



ISSN: 2583-7753

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

[ISSN: 2583-7753]

Volume 4 | Issue 3

2026

DOI: <https://doi.org/10.70183/lijdlr.2026.v04.329>

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com

Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)

To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript [Click here](#)

FACIAL RECOGNITION TECHNOLOGY AND THE RIGHT TO PRIVACY: COMPARATIVE CONSTITUTIONAL ANALYSIS

Gursimar Kour Sudan¹

I. ABSTRACT

Facial Recognition Technology (FRT), a form of automated identification based on biometric facial data, has become an important tool of State surveillance in modern times. Its use raises constitutional concerns because the collection, analysis and identification of a person's face by State authorities may interfere with the right to privacy. This paper conducts a comparative constitutional study of India, the United Kingdom, Canada and South Africa to examine the permissible limits of State use of FRT. The study adopts a doctrinal and comparative methodology by analysing constitutional provisions, judicial decisions and relevant legislation in the four jurisdictions. The Indian analysis centres on Articles 14 and 21 of the Constitution and the Supreme Court's ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India [(2017) 10 SCC 1], which recognises privacy as a fundamental right and applies proportionality to evaluate State action. This framework is compared with Article 8 of the European Convention on Human Rights and R (Bridges) v. Chief Constable of South Wales Police [[2020] EWCA Civ 1058], Section 8 of the Canadian Charter of Rights and Freedoms, and Section 14 of the South African Constitution. The paper compares the requirements of legality, legitimate State purpose, necessity, proportionality, equality and safeguards against arbitrary surveillance. It finds that while all four jurisdictions recognise protection against State interference with privacy, they differ in constitutional basis, judicial oversight and legal safeguards for technologically assisted surveillance. The Indian constitutional framework provides a basis for scrutinising FRT, but clearer procedural protections and stricter legality and proportionality standards are necessary to define the permissible limits of State use of facial recognition.

¹ 1st-Semester LL.M. Student at Lovely Professional University, Punjab (India). Email: gursimarkour18@gmail.com

II. KEYWORDS

Facial Recognition Technology; Right to Privacy; State Surveillance; Proportionality; Comparative Constitutional Law.

III. INTRODUCTION

Facial Recognition Technology (FRT) is a biometric technology that consists of the automatic identification or verification of people based on the analysis of facial features. Advances in artificial intelligence, machine learning and computer vision have given FRT greater ability to accurately identify human beings at a greater speed and scale.² This has therefore sparked a constitutional concern with its use by state authorities for policing, investigation, border control and identification.

While traditional surveillance can only capture who is present, FRT can interpret facial imagery, match it against the images in its database and identify the person in the image. The constitutional importance of the technology thus relates to the State's ability to transform an individual's physical appearance into a recognisable biometric data. The separation is the core of the connection between FRT and the right to privacy. Whether the State may subject an individual to automated identification is not determined by the fact that the individual's face is visible in the public space.

FRT requires an additional step of biometric analysis and identification which could lead to the State identifying who an individual is, linking that person to a specific place or event, and keeping the information. The rising notice by the Indian government of the use of FRT in law enforcement and identification programmes, such as the proposed National Automated Facial Recognition System (NAFRS) has placed this issue under the constitutional umbrella of 'privacy'.

The Supreme Court in the case of *Justice K.S. Puttaswamy (Retd.) v. Union of India*³ has established informational privacy as a fundamental right of every citizen. The Court

² Beibut Amirgaliyev, M. Mussabek, et al., "A review of machine learning and deep learning methods for person detection, tracking and identification, and face recognition with applications" 25 *Sensors* 1410 (2025).

³ *Justice K.S. Puttaswamy (Retd.) v. Union of India* [(2017) 10 SCC 1].

has found that privacy is not “absolute” and that the interference by the State must meet constitutional standards. The proportionality principle then evolved in the Indian jurisprudence to question whether the interference with the fundamental right was legally sanctioned, the interference was in pursuit of a legitimate objective and whether the interference bore a proportionate relationship to that objective.⁴

The principles are the constitutional basis for analysing State use of FRT but their scope and extent are not sufficiently developed with regard to automated facial identification. This paper aims to discuss the constitutional conflict between the growing adoption of Facial Recognition Technology (FRT) by the State and the basic right to privacy. The Supreme Court of India in *Justice K.S. Puttaswamy case* has declared privacy as a Fundamental Right and added that any action of the State against it is subject to constitutional tests like legality and proportionality.

These principles are, however, not adequately developed in the jurisprudence of the Indian constitution. This is particularly relevant to make a comparative examination. The United Kingdom offers direct judicial scrutiny of State use of FRT in the *R (Bridges) v. Chief Constable of South Wales Police*⁵ case before the Court of Appeal, which considered the use of live facial recognition by the police in the context of Article 8 of the European Convention on Human Rights⁶, which protects the right to private life.

There is a unique Canadian constitutional solution with respect to reasonable expectations of privacy in the context of State information-gathering, namely through the Canadian Charter of Rights and Freedoms, Section 8 and the jurisprudence in this area. The Constitution of South Africa, in turn, explicitly guarantees the right to privacy in Section 14, with the Protection of Personal Information Act 2013⁷ giving specific protection to biometric information.

⁴ A. K. Sikri, “Proportionality – A Balancing Act for Achieving Constitutional Rights: A Comparative Study” in M. P. Singh, et al. (eds.), *The Indian Yearbook of Comparative Law 2019* 111-129 (Springer Singapore, Singapore, 2021).

⁵ *R (Bridges) v. Chief Constable of South Wales Police* [(2020) EWCA Civ 1058].

