CyberPeace

CISF'S PROPOSED FACIAL RECOGNITION NETWORK

BALANCING AIRPORT SECURITY MODERNISATION WITH PRIVACY AND CIVIL LIBERTIES

SAFEGUARDS IN INDIA

STRENGTHENING AIRPORT SECURITY

PRIVACY BY DESIGN

PROTECTING CIVIL LIBERTIES

BUILDING PUBLIC TRUST

EXECUTIVE SUMMARY

In June 2026, the **Central Industrial Security Force (CISF)** announced plans to establish a centralised Data Fusion Centre in Delhi that would integrate facial recognition cameras at major Indian airports with the **National Intelligence Grid (NATGRID)**, enabling real-time identification of suspects and fugitives against government and potentially, private databases.CISF Director General Praveer Ranjan announced the proposal at the foundation-laying ceremony for the force's new headquarters, stating that a data fusion centre is proposed to be set up in Delhi and that facial recognition systems across major airports are under consideration with the concerned ministries. If implemented, the project could bring together feeds from nearly 150,000 CCTV cameras operating at airports, metro systems, ports, power facilities and government installations under CISF protection.

This white paper examines the initiative through the lens of India's constitutional privacy jurisprudence, its evolving data protection framework, comparative international practice, and prevailing cybersecurity and technical risk considerations. It does not adopt a political position on the desirability of the initiative; rather, it maps the legal terrain, identifies risks that any responsible implementation must address, and proposes a governance architecture that could allow India to pursue legitimate security objectives while remaining faithful to the constitutional guarantees articulated in **Justice K.S. Puttaswamy v. Union of India**. The central finding is that the proposal, as currently described, sits in a regulatory vacuum: it lacks a dedicated statutory basis, operates alongside a NATGRID architecture that itself has never been placed on a legislative footing, and would be substantially exempted from India's new data protection law by virtue of broad state-security carve-outs. Closing this gap through legislation, independent oversight, and technical safeguards is the central policy challenge this paper addresses.

1. BACKGROUND OF THE PROPOSED INITIATIVE

1.1 THE ANNOUNCEMENT AND ITS SCOPE

CISF has proposed a Delhi data fusion centre linking facial recognition cameras at six major airports of Delhi, Mumbai, Bengaluru, Hyderabad, Chennai, and Kolkata with NATGRID, aiming to boost real-time monitoring, suspect identification and support for law enforcement, while integrating 1.5 lakh CCTV. Reports on the precise scope diverge: the Hindu reported that authorities propose linking six major airports with NATGRID, while the Hindustan Times reported that CISF has sought permission for at least four airports Delhi, Bengaluru, Chennai, and Kolkata. Officials indicated that cameras would be positioned at key choke points such as entry and exit gates, rather than across all camera feeds, with data feeding into the Integrated Command and Control Centre (ICC) and cross-checked against NATGRID. As of the announcement, installations had not yet begun.

1.2 STATED OBJECTIVES

The stated purpose is narrow and security-oriented: the stated aim is to help identify fugitives and suspects in real time, and a CISF official described the integration as intended to strengthen "real-time monitoring, suspect identification and support to law enforcement agencies". The initiative sits within a broader modernisation push: Ranjan simultaneously announced a regional Centre of Excellence for drone and anti-drone technologies in Behror, Rajasthan .CISF's designation as the nodal agency for critical infrastructure drone defence, and specialised cyber security training in collaboration with technical institutions. The force secures 359 units at over 70 civil airports and a dozen major seaports, with plans to extend coverage to more of India's roughly 250 ports.

1.3 DISTINGUISHING THIS INITIATIVE FROM EXISTING BIOMETRIC SYSTEMS

It is important to distinguish the CISF proposal from two existing biometric deployments at Indian airports, since conflating them obscures the novel risk this initiative introduces:

Digi Yatra is a voluntary, passenger-facing convenience system operated by the Digi Yatra Foundation (DYF), a Section 8 not-for-profit company under the Companies Act, 2013, in which the Airports Authority of India holds a 26% stake while private airport operators hold the remainder. India already uses biometric systems at airports through Digi Yatra, which allows passengers to pass through checkpoints using facial recognition instead of physical documents; the CISF proposal, by contrast, goes beyond passenger convenience and places facial recognition within a law enforcement and intelligence framework.

