyzes how widespread deployment of facial recognition by both companies and government agencies threatens rights including privacy, freedom of expression, and freedom from discrimination. It then considers leading case studies and controversies to illustrate these concerns in practice. Finally, this article advances legal reforms and policy recommendations aimed at curbing the harms of facial recognition technology and better protecting human rights in the age of biometric surveillance. As this analysis will show, unchecked

facial recognition threatens to undermine the very liberties it purports to safeguard, and only a robust legal response can ensure that "face" surveillance does not erase fundamental rights.

II. FACIAL RECOGNITION TECHNOLOGY AND HUMAN RIGHTS CONCERNS

Facial recognition technology ("FRT") refers to a set of biometric software tools that identify or verify individuals by analyzing images of their faces.[1] Modern algorithms can scan a live video feed or photograph and compare facial features against a database of known images to find a match. This capability, while innovative, raises profound human rights concerns.[2] Unlike traditional CCTV cameras or eyewitness observations, facial recognition enables *persistent, automated, and indiscriminate* identification of people on a mass scale.[3]

The deployment of FRT by both state and private actors has been described as a potential "end of privacy as we know it," given its power to track individuals across time and place without their knowledge or consent.[4] This Part examines the core human rights at stake: privacy, freedom of expression and association, and freedom from discrimination.

---

1. *See Facial Recognition Technology*, NIST (Feb. 6, 2020), https://perma.cc/GC76-S2GZ.

2. *See* Anna Bacciarelli, *Time to Ban Facial Recognition from Public Spaces and Borders*, HUMAN RTS. WATCH (Sept. 29, 2023), https://perma.cc/2PV6-FJBD.

3. Unlike closed-circuit television systems, which rely on real-time human monitoring or after-the-fact manual review, facial recognition systems can continuously scan and analyze vast amounts of video footage without human intervention. This automation allows for persistent tracking of individuals across time and locations by matching facial features against stored biometric databases. The "persistent" nature refers to the system's ability to identify and re-identify individuals at multiple points, effectively turning any camera-equipped public space into a tool of long-term surveillance. The process is "automated" in that modern facial recognition algorithms process images in real time, extracting biometric identifiers and executing matches without requiring manual input for each search. It is also "indiscriminate" because the technology does not target specific individuals but scans all visible faces within the camera's scope, including those of unsuspecting and uninvolved members of the public. In this sense, facial recognition systems significantly expand the surveillance potential of CCTV, converting passive monitoring into active identification, often without the knowledge or consent of those being observed. *See* Woodrow Hartzog, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://perma.cc/F4TN-QRP5 (explaining how facial recognition systems are uniquely suited to mass surveillance due to their automatic and covert nature).

4. Terry Gross, *Exposing the Secretive Company at the Forefront of Facial Recognition Technology*, NPR (Sept. 28, 2023), https://perma.cc/8UEM-D6AX.

A. Privacy and Suveillance

The right to privacy is internationally recognized as a fundamental human right, enshrined in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.[5] Although the U.S. Constitution does not explicitly enumerate a general right to privacy, the Supreme Court has long interpreted various provisions—such as the Fourth Amendment[6]—to

5. The recognition of privacy as a fundamental human right in international law reflects a broad consensus on its essential role in safeguarding human dignity, autonomy, and freedom from arbitrary interference. Article 12 of the Universal Declaration of Human Rights ("UDHR") provides that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence," while Article 17 of the International Covenant on Civil and Political Rights ("ICCPR") echoes this language and adds that "[e]veryone has the right to the protection of the law against such interference." G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948); International Covenant on Civil and Political Rights art. 17, Mar. 23, 1976, T.I.A.S. No. 92-908, 999 U.N.T.S. 171. These provisions have been widely interpreted by scholars and international bodies to establish a normative baseline for privacy protections globally. *See* Oliver Diggelmann & Maria Nicole Cleis, *How the Right to Privacy Became a Human Right*, 14 HUM. RTS. L. REV. 441, 443–44 (2014) (noting the foundational role international human rights instruments play in shaping global privacy norms).

6. The Fourth Amendment to the U.S. Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. When law enforcement uses facial recognition, Fourth Amendment issues immediately arise. Traditional doctrine held that observations of a person in public generally are not a Fourth Amendment search, because a person has no reasonable expectation of privacy in what they "knowingly expose" to the public. Katz v. United States, 389 U.S. 347, 351 (1967). Under this view, police photographing or recognizing someone's face in public has been considered akin to plain observation, not a search. Some lower courts have thus suggested that using facial recognition on images obtained in public might not trigger the Fourth Amendment, on the theory that a face is a public fact. *See* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment,* 105 MINN. L. REV. 1105, 1128 (2021). However, a strong argument is emerging that high-tech facial surveillance is qualitatively different from casual public observation, and that it should indeed be considered a search under the Fourth Amendment, requiring a warrant or at least individualized suspicion. The Supreme Court's decision in *Carpenter v. United States* provides an important analogy. *See generally* Carpenter v. United States, 585 U.S. 296 (2018). In *Carpenter*, the Court confronted police access to historical cell phone location data, which revealed a person's movements over time. *See id.* at 301. Although that data was technically "shared" with a third-party phone company, the Court recognized that individuals maintain a reasonable expectation of privacy in the record of their physical movements. *See id.* at 399–406. Chief Justice Roberts noted that tracking a person's location over an extended period is an entirely different level of surveillance than what law enforcement could traditionally do, amounting to a search that requires a warrant. *See id.* at 403. By similar reasoning, tracking a person's identity everywhere they go via facial recognition could be seen as a search. Professor Andrew Guthrie Ferguson argued exactly this point: in light of *Carpenter*, certain uses of facial recognition, especially "dragnet" one-to-many searches in public, should be deemed unconstitutional searches without a warrant. Ferguson, *supra* note 6, at 1146, 1160-61.

protect aspects of individual privacy. In the context of facial recognition, privacy concerns arise because the technology facilitates pervasive surveillance. By converting consumer's faces into identifiers, FRT erodes "practical obscurity" —the idea that one can move through public spaces without being systematically tracked.[7] When any person's face can be captured by a camera and instantly linked to their identity and records, the *de facto* anonymity of public life is lost.

This loss of anonymity is more than an inconvenience; it strikes at personal autonomy and dignity. Individuals may reasonably expect that walking down a street or attending a public gathering will not automatically subject them to an identity check. Facial recognition upends that expectation. It allows both governments and companies to amass detailed profiles of where consumers go, who they meet, and what they do, all by matching faces from one context—say, a street protest—with data from another—a driver's license database or social media profile.

As Evan Greer, the director of Fight for the Future, put it, facial recognition is "biometric surveillance" that, if left unchecked, poses "*enormous potential for harm to our basic human rights.*"[8] Indeed, experts have likened the threat of facial recognition to an Orwellian "perpetual line up" of the entire populace, enabling continuous, suspicionless monitoring.[9] The technology thus implicates the right to privacy in its most classic sense: freedom from arbitrary or invasive observation by others, particularly the state.

It is important to distinguish between limited uses of facial recognition and broad, dragnet-style[10] deployments. Using facial recognition in a controlled setting—for example, to unlock one's own smartphone or verify identity at an airport checkpoint with consent—may carry minimal privacy intrusion. However, human rights concerns are sharply presented when FRT is used for mass surveillance. Mass surveillance occurs when authorities use FRT to scan crowds or public

7. *Practical Obscurity*, SOCIETY OF AMERICAN ARCHIVISTS DICTIONARY, https://perma.cc/866G-QMHN (last visited Apr. 19, 2026, at 18:23 ET) (defining "practical obscurity" as "the principle that private information in public records is effectively protected from disclosure as the result of practical barriers to access").

