Sharon Azarya*

Facial Recognition Technology: Navigating Privacy Rights and Regulatory Challenges

1. Introduction

Facial recognition technology has rapidly evolved from a futuristic concept to an everyday reality, permeating both public and private sectors across the globe. While proponents highlight its potential to enhance security and streamline services, critics warn of unprecedented threats to privacy, human rights, and social equity. The International Working Group on Data Protection in Technology, commonly known as the Berlin Group, has produced a comprehensive working paper that examines these competing concerns and proposes a framework for responsible governance of this transformative technology.[1]

This article analyzes the Berlin Group's findings on facial recognition technology, exploring its technical attributes, diverse applications, inherent risks, and the regulatory approaches necessary to safeguard fundamental rights.

2. Understanding Facial Recognition Technology

Facial recognition technology operates by converting images or videos of human faces into mathematical templates that can be compared against databases of known individuals. The technology performs four basic functions: detection, verification, identification, and facial analysis.[2] Detection recognizes that a face exists in an image. Verification confirms whether a person matches a claimed identity through one-to-one matching. Identification compares an unknown face against a gallery of known individuals through one-to-many matching. Facial analysis attempts to infer characteristics from facial features, though the scientific validity of such inferences remains highly contested.

Most contemporary systems rely on machine learning algorithms trained on large datasets of facial images. As these algorithms process more training data, they theoretically become more accurate in distinguishing individuals, though accuracy encompasses multiple considerations including false positive rates, false negative rates, and performance across different demographic groups.[3]

---

* Head of the International Department in the Israeli Privacy Protection Authority.

[1] International Working Group on Data Protection in Technology, Working Paper on Facial Recognition Technology, 2023, 1.

[2] Ibid, 4-5.

[3] Ibid, 5-6.

3. Applications and Controversies

The Berlin Group documents an extensive range of facial recognition applications in both private and public contexts. In the private sector, the technology serves functions including secure access to premises and devices, security monitoring in venues such as casinos and retail stores, marketing and customer service applications, and attendance monitoring in workplaces.[4] However, these deployments have not proceeded without opposition. Data protection authorities in the Netherlands and Canada have deemed certain retail facial recognition systems unlawful, establishing important precedents for privacy protection.[5]

Government agencies have embraced facial recognition for border control, access to digital services, law enforcement, and educational settings.[6] Law enforcement applications present particularly acute concerns, as police agencies use facial recognition to identify uncooperative suspects, maintain mugshot databases, investigate crimes, and deploy live facial recognition systems to locate wanted individuals in real time.[7] The introduction of facial recognition in schools has proven especially contentious, with critics arguing that subjecting minors to continuous biometric surveillance may harm their development and discriminate against students with autism spectrum disorders or physical conditions affecting facial appearance.[8]

4. Privacy Risks and Fundamental Rights Implications

Facial recognition systems deployed in public spaces capture the faces of all passersby indiscriminately, creating constant and pervasive surveillance that fundamentally erodes anonymity.[9] Such systems may reveal or enable inferences about individuals' political opinions, religious beliefs, medical conditions, and sexual orientation. The mere knowledge that facial recognition systems operate may deter people from attending demonstrations, visiting places of worship, or accessing health clinics, creating a chilling effect on democratic participation.[10]

Facial recognition systems have demonstrated documented patterns of accuracy errors that disproportionately affect certain populations. Research indicates that Asian and African American individuals face up to one hundred times greater likelihood of misidentification compared to white men.[11] Women, transgender individuals, non-binary people, and individuals with certain disabilities also experience higher error rates. The Privacy Commissioner of Canada emphasizes that facial recognition accuracy must be understood statistically rather than as binary truth, with system outputs

[4] Ibid, 7-10.
[5] Ibid, 8.
[6] Ibid, 11-12.
[7] Ibid, 13-14.
[8] Ibid, 12.
[9] Ibid, 14-15.
[10] Ibid, 15.
[11] Ibid, 16.

representing probabilistic inferences about identity rather than verified facts.[12] Training data quality fundamentally shapes algorithm performance; systems trained on non-representative datasets inevitably produce disparate accuracy across demographic groups.