The National Automated Facial Recognition System (NAFRS/AFRS), run by the National Crime Records Bureau (NCRB), is used to track criminals, identify the deceased and locate missing persons; Delhi Police have previously used AFRS during public order operations, drawing criticism from digital rights groups including the Internet Freedom Foundation over risks to civil liberties and mass surveillance.

The CISF Data Fusion Centre proposal is distinct in kind from both: it would connect a specific, high-thoroughput public chokepoint (airports) directly into a national intelligence-sharing backbone, for law-enforcement identification purposes, without passenger consent (as is inherent in Digi Yatra) and, unlike AFRS, with live real-time matching rather than post-hoc investigative queries.

1.4 NATGRID: THE ARCHITECTURE BEING INTEGRATED INTO

Understanding NATGRID is essential because it is not merely the airport cameras, it is the terminus of the biometric feed and the source of much of the paper's regulatory concern.

NATGRID is not just an airport security tool; it is a central intelligence platform created after the 26/11 Mumbai attacks to give authorised agencies quick access to government and private databases. Through the platform, authorised agencies can obtain information related to vehicle registrations, driving licences, Aadhaar records, banking data, airline travel details, FAST transactions, passport information, railway passenger records, and financial intelligence reports, and it also supports analysis of publicly available digital and social media information where legally permitted. NATGRID is a middleware platform allowing eleven central agencies to query databases across roughly 21 categories; it was cleared in 2012 by executive order and Cabinet Committee on Security decision, not through Parliament.

Recent expansion is directly relevant to any proportionality analysis of the CISF proposal:

- In December 2025, NATGRID was linked to the National Population Register, which contains family-wise details of 119 crore residents; the platform was also reported to be receiving around 45,000 requests a month.
- Access, once the preserve of central intelligence and investigative agencies, is being widely to police units down to the rank of Superintendent of Police, and a new analytical engine ("Gandiva") reportedly provides entity resolution and facial recognition capability, moving NATGRID from a query tool toward predictive, inferential surveillance.
- In February 2026, the Enforcement Directorate asked its zonal heads to increase use of NATGRID and FINnet while pursuing a target of 500 prosecution complaints.

2. Existing Legal and Regulatory Framework

2.1 The absence of a dedicated statute for facial recognition or Natgrid

No standalone Indian statute presently regulates the collection, use, retention, or sharing of facial biometric data by security agencies. Two long-running controversies illustrate the resulting legal uncertainty:

NO DEDICATED STATUTE

- NATGRID's legal basis. NATGRID was cleared not through an Act of Parliament but by executive order and the Cabinet Committee on Security, with a first-phase allocation of ₹1,002.97 crore. The constitutional question is not whether the state may ever conduct surveillance, but whether a project of this magnitude can operate without a statutory framework and independent oversight. Its oversight is confined to internal audit processes, with no external watchdog or judicial safeguard explicitly mandated, and even the Puttaswamy judgment has left gaps in the statutory underpinnings of intelligence programmes like NATGRID, which continue to operate under executive orders. As PRS-legislative research, India observed contemporaneously with NATGRID's approval, establishing such a project through government notification rather than legislation deprives Parliament of the opportunity to debate the conditions under which private individual information may be accessed, what information may be accessed, and for what purpose

AFRRS LEGAL BASIS

- **Automated Facial Recognition System's (AFRRS) legal basis.** When the NCRB sought to justify its own facial recognition system, it learned legally in a 2009 Cabinet Note on the Crime and Criminal Tracking Network and Systems (CCTNS) predating the 2017 Puttaswamy judgment which the Internet Freedom Foundation argued in its rejoinder is "not a statutory enactment but a record of proceedings" and therefore cannot establish legality. The Personal Data Protection Bill then under deliberation carved out exemptions for government agencies, suggesting that even a future data protection law might not adequately restrain such systems. That position has proven largely accurate under the eventual DPP Act (see 2.3 below).