8. Manuela López Restrepo, *She was denied entry to a Rockettes Show—then the Facial Recognition Debate Ignited*, NPR (Jan. 21, 2023) (emphasis added), https://perma.cc/YA83-62ZL.

9. Matt Mahmoudi, *Ban dangerous facial recognition technology that amplifies racist policing*, AMNESTY INTERNATIONAL (Jan. 26, 2021), https://perma.cc/BY66-LA8B.

10. *Dragnet*, CAMBRIDGE DICTIONARY, https://perma.cc/9ESR-KFBX (last visited Apr. 19, 2026, at 18:35 ET) (defining "dragnet" as "a series of actions taken by the police that are intended to catch criminals").

spaces in real-time, or when companies aggregate facial data on countless individuals, without individualized suspicion.[11] Such practices treat everyone as a potential subject of identification, regardless of any wrongdoing.[12] Amnesty International has warned that "indiscriminate" use of FRT amounts to a form of "mass surveillance" that is incompatible with human rights, because it intrudes on privacy and other freedoms without adequate justification.[13] The chilling effect of simply knowing that one's face can be tracked everywhere is itself a privacy harm, altering how people behave in public.

Notably, a 2020 investigative report revealed that a single company, Clearview AI,[14] had scraped billions of photographs from social media and other websites to build a gigantic facial recognition database. Clearview's database allows paying clients to identify an "unknown" face by finding matching photos online.[15] Such a system essentially puts everyone with an online image into a perpetual virtual lineup. The collection and processing of these faceprints occurs without the consent or even knowledge of the individuals affected, undermining any notion of informed privacy choice. As the ACLU noted in its lawsuit against Clearview, the company

11. Mass surveillance through facial recognition technology (FRT) involves the broad, non-targeted collection and processing of biometric data, often in public spaces, without warrants or individualized suspicion. This use of FRT enables continuous tracking of individuals' movements and behaviors, raising significant concerns under both privacy and human rights frameworks. Scholars and civil liberties advocates have emphasized that such practices can chill free expression, disproportionately impact marginalized communities, and erode the principle of presumption of innocence. *See* Clare Garvie, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEORGETOWN L. CENTER ON PRIVACY & TECH. (Oct. 18, 2016), https://perma.cc/8WNV-2PW7.

12. *See id*.

13. *Amnesty international Calls for Ban on The Use of Facial Recognition Technology for Mass Surveillance*, AMNESTY INTERNATIONAL (June 11, 2020), https://perma.cc/U6FG-P5YY.

14. No company is more synonymous with the facial recognition controversy than Clearview AI. Clearview burst into public consciousness in January 2020, when the investigative reports of Kashmir Hill revealed its startling business model: the company had collected billions of photos from social media and websites (including Facebook, Instagram, LinkedIn, and even personal blogs) to create a massive face-search database, which it then sold access to primarily to "law enforcement agencies." Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. TIMES (Jan. 19, 2020), https://perma.cc/BFS4-B37F. Clients could upload a photo of an unknown person (for example, from a crime scene or security camera) and Clearview's system would return matches, showing that person's identified images from across the internet. *See id.* This effectively allowed police to identify people with no more than a snapshot, therefore bypassing the traditional investigative legwork. Clearview's CEO infamously touted that there's never been a database like this and that they had collected over "three billion images" by 2020; by 2023 the database reportedly expanded to some 30 billion images, a figure well above the world's population. *Id.*

15. *Id*.

"treat[ed] people's unique biometric identifiers as an unrestricted source of profit," until courts stepped in.[16]

B. Overview of the Military Justice System

Beyond privacy, facial recognition also imperils freedom of expression and freedom of assembly and association, rights protected by the First Amendment of the U.S. Constitution[17] and by Articles 19 and 20 of the Universal Declaration of Human Rights.[18] The connection between surveillance and speech may not be immediately obvious. After all, FRT does not censor words. However, the mere presence of facial recognition can exert a powerful chilling effect on people's willingness to speak, protest, or associate freely. If individuals know that attending a protest, walking into a certain mosque or church, or meeting with certain individuals will mark them in a law enforcement database, many will think twice before exercising their rights.

The Supreme Court recognized this dynamic in *NAACP v. Alabama*, when it held that Alabama could not force the NAACP to disclose its

16. *In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law*, ACLU (May 9, 2022), https://perma.cc/5BK9-Z3SL.

17. While the First Amendment does not typically forbid surveillance outright, it can come into play if surveillance is targeted based on speech or is so pervasive that it deters protected activities. There is some precedent for courts intervening when government surveillance crosses into harassment of dissidents. In the 1970s, a federal court in *Handschu v. Special Services Division* oversaw limits on the NYPD's surveillance of political groups, recognizing potential First Amendment infringements. *See generally Handschu v. Special Servs. Div*., 605 F. Supp. 1384 (S.D.N.Y. 1985). A modern analogue might be a court finding that using facial recognition to monitor attendees of political rallies or religious services, absent any reasonable suspicion of criminal activity, violates the First Amendment. So far, no such case has been decided, but the issue is percolating. The ACLU and other groups have argued for a ban or moratorium on police use of facial recognition for First Amendment-sensitive contexts, noting that its presence "has a chilling effect on our rights to speak freely and associate with who we want." *Protest Surveillance During the DNC*, ACLU (Aug. 15, 2024), https://perma.cc/5BK9-Z3SL. An interesting twist is that companies developing facial recognition have sometimes tried to use the First Amendment in the opposite way: as a shield *against* regulation. Notoriously, Clearview AI has argued that its collecting of publicly available images and its creation of a face-identification app is protected by the First Amendment as information gathering and "dissemination." Jameel Jaffer & Ramya Krishnan, *Clearview AI's First Amendment Theory Threatens Privacy—and Free Speech, Too*, COLUMBIA UNIV.: KNIGHT FIRST AMENDMENT INST. (Nov. 17, 2020), https://perma.cc/7J8Q-RWU9. This argument posits that the act of creating biometric face templates from public photos is essentially the processing of information, which is "speech." *Id*. So far, courts have not accepted this broad free speech immunity for facial recognition providers, and such claims face an uphill battle, especially where privacy laws regulate commercial conduct rather than pure speech.

18. *See* G.A. Res. 217 (III) A, Universal Declaration of Human Rights, arts. 19, 20 (Dec. 10, 1948).

membership lists.[19] Requiring identification of members, the Court found, would expose them to harassment and retaliatory violence, chilling their association and advocacy; an impermissible burden on First Amendment freedoms.[20]

Facial recognition now threatens to create a similar deterrent effect on a massive, automated scale. Modern civil rights advocates argue that the "threat of identification chills protestors' speech and assembly rights by" making them fear retaliation or scrutiny simply for showing up.[21] If every face in a protest march or political rally can be identified and logged by police, or even by private adversaries, participants may worry that they could face consequences at work, in their community, or from the government for their views. This is not a speculative concern. There have been documented incidents in which U.S. police used facial recognition to identify and track protesters and activists, seemingly targeting them for their dissenting speech.[22] Such uses of facial recognition against protesters directly undermine the right to free expression and peaceful assembly.

The First Amendment has also been interpreted to protect a degree of anonymity in speech and association. As the Supreme Court observed, privacy in one's associations and beliefs can be "*indispensable to preservation of freedom of association*" for controversial groups.[23] In public spaces, while individuals generally have no legal right to anonymity in the sense of being unobservable—anyone can see a face in a crowd—pervasive facial recognition changes the equation. It transforms casual public observations into a systematic identification regime.