⁶ The European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950.

⁷ The Protection of Personal Information Act, 2013 (Act 4 of 2013).

A. Research Questions

1. Under Indian constitutional law, what is the extent of the right to privacy in the context of Facial Recognition Technology?
2. In the United Kingdom, Canada and South Africa what constitutional protections apply to the use of Facial Recognition Technology?
3. What are the differences between Indian position and comparative approach to privacy and Facial Recognition Technologies?

B. Research Objectives

1. To examine the constitutional aspects of privacy protection under a Facial Recognition Technology under the Indian Constitution including Articles 14 and 21 and judicial precedents.
2. To examine the constitutional protections available in the United Kingdom, Canada and South Africa to Facial Recognition Technology.
3. To examine the Indian Constitutional status on the basis of the strategies used in the three comparative jurisdictions.

C. Research Methodology

The study uses a comparative and doctrinal approach to analyse the connections between Facial Recognition Technology (FRT), and the right to privacy in India, the United Kingdom, Canada and South Africa. The doctrinal analysis is based on the analysis of constitution, legislation and judicial interpretation related to privacy and biometric identification in particular, including Article 14 and 21 of the Constitution of India and *Justice K.S. Puttaswamy (Retd.) v. Union of India*.

The constitution and law of the three comparative jurisdictions are looked at to identify what laws are relevant to FRT. The comparative analysis compares the four jurisdictions in terms of the extent of privacy protection and constitutional safeguards that are available with regards to FRT and highlights the difference in constitutional approaches and the position of India.

The major source of the study is based on the primary legal sources and supplemented with the literature of the study and the authority of the institutions. It is non-empirical,

qualitative and is only applied in the constitutional relationship between FRT and the right to privacy.

IV. CONSTITUTIONAL FRAMEWORK

The right to privacy and constitutional restrictions on the same are the constitutional framework of this study in India, United Kingdom, Canada and South Africa. The relevance here is the ability to electronically analyse and match facial images, known as Facial Recognition Technology (FRT), which is relevant to this framework. The “constitutional question” then has implications beyond the mere sighting of a person in a public place.

The jurisdiction of the Indian state is the primary focus and there is a comparative analysis of three different constitutional systems of handling matters of privacy in the United Kingdom, Canada and South Africa. The analysis focuses on three aspects i.e; the constitutional foundation of the right to privacy, the principles in judicial decisions to establish whether FRT infringes on the right to privacy, and the norms applied to make the decision whether the interference is constitutionally acceptable.

A. India

The Constitution of India does not have any specific provision to address facial recognition or biometric surveillance. Hence, the basis of the constitutionality of an examination of FRT comes primarily from Article 14 and Article 21 of the Constitution of India. Article 14 secures equality before the law, and equality of protection of the laws, Article 21 secures life and personal liberty. The nine-judge Bench of the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) has finally resolved the issue pertaining to the constitutional position of privacy.

The Court accepted the right to privacy as a basic human right and found its right to protection in the constitutional rights to liberty, dignity and autonomy.⁸ This is especially important for FRT since the information processed in facial recognition has

⁸ Vrinda Bhandari, Amba Kak, *et al.*, “An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict” 11 *IndraStra Global* 5 (2017).

the potential to identify an individual. The Puttaswamy judgement also laid down the constitutional yardstick to be applied in case of any restriction on privacy.

In order to be legally justifiable and in keeping with a legitimate state objective, the Court had to be based on an interference with privacy.⁹ The requirement of the legality aspect is that legal authority, in terms of the existence and the quality of legal authority is of relevance, the requirement of proportionality is that the interference must be proportionate to the objective that is being pursued.¹⁰

Article 14 operates in parallel with this without any contradiction and adds the constitutional non-arbitrariness condition to the principle of State action. Thus, the Indian framework for FRT is based on three interlinked issues; that privacy is a fundamental right, that there must be protection from arbitrary state action, and there must be some constraints on restrictions of privacy.

B. United Kingdom

In the UK, the main constitutional guarantee for FRT is Article 8 of the European Convention on Human Rights (ECHR), which provides protection for the right to respect their private and family life, home and their correspondence.¹¹ The Convention rights have been incorporated into domestic law by the Human Rights Act 1998, which imposes a duty on public bodies to act compatibly with the Convention rights. Under Article 8(2), interference with private life is allowed only if it is in accordance with the law, that it serves a recognised legitimate aim and that it is necessary in a democratic society.

The requirements are the key constitutional principles that justify consideration of State application of FRT. South Wales Police's use of live automatic facial recognition was the subject of the case. It was accepted by the Court of Appeal that the technology

⁹ Pamarthi Satyanarayana, "KS Puttaswamy v. Union of India to Data Protection: The Evolution of Privacy Jurisprudence in India" *Anusandhanvallari* 4562-4567 (2025).

¹⁰ Pawan Bindal and Ramveer Singh, "Survival of Right to Privacy under Administrative Surveillance: A Comparative Legal Study" 8(2) *Journal of Humanities and Education Development* 29-40 (2026).

¹¹ Nicole A. Moreham, "The right to respect for private life in the European Convention on Human Rights: a re-examination" (1) *European Human Rights Law Review* 44-79 (2008).

was used in a manner that involved Article 8 and looked to see whether the police had acted in a sufficiently specific legal framework.

Special focus was placed on the discretion that the technology would be applied under and who would be added to watchlists. The Court found that the framework of law was not sufficiently to restrict that discretion, and found that the interference was not “in accordance with the law” for the purposes of Article 8(2).¹² The Bridges case is important for the purposes of the present study because it offers the first judicial discussion of FRT in a constitutional privacy case, and because it incorporates legal clarity and limits on discretion at the core of the analysis.

