

Bias, Misuse, and Accountability in Facial Recognition Technology: Ethical, Legal, and Organizational Imperatives in the Age of Reverse Image Search

Lord DORDUNOO

*Doctoral Candidate, Marymount University, Arlington, VA, USA
ORCID: <https://orcid.org/0009-0007-7395-2677>*

Abstract: Facial recognition technology (FRT) has become an increasingly pervasive tool in law enforcement, immigration control, and commercial applications, yet its adoption raises pressing ethical, legal, and organizational concerns. Numerous studies have documented significant racial and gender biases in algorithmic performance, resulting in disproportionate misidentifications of minority groups and undermining public trust in technology-driven security solutions. Beyond technical shortcomings, the misuse of reverse image search applications, such as the use of PimEyes and or TinEye to dox immigration officers, has exacerbated the risks by weaponizing digital tools in ways that amplify existing societal tensions. This paper critically examines how the intersection of algorithmic bias and misuse of search technologies creates a compounded civil rights crisis, threatening constitutional protections, organizational legitimacy, and consumer trust. Drawing on recent policy reports, case studies, and scholarly literature, the study argues for a multi-stakeholder corrective framework emphasizing bias audits, inclusive dataset design, stronger regulatory oversight, and organizational accountability. By addressing these systemic deficiencies, stakeholders can simultaneously improve the accuracy of FRT, safeguard civil liberties, and foster inclusive innovation that builds sustainable trust in emerging technologies.

Keywords: Facial Recognition Technology, Algorithmic Bias, Reverse Image Search, Ethical Concerns, Legal Risks, Organizational Accountability, Civil Rights, Consumer Trust, Inclusive Innovation

1. Introduction

A review of contemporary studies reveals that facial recognition technology (FRT) has expanded from a limited security application into a global infrastructure for surveillance, commerce, and identification. Governments, corporations, and private actors now rely on algorithmic systems marketed as efficient, precise, and fast for identity verification (Garvie, 2019; Raji & Buolamwini, 2019; U.S. Commission on Civil Rights [USCCR], 2024). However, growing evidence demonstrates that these systems are far from neutral. Studies consistently show higher error rates for women, younger people, and racial minorities, raising profound concerns about fairness, due process, and equal protection (Buolamwini & Gebru, 2018; Koenecke et al., 2020). The USCCR (2024) concluded that such disparities undermine constitutional safeguards and widen civil rights gaps. These flaws should not be dismissed as mere technical anomalies but understood as systemic risks that challenge the legitimacy of institutions deploying FRT without accountability (Crawford, 2021; Whittaker et al., 2018).

The stakes became even higher in 2025, when FRT intersected with reverse image search applications in ways that magnified harm. While tools like Google Images, Pimeyes, and TinEye were initially designed for benign purposes such as copyright protection or verifying image authenticity, their capabilities have expanded into unregulated domains with damaging outcomes (FaceOnLive, 2025; Kosinski, 2021; Niederer & Colombo, 2024; Whittaker et al., 2018). A high-profile case involved activists leveraging PimEyes and TinEye to unmask and dox U.S. Immigration and Customs Enforcement (ICE) officers, releasing personal details that endangered officers and their families (Ng, 2025; U.S. Department of Homeland Security [USDHS], 2025). Scholars warn that this weaponization of reverse image search tools reflects a broader trend of function creep, where technologies migrate beyond intended contexts to enable surveillance and harassment (Brayne, 2020; Niederer & Colombo, 2024). When compounded with algorithmic disparities in FRT, such misuse creates a dual crisis: technical inequities combine with ethical misconduct, multiplying risks for vulnerable populations and eroding democratic governance.

These intertwined challenges carry urgent implications for organizations across both public and private sectors. For law enforcement and immigration authorities, biased or misused FRT threatens to erode the legitimacy of legal processes, expose agencies to litigation, and compromise officer safety (Garvie, 2019; Ng, 2025; USCCR, 2024). In commercial contexts, organizations using FRT in retail, financial services, or customer engagement face reputational damage, consumer backlash, and potential regulatory sanctions (Crawford, 2021; Selbst & Barocas, 2021). At the societal level, failures in governance entrench systemic discrimination while enabling opportunistic actors to exploit technological loopholes for vigilante justice (Benjamin, 2019; Niederer & Colombo, 2024). Thus, the debate over FRT extends well beyond accuracy into broader questions of ethics, organizational responsibility, and legal oversight.

This paper critically examines the compounded risks of bias in FRT and the misuse of reverse image search applications, with a focus on their ethical, legal, and organizational implications. Drawing on recent civil rights reports, case studies, and scholarly literature, the study argues that corrective measures must be embedded in a multi-stakeholder framework. Such a framework requires technical reforms such as bias audits and inclusive dataset design paired with organizational transparency and regulatory safeguards to ensure alignment with principles of fairness and accountability (Barocas et al., 2023; USCCR, 2024; Whittaker et al., 2018). The sections that review recent developments in algorithmic bias and civil rights debates analyze the implications of PimEyes and TinEye's misuse, and propose corrective strategies aimed at improving FRT accuracy, rebuilding public trust, and fostering inclusive innovation.

2. Review of recent developments

2.1. Bias in Facial Recognition Technology

Recent evaluations by the National Institute of Standards and Technology (NIST, 2025) confirm that racial and gender disparities in FRT accuracy remain persistent despite industry claims of progress. In large-scale testing of over 100 algorithms, NIST reported significantly higher false positive rates for Black and Asian individuals compared to white counterparts, with error gaps widening in one-to-many identification scenarios (Grother et al., 2019). These findings are consistent with more recent academic studies that emphasize how algorithmic inequities are deeply embedded in training datasets that overrepresent lighter-skinned faces (Mitchell et al., 2019; Raji et al., 2022). The persistence of these biases demonstrates that technical advancement alone has not addressed the structural roots of discrimination in algorithmic performance.