In a 2019 report, Barbora Bukovská, ARTICLE 19's Senior Director for Law and Policy, noted that when people "'*know they are being*

19. *See* NAACP v. Ala. ex rel. Patterson, 357 U.S. 449, 462–63 (1958) (determining that state demand for membership list violated the "right of private association" and would likely deter people from joining the group).

20. *See id*.

21. Tyler Valeska, *First Amendment Limitations on Public Disclosure of Protest Surveillance*, 121 COLUMBIA L. REV. FORUM 241, 241 (Dec. 15, 2021), https://perma.cc/5VA9-YK5C.

22. For example, during the 2020 Black Lives Matter protests in New York City, the NYPD used facial recognition to single out a protest organizer, Derrick Ingram, and later deployed dozens of officers (even helicopters) to his home in an extraordinary attempt to arrest him for a minor offense. George Joseph & Jake Offenhartz, *NYPD Used Facial Recognition Technology In Siege of Black Lives Matter Activist's Apartment*, GOTHAMIST (Aug. 14, 2020), https://perma.cc/ZW8R-WU7X. Ingram described the experience as being "'specifically targeted with this technology because of what we're protesting'," emphasizing that authorities were using FRT to intimidate those "'trying to deconstruct a system that they're a part of'." *Id.*

23. *Ala. ex rel. Patterson*, 357 U.S. at 462 (emphasis added).

watched, they are less likely to express themselves freely in public spaces and might not choose to exercise their rights'."[24] This sentiment was echoed by the European Court of Human Rights in a 2023 landmark ruling, which held that Russia's use of facial recognition to identify and arrest a peaceful protester in a subway violated his rights to free expression and privacy under the European Convention.[25]

In the Unites States, the prospect of police or even private entities using face-scanning to monitor who attends a protest, who enters a labor union meeting, or who visits a particular bookstore raises serious First Amendment issues. There is, as yet, little direct case law addressing facial recognition's First Amendment implications. However, existing doctrine on surveillance and associational privacy suggests that at some point, pervasive face-tracking of lawful activity could be deemed an unconstitutional burden on speech and assembly.[26] At minimum, the civil liberties community contends that use of FRT in contexts implicating political or religious expression should be tightly constrained, if not prohibited, to avoid infringing these rights.

C. Freedom from Discrimination and Bias

A third major human rights concern is freedom from discrimination, which encompasses the principle of equality under the law. Facial recognition systems have been shown to perform unevenly across different demographic groups, raising the specter of systemic bias and civil rights violations. Multiple studies, including a widely cited 2018 MIT report and

---

24. *European Court of Human Rights: Groundbreaking Ruling on Facial Recognition*, ARTICLE19 (Jul. 4, 2023), https://perma.cc/XFC4-UYPL.

25. In *Glukhin v. Russia*, the European Court of Human Rights addressed the Russian authorities' use of facial recognition technology to identify and arrest Nikolay Glukhin following his peaceful solo demonstration in the Moscow subway. *See* Glukhin v. Russia, App. No. 11519/20, ¶ 6-12 (July 4, 2023), https://perma.cc/AQG6-7GTB. The Court found that this use of facial recognition technology violated Glukhin's rights under Articles 8 and 10 of the European Convention on Human Rights, which protect the rights to privacy and freedom of expression, respectively. *See id.* at ¶ 56-57, 73. The Court emphasized that the processing of Glukhin's personal data in the context of his peaceful demonstration, which had not caused any danger to public order or safety, was "particularly intrusive" and "incompatible with the ideals and values of a democratic society governed by the rule of law." *Id.* at ¶ 86, 90.

26. The U.S. Supreme Court has long recognized that government surveillance can infringe upon First Amendment rights where it burdens the freedom of association or chills protected expression. *See generally Ala. ex rel. Patterson*, 357 U.S. More recently, courts and scholars have extended these principles to surveillance technologies, warning that persistent monitoring of individuals engaged in lawful activity—especially in public or political contexts—may violate constitutional protections. *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1951–56 (2013) (arguing that surveillance undermines intellectual privacy and can chill lawful democratic participation).

a comprehensive 2019 study by the National Institute of Standards and Technology ("NIST"), found that many facial recognition algorithms are significantly less accurate at identifying people of color, women, and other marginalized groups.[27] In particular, NIST observed "*higher false positive rates in women, African Americans, and particularly in African American women*" for the majority of facial recognition algorithms it evaluated.[28] In lay terms, this means these systems are far more likely to mistake two different Black women as the same person—a false match—compared to how often they make such errors for, say, white male faces. NIST found false positive disparities on the order of "*10 to beyond 100 times"* more frequent misidentification of Asian and Black faces compared to white faces in some algorithms.[29] These bias patterns represent a serious threat to equal protection and non-discrimination, especially when FRT is used in high-stakes contexts like policing.

When law enforcement uses a tool that is prone to misidentifying Black or Brown faces, members of those communities bear a greater risk of wrongful suspicion, arrest, or harassment. This is not just a theoretical problem; it has already occurred. In the United States, at least three Black men—Robert Williams, Michael Oliver, and Nijeer Parks—have been falsely arrested based on erroneous facial recognition matches.[30] These are the known, public cases, and there may be others that remain undisclosed. The case of Robert Williams was the first such incident to come to light: In 2020, Detroit police arrested Williams for theft, solely because facial recognition software had incorrectly matched his old driver's license photo to grainy security footage of the real suspect.[31] Williams was detained for some 30 hours and subjected to interrogation before the officers admitted 'the computer must have gotten it wrong' and released him.[32] Another Detroit man, Michael Oliver, was misidentified in a larceny case,[33] and Nijeer Parks in New Jersey was wrongly accused of shoplifting due to a bad facial recognition match, causing him to spend over a week in jail and thousands of dollars in legal fees before clearing

27. Larry Hardesty, *Study Finds Gender and Skin-type Bias in Commercial AI Systems*, MIT NEWS (Feb. 11, 2018), https://perma.cc/X67J-63VG.

28. *Facial Recognition Technology, supra* note 1 (emphasis added).

29. *Id*. (emphasis added).

30. *See* Kari Johson, *How Wrongful Arrests Based on AI Derailed 3 Men's Lives*, WIRED (Mar. 7, 2022), https://perma.cc/376Z-ZWHV.

31. *See Williams v. City of Detroit*, ACLU (Jan. 29, 2024), https://perma.cc/7VN9-TZAY.

32. *See id*.

33. *See* Elisha Anderson, *Controversial Detroit Facial Recognition Got him Arrested for a Crime he Didn't Commit*, DETROIT FREE PRESS (Jun. 20, 2020), https://perma.cc/YW2J-XF49.

his name.[34] These cases illustrate the human cost of algorithmic bias: the technology's imperfections disproportionately harm people of color, putting innocent individuals at risk of being entangled in the criminal justice system. From a human rights perspective, this implicates the rights to equality, due process, and freedom from arbitrary detention.

Discrimination concerns are not limited to government use. Private companies using facial recognition for their own purposes may also engage in practices that disproportionately burden certain groups. For instance, retail stores have implemented FRT to identify suspected shoplifters or to bar "undesirable" customers. Investigations reveal that these systems, wittingly or unwittingly, often target minority shoppers.[35] In one case, the pharmacy chain Rite Aid quietly installed facial recognition cameras in hundreds of stores, predominantly in lower-income, non-white neighborhoods.[36] Not only did this raise equity issues in who was being surveilled, but the technology also misidentified people, flagging innocent "Black, Latino, [and] Asian" customers as potential shoplifters at higher rates, according to reports.[37] Such false accusations can lead to humiliating incidents or denial of service, effectively resulting in discriminatory treatment in places of public accommodation. In 2023, the Federal Trade Commission ("FTC") went further, charging that Rite Aid's use of facial recognition harmed consumers and banning the company from using FRT for 5 years under a settlement order.[38]

Another prominent controversy erupted in New York, where Madison Square Garden Entertainment ("MSGE") used facial recognition to ban all lawyers affiliated with firms representing clients in litigation

---

34. *See* Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Dec. 29, 2020), https://perma.cc/U97P-ERH7.