C. Canada

The Canadian constitutional system has an approach to privacy in section 8 of the Canadian Charter of Rights and Freedoms, which protects against unreasonable search or seizure. Privacy is therefore “built-in,” not provided express as a right to privacy. The main doctrine is that of reasonable expectation of privacy, which was developed in *Hunter v. Southam Inc.*¹³ The doctrine involves looking at as there an expectation in the circumstances that the individual would be protected from State intervention.¹⁴

In the context of FRT, this doctrine is of specific importance as facial recognition could convert an image captured in a public place into data that allows for identification of a specific person. Canadian privacy law does not presume that all information that is public is without any reasonable expectation of privacy. The implications of the nature, purpose and extent of State information-gathering continue to be relevant to the constitutional inquiry. The Canadian framework is therefore applicable in the present juxtaposition as it offers a constitutional basis to consider the difference between observing an individual and using technology to identify an individual.

¹² Te Li, “Bridges v South Wales Police and emerging privacy concerns” 75(4) *Northern Ireland Legal Quarterly* 806-817 (2024).

¹³ *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145 (Canada).

¹⁴ Richard Jochelson and David Ireland, *Privacy in Peril: Hunter v Southam and the Drift from Reasonable Search Protections* (UBC Press, Vancouver, 2019).

D. South Africa

There is a constitutional guarantee of privacy in the South African Constitution. Section 14 of the Constitution of the Republic of South Africa, 1996¹⁵ protects a person from certain types of intrusion, such as searches of his person, searches of property, seizure of possessions and infringement of communications. Protection of Personal Information (POPIA) Act 4 of 2013 is a supplement to the constitutional guarantee.

POPIA dictates how personal information is processed through public and private bodies, and outlines conditions for the lawful processing of personal information. Significantly for FRT, the Act is explicit in its definition of biometric information as special personal information and in the extra restrictions it imposes on the processing of this information, subject to exceptions. The South African framework in turn gives protection to privacy both constitutionally and in terms of specific legislation.

E. Constitutional Basis of the Comparative Framework

The constitution is the basis of the comparative framework. The four jurisdictions have different ways of protecting privacy through their constitution.

The second column illustrates constitutional bases and principal doctrines relevant to facial recognition technology (FRT) across the four jurisdictions.

Jurisdiction	Constitutional Basis	Principal Doctrine Relevant to FRT
India	Articles 14 and 21	Privacy, legality and proportionality
United Kingdom	Article 8 ECHR	Private life, legality and necessity

¹⁵ Constitution of the Republic of South Africa, 1996 (Act No. 108 of 1996) , s. 14.

Canada	Section 8 Charter	Reasonable expectation of privacy
South Africa	Section 14 Constitution	Express constitutional privacy protection, supplemented by POPIA

The differences have significance for comparability of the study design. India's approach to privacy is via fundamental rights and proportionality, the United Kingdom's approach is through Article 8 and lawful and necessary interference, while the approach of Canada is the reasonable expectation of privacy under section 8, and that of South Africa is via an explicit right to privacy coupled with statutory protection of biometric information. These are the unique constitutional bases from which to approach and consider the treatment of FRT in the four jurisdictions in the following doctrinal and comparative analysis.

V. COMPARATIVE ANALYSIS

The comparison is structured in terms of the main constitutional issues that arise in the context of FRT i.e; do the biometric identifiers interfere with the exercise of rights to privacy, is this interference sufficiently justified by law, is the interference justified in terms of the purpose and scope of FRT. This allows the jurisdictions to be studied in relation to a series of 'universal' legal questions as opposed to each being analysed as their own legal system.

A. Facial Recognition as a Privacy Interference

The first comparison is with respect to the point at which the use of FRT comes under constitutional protection of privacy. What's important is whether it's a person who's in public versus technology that identifies that person by biometric analysis. The latter requires the extraction, comparison and processing of information that can enable a face image to be matched to an individual which can be identified.

In the U.K., this was explicitly addressed in *R (Bridges) v. Chief Constable of South Wales Police*. The Court found that the use of automated facial recognition, which was able to extract unique biometric information that would identify individuals, engaged Article 8. It was not the case that the facial features were visible or were visible to the community, which prevented Article 8 from being engaged. Section 8 of the Charter prohibits unreasonable search or seizure and the issue to be addressed is whether the person had a reasonable expectation of privacy in the circumstances.

In *R v Spencer*¹⁶, the Supreme Court pointed out that informational privacy encompasses control over information and further that 'anonymity' in appropriate circumstances is part of informational privacy. The Court applied its reasoning to a linkage of information with an identifiable person, even if the information itself was not secret. The South African Constitution also allows privacy to go beyond the physical trespass.¹⁷ Section 14 explicitly acknowledges the right to privacy; and South African privacy jurisprudence acknowledges that the protection does not only apply to the specified modes of intrusion in the section.

Hence, there is an important doctrinal difference that the mere fact of public exposure of a face does not automatically preclude the later identification of the face through biometrics to be outside the constitutional protection of privacy. The problem of the constitution comes from the extra facto information generated by technological identification.

B. Legal Authority and Control over FRT

Inherently intrusive surveillance practices that rely heavily on administrative discretion, as opposed to explicit legal mandates, render constitutional protection more and more vulnerable. The Court of Appeal in Bridges case concluded that the existing laws on the police use of live facial recognition were inadequate as too much discretion was given regarding who could be put on a watchlist and the circumstances under which it could be used.