DIGI YATRA'S LEGAL BASIS

- **Digi Yatra's legal basis.** Even the passenger-facing, ostensibly consensual biometric system operating at Indian airports rests on uncertain legal footing. The Digi Yatra Biometric Boarding System (DYBSS), Delhi, which envisages the formation, composition, and data flows of the system, does not have the force of law, being unthethered to any legal framework. This has drawn severe judicial scrutiny: the Kerala High Court issued a formal notice in March 2026, questioning whether sensitive biometric information of millions of travellers is being processed without the mandatory oversight of a functional Data Protection Board of India, and the petitioner sought remedial directions to ensure passenger data is handled in strict compliance with the GDPR Act and Rules, while the court maintains till date government to confirm whether the Data Protection Board under Section 18 of the Act has in fact been constituted.

The consistent pattern: AFRRS, NATGRID, and Digi Yatra all proceeding not on the mandate of congressional footing, rather than statute means the CISF Data Fusion Centre would, absent a change of approach, become the fourth major biometric-surveyance initiative to launch without dedicated legislative authorisation.

2.2 THE CONSTITUTIONAL BASELINE: ARTICLE 21 AND THE RIGHT TO PRIVACY

In August 2017, a nine-judge bench of the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India unanimously held that the right to privacy is a fundamental right protected

under Article 21 and traceable also to Articles 14 and 19 of the Constitution. The Court held that invasion of privacy must occur through a fair, reasonable and just procedure, meeting three conditions: legality (existence of law), a legitimate state aim, and proportionality; legitimate state aims include national security, crime prevention and investigation, and prevention of dissipation of welfare benefits.

The proportionality standard was elaborated further in the Aadhaar judgment (Puttaswamy II, 2018–19), where a four-component proportionality test drawing on the jurisprudence of former Israeli Chief Justice Aharon Barak was applied by the majority:

- **(i) a legitimate goal**
- **(ii) suitability/rational connection between the measure and the goal**
- **(iii) necessity, requiring that no less-restrictive alternative achieve the same purpose**
- **(iv) a final balancing between the state's objective and the individual's right.**

Justice Chandrachud's dissent in the Aadhaar case is instructive for the CISF proposal precisely because it addressed suspicionless, population-scale biometric collection: he held that collecting identity information from every citizen without requiring the state to first form a reasonable belief that a particular individual might be committing a crime or fraud rendered the programme "completely disproportionate to the objective sought to be achieved".

This is directly germane to airport FRC deployment. Passengers moving through entry/exit gates are not, by virtue of travelling, individually suspected of any offence; matching their faces against a national suspect database in real time raises the same "presumption of criminality" concern Chandrachud J. identified. Any legal defence of the CISF scheme would need to demonstrate that scanning is confined to defined chokepoints, that watchlists are narrowly and transparently constructed, and that less intrusive alternatives (e.g., targeted deployment based on specific intelligence, alerts rather than continuous scanning) were considered and found inadequate the "necessity" prong of the *Puttaswamy* test.

2.3 The Digital Personal Data Protection Act, 2023 and its State-Security Exemptions

India's first comprehensive data protection statute, the Digital Personal Data Protection Act (DPPD Act), was enacted in August 2023, following the Supreme Court's 2017 recognition of the fundamental right to privacy in Puttaswamy, but was not operationalised until the Ministry of Electronics and Information Technology notified the DPPD Rules 2025 on 13 November 2025. Implementation is phased: the substantive compliance obligations for most Data Fiduciaries only become effective from 13 May 2027, meaning the older IT Act privacy rules continue to govern in the interim.

TWO FEATURES OF THE ACT ARE DECISIVE FOR THE CISF PROPOSAL:

Section 17 ex temptions. The central government may exempt government agencies from the ACT's provisions on grounds including security of the state, public order, and prevention of offences; where notice regarding the nature and purpose of data collection is not required, it may be argued a data principal cannot meaningfully consent. The Act grants wide exemptions to government bodies for activities related to national security, public order, foreign relations, and crime prevention, and these processing purposes need only be formally notified to the government not to the public or the affected individuals. The exemption provisions are formally required to meet the Puttaswami proportionality test (legality, legitimate aim, proportionality), and exemptions are meant to be "narrowly tailored," but the statute leaves the government wide discretion in defining what counts as necessary for these purposes.