35. *See* Clare Garvie & Laura Moy, *America Under Watch: Face Surveillance in the United States*, GEORGETOWN LAW CTR. ON PRIVACY & TECH. 15–18 (2021), https://perma.cc/2H6X-G7QL (detailing retail FRT deployments and discriminatory impacts).

36. *See Rite Aid Banned from Using AI Facial Recognition*, REUTERS (Dec. 19, 2023), https://perma.cc/MU89-LVZB.

37. *Id*.

38. *See Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards*, FTC (Dec. 19, 2023), https://perma.cc/PY47-7DVZ. The FTC alleged that Rite Aid "failed to implement reasonable procedures [to] prevent harm to consumers in its [deployment] of facial recognition" systems across hundreds of stores. *Id.* Specifically, the FTC's complaint highlighted that the technology "disproportionately impacted people of color "and women, leading to false identifications and subsequent actions by store employees that included following, searching, and "publicly accusing" customers of wrongdoing. *Id.* The settlement also requires Rite Aid to "implement comprehensive safeguards to prevent [future] harm to consumers when deploying automated systems that use biometric information." *Id.*

against MSGE from entering its sports and entertainment venues.[39] This policy—facially neutral but applied to individuals based on their employment associations—drew public outcry and scrutiny from the New York Attorney General for its potential to facilitate retaliatory discrimination and perhaps violate laws against excluding patrons for non-security reasons. While MSGE defended the practice as a security measure, critics noted there was little evidence it improved safety, and it primarily served to punish a disfavored group—legal adversaries—using face-ID as an enforcement tool.[40]

In short, the freedom from discrimination is at risk when facial recognition is deployed without safeguards. The technology's errors do not affect everyone equally: they burden women and people of color more. And even when accurate, FRT may be used in ways that reflect bias, conscious or not, by targeting certain groups for surveillance. These realities demand that any use of facial recognition be examined through a civil rights lens. As Professor Hannah Bloch-Wehba observes, "facial recognition technology tends to misidentify people of color, and in particular, women of color", raising serious concerns about racial and gender bias in how the tech is used to screen people.[41] Absent intervention, these systems could reinforce structural inequalities under the guise of algorithmic objectivity. Protecting human rights in the biometric age thus requires grappling with both the disparate impact and potential for intentional misuse of facial recognition against marginalized communities.

III. THE U.S. LEGAL AND REGULATORY LANDSCAPE

Despite the far-reaching implications of facial recognition, as of 2025, the United States has *no comprehensive federal statute* specifically regulating the collection or use of biometric data such as facial recognition. In contrast to jurisdictions like the European Union, where the General Data Protection Regulation ("GDPR") treats biometric data as a special sensitive category, and the proposed AI Act may severely restrict face surveillance, U.S. privacy law remains sectoral and piecemeal. No federal privacy law broadly protects "consumer privacy" writ large. Certain sector-specific laws—for example, the Health Insurance Portability and Accountability Act for health data, or FERPA for educational records, might incidentally cover some biometric information in narrow contexts, but nothing related to a general rule for facial

39. *See* Restrepo, *supra* note 8.
40. *See id*.
41. *Id.* (internal quotation marks omitted).

recognition exists.[42] The absence of federal legislation means companies are largely free to deploy facial recognition on consumers with minimal oversight, aside from general consumer protection laws. The FTC has authority to police "unfair or deceptive practices," which it has used to address some privacy issues.[43] Conceivably, if a company misleads consumers about using facial recognition or fails to secure biometric data, the FTC could take action. However, the FTC cannot require upfront safeguards absent a rule, and its case-by-case enforcement is reactive.

There have been attempts in Congress to pass laws addressing facial recognition. One notable proposal is the Facial Recognition and Biometric Technology Moratorium Act—originally introduced in 2020 and reintroduced in subsequent sessions—which would halt federal use of facial recognition and withhold funds from local governments that use it, until certain conditions are met.[44] Another bill, the Fourth Amendment Is Not For Sale Act, would prohibit law enforcement from purchasing data, including possibly facial recognition data, from commercial vendors to

42. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects certain biometric data, such as facial images or fingerprints, when they are included in individually identifiable health information held by a covered entity or business associate. *See* 45 C.F.R. § 160.103 (2026). HIPAA defines "protected health information" to include biometric identifiers when used in connection with the provision of healthcare or payment for healthcare services. *Id.* However, HIPAA protections are limited to health-related contexts and do not apply to biometric data collected outside the healthcare sector. *See id.* Similarly, the Family Educational Rights and Privacy Act (FERPA) protects students' education records, which can include biometric identifiers like facial images or voiceprints when maintained by an educational institution. *See generally* 20 U.S.C. § 1232g (2026). Yet FERPA only applies to institutions receiving federal funding and does not regulate third-party technology vendors unless they act on behalf of the institution. *See id.* at (b)(4)(B). Neither law provides comprehensive or standalone regulation of facial recognition technology. *See* 45 C.F.R. § 164.514(b)(2)(i)(Q) (2026) (identifying "full face photographic images and comparable images" as direct identifiers under HIPAA); 34 C.F.R. § 99.3 (2026) (defining education records under FERPA to include biometric data when maintained by an educational agency or institution).

43. 15 U.S.C. § 45(a)(1) (2026). The Federal Trade Commission derives its authority to regulate privacy practices from Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce." *Id.* The FTC has interpreted this mandate to encompass certain privacy-related violations, such as failure to adequately disclose data practices, misrepresentations in privacy policies, or unreasonable data security measures. *See id.* Over the past two decades, the FTC has brought numerous enforcement actions against companies for mishandling personal data, including biometric and facial recognition information, often framing such conduct as either deceptive (when companies misrepresent their practices) or unfair (when the practices cause "substantial injury" not reasonably avoidable by consumers). *See id.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598–99 (2014).

44. *See* Facial Recognition and Biometric Technology Moratorium Act of 2023, S. 681, 118th Cong. (as reported by S. Comm. On the Judiciary, Mar. 7, 2023).

circumvent warrant requirements.[45] As of this writing, however, no such bills have become law.

A bipartisan coalition of lawmakers has expressed concern about unregulated facial recognition, especially after a Government Accountability Office ("GAO") report in 2021 found that dozens of federal agencies were experimenting with it without clear guidance.[46] Still, legislative inertia persists. According to Michael Mellon, facial recognition technology remains unregulated at the federal level in the United States, a situation that privacy advocates call on Congress to urgently change.[47] The result is that much of the governance of facial recognition has fallen to the states and localities.

The most important legal guardrail in the U.S. so far is the Illinois Biometric Information Privacy Act ("BIPA"). Enacted in 2008, BIPA is a pioneering state law that imposes strict requirements on private entities collecting biometric identifiers, including scans of face geometry.[48] BIPA requires companies to obtain informed written consent before collecting a person's biometric data, to disclose the purpose and duration of use, and to implement reasonable safeguards.[49] It also creates a private right of action, allowing individuals to sue for violations with statutory damages.[50]

BIPA's robust provisions have made Illinois a battleground for facial recognition litigation. It was under BIPA that Facebook faced a class action over its face-tagging feature, leading to a $650 million settlement in 2020 for using Illinois residents' face data without proper consent.[51] And in perhaps the most consequential enforcement, the ACLU and other plaintiffs sued Clearview AI under BIPA in 2020, alleging that Clearview's scraping of Illinois residents' photos and creation of faceprints without consent violated the law.[52] In 2022, Clearview agreed

45. *See* Fourth Amendment Is Not For Sale Act, H.R. 4639, 118th Cong. (2023).

