International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Balancing Aviation Security and the Right to Privacy

Mahima Jose

Student, Amity University

Abstract

Civil aviation is one of the most security-sensitive domains of contemporary governance. A single security lapse may result in mass casualties, panic, economic disruption, and lasting diplomatic consequences. For that reason, airports and airlines function within an unusually dense network of screening rules, identity checks, intelligence-sharing practices, and passenger-data systems. Yet the same measures that make aviation safer also interfere with privacy, bodily dignity, and informational autonomy. The core issue is therefore not whether aviation security is necessary, but how it should be structured in a constitutional democracy so that security does not become a standing justification for intrusive surveillance.1

This paper argues that aviation security and privacy should not be treated as mutually exclusive values. Privacy does not disable the state from protecting civil aviation; rather, it requires the state to act through clear law, limited means, and accountable procedures. The paper focuses on three areas where the conflict is most visible: passenger-data systems such as Advance Passenger Information and Passenger Name Record regimes, physical screening technologies such as body scanners, and biometric systems such as facial-recognition verification. It concludes that the most defensible model is one based on legality, necessity, proportionality, data minimization, transparency, and human oversight.2

Keywords: aviation security, privacy, PNR, biometrics, surveillance, proportionality

Introduction

Aviation has occupied a special place in security policy because aircraft and airports compress mobility, infrastructure, and vulnerability into one highly visible space. A breach in civil aviation rarely remains local. It can disrupt routes across jurisdictions, trigger international alerts, affect tourism and trade, and produce political pressure for rapid legal response. This explains why modern aviation governance has moved well beyond physical baggage checks. Contemporary systems now include pre-travel vetting, watchlist matching, document authentication, behavioral monitoring, API and PNR transfer, and increasingly biometric verification.3

At the same time, the airport is not a rights-free zone. Travelers disclose identity documents, itineraries, payment details, contact information, and at times their fingerprints or facial images. In a practical sense, aviation security today examines not only what a passenger carries, but also who the passenger is, how

1Universal Declaration of Human Rights, art. 12; International Covenant on Civil and Political Rights, art. 17.
2Justice K.S. Puttaswamy v Union of India, (2017) 10 SCC 1; Charter of Fundamental Rights of the European Union, arts. 7–8.
3 ICAO, Facilitation Manual, ch. 9, Passenger Data Exchange Systems (2026); ICAO, Interactive API Best Practice (2024).

the journey was booked, and whether the person fits a risk profile constructed by state systems. The legal concern is that exceptional measures introduced for aviation may become normalized and then copied into broader border and policing practices.

The right to privacy is important in this field for two reasons. First, privacy protects bodily dignity and personal autonomy against unjustified exposure. Second, it protects informational self-determination in an age when travel systems generate large amounts of personal data. The question is therefore not whether privacy survives in airports, but how far it can be limited without collapsing into permanent administrative surveillance. A lawful balance must show more than good intentions. It must show a valid legal basis, a legitimate aim, a tight relationship between means and ends, and effective safeguards against abuse.

I. The Security Imperative in Civil Aviation

No serious discussion of aviation law can deny that civil aviation requires strong security measures. Airports handle large numbers of passengers in compressed timeframes; they connect multiple jurisdictions; and they remain attractive targets for terrorism, trafficking, organized crime, sabotage, and identity fraud. Preventive security therefore has a rational foundation. States do not wait for a prohibited item or violent act to appear at the checkpoint; they increasingly try to identify risk before the passenger boards.4

This preventive orientation also explains the growth of information-led security. A passenger may pass through a metal detector and still present concern if the booking pattern, itinerary, or identity record suggests a connection with unlawful activity. Authorities therefore defend API and PNR systems as tools that permit earlier decision-making. From an operational point of view, this is sensible. The problem arises when the logic of prevention becomes limitless. A legal system committed to rights cannot accept the proposition that every additional data point or every new scanning technology is automatically justified simply because aviation is sensitive.

