Michael Voss
CST 300 GWAR
February 1, 2026

Regulating Mass Facial Recognition in Public Spaces

Introduction/Background

Facial recognition technology (FRT) matches facial features against reference databases, raising concerns about the use of sensitive personal data (Raposo, 2022). In public spaces, FRT can enable both real-time identification of individuals moving through monitored areas and retrospective searches of stored footage (Raposo, 2022). These capabilities create a policy dispute over whether governments should permit mass deployment for public-safety gains or restrict it to protect privacy and civil liberties (Raposo, 2022; Nissenbaum, 2004).

As surveillance infrastructure expanded, facial recognition was increasingly applied in public settings, which can enable automated identification beyond localized monitoring (Raposo, 2022). Law enforcement adopted FRT before legislatures established clear rules, resulting in a fragmented regulatory landscape (Robles et al., 2025). Compounding this governance gap, Buolamwini and Gebru (2018) documented substantial accuracy disparities in FRT performance across demographic groups, reporting error rates as high as 34.7% for darker-skinned females compared to 0.8% for lighter-skinned males. Broader evaluations by the National Institute of Standards and Technology similarly documented demographic performance differences across many tested algorithms (Grother et al., 2019).

Public-space FRT makes population-wide identification possible, and the retention of facial images raises concerns about downstream use (Raposo, 2022).

When these systems fail, the consequences can be severe. For example, in 2020, Robert Williams was wrongfully arrested after a false match and detained for thirty hours (American Civil Liberties Union [ACLU], 2024). However, the risks extend beyond isolated errors. Persistent identification can deter lawful participation when people expect that they can be identified and tracked in public (Raposo, 2022). It also undermines privacy because facial data collected in one context can later be reused to identify people in different, unrelated contexts (Nissenbaum, 2004).

Stakeholder Analysis

Given these competing risks and potential benefits, two principal groups stand on opposing sides. Law enforcement agencies and government security bodies seek to deploy FRT to reduce risk and improve investigative effectiveness (Johnson et al., 2024; Robles et al., 2025). Citizens and civil liberties organizations prioritize privacy, autonomy, and enforceable limits on biometric surveillance, arguing that routine mass identification poses unacceptable risks without strict safeguards (Raposo, 2022; Nissenbaum, 2004).

Stakeholder 1: Law Enforcement and Government Security Bodies

Values

Law enforcement stakeholders are guided by values of public safety, risk reduction, and investigative efficiency (Johnson et al., 2024). For these agencies, identifying suspects quickly is central to their public-safety mandate, and they view FRT as a tool that supports that mission. Effective identification directly affects outcomes in serious cases, making technological capability a central priority (Johnson et al., 2024).

Position on the Issue

Their position is that FRT should be permitted for investigative use under context-dependent limits rather than a blanket prohibition, with legitimacy depending on narrow scope and enforceable oversight (Ritchie et al., 2021; Johnson et al., 2024). Surveys indicate that public support varies by use case, with higher acceptance for serious-crime investigations than for broad public tracking (Ritchie et al., 2021). Limiting access could constrain investigative capacity in cases involving serious harm (Johnson et al., 2024).

Claims Supporting the Position

Research on police FRT adoption reports associations with reductions in serious violence, and proponents argue that improved identification can strengthen deterrence in targeted cases (Johnson et al., 2024). In defining acceptable use, they emphasize narrow investigative purposes, human verification, and clear limits on when and how the technology is applied (Ritchie et al., 2021). They also argue that public acceptance is higher when use is transparent and constrained to serious-crime contexts rather than broad monitoring (Ritchie et al., 2021). On this view, FRT is most defensible as a regulated investigative tool whose legitimacy depends on enforceable oversight and scope restrictions (Ritchie et al., 2021; Robles et al., 2025).

Stakeholder 2: Citizens and Civil Liberties Organizations

Values

Citizens and civil liberties groups are driven by values of privacy, autonomy, and protection from unchecked state power (Raposo, 2022; Nissenbaum, 2004). These organizations view biometric surveillance as requiring heightened scrutiny given the data's sensitivity and the difficulty of undoing collection (Raposo, 2022). Safeguarding

individuals from disproportionate state monitoring is central to their mission (Nissenbaum, 2004).