46. *See Facial Recognition Technology: Federal Law Enforcement Agency Efforts Related to Civil Rights and Training*, GAO (Mar. 8, 2024), https://perma.cc/6KF7-8W2J.

47. *See* Michael Mellon, *Facial Recognition Technology and the Dire Need to Regulate It*, 77 SMU L. REV. F. 272, 273 (2024).

48. *See generally* 740 Ill. Comp. Stat. §§ 14/1–14/99 (2008) (establishing requirements for private entities collecting, storing, and using biometric identifiers, including informed consent, data retention policies, and a private right of action).

49. *See* 740 Ill. Comp. Stat. § 14/15(a)–(e) (2008).

50. *See* 740 Ill. Comp. Stat. 14/20 (2008) (providing a private right of action and statutory damages for negligent and intentional violations).

51. *See* Jennifer Bryant, *Facebook's $650M BIPA Settlement 'a make-or-break moment,'* IAPP (Mar. 5, 2021), https://perma.cc/899V-BN8X.

52. The human rights and privacy concerns with Clearview's model are manifold. First, individuals whose photos were scraped never consented to their images being converted into biometric identifiers and sold. This is a violation of privacy and data

to a sweeping settlement: it is "permanently banned, nationwide, from" selling or providing its faceprint database to most private entities and even barred from doing business with Illinois law enforcement for five years.[53] This settlement essentially forces Clearview to limit its sales to federal and state law enforcement, outside Illinois, and to stop working with private companies—a significant victory for privacy, albeit one tied to Illinois residents' rights.[54]

The Clearview case demonstrates BIPA's power as a check on the private biometrics industry. However, no other state has a law as strong as Illinois' BIPA, at least not with a private lawsuit mechanism. Texas and Washington have biometric privacy statutes, but they lack private rights of action and enforcement is left to Attorneys General.[55] A few other states, like California—in its California Consumer Privacy Act—and New York—via the SHIELD Act for data security—include biometric data in their broader privacy regimes but with relatively limited effect on facial recognition specifically.[56]

---

protection norms. As Kashmir Hill put it in her book, Clearview "might end privacy as we know it" by erasing the practical anonymity people enjoyed in their casual online photos. KASHMIR HILL, YOUR FACE BELONGS TO US: A SECRETIVE STARTUP'S QUEST TO END PRIVACY AS WE KNOW IT 153–59, 237–45 (2023). Second, Clearview's clients included not just police solving serious crimes, but also private companies and even authoritarian foreign governments (according to news investigations), raising the risk of abuse. *See id.* For instance, retail chains and casinos reportedly tested Clearview to identify VIP customers or shoplifters, and law enforcement usage ranged from legitimate criminal investigations to identifying protesters and bystanders. *See id.* With minimal oversight, the technology could easily be misused to stalk or harass individuals. Third, Clearview's system implicated free expression concerns because police could identify protesters or political opponents en masse. *See id.* After January 6, 2021, Clearview boasted of a spike in law enforcement searches; while catching rioters may be laudable, the same tool could be turned on peaceful demonstrators in the future. *See id.*

53. *In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law, supra* note 16.

54. *See id*.

55. *See generally* Tex. Bus. & Com. Code Ann. §§ 503.001–.003 (LexisNexis 2025) (prohibiting the capture of biometric identifiers for a commercial purpose without informed consent and limiting disclosure, with enforcement by the Texas Attorney General); Wash. Rev. Code Ann. §§ 19.375.010–.900 (LexisNexis 2026) (regulating the collection and use of biometric identifiers, requiring notice and consent, and providing for enforcement exclusively by the Washington Attorney General).

56. The California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act ("CPRA"), defines "biometric information" to include facial imagery and allows consumers to request access to, deletion of, and restrictions on the use of such data. *See* Cal. Civ. Code §§ 1798.100 (2026). However, the statute focuses on consumer rights and transparency, rather than regulating the use of facial recognition technology per se. *See generally* Cal. Civ. Code §§ 1798.100–1798.199.100. New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act amends the state's data breach notification law to include biometric data as private information and requires businesses to implement reasonable security measures to protect it, but it

At the municipal level, there has been a wave of bans or moratoriums on government, especially police, use of facial recognition. Starting with San Francisco in 2019, at least a dozen U.S. cities and localities, including Boston, Oakland, Portland (Oregon), Portland (Maine), and Jackson (Mississippi), have passed laws forbidding their city agencies from using facial recognition technology.[57] These measures are often driven by concerns about civil liberties and accuracy. For instance, Boston's city council unanimously banned facial recognition use by city government in 2020, declaring that the risks to citizens' rights outweighed any purported benefits.[58] Portland, Oregon went even further, not only banning city use, but also banning private businesses from using facial recognition in places open to the public, like stores, hotels, etc., citing bias and privacy concerns, making this ordinance the most sweeping municipal restriction in the country.[59]

In summary, current U.S. law leaves wide gaps. Private corporations can often deploy facial recognition without transparency or consent outside of Illinois and, to a lesser degree, Texas and Washington. Government agencies can experiment with facial recognition largely at their discretion, unless restrained by local laws or internal policies. There is a growing chorus of civil society voices urging comprehensive legislation: perhaps a federal biometric privacy act modeled on BIPA, or at minimum strict rules on law enforcement use, such as requiring warrants or limiting it to serious crimes, along with audits for bias. Absent such measures, many feel the balance is skewed in favor of surveillance over rights. The next Part will delve into legal reforms and policy recommendations.

IV. LEGAL REFORMS AND POLICY RECOMMENDATIONS

In light of the significant threats posed by facial recognition to privacy, free expression, and equality, a robust legal and policy response is imperative. This Part proposes a set of reforms, drawing on human rights principles and emerging best practices, to better protect civil liberties in the era of facial recognition. The recommendations span federal and state

---

does not specifically govern the collection or use of facial recognition. *See generally* N.Y. Gen. Bus. Law §§ 899-aa–899-bb (2026).

57. *See* Shannon Flynn, *13 Cities Where Police are Banned from Using Facial Recognition Tech*, INNOVATION & TECH, https://perma.cc/45KG-FN2M (last visited Apr. 25, 2026).

58. *See* Ally Jarmanning, *Boston Bans Use Of Facial Recognition Technology. It's The 2nd-Largest City To Do So*, WBUT (Jun. 24, 2020), https://perma.cc/EZ7W-QLC6.

59. *See* Sarah Wray, *Portland Bans Private Companies from Using Facial Recognition Technology*, CITIES TODAY (Sept. 17, 2020), https://perma.cc/SFN2-J7N4.

legislation and corporate policy changes. The overarching goal is to reclaim individual control over personal biometric data and prevent the normalization of mass surveillance.

A. Enact a Comprehensive Federal (Biometric) Privacy Law

First and foremost, Congress should pass a federal law regulating the collection and use of biometric identifiers in the private sector. This law should be modeled on effective elements of Illinois' BIPA and international standards.

Key provisions of this proposed law should include: (1) requiring affirmative, opt-in consent from individuals before a company can collect or utilize their facial data, with a clear explanation of the purpose and duration of use; (2) prohibiting the sale or sharing of biometric data to third parties without separate consent; (3) mandating strong data security safeguards and prompt breach notification if biometric data is compromised; (4) providing a private right of action so that individuals can sue for violations and obtain statutory damages, which is crucial for enforcement, as demonstrated by BIPA's success in Illinois; and (5) requiring bias testing and transparency, making companies providing facial recognition services obligated to test their algorithms for accuracy across different demographics and report the results. In relation to the fifth key provision, if error rates for any demographic are above a certain threshold, the technology should be deemed not fit for broad deployment. This type of law could empower the FTC to set accuracy standards over time.