In that sense, the real legal challenge is not whether security matters, but how security is bounded. A democratic system may allow intensive screening in airports, but it still has to ask whether the measure is authorized by law, whether it is necessary in the relevant threat context, whether a less intrusive alternative is available, and whether there are safeguards for error, misuse, and discriminatory impact. The stronger the security claim, the stronger the duty to justify it.

II. Legal Provisions and Judicial Standards

The privacy baseline in this debate comes from both international human rights law and domestic constitutional law. At the international level, Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights protect persons against arbitrary or unlawful interference with privacy. In Europe, Article 8 of the European Convention on Human Rights and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union provide a particularly important framework because they separate respect for private life from the protection of personal data.5

4ICAO security practice treats pre-departure vetting and passenger-data exchange as core tools of preventive aviation security.

5European Convention on Human Rights, art. 8; Charter of Fundamental Rights of the European Union, arts. 7–8.

In India, the clearest constitutional statement is the nine-judge decision in Justice K.S. Puttaswamy v Union of India, where the Supreme Court recognized privacy as a fundamental right connected to dignity, liberty, autonomy, and control over personal information. That judgment matters in aviation not because it speaks directly about airports, but because it explains why informational privacy deserves protection even when the state claims administrative necessity. A traveler does not lose constitutional personality merely by entering a regulated transport hub.6

The second major step is proportionality. In the Aadhaar decision, the Supreme Court accepted that the state may pursue legitimate goals through data systems, but insisted that legality, legitimate state aim, rational connection, necessity, and proportionality remain central to constitutional review. This proportionality approach is especially useful in aviation law because it allows security interests to be taken seriously without allowing them to become self-proving. A measure may be useful in some abstract sense and still fail because it is overbroad, indefinite, weakly supervised, or more invasive than the threat actually requires.7

European case law moves in a similar direction. The Strasbourg Court has repeatedly treated retention, search, and surveillance powers as privacy interferences that require strong legal safeguards. The most important lesson from that jurisprudence is that arbitrary powers are the real danger. Where state systems retain sensitive information for long periods, authorize suspicion-less interference on broad terms, or conceal the scope of surveillance from the public, privacy protection becomes fragile even if the official purpose is security.

III. Passenger-Data Systems: API, PNR, and Predictive Security

Passenger-data systems create the sharpest tension between aviation security and privacy because they operate at scale and often before the traveler reaches the airport. API is usually derived from travel document information and transmitted for border-control purposes. PNR is broader and can include itinerary details, contact information, baggage information, payment method, travel agency data, and other booking-related elements. When combined with watchlists and risk rules, these datasets allow states to assess passengers in advance.8

The privacy concern is obvious. PNR data can reveal patterns of movement, associations, and inferred behavior. Even when each data point appears innocuous in isolation, aggregation changes its significance. A system capable of mapping repeated routes, one-way travel, last-minute bookings, or linked reservations can generate a detailed profile of ordinary life. That is why the legal design of passenger-data regimes matters so much. The issue is not only collection but also purpose limitation, filtering, retention, onward transfer, and the human review of automated matches.

The European PNR Directive is an important example of an attempt to strike this balance through legislation. It allows PNR processing for the prevention, detection, investigation, and prosecution of terrorist offences and serious crime, but it also places structural limits on use. The Directive restricts sensitive data processing, requires masking after an initial period, regulates retention, requires Passenger Information Units and data-protection oversight, and obliges information to be given to passengers.

6Justice K.S. Puttaswamy v Union of India, (2017) 10 SCC 1 (privacy recognized as a fundamental right tied to dignity and autonomy).
7Justice K.S. Puttaswamy (Aadhaar-5J) v Union of India, (2019) 1 SCC 1, judgment dated 26 Sept. 2018, applying legality and proportionality review.
8ICAO, Guidelines on Passenger Name Record (PNR) Data, Doc 9944 (2010), explaining the breadth of PNR data elements.