Absence of a special category for sensitive/biometric data. Unlike the GDPR, the GDPR does not recognise special categories of personal data such as biometric, racial, or health data that receive enhanced protection, and does not impose additional requirements for entities handling sensitive personal data. This means facial biometric data collected at airports would, under Indian law, receive no more statutory protection than an email address, notwithstanding its irrevocable and uniquely identifying character.

No Section 17(4) (5) requirement of independent authorisation. Section 17(4) relaxes obligations for State processing not direct of decisions affecting a specific data principal, and Section 17(5) allows government to exempt entire classes of Data Fiduciaries from any provision of the Act for up to five years by notification a mechanism that could, in principle, be used to exempt the CISF/NATGRID data fusion architecture wholesale.

The upshot is that even once the GDPR Act is fully in force, the CISF facial recognition network would very likely qualify for exemption from most of its substantive obligations including purpose limitation, storage limitation, and notice by virtue of falling within the "security of the state" and ‘prevention of offences’ categories. This is not unique to India: comparable government/national-security carve-outs also exist in the UK’s Data Protection Act 2018, discussed in Section 6. The distinguishing weakness in the Indian case is that, unlike the UK (where a warrant and judicial approval regime under the investigative Powers Act 2016 constrains bulk government data use, see Section 6.1). India does not have any equivalent legal framework specifically regulating bulk processing of personal data by government agencies for intelligence and law enforcement activities.

2.4 SURVEILLANCE AND INTERCEPTION LAW PREDATING THE DPD ACT

Independent of data protection law, older surveillance statutes remain relevant background:

- **The Indian Telegraph Act, 1885** permits interception "in the interest of the sovereignty and integrity of India... security of the State... public order," and is cited as part of the legal architecture within which programmes like NATGRID are said to operate, though NATGRID is not itself created under this Act.

- **The Information Technology Act, 2000** and its associated 2011 Sensitive Personal Data Rules formed the primary data protection framework prior to the DPDP Act and will continue to apply until the DPDP Act's substantive provisions take full effect in May 2027.

Neither statute was drafted with facial recognition or biometric data-fusion architectures in mind, and neither provides a judicial-warrant mechanism analogous to the UK's Investigatory Powers Act for authorising bulk biometric matching against a national grid.

3. PRIVACY IMPLICATIONS OF CENTRALISED BIOMETRIC SURVEILLANCE

3.1 PROPORTIONALITY AND NECESSITY

Applying the *Puttaswamy/Aadhaar four-part proportionality* framework to the CISF proposal:

- **Legitimate goal:** Identifying fugitives and terror suspects at high-throughput national infrastructure is an ambiguously legitimate state aim, particularly given CISF's mandate over critical infrastructure protection.
- **Suitability:** Facial recognition is a rational means of achieving this goal, though its rational connection is qualified by the accuracy limitations discussed in Section 4.
- **Necessity:** This is the weakest link. The government has not published, nor do public reports suggest, an assessment of whether the same objective (identifying a defined, relatively small watchlist of fugitives and suspects) could be achieved through less invasive means for example, targeted deployment triggered by specific intelligence, rather than continuous, blanket capture of every passenger's face at entry/exit points. Officials have indicated cameras may be confined to entry/exit "hoke points" rather than all camera feeds, which is a proportionality—reducing design choice, but this remains an operational assurance rather than a binding legal limitation.
- **Balancing:** The scale of the underlying database approximately 150,000 CCTV feeds across airports and other critical infrastructure, feeding into a platform now linked to the 119-crore-person National Population Register means the balancing exercise is not confined to a bounded, purpose-specific dataset but to a near-universal population register. This materially shifts the balance away from the individualised suspicion model contemplated by the Court's proportionality jurisprudence.

3.2 PURPOSE LIMITATION AND FUNCTION CREEP

The single most significant privacy risk identified across all comparative and domestic experience is *function creep* the expansion of a system's use beyond its original, narrowly stated purpose. Civil society analysis of the NCRB's earlier AFRS tender warned that the introduction of ambiguous "N:N combination search" capabilities without clarity on their intended use case creates the possibility of function creep, since vagueness in purpose allows a system's actual use to drift from its stated justification.