The risks are magnified when biased systems are deployed in high-stakes environments such as policing, border control, and immigration. Inaccurate identifications have already resulted in wrongful arrests in U.S. cities, raising public awareness of the harms associated with algorithmic over-reliance (American Civil Liberties Union [ACLU], 2024; Hobson et al., 2023; Raji et al., 2022; USCCR, 2024). Scholars warn that such outcomes are not aberrations but predictable consequences of skewed training practices and insufficient external auditing (Dordunoo, 2024; Raji & Buolamwini, 2019; Richardson et al., 2019). European Parliament adds that bias audits are not just technical safeguards but political tools that determine whether organizations meaningfully confront accountability or merely perform it symbolically (European Parliament, 2024). These failures highlight the inadequacy of vendor-driven self-regulation, as companies continue to prioritize rapid deployment over fairness verification, thereby normalizing discriminatory errors as acceptable trade-offs for efficiency.

Policy and advocacy groups increasingly describe this dynamic as a form of bias laundering, in which systemic inequities are concealed under the guise of algorithmic neutrality. Reports from the Algorithmic Justice League and other watchdog organizations argue that voluntary compliance frameworks are inadequate, calling instead for mandatory bias audits, legally enforceable performance benchmarks, and inclusive dataset requirements (Ajunwa, 2023; Raji et al., 2022). Without corrective oversight, FRT risks institutionalizing inequities under the appearance of objectivity, legitimizing discriminatory outcomes in legal, commercial, and governmental decision-making. These insights underscore the need for proactive reforms that address not just technical shortcomings but also the broader organizational and societal structures that reproduce algorithmic bias.

2.2 Legal and Civil Rights Implications

The legal implications of FRT have intensified as courts, policymakers, and advocacy groups grapple with its conflicts with constitutional protections. In the United States, *Woodruff v. Detroit* (ACLU, 2024) stands as a landmark case, illustrating how misidentifications can directly lead to wrongful arrests and prolonged detentions. Civil liberties advocates argue that such cases highlight violations of the Fourth Amendment's protection against unreasonable searches and seizures, as well as Fourteenth Amendment guarantees of equal protection (ACLU, 2024). At the federal level, the USCCR (2024) concluded that FRT's disproportionate errors against racial minorities raise systemic constitutional concerns, while state legislatures have enacted moratoria restricting police use of FRT (Friedman et al., 2023; Patel, 2023; Yates, 2021). Scholars note that this patchwork approach underscores the urgent need for consistent federal legislation to close gaps in civil rights protections (Citron, 2022; USCCR, 2024).

Globally, similar debates emphasize the tension between technological innovation and privacy rights under international law. The European Union's forthcoming Artificial Intelligence Act designates FRT as a high-risk technology, requiring rigorous oversight, human review, and proportionality assessments for its deployment in public spaces (European Parliament, 2024). Legal analysts interpret this designation as a shift toward embedding fundamental rights protections into algorithmic governance, though critics warn that broad exemptions for border control and national security undermine its intended safeguards (Gstrein et al., 2024). Almeida et al. (2022) and Sekalala et al. (2020) argue that such loopholes weaken international human rights protections by allowing biometric surveillance to persist in precisely the contexts where the harms are most acute. In Canada, the Office of the Privacy Commissioner (OPC, 2021) has investigated local police forces for unauthorized use of FRT, arguing that existing privacy laws lack sufficient clarity for biometric surveillance. Australia's Human Rights Commission (AHRC, 2021) has similarly called for comprehensive biometric regulation, citing risks of discrimination and

disproportionate surveillance. These developments suggest that while momentum is building toward stronger governance, uneven implementation leaves many populations vulnerable.

The reliance on fragmented or voluntary regulatory standards creates significant risks for both individuals and organizations. Absent comprehensive legal frameworks, municipalities, corporations, and federal agencies remain exposed to lawsuits, regulatory penalties, and public backlash when harm occurs. Recent study warns that piecemeal oversight effectively privatizes civil rights protections, forcing individuals to rely on litigation rather than proactive safeguards (Citron, 2022; Matulionyte & Zalnieriute, 2024). At the same time, multinational organizations face compliance uncertainty as they navigate inconsistent rules across jurisdictions, which increases costs and legal liability (Stahl et al., 2023). These insights highlight that ensuring civil rights in the age of FRT requires harmonized, enforceable standards that extend beyond reactive remedies. Only through binding regulations that prioritize transparency, accountability, and individual rights can legal frameworks effectively mitigate the risks of algorithmic surveillance and protect democratic governance.

2.3 Case Study: Pimeyes/TinEye and the Doxxing of Immigration Officers

The events of 2025, in which activists leveraged Pimeyes, TinEye and other reverse image search tools to unmask U.S. Immigration and Customs Enforcement (ICE) officers, illustrate how non-biometric technologies can create civil rights and security crises. Investigative reporting revealed that publicly available photographs were cross-referenced with reverse image databases, generating matches that exposed the names, workplaces, and in some cases, family connections of federal officers (Ng, 2025). The USDHS (2025) condemned the campaign as a severe threat to officer safety, while the DHS Press Office reported a surge in harassment and threats targeting its members (USDHS, 2025). Legal commentators noted that this form of doxxing blurred the line between political activism and digital harassment, raising unresolved questions about the liability of platforms that enable such activity (Citron, 2022; Gillespie, 2010). The case demonstrates how technologies designed initially for benign purposes can be weaponized in ways that destabilize institutional legitimacy and compromise individual safety.