These features show that even a security-heavy regime accepts that data governance cannot be open-ended.9

Judicial scrutiny has further tightened these limits. In Opinion 1/15 on the proposed EU-Canada PNR Agreement, the Court of Justice of the European Union made it clear that broad international PNR transfer is not acceptable unless the receiving framework satisfies strict standards of necessity and data protection. Later, in Ligue des droits humains, the Court upheld the possibility of PNR processing only by reading the Directive narrowly and stressing that the regime cannot become a generalized system of predictive surveillance detached from terrorism or serious crime. The message is important: PNR may be permitted, but indiscriminate or self-expanding PNR is not.1011

ICAO guidance points in the same general direction, even from within a security-centered institutional environment. Its guidance stresses relevance, the preference for the push method of data transfer, and the need for privacy and data-protection safeguards when passenger information is exchanged. This matters because aviation governance is often described as technically necessary and therefore politically neutral. In reality, technical design choices determine the depth of privacy intrusion. A narrow data architecture is not a minor procedural choice; it is a substantive rights safeguard.12

IV. Physical Screening and Bodily Privacy

If passenger-data systems implicate informational privacy, body screening raises the question of bodily dignity more directly. Security scanners, pat-downs, secondary inspection, and private screening procedures all involve degrees of physical or visual exposure. Travelers may accept these procedures as part of air travel, but acceptance should not be confused with consent in a legal sense. The person is often complying because refusal may mean delay, missed travel, or exclusion from the flight.

European rules on airport security scanners are instructive because they attempt to reduce unnecessary humiliation. The official framework allows the use of scanners only under specific conditions: images may not be stored, copied, printed, or retrieved; unauthorized access must be prevented; faces should not be visible to the remote reviewer; passengers may request a reviewer of a chosen gender; and there must be an alternative screening method for those who opt out. These are not cosmetic safeguards. They show that bodily screening can be designed more narrowly when the state takes dignity seriously.13

Case law also illustrates why restraint matters. In S. and Marper v United Kingdom, the European Court of Human Rights treated the retention of fingerprints and DNA profiles of persons not convicted as a serious privacy issue, making clear that biometric data are not administratively trivial. Likewise, in Gillan and Quinton v United Kingdom, the Court held that broad stop-and-search powers violated Article 8 because of the risk of arbitrariness and abuse. Although neither case arose from airport screening in the strict sense, both are highly relevant: they show that suspicion-less security powers are most vulnerable when they are generalized and weakly constrained.1415

9Directive (EU) 2016/681, arts. 1, 6, 12 and 13.
10Ligue des droits humains v Conseil des ministres, Case C-817/19, EU:C:2022:491.
11Opinion 1/15, EU-Canada PNR Agreement, EU:C:2017:592.
12ICAO, Doc 9944, emphasizing necessity, relevance, the push method of transfer, and transparency to passengers.
13European Commission, Aviation Security Policy: Security Scanners, requiring non-storage of images and an alternative screening option.
14Gillan and Quinton v United Kingdom (2010) 50 EHRR 45.
15S. and Marper v United Kingdom (2008) 48 EHRR 50.

V. Biometrics, Facial Recognition, and Function Creep

Biometric identification is now presented as the future of seamless travel. In theory, one-to-one facial verification can reduce queue time, improve document matching, and make identity fraud harder. From the perspective of airport operators and border agencies, this seems like an ideal combination of efficiency and security. Yet biometrics create a deeper privacy issue than conventional ID checks because the body itself becomes the credential. Once faces or templates are captured, the danger is not only misidentification, but function creep: a system introduced for boarding may later be connected to broader law-enforcement or migration databases.