¹⁶ *R. v. Spencer*, [2014] 2 S.C.R. 212 (Canada).

¹⁷ J. Neethling, "The Concept of Privacy in South African Law" 122(1) *South African Law Journal* 18-28 (2005).

The Court thus ruled that the use of the technology was not “in accordance with the law” for the purposes of Article 8(2).¹⁸ An ability to use a general policing power to identify members of the public through the use of technology does not necessarily provide legal certainty. The Indian position is different in terms of the institutional issue. Puttaswamy provides the constitutional framework for the evaluation of privacy restrictions but for FRT, it is necessary to take stock of the legal foundations for the specific deployment and the limits set.

It is not just because FRT has a recognised public purpose that it is legal, however, but because the legal framework also provides a scope of use, a time of use and a purpose for use. The principles of lawful authority are also important in Canada when it comes to State information-gathering that involves a reasonable expectation of privacy. In *R v. Spencer*, the Supreme Court determined that the police request to enable disclosure of subscriber information did not have lawful authority and this was relevant to the Section 8 analysis.

South Africa is an additional example because its constitution is built on a framework of privacy that is in addition to existing laws that govern personal information. The Protection of Personal Information, 2013 is expressly to protect biometric information as special personal information, which would give a statutory level of protection to the processing of facial biometric information.¹⁹

C. Purpose and Necessity of FRT Use

The presence of an objective does not automatically mean the constitutional validity of FRT. Law-enforcement agencies can use FRT for purposes of crime prevention, suspect identification or public safety, but the constitutional question must also be whether or not the specific use of FRT is justified by any of those purposes.²⁰ This demands consideration to the type and scale of deployment. A targeted system, where

¹⁸ Christine Carpenter, “Privacy and proportionality: Examining mass electronic surveillance under Article 8 and the Fourth Amendment” 20(1) *International and Comparative Law Review* 27-57 (2020).

¹⁹ Hannah Zimmerman, “The Data of You: Regulating Private Industry’s Collection of Biometric Information” 66(3) *University of Kansas Law Review* 637 (2017).

²⁰ Vera Lúcia Raposo, “The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal” 29(4) *European Journal on Criminal Policy and Research* 515-533 (2023).

an identified watchlist is used for a specific law-enforcement objective, raises other constitutional considerations than does indiscriminate identification of all those who may be wandering through a public space.

This is evident in Bridges' example. The Court took into account the nature of the deployments, the limited time and geographical scope of specific deployments, the purpose of the use of watchlists, and the automatic removal of data that could not be matched. The following features were part of the proportionality assessment. The significance is that the constitutional review will consider how FRT is actually being used, not the potential usefulness of the technology in general, for India. The question remains whether the specific collection and identification effort exceeds the necessary means to accomplish the purpose stated.

The Canadian model also needs to be understood in the context of the situation in which the State gathers information, rather than simply focusing on whether or not it is publicly available.²¹ Spencer notes information's nature, and the implications of associating it with a specific individual, are pertinent to the privacy inquiry.

D. Proportionality and the Scope of Intrusion

While the doctrine has its roots in various constitutional frameworks, the Indian and UK approaches converge at the principle of proportionality. The proportionality principle in India implies a comparison between the fundamental right which is being curtailed and the legitimate purpose which is being served. The assessment of the applied FRT should consider the intrusiveness, scale, duration, purpose of the biometric identification without lumping together all forms of facial recognition as constitutionally equivalent.

The interference test for the UK approach under Article 8 is also based on the conditions laid out in Article 8(2). The Court eventually ruled the specific deployments to be proportional, but in concluding that the broader legal framework was lacking, it also determined that there was too much discretion over deployment

²¹ Lori Kiefer, *et al.*, "Fostering evidence-based decision-making in Canada: examining the need for a Canadian population and public health evidence centre and research network" 96(3) *Canadian Journal of Public Health* I1-I19 (2005).

and watchlists. The legal framework under which FRT is used may be constitutionally inadequate but the practice itself may be proportionate.²²

The concept of legality and proportionality thus serves different purposes but in a related way. Similarly, South Africa acknowledges that privacy is not absolute in the constitution and can be restricted if allowed by the Constitution's general limitation provisions.²³ The South African model is thus relevant to the comparison as it is an express constitutional right to privacy and there are laws providing controls over personal information.

E. Constitutional Control over Administrative Discretion

The use of FRT raises a unique public law issue as the technology must be deployed with decisions on who should be identified and where, and how, the information gathered and processed will be used. This is especially prevalent in Bridges' case where the court singled out the lack of boundaries around the "who" and "where" questions as major gaps in the law.

This offers a valuable benchmark for India. If the legal basis for deploying FRTs leaves large degrees of discretion to either the executive or the police, then the question of sufficient structuring of such discretion should be subject to constitutional review.²⁴ What is a concern is the discretion (or lack of it) in the use of a technology that has the capacity to identify many people.

The Canadian model also illustrates the need for judicial review when government intrusion into information-gathering takes place within a reasonable expectation of privacy. In Section 8, the State's investigatory practices are reviewed against the constitutional protection against unreasonable searches and seizures.

²² B. Shruthi, "Facial Recognition Technology (FRT) and Privacy: A Delicate Balance" 6(6) *International Journal of Legal Science and Innovation* 291-304 (2024).

²³ Dorcas Basimanyane, "The regulatory dilemma on mass communications surveillance and the digital right to privacy in Africa: the case of South Africa" 30(3) *African Journal of International and Comparative Law* 361-382 (2022).