Such federal legislation would set a baseline nationwide, ending the current patchwork where consumers' faces might be protected in Illinois but not in Georgia. It would also ensure companies like Clearview cannot simply move to a different state to escape liability. Notably, a comprehensive federal privacy law has been in discussion in Congress and biometric data is often included in those proposals.[60] This law should explicitly cover facial recognition practices, avoiding any loopholes carving the practice out of the law.

Treating facial biometrics as sensitive data deserving special protection would align the United States more with international human

60. *See* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. §§ 2(3), 2(28)(A), 204(b)(1)(B), 208(b)(1)(A) (2022); *see also* Consumer Online Privacy Rights Act, S. 3195, 116th Cong. § 2(18) (2020); Data Protection Act of 2021, S. 2134, 117th Cong. § 2(4) (2021); American Privacy Rights Act of 2024, H.R. 8818, 118th Cong. §§ 101(1)(B), 101(2), 102(c) (2024).

rights norms on privacy. As one ACLU technologist put it, "other states should follow Illinois' lead in enacting strong biometric privacy laws,"[61] and a federal law can achieve that uniformly.

B. Impose Moratoria and Strict Limits on Government Use

Given the profound civil liberties implications, advocates urge a moratorium on government, especially law enforcement, use of facial recognition. A temporary ban, at least on the most surveillance-oriented uses, would provide breathing room to assess the technology and implement regulations. This temporary ban can be accomplished through federal legislation like the proposed Facial Recognition and Biometric Technology Moratorium Act, which would halt all federal use and pressure local use, or through state laws prohibiting use by state and local agencies.[62]

Congress or states should require that law enforcement obtain a warrant before using facial recognition to either identify an unknown individual or to track and monitor an identified person, with the warrant supported by probable cause that the search will yield evidence of a serious crime. This treats face searches akin to phone searches or GPS tracking, bringing Fourth Amendment principles into play statutorily if courts haven't yet mandated it. Exceptions can be made for exigent circumstances such as imminent threats, but then after-the-fact oversight must occur.[63]

---

61. *In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law, supra* note 16.

62. The Facial Recognition and Biometric Technology Moratorium Act, first introduced in 2020 and reintroduced in subsequent Congresses, would prohibit federal agencies from using facial recognition and other biometric surveillance technologies and would restrict the use of federal funds to support biometric surveillance by state and local law enforcement. *See* Facial Recognition and Biometric Technology Moratorium Act of 2023, S. 681, 118th Cong. (as reported by S. Comm. On the Judiciary, Mar. 7, 2023). The bill reflects growing concerns about the civil rights and privacy implications of these technologies, particularly their disproportionate impact on marginalized communities. *See id.*

63. Requiring a warrant for the use of facial recognition aligns with the logic of recent Supreme Court decisions recognizing that certain forms of technologically enhanced surveillance intrude upon reasonable expectations of privacy and therefore constitute searches under the Fourth Amendment. *See* Carpenter v. United States, 585 U.S. 296, 309-10 (2018) (finding that historical cell-site location tracking constituted a Fourth Amendment search) and United States v. Jones, 565 U.S. 400, 404 (2012) (finding that GPS monitoring constituted a Fourth Amendment search). While courts have not yet uniformly extended this reasoning to facial recognition, legal scholars argue that biometric surveillance tools are similarly invasive, capable of enabling "pervasive," "retrospective," and "suspicionless" tracking of individuals across time and space. Ferguson, *supra* note 6, at 1141-46.

Even with a warrant, the use of FRT should be limited to certain serious offenses and barred for low-level misdemeanors, petty offenses, and general intelligence gathering. This policy prevents "mission creep" where police start using the technology for trivial matters and broad surveillance of communities. It also inherently reduces how often the technology is used, mitigating bias impact. Policy should also prohibit real-time or "persistent" facial recognition surveillance of public spaces. In other words, law enforcement should not be allowed to live-monitor crowds or public feeds with face identification, absent an extreme emergency or a court order in a particular instance of national security. Also, when facial recognition is used in a criminal investigation, that fact must be disclosed to the defendant and in any court proceedings, much like how use of confidential informants or wiretaps must be disclosed. This allows the defendant to challenge the reliability of the identification and the technology used.

Additionally, any authorized use of facial recognition by agencies must be logged and subject to periodic audits by independent auditors or inspectors general. The audits should check for compliance with policies, accuracy of results, and any signs of misuse. Results of audits can be reported to legislatures and made public, with appropriate redactions in accordance with the Freedom of Information Act.

Any entity, public or private, using facial recognition that affects the public should be required to provide transparency. This means police departments should publish annual reports on how many face searches they did, for what types of crimes, and what the outcomes were. Companies that use FRT in stores or other customer-facing situations should post signage—as NYC law requires, for example—and have easily accessible privacy policies explaining their use.

Finally, technology companies developing facial recognition should be required to disclose their role to regulators. These companies should follow principles like those proposed by the OECD and ACM, ensuring privacy by design.[64] For example, companies can design systems to

64. Industry standards and policy frameworks increasingly urge technology companies to embed privacy protections into the design of facial recognition systems, minimizing risks of misuse and rights violations. The Organisation for Economic Co-operation and Development ("OECD") recommends adopting privacy-by-design practices and conducting impact assessments to ensure responsible stewardship of biometric data. *See* Organisation for Economic Co-operation and Development [OECD], *Recommendation of the Council on Artificial Intelligence*, OECD Doc. LEGAL/0449 (May 22, 2019), https://perma.cc/K2F9-YKM3. The Association for Computing Machinery ("ACM") similarly advocates for algorithmic accountability and system transparency to mitigate discriminatory and privacy-invasive outcomes. *See* ACM U.S.

operate locally on users' devices, thereby avoiding cloud storage of images, while reducing data retention and incorporating audit logging mechanisms to deter misuse. While these corporate measures are largely voluntary, they align with a human rights due diligence approach, as per the UN Guiding Principles on Business and Human Rights, where companies should avoid contributing to rights abuses.[65]

To achieve these changes, a coalition of stakeholders is needed. Civil society must keep raising awareness and litigating pivotal cases. Lawmakers at city, state, and federal levels cannot wait for a perfect consensus; they should act where they have jurisdiction, as many cities have. The new Congress should prioritize a biometric privacy act and consider attaching facial recognition limits to must-pass bills. Meanwhile, the executive branch can affect change through procurement rules: the federal government should decide it will not purchase facial recognition tech that doesn't meet certain standards, as it did with AI principles for federal agencies.[66] The FTC should also signal that certain uses of facial recognition, like surreptitious scanning of customers, will be pursued as unfair practices, essentially discouraging the behavior industry-wide.

C. Strengthen Transparency, Auditing, and Public Oversight Mechanisms

Effective regulation of facial recognition technology should begin with robust transparency mandates at all levels of government. Statutory reforms can require agencies and companies to disclose when and how facial recognition is used, evaluated, and governed. For example, Washington State's pioneering 2020 law SB 6280 obligates state and local agencies to publish detailed Accountability Reports before deploying facial recognition, documenting the system's purpose, data management practices, and potential impacts on civil rights.[67] The same law compels periodic testing and "meaningful human review" of any facial recognition system that could produce significant legal effects.[68] New York City's POST Act similarly increased transparency by requiring the NYPD to publish public surveillance "impact and use policies" for each tool it

Tech. Policy Comm., *Statement on Principles for Responsible Algorithmic Systems* (Oct. 26, 2022), https://perma.cc/5NS9-FYNA.