Position on the Issue

Their position is that public-space FRT should not be permitted as a default, and any allowed use must be narrowly limited with enforceable transparency and oversight (Raposo, 2022; Nissenbaum, 2004; Robles et al., 2025). Documented errors and disparities show the technology can impose concrete harms on misidentified individuals (Buolamwini & Gebru, 2018; ACLU, 2024). Without clear legal limits, deployment will expand beyond its stated purpose and normalize routine identification (Raposo, 2022).

Claims Supporting the Position

Error rates vary sharply across demographic groups, raising concerns about unequal error burdens (Buolamwini & Gebru, 2018; Grother et al., 2019). Civil liberties groups argue that persistent identification can discourage lawful speech and protest, so biometric data warrants heightened protection (Raposo, 2022; Nissenbaum, 2004). They contend that routine identification is not a justified tradeoff for administrative efficiency when surveillance constrains what people feel free to do in public (Nissenbaum, 2004). They frame mass identification as population-level monitoring requiring strict necessity rather than routine use (Raposo, 2022; Nissenbaum, 2004; Robles et al., 2025).

Argument Question

Should governments deploy facial recognition technology for mass surveillance in public spaces, or should it be restricted or prohibited to protect privacy, autonomy, and civil liberties?

Stakeholder Argument

Stakeholder 1

Utilitarianism

Utilitarianism, associated with Bentham and Mill, evaluates actions and policies based on whether they maximize overall well-being and minimize harm, treating consequences as the central moral standard (Sinnott-Armstrong, 2020). An action is morally right if it produces more overall good, and less overall harm, than any other available option (Sinnott-Armstrong, 2020). The framework therefore seeks the course of action that generates the greatest total benefit for everyone affected.

Application to Surveillance

Applied to public-space FRT, law enforcement argues that the technology can increase overall social benefit by reducing serious harm in specific investigative contexts (Johnson et al., 2024). However, a utilitarian analysis must also consider the costs of misidentifications, demographic accuracy disparities, and reduced public trust, all of which can outweigh benefits when deployment becomes widespread (Buolamwini & Gebru, 2018; Grother et al., 2019; Raposo, 2022). Safeguards such as human review and enforceable oversight can limit these harms while preserving potential benefits, making narrowly restricted use more likely to produce the greatest overall good (Grother et al., 2019; Robles et al., 2025).

Course of Action

Utilitarianism supports permitting FRT under enforceable safeguards rather than adopting a blanket prohibition, because some regulated contexts can produce greater overall benefits when properly governed and audited (Johnson et al., 2024; Robles et

al., 2025; Ritchie et al., 2021). Regulated deployment is therefore the policy most likely to increase overall well-being while limiting preventable harm. A blanket ban would eliminate potential benefits without meaningfully reducing harms that safeguards are designed to address.

Gains and Losses

The potential gain is reduced serious harm through improved investigative efficiency under regulated use (Johnson et al., 2024). The loss is reduced access to a tool law enforcement considers valuable in high-stakes investigations (Ritchie et al., 2021). From a utilitarian perspective, the overall benefits of regulated access outweigh the costs of restricting the technology entirely.

Stakeholder 2

Rights-Based Ethics

Rights-based ethics argues that basic individual rights limit what the state may do, even when officials claim their actions would benefit society overall (Wenar, 2021). Nissenbaum's theory of contextual integrity adds that privacy depends on whether personal information is used in ways people reasonably expect in that social setting (Nissenbaum, 2004). Together, these views maintain that some state actions are morally wrong when they violate individual rights, even if they are said to promote broader social benefits (Wenar, 2021; Nissenbaum, 2004).

Application to Surveillance

Public-space FRT violates privacy when facial data collected in one context is later reused for identification without clear legal limits (Nissenbaum, 2004; Raposo, 2022). From a rights-based perspective, broad public identification raises rights

concerns because potential safety benefits are not considered sufficient to justify routine surveillance by default (Wenar, 2021; Raposo, 2022). Uneven accuracy and documented wrongful arrests further show that misidentification can result in serious harms to individual liberty (Buolamwini & Gebru, 2018; Grother et al., 2019; ACLU, 2024).