²⁴ Harry Aniulis, "Facial recognition technology, privacy and administrative law" 45(4) *University of New South Wales Law Journal* 1513-1549 (2022).

VI. JUDICIAL AND LEGISLATIVE DEVELOPMENTS

Facial Recognition Technology (FRT) in its constitutional position has evolved as a result of judicial rulings and laws, rather than constitutional provisions for FRT. The developments mentioned below are restricted to those authorities that have a direct bearing on the issue of facial identification and the right to privacy.

A. India

The principal judicial development is *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) wherein the Supreme Court held that privacy is a fundamental right and thus included informational privacy in the ambit of privacy. The decision is important to FRT because if facial images are processed for identification they become "information" that can be used to connect an individual to a specific identity. The Court also imposed conditions on limitations on privacy that it believed must be met before the limitations are constitutional, namely that they are necessary for a legitimate State purpose, legal, and proportional.²⁵

While the Supreme Court has not yet delivered a comprehensive judgment on the constitutional validity of Facial Recognition Technology, *Puttaswamy* provides the key constitutional test that can be invoked to assess FRT usage. A significant pending development is *A.A. Rahim M.P. v. Union of India*, an Article 32 petition challenging the Delhi Police's alleged deployment of Facial Recognition Technology and allied biometric-surveillance measures at protest sites. The petition reportedly raises concerns under Articles 14, 19 and 21, including privacy, equality and the chilling effect of biometric surveillance on the right to protest.

This proceeding is important because it places police use of FRT directly before the Supreme Court for constitutional scrutiny, although its outcome remains pending. The Information Technology Act, 2000 does not contain a dedicated regime for facial recognition. The Digital Personal Data Protection Act, 2023, together with the Digital Personal Data Protection Rules, 2025, provides the operative general framework for

²⁵ Kristina Trykhlil, "The principle of proportionality in the jurisprudence of the European Court of Human Rights" 4 *EU and Comparative Law Issues and Challenges Series (ECLIC)* 128-154 (2020).

processing digital personal data, including biometric data processed through FRT deployments. However, neither the Act nor the Rules create a technology-specific regime for facial recognition. The absence of FRT-specific statutory safeguards therefore remains significant in light of the constitutional principles of legality, proportionality and procedural protection laid down by the Supreme Court.

B. United Kingdom

The United Kingdom has developed the most direct judicial scrutiny of live facial recognition among the jurisdictions examined. In *R (Bridges) v. Chief Constable of South Wales Police*, the Court of Appeal held that the police use of live automated facial recognition engaged Article 8 ECHR and that the applicable framework did not sufficiently regulate who could be placed on a watchlist or where the technology could be deployed. The interference was therefore not “in accordance with the law.” The Court also found deficiencies relating to the Public Sector Equality Duty and the Data Protection Act 2018.

However, the post-*Bridges* position has been refined by *R (Thompson and Carlo) v. Commissioner of Police of the Metropolis* [2026] EWHC 915 (Admin). In that case, the High Court considered the Metropolitan Police’s revised live facial recognition policy, adopted on 11 September 2024, and upheld it against challenges under Articles 8, 10 and 11 ECHR. The Court distinguished *Bridges* on the basis that the revised policy contained more structured and interlocking controls over the “why”, “who” and “where” of deployment, including watchlist criteria, location-based constraints and a mandatory proportionality assessment.

The Court held that the policy did not authorise arbitrary decision-making and that it satisfied the requirements of being “in accordance with the law” and “prescribed by law.” This development shows that the UK position is not simply that LFR lacks a lawful framework; rather, UK courts have accepted that LFR may be lawful where discretion is adequately structured and accompanied by clear safeguards.

C. Canada

So far, Canadian developments have been primarily based on privacy and regulatory actions, rather than a constitutional judgment that would make the use of police facial recognition legal. The federal and provincial privacy authorities, in particular, are focusing on the investigation of clearview AI in 2021. The investigation revealed the use of facial images collected from websites freely accessed by the public as biometric identifiers and for identification purposes without the consent of the individuals.²⁶

The authorities saw facial biometric data as very sensitive and decided that indiscriminate collection and identification might amount to mass surveillance. The investigation into the use of clearview AI by the Royal Canadian Mounted Police (RCMP) revealed that the RCMP had violated the federal privacy act for their collection of personal data from the service.

The police guidance included guidance around controls on the use of FRT and minimising privacy risks. The developments are of interest in the context of the constitutional comparison because they provide an example of how Canadian privacy law gives facial biometric identification a higher level of intrusiveness than access to publicly available images.²⁷

D. South Africa

South African development is most important in the context of the interaction between the constitutional guarantee of privacy and the Protection of Personal Information Act 2013 (POPIA). POPIA expressly defines biometric information as a special form of personal information and prescribes further requirements for processing biometric information.²⁸ This affords a “statutory layer of protection” over biometric information in addition to the constitutional protection of privacy afforded by section 14.

²⁶ Lamyamba Laishram, M. Shaheryar, *et al.*, “Toward a privacy-preserving face recognition system: A survey of leakages and solutions” 57(6) *ACM Computing Surveys* 1-38 (2025).

²⁷ Jawahitha Sarabdeen, “Protection of the rights of the individual when using facial recognition technology” 8(3) *Heliyon* e09086 (2022).

²⁸ Ciara Staunton, Rachel Adams, *et al.*, “Protection of Personal Information Act 2013 and data protection for health research in South Africa” 10(2) *International Data Privacy Law* 160-179 (2020).