American materials on airport facial comparison commonly emphasize that participation is voluntary and that passengers may opt for manual identity verification instead. That opt-out matters, but it is not sufficient by itself. A genuine balance requires more than formal choice. The non-biometric route must be practical, non-stigmatizing, and available without penalty. Otherwise, consent becomes largely fictional.16

Data-protection law helps define the minimum safeguards. Under the GDPR, personal data must be processed lawfully, fairly, and transparently; collection must be limited to specified purposes; data must be adequate, relevant, and limited to what is necessary; and special categories of data, including biometric data used to uniquely identify a person, require stricter treatment. Article 22 is also relevant because serious decisions should not rest exclusively on automated processing where the consequences for the individual are substantial. These principles are directly applicable to aviation biometrics. If a facial-recognition system stores templates longer than necessary, shares them too widely, or leaves no meaningful human review, the privacy risk becomes structural rather than incidental.17

The practical lesson is that biometric aviation systems should be narrow by design. They should be limited to one-to-one verification, immediate deletion should be the default, independent accuracy audits should be required, and data use should not be silently expanded through interoperability. The convenience narrative surrounding facial recognition is powerful, but convenience is not a constitutional ground for permanent identity infrastructure.

VI. Toward a Rights-Based Balancing Model

The best way to balance aviation security and privacy is to reject two easy but unhelpful positions. The first says that privacy must simply yield whenever security is invoked. The second says that aviation surveillance is inherently illegitimate. Neither position is convincing. Aviation does require exceptional precautions, but exceptional precautions must remain exceptional in legal method as well. The correct question is not whether the state may act, but under what conditions it may act.

A workable model should rest on six principles. First, legality: every intrusive security measure must have a clear and accessible legal basis. Second, legitimate aim: the measure must address a real aviation-security objective. Third, necessity: the state should show that less intrusive options would not achieve the same purpose effectively. Fourth, proportionality: the intensity of intrusion must be justified by the seriousness and likelihood of the threat. Fifth, accountability: systems require oversight, audit, and complaint mechanisms. Sixth, minimization: the state should collect and retain no more than is genuinely needed.

16Transportation Security Administration, Facial Comparison Technology Factsheet; US DHS, Privacy Impact Assessment for TSA facial-recognition use.
17Regulation (EU) 2016/679 (GDPR), arts. 5, 6, 9 and 22.

This model is not abstract theory. It follows from the structure of the cases discussed above. Puttaswamy rejects unbounded data extraction. S. and Marper rejects indefinite retention of highly personal identifiers. Gillan and Quinton warns against uncontrolled discretion. Opinion 1/15 and Ligue des droits humains reject indiscriminate passenger-data transfer. Big Brother Watch, although decided in the context of communications surveillance, reinforces a wider point that secret or bulk systems must be surrounded by clear law, independent supervision, and post-facto accountability if they are to remain compatible with democratic rights standards.18

There is also a practical reason for preferring a rights-based model: overbroad systems often perform badly. They collect excessive data, produce false positives, and dilute institutional focus. By contrast, a system designed around relevance, reviewability, and limited retention is not only more lawful but often more operationally precise. Privacy and security therefore need not be enemies. Properly understood, privacy disciplines security so that security can remain effective without becoming arbitrary.

Conclusion

The conflict between aviation security and privacy is real, but it is frequently overstated as a choice between safety and rights. That framing is misleading. The real issue is how a legal order should design security powers in a domain where risk is undeniable but where intrusive technologies are increasingly normalized. Passenger-data systems, body scanners, and facial recognition all serve identifiable security aims, yet each also threatens to widen the routine reach of state observation.19

The better view is that privacy is not an obstacle to aviation security. It is the framework that requires aviation measures to remain lawful, limited, and reviewable. Once that point is accepted, the balance becomes easier to state. States may secure civil aviation vigorously, but they must do so through clear law, careful tailoring, short retention, transparency where possible, human review, and effective remedies. In that sense, privacy does not weaken aviation security. It prevents aviation security from becoming a permanent excuse for disproportionate surveillance.20

18Big Brother Watch and Others v United Kingdom [GC], Apps 58170/13, 62322/14 and 24960/15, judgment of 25 May 2021.

19GDPR art. 22 and comparable constitutional proportionality standards require meaningful human review where decisions significantly affect the traveler.

20ICAO, Interactive API Best Practice (2024), stresses a clear legal basis and privacy-compliant design when passenger data are used for boarding-control decisions.