Course of Action

This framework supports prohibiting real-time public-space scanning as the default, permitting identification only for narrow, legally authorized uses with necessity and proportionality safeguards (Raposo, 2022; Robles et al., 2025; Nissenbaum, 2004). Without such limits, deployment will normalize beyond its original justification (Raposo, 2022). A default prohibition preserves the rights that routine identification would erode.

Gains and Losses

The gain is stronger protection of privacy, autonomy, and civil liberties, with fewer instances of facial data being reused across different contexts (Raposo, 2022; Nissenbaum, 2004). The loss is reduced investigative effectiveness, although proponents argue that this limitation does not justify routine mass identification (Johnson et al., 2024; Ritchie et al., 2021). From this perspective, protecting individual rights is more important than the additional benefits claimed for broad deployment.

Student Position

After examining both positions, I believe the default should be a prohibition on mass public-space FRT. Population-wide identification combined with documented accuracy disparities creates risks outweighing the benefits of routine deployment. However, a complete prohibition would be difficult to justify given evidence that FRT can

aid safety in targeted cases. I support banning real-time scanning while permitting rare, retrospective identification for serious investigations subject to judicial authorization, human verification, and independent auditing (Raposo, 2022; Nissenbaum, 2004; Grother et al., 2019; Robles et al., 2025).

Alignment and Justification

My position aligns most closely with Stakeholder 2, because mass identification creates disproportionate risks to rights given documented disparities (Buolamwini & Gebru, 2018; Grother et al., 2019; ACLU, 2024). The narrow retrospective exception acknowledges investigative value without accepting mass deployment risks (Johnson et al., 2024; Ritchie et al., 2021). This balance preserves core protections that routine surveillance would undermine while leaving room for targeted, accountable use.

Recommendation

The most defensible policy bans real-time scanning while permitting tightly defined retrospective use for serious crimes with warrants, human verification, and mandatory audits (Raposo, 2022; Grother et al., 2019; Robles et al., 2025). Under this approach, mass identification is not the default practice but a rare and narrowly authorized measure, supported by transparency safeguards that prevent gradual expansion. By anchoring policy in enforceable limits rather than technological capability, this approach keeps identification accountable to the rights it affects.

References

American Civil Liberties Union. (2024). *Williams v. City of Detroit: Face recognition false arrest*. https://www.aclu.org/cases/williams-v-city-of-detroit-face-recognition-false-arrest

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research, 81*, 77–91. http://proceedings.mlr.press/v81/buolamwini18a.html

Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face recognition vendor test (FRVT) Part 3: Demographic effects* (NISTIR 8280). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280

Johnson, T. L., Johnson, N. N., Topalli, V., McCurdy, D., & Wallace, A. (2024). Police facial recognition applications and violent crime control in U.S. cities. *Cities*, *155*, 105472. https://doi.org/10.1016/j.cities.2024.105472

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119–157. https://nissenbaum.tech.cornell.edu/papers/H.%20Nissenbaum%2C%20_Privacy%20as%20Contextual%20Integrity.pdf

Raposo, V. L. (2022). The use of facial recognition technology by law enforcement in Europe: A non-Orwellian draft proposal. *European Journal on Criminal Policy and Research, 29(4)*, 515–533. https://pmc.ncbi.nlm.nih.gov/articles/PMC9156832/

Ritchie, K. L., Cartledge, C., Growns, B., Yan, A., Wang, Y., Guo, K., Kramer, R. S. S., Edmond, G., Martire, K. A., San Roque, M., & White, D. (2021). Public attitudes towards the use of automatic facial recognition technology in criminal justice

systems around the world. *PLOS ONE*, *16*(10), e0258241. https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0258241

Robles, P., Mallinson, D. J., Best, E., Devaney, C., & Azevedo, L. (2025). Global perspectives on regulating facial recognition technology utilization for criminal justice arrests. *Global Public Policy and Governance*, *5*, 186–204. https://doi.org/10.1007/s43508-025-00117-9

Sinnott-Armstrong, W. (2020). Consequentialism. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Spring 2020 ed.). Stanford University. https://plato.stanford.edu/archives/spr2020/entries/consequentialism/

Wenar, L. (2021). Rights. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Spring 2021 ed.). Stanford University. https://plato.stanford.edu/archives/spr2021/entries/rights/