Scholars characterize this incident as a prominent example of function creep, where tools created for narrow applications migrate into politically charged domains with unanticipated consequences. While biometric FRT systems have received considerable scrutiny from regulators and civil liberties advocates, reverse image search technologies such as PimEyes and TinEye continue to operate in regulatory blind spots (FaceOnLive, 2025; Ng, 2025). This lack of oversight enables adversarial uses that extend far beyond copyright enforcement or image verification, allowing activists, hackers, and other groups to repurpose the technology for surveillance and intimidation. The ICE case illustrates how the harms associated with reverse image tools are not hypothetical but immediate and tangible, particularly when combined with widespread frustration over opaque immigration enforcement practices. Without clear governance frameworks, reverse image platforms risk becoming normalized tools of digital vigilantism, eroding both civil liberties and public trust. Noble (2018) reminds us that such technologies, when left unregulated, often reproduce and magnify existing social hierarchies of oppression, particularly when weaponized in politically charged settings.

The broader implications of the PimEyes doxxing incident highlight how adjacent technologies can exacerbate existing controversies surrounding FRT and digital surveillance. Scholars of online governance warn that such episodes accelerate a culture of digital vigilantism, where individuals and groups take justice into their own hands by exploiting technological loopholes (Loveluck, 2020; Trottier, 2017). The overlap of biased

FRT with unregulated reverse image tools creates a compounded crisis: marginalized populations remain vulnerable to algorithmic misidentification, while government employees and private citizens alike face risks of exposure and harassment. Regulators and policymakers must therefore consider not only biometric technologies but also ancillary tools that amplify surveillance harms when left unchecked (AHRC, 2021; OPC, 2021). This case underscores the urgent need for comprehensive oversight frameworks that address both biometric and non-biometric tools, ensuring that innovation does not come at the expense of civil rights or democratic resilience.

2.4 Organizational Responsibility and Public Trust

Organizations that deploy FRT are increasingly evaluated not only by technical accuracy but also their governance practices and capacity to maintain public trust. Surveys show that consumers are more skeptical of companies that adopt biometric systems without transparency, particularly among younger populations who express heightened concern about digital privacy and fairness (Kostka, 2023; Niederer & Colombo, 2024; Rainie et al., 2022). Law enforcement agencies, meanwhile, have faced legitimacy crises after wrongful arrests tied to FRT errors, which intensified perceptions of racial bias and lack of accountability in policing (Schwartz, 2020). Scholars argue that organizational responsibility in FRT governance is a key determinant of legitimacy, requiring firms and agencies to integrate fairness and accountability into decision-making processes rather than treating them as compliance afterthoughts (Dordunoo, 2024; Stahl et al., 2023; Veale & Binns, 2017).

The risks of neglecting governance extend beyond reputational harm to legal and financial consequences. In the United States, state-level biometric privacy laws such as Illinois' Biometric Information Privacy Act (BIPA) have already led to multimillion-dollar settlements against firms that failed to safeguard biometric data adequately (ACLU, 2024; Sarabdeen, 2022; Wang et al., 2024). In Europe, the forthcoming Artificial Intelligence Act places heightened obligations on organizations using high-risk technologies like FRT, including record-keeping, bias testing, and external auditing, with penalties for noncompliance reaching up to 7% of global turnover (European Parliament, 2024). Scholars note that these measures reflect a broader trend of shifting accountability from consumers to corporations, demonstrating that voluntary codes of conduct are increasingly insufficient in protecting public trust (Matulionyte & Zalnieriute, 2024). Organizations that fail to anticipate these legal shifts risk not only regulatory sanctions but also long-term erosion of their social license to operate.

Conversely, organizations that adopt proactive governance strategies can transform responsibility into a competitive advantage. Recent studies show that firms that disclose audit results, implement algorithmic impact assessments, and engage with external stakeholders are more likely to retain consumer confidence and strengthen relationships with regulators (Oduro et al., 2022). Public-sector agencies that establish oversight boards and engage communities in FRT deployment decisions have also reported higher levels of cooperation and trust from citizens (AHRC, 2021; OPC, 2021). These findings suggest that trust should be treated not merely as a reputational byproduct but as a strategic resource that underpins organizational resilience in an era of contested technology. By embedding accountability, inclusivity, and transparency into their governance frameworks, organizations can mitigate risks while fostering more sustainable innovation in biometric technologies.

3. Problem Statement and Solution Approach

3.1 *The Compounded Problem*

The compounded problem of FRT begins with its persistent algorithmic inequities, which multiple independent audits and governmental evaluations have confirmed. A 2025 NIST report found that false positive rates for Black and Asian individuals remain significantly higher than for their white counterparts, particularly in one-to-many identification scenarios. Complementary academic research shows that these disparities persist even when models are trained on larger datasets, suggesting structural flaws in how training data is collected and classified (Mitchell et al., 2019; Raji et al., 2022). Real-world harms include wrongful arrests, employment discrimination, and travel disruptions, illustrating how bias in FRT extends beyond technical error into systemic violations of civil rights (ACLU, 2024; USSCCR, 2024). Left unaddressed, these inequities risk becoming institutionalized in law enforcement and immigration systems, where algorithmic results are often presented as authoritative evidence.

The misuse of adjacent technologies, such as reverse image search platforms, has compounded this foundational bias. In 2025, activists used PimEyes to unmask U.S. Immigration and Customs Enforcement (ICE) officers, cross-referencing professional and personal photographs to reveal names, workplaces, and even family associations (Ng, 2025). While some advocates framed the campaign as digital transparency aimed at exposing government overreach, federal agencies and officer unions condemned it as doxxing that endangered employees and their households (USDHS, 2025). Scholars describe this development as an example of digital vigilantism, where technology enables actors outside formal institutions to exact justice in ways that blur the boundaries between political protest and targeted harassment (Loveluck, 2020; Trottier, 2017). The PimEyes case demonstrates how non-biometric technologies can be repurposed into surveillance tools, magnifying tensions between state actors and civil society.