South Africa has not yet produced an equivalent leading constitutional judgment to *Bridges* that sets out to directly scrutinise the use of live FRT by police, unlike the United Kingdom. The South African framework is therefore especially important to consider in the context of how an express constitutional right to privacy interacts with a law that allows for a specific recognition of the sensitivity of biometric information.

E. Comparative Significance

The above illustrate four types of legal control pertinent to FRT. Although India has no legislation on FRT, but has a constitutional privacy and proportionality framework, the United Kingdom sees direct judicial review of live facial recognition and a requirement for a sufficiently precise legal framework, while Canada provides for the regulation of facial biometrics as highly sensitive information, and South Africa combines an explicit constitutional privacy guarantee with statutory protection for biometric information. These developments collectively give legal backing to the next step of comparing the acceptable limits of facial recognition in the four jurisdictions.

VII. CRITICAL ANALYSIS

One strong point of the comparative frame is that it analyses FRT from the point of view of known constitutional principles, and not only in terms of technology. The four jurisdictions have different approaches to the rule of privacy: in India, through fundamental rights and proportionality, in the United Kingdom, through Article 8, and reasonable expectations of privacy, in Canada, and an express constitutional right with statutory protection for biometric information in South Africa. This difference is helpful in understanding the differences between the types and levels of constitutional protection.

One challenge with the current legal landscape is that there is a lack of uniformity in the underlying legal perspective. While the Indian, Canadian and South African positions are more dependent on general privacy principles, laws and regulations, the United Kingdom now offers a more developed line of judicial consideration of live facial recognition through both *Bridges* and *Thompson and Carlo*. *Bridges* demonstrates the constitutional difficulty created by insufficiently structured police discretion, whereas *Thompson and Carlo* show that a revised policy may withstand review where

it contains clearer safeguards governing the purpose, location and watchlist criteria for deployment. The comparison can therefore not be limited to the finding of unlawfulness in *Bridges*, but must also account for the later judicial acceptance of a more structured LFR policy. It is important for India because, although *Puttaswamy* has built a sturdy constitutional framework for the deployment of facial recognition, it has not given any detailed guidance.

It is a continuing issue whether the facial image acquired in public has a legal value. The opposing arguments are that public visibility diminishes the expectation of privacy, or that automated biometric identification establishes an additional privacy interest. *Bridges* and the Canadian clearview investigations favor the latter, but it's far from resolved interjurisdictional. Where FRT can be used to identify a person on a larger scale, the controversy is heightened because the constitutional implications are broader than that of the individual image and involve the creation and use of an identifiable biometric profile.²⁹

While principles like legality and proportionality serve as a set of guidelines to guide the review of FRT, they do not themselves dictate the length of time it can be retained, the conditions for creating watchlists, when or if information should be removed because of a false match, and when or if it should be deleted. South Africa's statutory treatment of biometric information, and the regulatory reaction in Canada to Clearview, are more specific examples of control, as is *Bridges*' discussion of the need to limit administrative discretion. The developments suggest that the protection of privacy under the constitution is not only a matter of effectiveness, but also of the legal and institutional arrangements that are used to implement the protection.

Another restriction relates to the handling of technological accuracy and unequal impact. FRT is not a neutral identification mechanism where error or differences in accuracy are likely to impact on people differently. Where an incorrect identification leads to police action or other adverse consequences it becomes constitutionally relevant. The issue of Article 14 in the Indian framework then becomes important,

²⁹ Rebecca Crookshanks, "Police Surveillance and Use of Facial Recognition Technology: Charter Issues, Legal Frameworks and Oversight Mechanisms" (University of Saskatchewan, 2026).

rather than just for the issue of general non-arbitrariness, because it is a basis to evaluate whether the consequences of the exercise of FRT related powers are unreasonable or unequal.³⁰

But, the Indian constitutional doctrine has not yet evolved a specific framework to address these questions in the context of facial recognition. The absence of constitutional protection, however, is not the principal deficit compared to India, rather the lack of clarity on how constitutional principles ought to be applied in the situation of FRT. Improved standards for privacy protection are observed where constitutional standards are supported by delineation of discretion limits, establishment of conditions for use, and institutionalized oversight.

Simultaneously, none of the jurisdictions offers a full model ready for adoption as is. The usefulness of the comparison, therefore, is to pinpoint the advantages and disadvantages of various constitutional solutions, and acknowledge the need for the current framework of privacy rights to be interpreted in a way that accounts for its specific biometric and identification properties in the context of FRT.³¹

VIII. FINDINGS

The comparative analysis shows that the constitutional treatment of the Facial Recognition Technology (FRT) does not rely on a technology-specific constitutional provision. The current privacy assurances can be sufficient to deal with FRT, since information processed by automated facial identification can be used to identify an individual. The concern with the constitution is not that a facial image is captured, but rather that it is identified and then used to identify the person.

The analysis also reveals that the four jurisdictions take varying “legal paths” to privacy protection. India has relied primarily upon Articles 14 and 21 and the

³⁰ Patricia Faraldo Cabana, “Technical and Legal Challenges of the Use of Automated Facial Recognition Technologies for Law Enforcement and Forensic Purposes” in Aleš Završnik and Katja Simončič (eds.), *Artificial Intelligence, Social Harms and Human Rights* 35-54 (Springer International Publishing, Cham, 2023).

