

The Ethical Implications of Facial Recognition Technology in Public Surveillance

Format: Analytical/Argumentative | Level: IB Extended Essay | ~1,000 words

The deployment of facial recognition technology in public spaces has outpaced the legal frameworks designed to govern it. In 2019, the Metropolitan Police Service in London expanded its live facial recognition program to public events, with an accuracy rate later reported as approximately 81 percent, meaning roughly one in five identifications produced a false match. Under the proportionality principle established in Article 8 of the European Convention on Human Rights, a surveillance measure is only justifiable if its benefits are proportionate to the privacy cost it imposes. An 81 percent accuracy rate applied to a crowd of ten thousand people generates approximately two thousand false identifications per event, a number that fails the proportionality test regardless of whether the underlying law permits the deployment.

Research Question

Does the deployment of live facial recognition technology in public surveillance contexts meet the proportionality standard required under Article 8 of the European Convention on Human Rights, evaluated through case studies in the United Kingdom, China, and the United States?

The Proportionality Framework

Article 8 of the European Convention on Human Rights guarantees the right to respect for private and family life, with permitted interference only when it is in accordance with law, necessary in a democratic society, and proportionate to the legitimate aim pursued. The proportionality test requires that the measure be no more invasive than necessary to achieve its stated purpose, and that the benefits to the public interest be weighed against the costs to individual rights. This framework was developed before the digital age but has been applied by European courts to surveillance technology, most notably in the 2017 European Court of Human Rights judgment in *Barbulescu v. Romania*, which established that digital monitoring of communications must satisfy proportionality requirements.

Case Study 1: United Kingdom

The UK's deployment of live facial recognition by the Metropolitan Police has been evaluated by the Information Commissioner's Office, which issued a formal warning in 2019 noting insufficient evidence of proportionality. The stated purpose of the technology is the identification of individuals on a police watchlist in public spaces. The accuracy rate of 81 percent means that for every genuine identification, the system generates approximately four false positives among members of the public

who have no connection to any watchlist. Independent researchers at the University of Essex evaluated a separate deployment and found zero accurate identifications from 35 alerts generated, all of which were false matches. A measure that fails to achieve its stated purpose at all cannot satisfy the proportionality test.

Case Study 2: China

China operates the world's most extensive public facial recognition network, deployed for purposes including traffic enforcement, subway fare collection, and the monitoring of ethnic minority populations in Xinjiang province. The proportionality framework applied in the European context is not formally applicable in China, but international human rights standards provide a comparable evaluative basis. The documented use of facial recognition as a component of a broader surveillance system targeting Uyghurs on the basis of ethnicity represents a categorical failure of proportionality under any human rights framework: the technology is being used not to identify individuals suspected of specific offenses but to monitor an entire ethnic group as a class.

Case Study 3: United States

The United States has no federal regulatory framework governing facial recognition in public spaces. Municipal bans exist in San Francisco, Boston, and approximately two dozen other cities, but the technology is deployed without restriction in the majority of US jurisdictions. A 2019 study by the National Institute of Standards and Technology found that the most widely used facial recognition algorithms produced significantly higher false positive rates for darker-skinned individuals, particularly women, compared to lighter-skinned individuals. The differential accuracy rates mean that the technology imposes disproportionately higher costs on already-marginalized communities, compounding existing inequities in policing rather than providing a neutral surveillance tool.

Conclusion

Across all three case studies, the deployment of live facial recognition technology in public surveillance contexts fails to satisfy the proportionality standard when evaluated against documented accuracy rates, patterns of use, and impact on affected populations. In the UK, the technology has not demonstrated effectiveness sufficient to justify its privacy costs. In China, it is deployed for population monitoring rather than specific criminal identification. In the US, its differential accuracy rates impose disproportionate burdens on minority communities. The ethical case against unrestricted public deployment of facial recognition is not that the technology is inherently impermissible, but that no deployment evaluated in this research has demonstrated benefits proportionate to the costs it imposes. Regulatory frameworks that impose mandatory accuracy thresholds, independent oversight, and demographic impact assessments as prerequisites for deployment are the minimum necessary conditions for proportionate use.