The convergence of biased FRT systems and weaponized reverse image tools thus represents a dual crisis for democratic governance. On one level, algorithmic disparity continues to burden marginalized populations by embedding discriminatory outcomes into policing, immigration control, and consumer services. On another, the ability to weaponize publicly available tools for doxxing demonstrates that risks extend beyond state misuse to include civil society actors and adversarial groups (Citron, 2022; Gillespie, 2010). Together, these dynamics destabilize institutional legitimacy, fuel public distrust in technology, and intensify calls for systemic oversight. Ng (2025) notes that such risks are exacerbated by governance gaps, as fragmented oversight regimes leave compounded harms like FRT bias and reverse image misuse largely unaddressed. Without coordinated reforms across technical, legal, and organizational domains, FRT will continue to serve as a mechanism for amplifying inequities while simultaneously enabling new forms of technological vigilantism. This compounded problem underscores the urgency of developing multi-stakeholder solutions that embed accountability, fairness, and civil rights protections at the core of innovation.

3.2 *Framework for Analysis*

A comprehensive framework for addressing the compounded risks of FRT must begin with ethical principles that foreground fairness, inclusivity, and accountability. Scholars argue that bias in FRT should not be seen as a purely technical defect but as a justice issue tied to historical inequities in representation (Gentzel, 2021; Raji & Buolamwini, 2019). Recent study calls for mandatory algorithmic audits and subgroup performance disclosures to ensure that disparate impacts are not hidden by aggregate accuracy claims (Dordunoo,

2026; Mitchell et al., 2019; Raji et al., 2022). Ethical frameworks also highlight the importance of participatory governance, where impacted communities play an active role in shaping training data and evaluation criteria rather than being passive subjects of surveillance (Ajunwa, 2023). These perspectives demonstrate that embedding ethical commitments into system design is essential to prevent FRT from reinforcing the very inequities it purports to solve.

From a legal perspective, the framework must account for rapidly evolving domestic and international regulatory regimes. In the United States, cases such as *Woodruff v. Detroit* (ACLU, 2024) and state-level moratoria reflect constitutional tensions around Fourth Amendment protections and Fourteenth Amendment equal protection guarantees (ACLU, 2024; Matulionyte & Zalnieriute, 2024). Internationally, the European Union's Artificial Intelligence Act (European Parliament, 2024) requires human oversight and impact assessments for high-risk applications, while legal scholars warn that exemptions for border control may undermine its effectiveness (Gstrein et al., 2024). AHRC (2021) and OPC (2021) have issued similar calls for comprehensive biometric regulation. Collectively, these developments illustrate the growing recognition that fragmented, voluntary standards are insufficient and that binding legal frameworks are essential to safeguarding fundamental rights in the age of biometric surveillance.

Organizational responsibility forms the third pillar of this framework, emphasizing how companies and agencies can embed accountability beyond baseline compliance. Research shows that organizations that publish algorithmic impact assessments and engage in external audits build stronger consumer trust and regulatory goodwill (Oduro et al., 2022; Stahl et al., 2023). Corporate governance scholars argue that effective accountability requires embedding AI ethics into decision-making processes, workforce training, and procurement standards, rather than relegating them to public relations efforts (Bietti, 2020). Mucci and Stryker (2024) extend their view by emphasizing that accountability must also confront power asymmetries in AI governance, ensuring organizations cannot sidestep responsibility through superficial ethics programs. Public agencies adopting oversight boards and mechanisms for citizen redress have reported improved legitimacy and cooperation (AHRC, 2021; OPC, 2021). These insights suggest that organizational responsibility should be viewed not just as risk mitigation but as a strategic resource that sustains legitimacy in contested technological environments. By uniting ethical, legal, and organizational safeguards, this framework creates a pathway for aligning innovation with democratic accountability.

4. Results and Discussion

4.1 Ethical Concerns

Ethical debates surrounding FRT focus on its tendency to reproduce structural inequities while presenting outcomes as objective and neutral. A growing body of research shows that skewed training datasets and unrepresentative benchmarks drive error disparities for women, youth, and racial minorities, raising profound concerns about fairness and justice (Mitchell et al., 2019; Raji et al., 2022). Reports from advocacy groups such as the Algorithmic Justice League confirm that these disparities persist across both commercial and law enforcement deployments, even when vendors advertise improvements (Ajunwa, 2023). Scholars argue that embedding discrimination in automated systems undermines democratic values by cloaking inequities in technical language (Eubanks, 2018). These insights suggest that unless fairness is designed into FRT from the outset, the technology will continue to reinforce historical biases rather than correct them.

Another ethical challenge arises from the lack of consent and transparency in FRT deployments across public and private domains. Studies show that individuals are often

unaware when their biometric data is being captured, whether in airports, workplaces, or commercial spaces, leaving them unable to opt out or challenge its use (Bietti, 2020; Wang et al., 2024). Civil liberties organizations argue that this covert surveillance violates principles of autonomy and self-determination, since biometric identifiers are immutable and cannot be revoked once compromised (OPC, 2021). The 2025 PimEyes case illustrates how reverse image search tools can be misused to expose personal identities without consent, creating risks of harassment and intimidation (Ng, 2025). Ethically, such practices represent a breakdown of trust in both institutions and technology providers, revealing how surveillance practices can erode fundamental human rights.