65. *See* U.N. Hum. Rts. Council, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, at principles 11–17, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011).

66. *See* Covington & Burling LLP, *OMB Releases Requirements for Responsible AI Procurement by Federal Agencies* (Oct. 24, 2024), https://perma.cc/Q885-MH4E.

67 *See* Jessica Sganga, *Washington State's Facial Recognition Law: Attempt at Transparency Still Leaves Civil Liberties Questions*, KNOBBE (Aug. 10, 2020), https://perma.cc/8FW2-Q6ZF.

68. *Id*. (internal quotation marks omitted).

employs.[69] In practice, these disclosures allowed the public and policymakers to scrutinize how facial recognition is being used and whether safeguards are in place. To ensure transparency rules have teeth, periodic audits of compliance are essential.[70] The POST Act, for instance, tasks the Inspector General with annual audits of the NYPD's surveillance tech policies—an oversight mechanism that revealed the NYPD had evaded full disclosure through "boilerplate language" and umbrella policies.[71] Strengthening such laws, as New York is now considering, can close loopholes and penalize evasive practices.[72]

Model provisions should also impose algorithmic audit mandates, requiring independent bias and performance testing of facial recognition systems on a regular schedule. These audit mandates can be implemented via statutes or procurement rules. The Algorithmic Accountability Act, a federal legislative proposal, would require companies to conduct and submit impact assessments of "critical" automated decision systems, including those using facial recognition, "for bias, effectiveness, and other [risks]."[73] The Act would create a "public repository" of these assessments at the FTC, ensuring both regulators and the public gain insight into algorithmic decision-making processes.[74] At the local level, New York City has already embraced audit mandates in a narrower context. Local Law 144 requires independent "bias audit[s]" of automated hiring tools.[75] Similar requirements could be extended to facial recognition. For example, laws could obligate any facial recognition system used by law enforcement or in high-stakes settings to undergo third-party accuracy and bias audits annually, with summary results published. Washington's SB 6280 took a step in this direction by requiring vendors to enable "independent testing" of their systems for accuracy and disparate impacts across racial and demographic groups.[76] If testing finds unfair bias, the vendor must mitigate that bias "within 90 days."[77] Federal guidance is starting to echo this approach. Recent White House procurement policy

69. *The Public Oversight of Surveillance Technology (POST) Act: A Resource Page,* BRENNAN CENTER FOR JUSTICE (June 12, 2017), https://perma.cc/9AQR-753A.

70. *See id*.

71. *Id*.

72. *See id*.

73. *Wyden, Booker and Clarke Introduce Algorithmic Accountability Act of 2022 To Require New Transparency And Accountability For Automated Decision Systems*, WYDEN (Feb. 2, 2023), https://perma.cc/MB6M-GSZY.

74. *Id*.

75. *Automated Employment Decision Tools (AEDT*), NYC CONSUMER & WORKER PROTECT, https://perma.cc/DVV2-ZX5N (last visited Ap. 26, 2026).

76. Jessica Sganga, *Washington State's Facial Recognition Law: Attempt at Transparency Still Leaves Civil Liberties Questions*, KNOBBE MARTENS (Aug. 10, 2020), https://perma.cc/P4PD-5GHZ.

77. *Id*.

directs agencies to ensure contracts allow ongoing monitoring and "require vendors to perform regular assessments" and risk mitigation for AI systems.[78] One concrete measure is to mandate that any facial recognition product procured by government has been assessed in NIST's Face Recognition Vendor Test ("FRVT") program.[79]

Transparency and audits should be coupled with mechanisms for public oversight. One successful model has been the adoption of local surveillance oversight ordinances, often referred to as Community Control Over Police Surveillance ("CCOPS") laws.[80] These laws, now enacted in over two dozen U.S. cities, require police and city agencies to seek city council approval and invite community recommendations before acquiring or deploying surveillance technologies, including facial recognition.[81] They also mandate agencies to publish use policies and annual reports, ensuring ongoing accountability.[82] For instance, Oakland, California created a "Privacy Advisory Commission"—a civilian board with broad authority to review and veto surveillance technology proposals.[83] That commission was instrumental in Oakland's decision to "ban[] municipal use of facial recognition" and has become a national model for local oversight.[84] The Commission's existence means that in Oakland "there's a body looking at the issues" of surveillance technology before it is deployed, rather than secret police adoption of this technology.[85] Legislators should consider requiring independent oversight boards or committees, at the municipal or state level, to supervise facial recognition use. These bodies could review impact assessments, approve or deny high-risk uses, and serve as an ongoing watchdog. Statutory oversight bodies can also be created at the state level. For example, a state could establish a facial recognition use commission comprised of technologists, civil rights experts, and community representatives, tasked with reviewing and approving any government use of the technology. In

78. *OMB Issues Revised Policies on AI Use and Procurement by Federal Agencies*, HUNTON: PRIV. & CYBERSECURITY L. BLOG (Apr. 23, 2025), https://perma.cc/3EX5-X4EG.

79. *See* Off. of Mgmt. and Budget, *Memorandum on Advancing the Responsible Acquisition of Artificial Intelligence in Government* (Sept. 24, 2024), https://perma.cc/R278-TV2G.

80. *See Community Control over Police Surveillance*, ACLU, https://perma.cc/26HE-9C9K (last visited Apr. 9, 2026).

81. *See id.*

82. *See generally* Stevie DeGroff & Albert Fox Cahn, *An Early Assessment of Community Control Over Police Surveillance Laws* (Feb.. 10, 2021), https://perma.cc/SBA9-TN4Q.

83. Alan Greenblatt, *What Cities Can Learn from the Nation's Only Privacy Commission*, GOVERNING (Feb. 21, 2020), https://perma.cc/6TS3-GHL5.

84. *Id*.

85. *Id*.

the federal context, while no dedicated facial recognition commission exists, agencies are increasingly encouraged to integrate privacy and civil liberties officials into AI governance boards.[86]

D. Increase Vendor Accountability and Supply Chain Governance in Facial Recognition

A comprehensive regulatory approach must also place direct responsibilities on the companies that build and sell facial recognition systems. Currently, many vendors have little incentive to address the downstream harm caused by their technology. New legal requirements can change this by imposing affirmative human rights due diligence obligations, setting procurement eligibility standards, and establishing liability for negligent or harmful deployments. In the international arena, frameworks like the OECD Guidelines for Multinational Enterprises explicitly call on tech companies to conduct "risk-based due diligence" throughout the AI system lifecycle, not only in their own operations but also across their "value chain", including impacts on end-users.[87] This means an AI developer should identify and mitigate potential harms that their facial recognition software might enable, even when used by third parties. U.S. law can mirror these principles. For example, Congress should require that any company providing facial recognition services implement a due diligence program to evaluate the civil rights, privacy, and safety risks of its products, akin to how companies must perform environmental or supply-chain due diligence in other sectors. The FTC has signaled it will treat certain lapses in AI risk mitigation as unfair or deceptive practices under consumer protection law.[88] In 2023, the FTC issued a policy statement warning that companies should "assess foreseeable harms" of biometric technologies, address known risks like bias or security vulnerabilities, and "evaluate the practices" of third-party partners and clients, or else face liability under the FTC Act.[89] This oversight effectively pushes vendors to conduct internal audits and to ensure that those they do business with, including law enforcement customers and subcontractors, adhere to safeguards.