Certain applications present accuracy and bias problems so severe that ethical deployment becomes impossible. Emotion recognition systems presume universal emotional expression, assumptions contradicted by cross-cultural research.[13] These systems frequently assign more aggressive emotions to Black faces regardless of actual expression, perpetuating racist stereotypes. Biometric categorization systems that claim to predict sexuality, criminality, or other traits from facial features rest on premises virtually indistinguishable from discredited pseudosciences like phrenology.[14]

The permanent and unchangeable nature of facial biometric data magnifies the consequences of security breaches. Unlike passwords or credit card numbers, faces cannot be reset or replaced following data compromise.[15] Hackers gaining access to facial recognition data may steal identities, impersonate victims, or conduct illegal activities using stolen biometric identities. Major breaches have already occurred, including a Chinese database containing millions of facial records left exposed online for months.[16]

Live facial recognition technology presents additional risks beyond retrospective analysis. These systems automatically collect biometric data in real time, indiscriminately processing information about all individuals who pass through monitored areas.[17] A documented case from London illustrates potential abuse: Metropolitan Police officers stopped and questioned a fourteen-year-old schoolboy based on a false match later confirmed as non-credible.[18]

5. Regulatory Approaches and Recommendations

The Berlin Group proposes multiple strategies for mitigating facial recognition risks, ranging from outright prohibitions to technical safeguards and procedural requirements. Before implementing any system, controllers must conduct comprehensive risk assessments considering factors including the scope of individuals affected, whether data storage is centralized or decentralized, whether the system includes search capabilities, how templates are stored, whether data collection is mandatory or voluntary, the transparency and consent framework, and target environment characteristics.[19]

Many jurisdictions have concluded that certain applications pose such severe

[12] Ibid, 18-19.
[13] Ibid, 16-17.
[14] Ibid, 17-18.
[15] Ibid, 21.
[16] Ibid, 22.
[17] Ibid, 23.
[18] Ibid, 24.
[19] Ibid, 25-27.

threats to fundamental rights that outright prohibition represents the only appropriate response. The European Data Protection Board and European Data Protection Supervisor have called for a general ban on automated recognition of human features in publicly accessible spaces.[20] The European Parliament has advocated for permanent prohibition of automated individual recognition in public spaces and bans on private facial recognition databases like Clearview AI.[21] These proposals emerged following enforcement actions by data protection authorities across Europe, Australia, and Canada against companies operating facial recognition systems without adequate legal basis or safeguards.

Several U.S. jurisdictions have enacted prohibitions, with Vermont, Maine, New Hampshire, Oregon, and California restricting or banning facial recognition in various contexts.[22] Over one hundred organizations and hundreds of experts from more than forty countries have endorsed recommendations that countries suspend further deployment of facial recognition for mass surveillance pending establishment of adequate legal frameworks.[23]

Where facial recognition deployment is not categorically prohibited, clear and specific legal basis must exist for processing biometric data.[24] For high-risk deployments, organizations should consult competent data protection authorities prior to implementation. Facial recognition in public spaces must serve necessary and important public interests that cannot be protected through less invasive means.

Consent represents a problematic legal basis in many contexts due to power imbalances and the practical impossibility of meaningful consent in public spaces.[25]

The public deserves notification about facial recognition deployment in public spaces.[26] Transparency should extend to data protection impact assessments and results of accuracy and bias testing. Signage must be prominently visible before individuals enter surveilled areas and clearly indicate that facial recognition is operating.

Controllers must implement multiple technical measures to mitigate risks. Data accuracy requires optimal conditions for training datasets, comparison databases, cameras, lighting, and imaging.[27] Regular examination of datasets must ensure diversity across ages, genders, and skin tones. Controllers should establish appropriate confidence thresholds and performance metrics, discontinuing processing when systems fail to meet requirements. Where facial recognition decisions affect data subjects, final decisions must involve human intervention by well-trained professionals rather than relying on automated processing alone.[28]

[20] Ibid, 28.
[21] Ibid, 28-29.
[22] Ibid, 30.
[23] Ibid.
[24] Ibid, 30-31.
[25] Ibid, 32.
[26] Ibid.
[27] Ibid, 32-33.
[28] Ibid, 33.

Data minimization strategies should guide system design and operation.[29] Controllers should limit stored personal data, delete raw images after extracting templates when no longer required, implement automatic erasure after defined retention periods, avoid unnecessary cross-referencing with other data sources, store templates separately from identifying information, encrypt and anonymize data, and restrict data retention to periods necessary for specified purposes. Comprehensive data security measures must address vulnerabilities throughout the data flow cycle.[30]

6. Conclusion

The Berlin Group's working paper provides a rigorous framework for understanding and addressing the profound challenges facial recognition technology poses to privacy, human rights, and social equity. While acknowledging potential beneficial applications, the document makes clear that facial recognition's capacity for intrusive, arbitrary, and discriminatory surveillance demands robust regulatory responses that prioritize fundamental rights protection.

The variety of regulatory approaches emerging globally reflects ongoing societal deliberation about appropriate boundaries for biometric surveillance in democratic societies. The working paper's emphasis on comprehensive risk assessment, clear legal frameworks, meaningful transparency, accuracy accountability, and technical safeguards offers practical guidance for policymakers, data protection authorities, and deploying organizations.

Bibliography:

1. International Working Group on Data Protection in Technology, Working Paper on Facial Recognition Technology, 2023.

[29] Ibid, 34.
[30] Ibid, 35.