NATGRID's own history is the clearest domestic illustration of this dynamic: conceived narrowly for post-26/11 counterterrorism coordination, it has since been linked to the National Population Register, opened to police at the rank of Superintendent of Police, and equipped with a facial recognition-capable analytical engine moving the platform "from tracking discrete events as intelligence inputs to mapping every Indian citizen".

recognition feed originally justified as a tool to spot a defined list of fugitives at airports could, once connected to this architecture, plausibly be repurposed for broader population monitoring, protest surveillance, or routine law enforcement uses considerably more intrusive than the stated objective. Delhi Police's earlier use of AFRS during the 2019 riots investigations, which drew criticism from digital rights groups over risks to speech, assembly, and political participation, illustrates that this is not a hypothetical concern in the Indian context.

3.3 DATA MINIMISATION, RETENTION, AND TRANSPARENCY

No public information specifies: (i) how long facial images and match data captured at airports would be required; (ii) whether images of non-matched individuals (the overwhelming majority of travellers) are discarded immediately or retained for training, audit, or future matching; (iii) whether independent audit logs record every query made against the fused database, or (iv) what mechanisms exist for an individual to learn whether their data was captured, matched, or shared, and to seek correction or deletion.

This absence of published retention and transparency policy mirrors the NCRB's earlier posture: the NCRB stated there would "not be proportionality/safeguards" in response to concerns about unchecked surveillance and lack of legal framework for informational privacy, and did not clarify how long CCTV-derived images of non-suspects would be retained. It contrasts unfavourably with disclosed practice in comparable systems abroad:

the UK Home Secretary stated that non-matching live facial recognition images are deleted within 0.2 seconds, and the US CBP discards US citizens' photos within 12 hours of identity verification, while non-citizen images are retained in the DHS Biometric Identity Management System for up to 75 years itself contested, but at least publicly documented.

3.4 Accountability and Oversight Gaps

NATGRID's oversight is presently confined to internal audit processes, with no external watchdog or judicial safeguard explicitly mandated. No independent regulator equivalent to the UK's Information Commissioner's Office or an equivalent to judicial pre-authorisation for bulk biometric searches (as under the UK's Investigatory Powers Act, discussed below) currently governs NATGRID or would, on present indications, govern the CISF Data Fusion Centre.

The Data Protection Board of India, created under the_dp Act, is empowered to receive and investigate complaints from data principals only after internal grievances redress is exhausted, and does not have general audit or licensing authority over government surveillance systems and, as the Kerala High Court proceedings on Digi Yatra reveal, its actual operational constitution remained uncertain as of March 2026.

4. CYBERSECURITY AND TECHNICAL VULNERABILITIES

4.1 Centralisation as a Single Point of Failure

A Data Fusion Centre that aggregates biometric feeds from six major airports, 150,000 CCTV cameras, and multiple national databases (Aadhaar, passport, banking, telecom, NPR) constitutes an extraordinarily high-value target. Centralisation, while operationally convenient, concentrates risk: a single breach could expose biometric identifiers of a very large share of India's air-travelling population alongside financial, residence, and travel history data drawn from linked databases. Unlike passwords, facial biometrics cannot be reset once compromised a point raised prominently in the US debate over expanding biometric entry-exit collection: members of the US Congress warned Homeland Security that biometric identifiers, once compromised, cannot be changed, making them permanently vulnerable to misuse or breach.

4.2Algorithmic Accuracy and Demographic Bias

Independent technical evaluation is unambiguous that facial recognition accuracy varies materially by algorithm, image quality, and critically demographic group. NIST's Face Recognition Vendor Test (FRVT) Part 3 found that the majority of algorithms tested exhibited demographic differentials: for one-to-one matching, false positive rates for Asian and African American faces were 10 to 100 times higher than for Caucasian faces in many algorithms, and for one-to many matching, the highest false positive rates occurred for African American women raising the risk of false accusions. Later NIST work refined this picture: false positive differentials were found to be widespread even in high-quality images, and varied by up to a factor of 7,203 across demographic groups for some algorithms, far exceeding the variation in

false negative rates. While NIST found that the most accurate algorithms show "undetectable" demographic differentials, and that government agencies including the FBI and CBP already use some of these higher-performing algorithms, this finding underscores that algorithm choice and independent testing not an assumption that "facial recognition is unbiased" must be a mandatory governance requirement, particularly given that CISF has not disclosed which vendor or algorithm it intends to deploy or whether NIST/FRVT-equivalent independent testing (of the kind the UK's National Physical Laboratory conducted for South Wales and Metropolitan Police algorithms) will be undertaken before deployment.