The compounded misuse of FRT and reverse image technologies also raises concerns about the normalization of surveillance and the emergence of digital vigilantism. Scholars caution that societies are drifting toward a surveillance culture, where individuals accept constant monitoring as inevitable despite its discriminatory consequences (Lyon, 2018). As Floridi (2023) argues, ethical frameworks for AI must move beyond abstract principles to address how technologies reshape social power and civil rights in practice. The PimEyes doxxing incident highlights how even non-biometric platforms can be weaponized to target individuals, amplifying harm for vulnerable populations while eroding trust in government institutions (Citron, 2022; Gillespie, 2010; Ng, 2025). Without proactive safeguards, these technologies risk legitimizing both state and non-state actors' misuse of personal data, creating new layers of ethical misconduct. As a result, scholars and policymakers argue for shifting from reactive crisis management to proactive governance, emphasizing fairness, transparency, and civil rights protections as ethical imperatives in biometric innovation (Stahl et al., 2023).

4.2 Legal Risks

Legal risks associated with FRT stem from its tension with constitutional protections, statutory privacy laws, and evolving civil rights frameworks. In the United States, cases such as *Woodruff v. Detroit* (ACLU, 2024) have exposed how biased FRT systems can result in wrongful arrests, triggering lawsuits that highlight potential violations of Fourth Amendment protections against unreasonable searches and seizures (ACLU, 2024). The USCCR (2024) similarly warned that disproportionate misidentifications of minority populations may constitute violations of the Fourteenth Amendment's equal protection clause. Recent state-level reforms, including restrictions in Delaware, for instance, illustrate how fragmented governance has created a patchwork of protection that complicates enforcement and compliance (Friedman et al., 2023; Jones, 2020; Yates, 2021). Scholars emphasize that these gaps expose municipalities and law enforcement agencies to costly litigation, as plaintiffs increasingly pursue remedies for algorithmic harms under civil rights law (Citron, 2022; Matulionyte & Zalnieriute, 2024).

Internationally, regulatory responses underscore both progress and ongoing challenges in balancing innovation with civil rights. The European Union's Artificial Intelligence Act, expected to take effect in 2026, designates FRT as a high-risk system and mandates rigorous compliance requirements, including human oversight and algorithmic transparency (European Parliament, 2024). However, scholars note that broad exemptions for national security and border control weaken the law's protective scope, potentially allowing disproportionate surveillance in sensitive contexts (Gstrein et al., 2024). In the Asia-Pacific region, Japan and South Korea have begun exploring data protection frameworks that address biometric risks, though critics argue these efforts remain preliminary and lack enforcement mechanisms (Matulionyte & Zalnieriute, 2024; Mercurio & Yu, 2022). Similarly, Canada's Privacy Commissioner (2021) has criticized local police for unauthorized FRT trials, urging Parliament to adopt explicit biometric legislation.

Together, these global debates show that despite growing consensus on the risks of FRT, regulatory responses remain uneven, leaving significant vulnerabilities in cross-border governance.

Beyond regulatory compliance, organizations face growing exposure to legal liability when FRT harms individuals or when privacy protections are inadequate. Consumer lawsuits under Illinois' BIPA have already resulted in multimillion-dollar settlements against major technology companies, demonstrating how statutory enforcement can carry steep financial penalties (Cook, 2024; McKnight, 2021; Sarabdeen, 2022; USCCR, 2024). The 2025 PimEyes incident further complicates liability, as courts and policymakers' debate whether reverse image search platforms should be held responsible for enabling digital harassment and doxxing (Ng, 2025; USDHS, 2025). Legal scholars argue that without clear statutory guidance, courts will continue to adjudicate these cases reactively, creating uncertainty for both victims and organizations (Bietti, 2020). This reactive model underscores the urgent need for comprehensive and harmonized legal frameworks that prevent harm before it occurs, balancing the benefits of technological innovation with the protection of civil rights.

4.3 Organizational and Business Impacts

The organizational and business risks associated with FRT begin with reputational exposure when inaccuracies and discriminatory outcomes are revealed. High-profile cases of wrongful arrests linked to FRT have been widely covered in mainstream media, eroding public trust not only in law enforcement but also in the companies that design and sell these systems (Skolnik, 2023; USCCR, 2024). Surveys indicate that consumers are particularly skeptical of firms deploying biometric tools without visible accountability measures, with trust deficits most pronounced among younger demographics and marginalized communities (Niederer & Colombo, 2024; Paik et al., 2022; Rainie et al., 2022). Scholars of corporate governance argue that reputational legitimacy is fragile in contexts of emerging technology, as one scandal can trigger cascading effects including boycotts, shareholder activism, and heightened regulatory scrutiny (Bietti, 2020; Stahl et al., 2023). For organizations across sectors, reputational harm remains one of the most immediate and costly risks of FRT misuse.

Financial and regulatory consequences compound these reputational risks, as organizations increasingly face lawsuits and compliance costs tied to FRT deployments. In the United States, enforcement of Illinois' BIPA has already resulted in multimillion-dollar settlements, setting a precedent for biometric litigation that is now being emulated in other jurisdictions (Citron, 2022; Sarabdeen, 2022; USCCR, 2024). In Europe, the Artificial Intelligence Act requires firms deploying high-risk systems such as FRT to undergo third-party conformity assessments and maintain detailed compliance documentation, creating significant operational costs (European Parliament, 2024; Matulionyte & Zalnieriute, 2024). Companies that fail to comply face penalties of up to 7% of annual global turnover, which for multinational firms can equate to billions in potential liability (European Parliament, 2024). Legal scholars note that this fragmented regulatory environment generates compliance uncertainty for organizations operating across borders, increasing both financial risk and administrative burden (Mercurio & Yu, 2022).