Government procurement rules are a powerful lever to enforce vendor accountability. Legislation or executive action could bar federal agencies, and incentivize states and municipalities to bar their agencies,

86. *See OMB Issues Revised Policies on AI Use and Procurement by Federal Agencies, supra* note 78.

87. *OECD Guidelines on Responsible Business Conduct: Key Considerations for Multinational Enterprises,* COOLEY (May 31, 2024), https://perma.cc/ZFU2-XPXF.

88. *FTC Warns About Misuses of Biometric Information and Harm to Consumers*, FTC (May 18, 2023), https://perma.cc/2W2K-AD5W.

89. *Id*.

from purchasing or using facial recognition systems that do not meet defined ethical and technical standards. This concept has precedent: experts have proposed amending the Federal Acquisition Regulation ("FAR") to require bias testing and accuracy benchmarks for any facial recognition product bought with federal funds. By conditioning lucrative government contracts on compliance, vendors would be pressed to improve their systems and business practices. For instance, Congress might mandate that any facial recognition system under consideration for federal procurement must demonstrate minimal demographic bias in independent evaluations, implement privacy safeguards such as data minimization and security, and provide detailed documentation about training data and algorithms for agency review. The White House's 2024 AI acquisition guidance instructs agencies to include contract terms for ongoing monitoring of AI systems and to require vendors to perform regular risk assessments and corrections to any performance drifts.[90] It also urges agencies to prevent "vendor lock-in" and to demand transparency.[91] In the specific context of facial recognition, OMB has advised that solicitations should require vendors to submit their algorithms to NIST's rigorous FRVT prior to deployment.[92] Incorporating such requirements into law or binding policy ensures that vendors cannot treat accuracy and fairness as mere options; they become prerequisites for market access, at least in the public sector. Over time, these standards tend to ripple out to private-sector uses as well, especially if large tech purchasers adopt similar procurement criteria.

A more challenging but crucial aspect of vendor accountability is establishing clear liability when facial recognition technology causes harm. Under current law, individuals wrongfully arrested or harmed due to a false facial recognition match have little recourse against the software providers. Liability typically falls, if at all, on the end-user or government agency. Policymakers are considering ways to change this, drawing on analogies to product liability and negligence. One approach is to create a statutory cause of action for "algorithmic harm." For example, if a facial recognition developer sells a system known or that should be known to have high error rates among certain demographics, and that flaw leads to a concrete injury, such as an unjust arrest or denial of services, the affected individual could sue the vendor for damages. The BIPA, as explained before, offers a blueprint for empowering individuals to hold companies accountable. Building on BIPA, lawmakers could expand liability so that

90. *See OMB Issues Revised Policies on AI Use and Procurement by Federal Agencies, supra* note 78.

91. *Id*.

92. *See* Off. of Mgmt. and Budget, *supra* note 79.

if vendors knowingly supply facial recognition for uses that violate civil rights or data protection laws, they share responsibility. Additionally, tort law could evolve to recognize a duty of care on AI vendors to ensure their products, when used as intended, do not pose unreasonable risks to the public. While defining the scope of such liability is complex, even targeted measures like enabling state attorneys general to sue vendors for egregious failures, such as not rectifying an algorithm known to produce biased results, would create incentive for better industry self-policing.

Part of supply chain governance is setting clear standards and best practices for vendors. Agencies like NIST and OSTP have begun issuing frameworks that vendors can be expected to follow. The NIST AI Risk Management Framework, for example, provides a blueprint for identifying and mitigating risks throughout an AI system's life cycle, and it backs measures like third-party audits and documentation of training data.[93] Similarly, the White House's Blueprint for an AI Bill of Rights articulates that automated systems should be built with protections against algorithmic discrimination and with provisions for explanation and human oversight. While these are advisory, they lay the groundwork for binding standards. Regulators could require that vendors certify compliance with such frameworks as a condition of certain contracts or even market entry. Internationally, the EU's AI Act imposes direct obligations on AI providers, from quality and transparency requirements to post-market monitoring, with fines "up to 7%" of global turnover for non-compliance.[94] Notably, providers of "high-risk AI" in Europe have to implement risk management, log performance data, and conform to safety standards before product launch.[95] U.S. companies eyeing global markets will likely adhere to these norms due to the brussels effect, and U.S. policymakers can similarly mandate "secure by design" and "fair by design" practices.

In sum, increasing vendor accountability means recalibrating the incentives so that those who profit from facial recognition also bear responsibility for its societal impacts. Through a combination of legal mandates—due diligence, transparency, and non-discrimination requirements—procurement policies that reward responsible actors, and liability frameworks that redress harms, the law can shift the facial recognition industry toward a higher standard of care. Importantly, these measures also protect the integrity of the supply chain by ensuring that

93. *See Algorithmic Accountability: Moving Beyond Audits*, AI NOW INST. (Apr. 11, 2023), https://perma.cc/63GF-XJ2U.

94. 2024 O.J. (L 1689) art. 99(3).

95. *See EU AI Act: First Regulation on Artificial Intelligence*, EUROPEAN PARLIAMENT (Jun. 8, 2023), https://perma.cc/3J5W-4UV2.

from development to deployment, facial recognition technologies are subject to checks that minimize the risk of "downstream" abuses and rights violations. Centering vendor accountability in reform efforts recognizes that meaningful facial recognition regulation cannot focus solely on end-users; it must also "raise the floor" of corporate conduct in this high-stakes sector.

V. CONCLUSION

Facial recognition technology presents a defining test for the future of privacy and human rights in America. If allowed to proliferate unchecked, it could enable a level of surveillance and social control incompatible with a free, open society. The potential harms are not abstract: they are visible in the wrongful arrests of Black men in Detroit, the identification of protesters in D.C., the banning of attorneys at Madison Square Garden, and the quiet tracking of shoppers in Rite Aid stores. These examples show how facial recognition, absent rules, tends to be deployed in ways that encroach on civil liberties and exacerbate inequality. In the United States, a country that prides itself on constitutional freedoms, this technology's trajectory must be guided by those fundamental values.

The current U.S. legal framework has not kept pace with the technology's rapid advance. A clear gap in federal law has left individuals' biometric privacy largely unprotected, even as companies and police forces rush to adopt face-scanning systems. Constitutional doctrines are only beginning to grapple with scenarios that ubiquitous facial recognition creates, from continuous public monitoring to chilled assembly. This article has argued that both legislative action and constitutional evolution are needed to prevent the worst outcomes. Fortunately, the challenge has been recognized, and momentum for reform is building at the state and municipal levels. Courts are seeing the first lawsuits that address face surveillance, cities are banning it, and even tech companies have called for "AI regulation" to ensure responsible use.

Grounding the analysis in human rights principles provides a moral compass. The right to privacy, to free expression, to due process and equality—these are non-negotiable rights that any new technology must respect. This article's recommendations outline a blueprint for the ethical use of this emerging technology: enforce consent and transparency in the private sector, constrain and oversee government use, ban the most dangerous applications, and give individuals tools to fight back when their rights are infringed. Implementing these will require political will and public pressure.

In closing, the intersection of consumer privacy, facial recognition technology, and human rights reveals critical tensions between individual liberties and technological advancement. The question of whether individuals can move freely without persistent monitoring and whether their facial data remains within their control highlights the urgent need for comprehensive legal safeguards. The United States has the opportunity—and responsibility—to align its regulatory approach with fundamental human rights principles, balancing innovation against privacy and dignity. Ensuring facial recognition technology respects privacy rather than eroding civil liberties requires proactive legislative measures. Such measures must establish clear boundaries to protect individuals from invasive surveillance practices. Without deliberate regulatory action, facial recognition technology risks becoming a pervasive threat rather than a beneficial innovation, ultimately undermining the very freedoms it purports to enhance.