4.3 FALSE POSITIVES AND OPERATIONAL CONSEQUENCES

The consequence of a false positive in an airport identification context is not abstract. UK experience offers a instructive real-world data point: the National Physical Laboratory found an 89% chance of correctly identifying someone on a specific watchlist, alongside a worst-case 1 in–6,000 chance of a false alert against a 10,000-image watchlist and even with a well-regarded algorithm, documented misidentifications have included children in school uniforms being stopped, questioned, and required to provide fingerprints, and adult misidentification leading to wrongful detention. In the Indian airport context, where daily passenger volumes across six major hubs run into the hundreds of thousands, even a low false-positive rate could translate into a substantial absolute number of wrongful stops, detentions, or referrals for secondary screening with attendant reputational, logistical, and (for the affected individual) potential liberty consequences under CISF's law-enforcement mandate.

4.4 UNAUTHORISED ACCESS, INSIDER THREAT, AND DATA FUSION RISK

Because the Data Fusion Centre would aggregate access to a wide array of underlying government and (per the proposal's potentially private databases, the security architecture must guard not only against external breach but against unauthorised internal query i.e., agency personnel using the system for purposes (personal, political, commercial) beyond its authorised law enforcement mandate. The absence of any external audit mechanism for NATGRID access presently means such misuse would be difficult to detect

independently of internal reporting. India has documented instances of unauthorised access and leakage involving other centralised government databases and platforms (e.g., publicised concerns around the CoWin vaccination data leak referenced in civil society commentary on Digi Vatra as "a testament to the fact that data protection measures adopted by government[systems] "require closer scrutiny), underscoring that centralised architecture risk is not a merely theoretical concern in the Indian context.

4.5 IDENTITY THEFT AND DOWNSTREAM HARM

Because facial biometric templates, once created, are durable and cannot be revoked or reissued (" unlike a password or even, arguably, an Aadhaar number), a breach of the Data Fusion Centre's biometric store would create a permanent identity-theft exposure for every affected individual, magnified by the linkage to Aadhaar, passport, and financial records accessible through NATGRID.