At a strategic level, organizations that mishandle FRT risk undermine their long-term competitiveness and innovation capacity. Research in business ethics shows that firms that adopt proactive accountability measures such as publishing algorithmic impact assessments, engaging independent auditors, and consulting civil society groups are better positioned to sustain consumer loyalty and regulatory goodwill (Oduro et al., 2022). Conversely, companies that frame compliance as box-ticking exercise often suffer from ethics washing, where superficial commitments fail to resolve underlying harms and deepen public distrust

(Bietti, 2021; Gillespie, 2010). Public agencies face parallel risks: failures in FRT deployment not only diminish institutional legitimacy but can also provoke public calls for the abolition of biometric surveillance, threatening the long-term viability of these tools (AHRC, 2021; OPC, 2021). Collectively, these findings underscore that organizational responsibility is not only a moral duty but also a strategic necessity, shaping whether firms and agencies can thrive in an environment of contested technological innovation.

4.4 Toward Corrective Action

Corrective action to address the compounded risks of FRT must begin with technical reforms that embed fairness, transparency, and inclusivity at the design stage. Scholars argue that vendor-led improvements are inadequate, since average accuracy metrics often obscure subgroup disparities (Mitchell et al., 2023; Raji et al., 2022). Mandatory bias audits and publicly available impact reports are increasingly recognized as essential to ensuring accountability (Ajunwa, 2023; Raji & Buolamwini, 2019; Raji et al., 2020). Equally important is diversifying training datasets to include underrepresented racial, gender, and age groups, which research has shown can significantly reduce misidentification rates (Mitchell et al., 2019; Raji & Buolamwini, 2019). Emerging approaches such as explainable AI (XAI) also hold promise by demystifying algorithmic decision-making processes and allowing external stakeholders to interrogate outcomes (Doshi-Velez & Kim, 2017). Together, these reforms provide a pathway for reducing technical inequities and increasing confidence in the reliability of FRT.

Organizational governance represents the second dimension of corrective action, requiring firms and agencies to embed accountability into institutional practice proactively. Studies show that organizations publishing transparency reports, commissioning independent audits, and engaging affected communities are better able to preserve legitimacy in contested technological environments (Bietti, 2020; Stahl et al., 2023). Corporate governance scholars caution that without embedding ethics into workforce training and procurement policies, commitments to fairness risk becoming shallow exercises in ethics washing (Bloch-Wehba, 2022; Gillespie, 2010). Public-sector reforms, including independent oversight boards and citizen redress mechanisms, have been shown to improve community trust and cooperation (AHRC, 2021; OPC, 2021). These measures underscore that organizational responsibility must extend beyond compliance checklists, evolving into long-term cultural commitments to ethical innovation.

At the policy level, corrective action requires harmonized legal frameworks that establish clear boundaries for biometric surveillance and related technologies. In the United States, advocacy groups continue to call for federal standards that build on state precedents like Illinois' BIPA but extend protections nationwide (ACLU, 2024; Citron, 2022). The European Union's Artificial Intelligence Act (2024) provides a model of high-risk classification and rigorous compliance obligations, though critics argue exemptions for border control may undermine its impact (Qiang & Jing, 2024). Policymakers must also address adjacent technologies such as reverse image search platforms, which currently operate in regulatory blind spots despite their role in enabling doxxing and digital harassment (FaceOnLive, 2025; Gillespie, 2010; Ng, 2025). By establishing comprehensive safeguards that integrate technical standards, organizational accountability, and legal protections, governments can prevent misuse while fostering innovation that is both trustworthy and inclusive.

5. Conclusion

The evidence reviewed in this paper demonstrates that FRT poses a compounded problem, where persistent algorithmic bias intersects with the misuse of reverse image search tools to

create layered harms. Despite claims of progress, independent evaluations confirm that misidentification rates for racial minorities, women, and younger populations remain disproportionately high, raising concerns about fairness and constitutional protections (Mitchell et al., 2019; NIST, 2025). The 2025 PimEyes doxxing incident further illustrates how non-biometric platforms can be weaponized to expose personal information, destabilize governance, and erode institutional trust (Ng, 2025). Scholars warn that these dynamics collectively normalize discrimination and digital vigilantism under the guise of technological neutrality (Loveluck, 2020; Trottier, 2017). Without systemic reforms, FRT will continue to function less as a tool for innovation and more as an instrument for amplifying inequities in democratic societies.

Addressing these challenges requires a multi-dimensional corrective framework that integrates technical, organizational, and legal safeguards. Technical reforms such as bias audits, inclusive dataset design, and explainable AI are essential to ensuring algorithmic transparency and fairness (Doshi-Velez & Kim, 2017; Raji et al., 2022). Organizational reforms, including external audits, transparency reporting, and human rights impact assessments, are critical for rebuilding consumer trust and protecting institutional legitimacy (Bietti, 2020; Stahl et al., 2023). At the policy level, binding legal frameworks such as the European Union's Artificial Intelligence Act and proposed U.S. federal standards offer models for harmonized governance but must be strengthened to close loopholes that enable overreach or adjacent misuse (Citron, 2022; European Parliament, 2024). Together, these reforms demonstrate that accountability must be shared across stakeholders to ensure that technological development aligns with democratic values.

Ultimately, the trajectory of FRT will be determined not solely by technological advances but by society's ability to align innovation with civil rights and ethical responsibility. Without corrective measures, FRT risks entrenching systemic inequities and legitimizing surveillance cultures that undermine democratic governance (Ajunwa, 2023; Eubanks, 2018). Conversely, when stakeholders embed accountability, inclusivity, and transparency into system design and deployment, FRT can evolve into a technology that enhances security while upholding fairness and trust. This paper contributes to that ongoing debate by highlighting the compounded risks of algorithmic bias and misuse, while outlining corrective strategies to prevent further erosion of civil liberties. By adopting a multi-stakeholder framework that integrates ethical, legal, and organizational imperatives, policymakers, organizations, and civil society can transform FRT from a liability into a tool for inclusive innovation and democratic resilience.