³¹ Saeed Al Ali, Ibrahim Al Shawabkeh, *et al.*, “Facial Recognition Technology: Protecting Biometric Privacy in the Digital Age” 18(2) *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction* 06526002 (2026).

principles enshrined in *Puttaswamy*. The United Kingdom has developed its approach through Article 8 ECHR, particularly in *Bridges* and, more recently, *Thompson and Carlo*. These cases together show that UK courts focus not only on whether LFR interferes with privacy, but also on whether the legal and policy framework sufficiently limits police discretion over deployment, watchlists and proportionality. Canada has relied on Section 8 of the Charter and the reasonable expectation of privacy, while South Africa combines Section 14 with statutory protection of biometric information.³²

South Africa has combined Section 14 with statutory protection of biometric information. These variations show that the protection afforded to privacy is not only a function of recognition of privacy but also of the legal standards and institutional controls that are imposed on the restriction of privacy. An important finding is that subsequent facial identification cannot, in itself, be treated as constitutionally valid merely because the face was visible in public. The linking of a facial image with an identifiable person through FRT adds a further layer of information and thereby gives greater constitutional significance to the subsequent use of that information.³³

This study also reveals that the legal authority and control over discretion is at the very heart of the constitutional evaluation of FRT. In areas where facial recognition is used for a legitimate law-enforcement purpose, such as law enforcement, when the powers of facial recognition are not sufficiently defined, there may still be a constitutional deficiency, *Bridges* shows. The same is true of India which has general constitutional guidelines but lacks specific guidelines for FRT. The Indian framework is well supported by the Constitution, but it is not well articulated with the technologies. This is not a lack of privacy protection, but a lack of clear rules around when, how and who can use facial recognition.

³² Abhinash Mohanta, Shyamantak Misra, *et al.*, "Judicial Activism in the Age of Artificial Intelligence: Safeguarding Fundamental Rights Amid Rapid Technological Evolution" in Iris-Panagiota Efthymiou and Konstantinos Kouroupis (eds.), *Legal and Regulatory Impacts on AI Development* 117-162 (IGI Global Scientific Publishing, Hershey, 2026).

³³ Sarabdeen, *supra* note 28.

IX. SUGGESTIONS

1. There should be a clear legal basis for the deployment of FRT. The use of facial recognition must be based on clear laws, not simply on wide administrative or policing powers. The legal regime should clearly define the uses of FRT and conditions for their use.
2. The extent to which it is allowed to be used should be specified. There should be a clear difference between the use of a camera for a specific investigative purpose and for broader identification of individuals in public areas. These differences would eliminate undue discretion and give a greater basis for constitutionality review.
3. Watchlists should be protected by specified safeguards. Inclusion and length of time on watchlists and removal of individuals from watchlists should be prescribed. The process should also ensure regular review to avoid inappropriate or extended identification.
4. Legal supervision should include accuracy and false identification. If an FRT match were to be a basis for police or other action, some type of verification should be required before the match is considered adequate evidence for further action. Using automatic matches alone cannot be the basis of the determination of legal status.
5. Retention and deletion rules should be specified. Any facial biometric information not necessary for the authorized use should not be maintained over an undue period. Retention periods, access, further use, deletion should be regulated by clear rules.
6. FRT deployment should be accompanied by independent oversight. Supervision is required to ensure that the laws that regulate its use are followed. Regular audits on deployment, safeguards and complaints would further promote accountability and minimise the risk of unchecked deployment.

7. Where the consequences of FRT are unequal or arbitrary, they should be considered meaningfully in Article 14. The question of constitutionality should not only be raised about privacy, but also regarding the way the technology of facial recognition is used, such as when it misidentifies people or if it performs differently for different people.

X. CONCLUSION

The study concludes that Article 14 and Article 21 of the Constitution of India afford privacy rights to the use of Facial Recognition Technology for identification of facial information. The main constitutional law points are found in *Justice K.S. Puttaswamy (Retd.) vs Union of India*, which involved the recognition of informational autonomy and privacy, as well as the demand for legality and proportionality. Therefore, the constitutionality of FRT is not only based on the acquisition of a photo of their face, but more importantly on what happens after that image is acquired, that is, the processing of that information in order to identify an individual.

The comparative analysis shows how the jurisdictions studied approach privacy protection. The United Kingdom, in the case of Article 8 and *ECHR v. R (Bridges) v. Chief Constable of South Wales Police*, is especially concerned with the "control of discretion" and "legal certainty". Both countries address the question differently, Canada relies on Section 8 of the Canadian Charter, and the reasonable expectation of privacy, and South Africa is based on its constitutional protection of rights under Section 14, and statutory protection of biometric information under POPIA. These methods offer various types of protection, yet acknowledge the privacy concerns of technologically supported identification.

The Indian framework is thus very well entrenched in the constitution but is relatively underdeveloped in terms of its direct application to FRT. Unlike the United Kingdom, India does not yet have a decided judgment comparable to *Bridges* on the limits of FRT deployment and administrative discretion. However, the pending *A.A. Rahim M.P. v. Union of India* petition marks an important forward-looking development, as it brings a direct constitutional challenge to police use of facial recognition and biometric surveillance before the Supreme Court. The comparative analysis therefore shows that

a separate constitutional right to address FRT is not required; rather, existing constitutional standards must be applied with specificity to FRT's biometric, identification and surveillance functions.

The study finds that the constitutional regulation of FRT in India needs to be evaluated based on the interplay of the three requirements, namely legal authority, limitations, and proportionality and appropriate procedural safeguards. This would help to maintain the lawful applications of facial recognition while also preventing the scope of interferences of the right to privacy being determined by technology.