5. CONSTITUTIONAL AND LEGAL CONSIDERATIONS

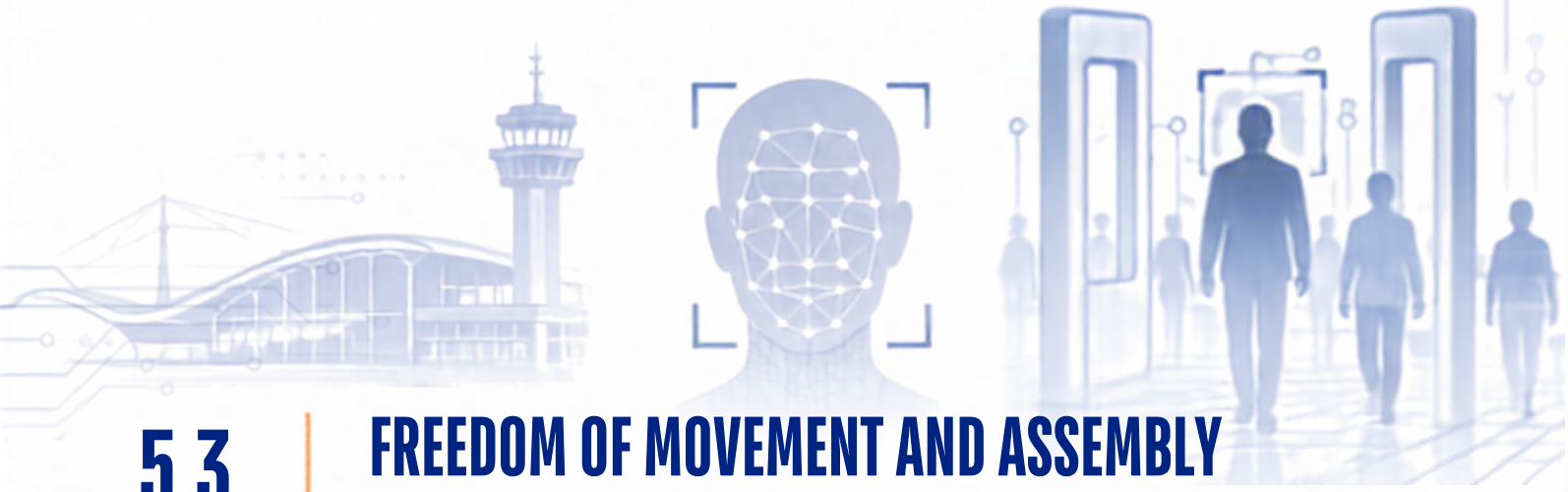
5.1 ARTICLE 21 AND THE LEGALITY REQUIREMENT

As established in Section 2.2, any restriction on privacy must satisfy legality the existence of "a defined regime of law." Civil society legal analysis of the NCRB's AFRS project concluded that, in the absence of any anchoring legislation regulating the use of facial recognition, the first requirement for lawful restriction on privacy legality was not met. The same analysis applies with equal, if not greater, force to the CISF proposal, given its explicit integration with NATGRID (itself lacking statutory basis) and its extension into a law-enforcement identification function considerably more intrusive than AFFRS's investigative/query model.

5.2 REASONABLE CLASSIFICATION AND ARTICLE 14

Legal commentary on AFFRS has argued that a system intended to screen every person passing through its purview rather than a defined, differentiated class of suspects fails a "reasonable classification" test under Article 14, since sweeping provisions targeting the entire population cannot be justified merely by reference to the goal of preventing crime, drawing on the

Aadhaar judgment's reasoning that mass, undifferentiated biometric collection is disproportionate absent individualised suspicion. Airport FRCs scanning all passengers at entry/exit gates rather than being triggered by specific intelligence about a particular flight, individual, or threat would face the same classification challenge unless the CISF architecture builds in meaningful ex ante targeting criteria.