References

- Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, 2(3), 377–387. <https://doi.org/10.1007/s43681-021-00077-w>
- Ajunwa, I. (2023). *The quantified worker: Law and technology in the modern workplace*. Cambridge University Press.
- American Civil Liberties Union (ACLU). (2024). *Facial recognition technology*. <https://www.aclu.org/>
- Australian Human Rights Commission (AHRC). (2021). *Human rights and technology final report*. <https://humanrights.gov.au/>
- Barocas, S., Hardt, M., & Narayanan, A. (2023). *Fairness and machine learning: Limitations and opportunities*. MIT Press.
- Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim code*. Polity.
- Bietti, E. (2020). From ethics washing to ethics bashing: A view on tech ethics from within moral philosophy. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 1(27), 210-219.
- Bietti, E. (2021). From Ethics Washing to Ethics Bashing: A Moral Philosophy View on Tech Ethics. *Journal of Social Computing*, 2(3), 266–283. <https://doi.org/10.23919/JSC.2021.0031>
- Bloch-Wehba, H. (2022). Algorithmic Governance from the Bottom Up. *BYU Law Review*, 48(1), 1-69.
- Brayne, S. (2020). *Predict and surveil: Data, discretion, and the future of policing*. Oxford University Press.

- Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, 81, 77–91.
- Citron, D. K. (2022). *The fight for privacy: Protecting dignity, identity, and love in the digital age*. W. W. Norton & Company.
- Cook, A. (2024). Illinois BIPA: A litigation nightmare for employers. *UIC Law Review*, 57(2), 1-25.
- Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.
- Dordunoo, L. (2024). Integrating organizational and social network theories to mitigate racial bias in facial recognition technology. In *Organizational Readiness and Research: Security, Management, and Decision Making* (pp. 283–348). IGI Global. <https://doi.org/10.4018/979-8-3693-8562-3.ch009>
- Dordunoo, L. (2026). Building Trust in Artificial Intelligence. In *Advancing Safety, Service, and Performance in Organizations With Impactful Leadership* (pp. 251-278). IGI Global Scientific Publishing. DOI: 10.4018/979-8-3373-5686-0.ch010
- Doshi-Velez, F., & Kim, B. (2017). *Toward a rigorous science of interpretable machine learning*. Nature Machine Intelligence. DOI: <https://doi.org/10.48550/arXiv.1702.08608>
- Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.
- European Parliament. (2019). *A governance framework for algorithmic accountability and transparency*. European Parliamentary Research Service.
- European Parliament. (2024). *Artificial Intelligence Act: Legislative proposal and updates*. <https://www.europarl.europa.eu/>
- FaceOnLive.com. (2025). *Legal issues around reverse image search you need to know*. <https://faceonlive.com/legal-issues-around-reverse-image-search-you-need-to-know/>
- Friedman, B., Harmon, R., & Heydari, F. (2023). The Federal Government's Role in Local Policing. *Virginia Law Review*, 109(8), 1527-1627.
- Floridi, L. (2023). *The ethics of artificial intelligence: Principles, challenges, and opportunities*. Oxford University Press.
- Garvie, C. (2019). *Garbage in, garbage out: Face recognition on flawed data*. Georgetown Law Center on Privacy & Technology.
- Gentzel M. (2021). Biased Face Recognition Technology Used by Government: A Problem for Liberal Democracy. *Philosophy & Technology*, 34(4), 1639–1663. <https://doi.org/10.1007/s13347-021-00478-z>
- Gillespie, T. (2010). The politics of 'platforms'. *New Media & Society*, 12(3), 347-364. <https://doi.org/10.1177/1461444809342738>
- Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. NIST. <https://doi.org/10.6028/NIST.IR.8280>
- Gstrein, O.J., Haleem, N., & Zwitter, A. (2024). General-purpose AI regulation and the European Union AI Act. *Internet Policy Review*, 13(3). <https://doi.org/10.14763/2024.3.1790>
- Hobson, Z., Yesberg, J. A., Bradford, B., & Jackson, J. (2023). Artificial fairness? Trust in algorithmic police decision-making. *Journal of Experimental Criminology*, 19(1), 165–189. <https://doi.org/10.1007/s11292-021-09484-9>
- Jones, C. (2020). Law enforcement use of facial recognition: bias, disparate impacts on people of color, and the need for federal legislation. *NCJL & Tech.*, 22, 777.
- Koenecke, A., Nam, A., Lake, E., Nudell, J., Quartey, M., Mengesha, Z., Toups, C., Rickford, J. R., Jurafsky, D., & Goel, S. (2020). Racial disparities in automated speech recognition. *Proceedings of the National Academy of Sciences of the United States of America*, 117(14), 7684–7689. <https://doi.org/10.1073/pnas.1915768117>
- Kosinski, M. (2021). *Facial recognition technology can expose political orientation from naturalistic facial images*. *Scientific Reports*, 11(1), 100. <https://doi.org/10.1038/s41598-020-79310-1>
- Kostka, G. (2023). Digital doubters in different political and cultural contexts: Comparing citizen attitudes across three major digital technologies. *Data & Policy*, 5, e27.
- Loveluck, B. (2020). The many shades of digital vigilantism. A typology of online self-justice. *Global Crime*, 21(3-4), 213-241.
- Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. John Wiley & Sons.
- Matulionyte, R., & Zalnieriute, M. (2024). *The Cambridge handbook of facial recognition in the modern state*. Cambridge University Press.
- McKnight, P. (2021). *Historic biometric privacy suit settles for \$650 million*. American Bar Association
- Mercurio, B., & Yu, R. (2022). *Regulating cross-border data flows: Issues, challenges and impact*. Anthem Press.
- Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., Spitzer, E., Raji, I. D., & Gebru, T. (2019). Model Cards for Model Reporting. In *FAT* '19: Conference on Fairness, Accountability, and Transparency*, January 29–31, 2019, Atlanta, GA, USA. ACM, New York, NY, USA, 10 pages. <https://doi.org/10.1145/3287560.3287596>