XI. REFERENCES

1. Al Ali, S., Al Shawabkeh, I., & Alqodsi, E. M. (2026). Facial recognition technology: Protecting biometric privacy in the digital age. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, 18(2), Article 06526002.
2. Amirgaliyev, B., Mussabek, M., Rakhimzhanova, T., & Zhumadillayeva, A. (2025). A review of machine learning and deep learning methods for person detection, tracking and identification, and face recognition with applications. *Sensors*, 25(5), Article 1410.
3. Aniulis, H. (2022). Facial recognition technology, privacy and administrative law. *University of New South Wales Law Journal*, 45(4), 1513–1549.
4. Basimanyane, D. (2022). The regulatory dilemma on mass communications surveillance and the digital right to privacy in Africa: The case of South Africa. *African Journal of International and Comparative Law*, 30(3), 361–382.
5. Bhandari, V., Kak, A., Parsheera, S., & Rahman, F. (2017). An analysis of Puttaswamy: The Supreme Court's privacy verdict. *IndraStra Global*, (11), Article 5.
6. Bindal, P., & Singh, R. (2026). Survival of right to privacy under administrative surveillance: A comparative legal study. *Journal of Humanities and Education Development*, 8(2), 29–40.

7. Bu, Q. (2021). The global governance on automated facial recognition (AFR): Ethical and legal opportunities and privacy challenges. *International Cybersecurity Law Review*, 2(1), 113–145.
8. Carpenter, C. (2020). Privacy and proportionality: Examining mass electronic surveillance under Article 8 and the Fourth Amendment. *International and Comparative Law Review*, 20(1), 27–57.
9. Constitution of the Republic of South Africa, 1996 (Act No. 108 of 1996).
10. Crookshanks, R. (2026). *Police surveillance and use of facial recognition technology: Charter issues, legal frameworks and oversight mechanisms* (Unpublished master's thesis). University of Saskatchewan, Saskatoon, Canada.
11. Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023) (India).
12. European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221, E.T.S. 5.
13. Faraldo Cabana, P. (2023). Technical and legal challenges of the use of automated facial recognition technologies for law enforcement and forensic purposes. In A. Završnik & K. Simončič (Eds.), *Artificial Intelligence, Social Harms and Human Rights* (pp. 35–54). Springer, Cham.
14. *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145 (Canada).
15. Information Technology Act, 2000 (Act No. 21 of 2000) (India).
16. Jochelson, R., & Ireland, D. (2019). *Privacy in peril: Hunter v Southam and the drift from reasonable search protections*. UBC Press.
17. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
18. Kiefer, L., Frank, J., Di Ruggiero, E., Dobbins, M., Manuel, D., Gully, P. R., & Mowat, D. (2005). Fostering evidence-based decision-making in Canada: Examining the need for a Canadian population and public health evidence centre and research network. *Canadian Journal of Public Health*, 96(3), I1–I19.

19. Laishram, L., Shaheryar, M., & Kumar, S. (2025). Toward a privacy-preserving face recognition system: A survey of leakages and solutions. *ACM Computing Surveys*, 57(6), 1–38.
20. Li, T. (2024). Bridges v South Wales Police and emerging privacy concerns. *Northern Ireland Legal Quarterly*, 75(4), 806–817.
21. Mohanta, A., Misra, S., & Gouda, S. (2026). Judicial activism in the age of artificial intelligence: Safeguarding fundamental rights amid rapid technological evolution. In I.-P. Efthymiou & K. Kouroupis (Eds.), *Legal and Regulatory Impacts on AI Development* (pp. 117–162). IGI Global Scientific Publishing.
22. Moreham, N. A. (2008). The right to respect for private life in the European Convention on Human Rights: A re-examination. *European Human Rights Law Review*, (1), 44–79.
23. Neethling, J. (2005). The concept of privacy in South African law. *South African Law Journal*, 122(1), 18–28.
24. Protection of Personal Information Act, 2013 (Act No. 4 of 2013) (South Africa).
25. R (Bridges) v. Chief Constable of South Wales Police, [2020] EWCA Civ 1058 (United Kingdom).
26. R. v. Spencer, [2014] 2 S.C.R. 212 (Canada).
27. Raposo, V. L. (2023). 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.
28. Sarabdeen, J. (2022). Protection of the rights of the individual when using facial recognition technology. *Heliyon*, 8(3), Article e09086.
29. Satyanarayana, P. (2025). KS Puttaswamy v. Union of India to data protection: The evolution of privacy jurisprudence in India. *Anusandhanvallari*, 4562–4567.
30. Shruthi, B. (2024). Facial recognition technology (FRT) and privacy: A delicate balance. *International Journal of Legal Science and Innovation*, 6(6), 291–304.

31. Sikri, A. K. (2021). Proportionality – A balancing act for achieving constitutional rights: A comparative study. In M. P. Singh et al. (Eds.), *The Indian Yearbook of Comparative Law 2019* (pp. 111–129). Springer, Singapore.
32. Staunton, C., Adams, R., Botes, M., Dove, E. S., Horn, L., Labuschaigne, M., ... & de Vries, J. (2020). Protection of Personal Information Act 2013 and data protection for health research in South Africa. *International Data Privacy Law*, 10(2), 160–179.
33. Tinna, N. (2026). *Judicial cognitive legitimacy and the constitutional limits of AI-assisted adjudication: Beyond explainability, human oversight, and algorithmic authority* (Working Paper).
34. Trykhlil, K. (2020). The principle of proportionality in the jurisprudence of the European Court of Human Rights. *EU and Comparative Law Issues and Challenges Series (ECLIC)*, 4, 128–154.
35. Zimmerman, H. (2017). The data of you: Regulating private industry's collection of biometric information. *University of Kansas Law Review*, 66(3), 637–664.