- Mucci, T., & Stryker, C. (2024). *What is AI governance*. <https://www.ibm.com/think/topics/ai-governance>
- National Institute of Standards and Technology (NIST). (2025). *Face recognition technology evaluation (FRTE): Verification performance*. <https://www.nist.gov/>
- Ng, A. (2025). *AI is unmasking ICE officers. Can Washington do anything about it?* <https://www.yahoo.com/news/articles/ai-ummasking-ice-officers-washington-180000957.html>
- Niederer, S., & Colombo, G. (2024). *Visual methods for digital research: An Introduction*. Polity Press
- Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.
- Oduro, S., Moss, E., & Metcalf, J. (2022). Obligations to assess: Recent trends in AI accountability regulations. *Patterns (New York, N.Y.)*, 3(11), 100608. <https://doi.org/10.1016/j.patter.2022.100608>
- Office of the Privacy Commissioner of Canada (OPC). (2021). *Police use of facial recognition technology in Canada and the way forward*. <https://www.priv.gc.ca/>
- Paik, S., Mays, K. K., & Katz, J. E. (2022). Invasive Yet Inevitable? Privacy Normalization Trends in Biometric Technology. *Social Media + Society*, 8(4). <https://doi.org/10.1177/20563051221129147>
- Patel, S. (2023). *Regulating Federal Law Enforcement's Use of Facial Recognition Technology*. Defense Technical Information Center.
- Qiang, R. E. N., & Jing, D. U. (2024). Harmonizing innovation and regulation: The EU Artificial Intelligence Act in the international trade context. *Computer Law & Security Review*, 54, 106028.
- Rainie, L., Funk, C., Anderson, M., & Tyson, A. (2022). *Public more likely to see facial recognition use by police as good, rather than bad for society*. <https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society/>
- Raji, I. D., & Buolamwini, J. (2019). Actionable auditing: Investigating the impact of publicly naming biased performance results of commercial AI products. *Conference on Artificial Intelligence, Ethics, and Society*, 429-435. DOI: 10.1145/3306618.3314244
- Raji, I. D., Kumar, I. E., Horowitz, A., & Selbst. A. D. (2022). *The fallacy of AI functionality*. <https://doi.org/10.1145/3531146.3533158>
- Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., Barnes, P., (2020). Closing the AI accountability gap: defining an end-to-end framework for internal algorithmic auditing. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 33 – 44. <https://doi.org/10.1145/3351095.337287>
- Raji, D. I., Xu, P., Honigsberg, C., Ho, D. (2022). Outsider oversight: Designing a third party audit ecosystem for AI governance. *AIES '22: Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society*. Pages 557 – 571. <https://doi.org/10.1145/3514094.3534181>
- Richardson, R., Schultz, J. M., & Crawford, K. (2019). *Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice*. AI Now Institute.
- Sarabdeen J. (2022). Protection of the rights of the individual when using facial recognition technology. *Heliyon*, 8(3), e09086. <https://doi.org/10.1016/j.heliyon.2022.e09086>
- Schwartz S. A. (2020). Police brutality and racism in America. *Explore (New York, N.Y.)*, 16(5), 280–282. <https://doi.org/10.1016/j.explore.2020.06.010>
- Sekalala, S., Dagon, S., Forman, L., & Meier, B. M. (2020). Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis. *Health and Human Rights*, 22(2), 7–20.
- Selbst, A. D., & Barocas, S. (2021). The intuitive appeal of explainable machines. *SSRN Electronic Journal*, 87(3). DOI: 10.2139/ssrn.3126971
- Skolnik, T. (2023). Policing, technology, and the erosion of constitutional rights. *Queen's LJ*, 49, 40.
- Stahl, B. C., Schroeder, D., & Rodrigues, R. (2023). *Ethics of artificial intelligence: Case studies and options for addressing ethical challenges*. Springer. <https://doi.org/10.1007/978-3-031-17040-9>
- Trottier, D. (2017). Digital vigilantism as weaponisation of visibility. *Philosophy & Technology*, 30(1), 55-72.
- Veale, M., & Binns, R. (2017). Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data. *Big Data & Society*, 4(2). <https://doi.org/10.1177/2053951717743530>
- United States Commission on Civil Rights (USCCR). (2024). *The civil rights implications of the federal use of facial recognition technology*. <https://www.usccr.gov/>
- United States Department of Homeland Security (USDHS). (2025). *Anarchists and rioters in Portland illegally dox ICE officers and federal law enforcement*. DHS Press Office.
- Wang, X., Wu, Y. C., Zhou, M., & Fu, H. (2024). Beyond surveillance: privacy, ethics, and regulations in face recognition technology. *Frontiers in Big Data*, 7, 1337465. <https://doi.org/10.3389/fdata.2024.1337465>
- Whittaker, M., Crawford, K., Dobbe, R., Fried, G., Kazianus, E., Mathur, V., West, S. M., Richardson, R., Schultz, J., & Schwartz, O. (2018). *AI Now Institute*. <https://ainowinstitute.org/>
- Yates, S. E. (2021). The digitalization of the carceral state: The troubling narrative around police usage of facial recognition technology. *Colo. Tech. LJ*, 19, 483.