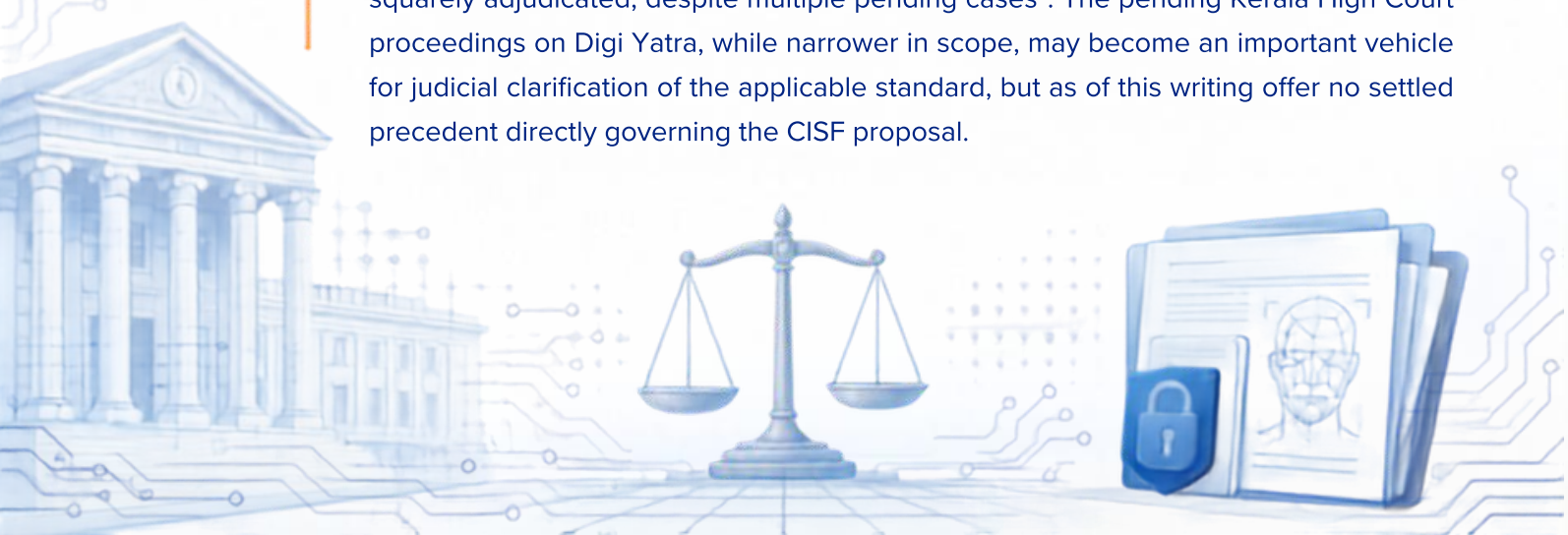


5.3 FREEDOM OF MOVEMENT AND ASSEMBLY (ARTICLES 19(1)(D) AND 19(1)(B))

Beyond Article 21, real-time biometric identification implicates the freedom of movement and, by extension (given the possibility of extending similar architecture beyond airports to other CISF-protected sites such as metros), freedom of peaceful assembly. Civil society submissions on AFRS specifically warned that use without safeguards could result in illegal state-sponsored mass surveillance with a chilling effect on freedom of expression, movement, and association, deterring individuals from exercising the fundamental right to protest through fear of identification and retaliation.

5.4 THE ABSENCE OF ADJUDICATED PRECEDENT ON NATGRID AND AIRPORT FRCS SPECIFICALLY

It bears emphasis that, unlike the UK's Bridges litigation (Section 6.1) or the extensive US EPIC litigation on CBP's biometric programme (Section 6.3), no Indian court has yet definitively adjudicated the legality of a real-time, live facial recognition deployment integrated with a national intelligence database. The legality of intelligence programmes lacking clear statutory foundation or meaningful oversight "has not been squarely adjudicated, despite multiple pending cases". The pending Kerala High Court proceedings on Digi Yatra, while narrower in scope, may become an important vehicle for judicial clarification of the applicable standard, but as of this writing offer no settled precedent directly governing the CISF proposal.



6. COMPARATIVE ANALYSIS

6.1 UNITED KINGDOM

The UK offers the most legally developed comparator, because live facial recognition (L/FR) by police has already been extensively litigated. In **R (Bridges) v Chief Constable of South Wales Police** [2020] EWCA Cv 1058, the Court of Appeal held that South Wales Police's use of L/FR was unfairful due to "fundamental deficiencies" in the legal and policy framework, amounting to a break of privacy, data protection and equality laws, because there were no clear limitations on where the software could be used or who could be placed on a watchlist, giving officers extraively the opportunity to freely access the data collected, without connecting with the legal framework's adequacy, not with the proportionality of the technology, as such as a distinction directly relevant to India, where the absence of any framework at all is a more fundamental deficiency than the one identified in Bridges.

Post-Bridges, UK practice evolved toward documented safeguards rather than prohibition: the College of Policing issued Authorised Professional Practice guidance defining permissible circumstances and watchlist categories, and the National Physical Laboratory independently tested the algorithm in current use, finding no statistically significant demographic performance differences at the settings deployed. The Information Commissioner's Office has been clear that facial recognition technology "does not operate in a legal vacuum," and has launched a rolling programme of police audits, with an Outcomes Report due in 2026. Nonetheless, civil liberties organisations continue to document expansion (a fleet of new L/FR vans, watchlists reported including people not suspected of wrongdoing, and children as young as 12 being scanned), alongside racial bias findings that led at least one force (Esssex Police) to cause up of the technology in 2026. **Lesson for India: a published legal framework, independent algorithmic testing, and an active regulator materially improved (though not eliminate) rights compliance but genuine improvement required years of litigation-driven pressure that India's current governance vacuum has not yet generated.**

6.2 EUROPEAN UNION

The EU's approach is the most restrictive among the comparators. The EU AI Act prohibits, among other practices, untargeted scraping of CCTV or internet material to build facial recognition databases, biometric categorisation to infer protected characteristics, and real-time remote biometric identification for law enforcement in publicly accessible spaces; these prohibitions took effect in February 2025. Real-time law enforcement use is not absolutely banned but is confined to three narrow objectives: searching for abduction or trafficking victims, preventing a specific, substantial and imminent threat to life or a terrorist attack, or identifying suspects of serious crimes carrying a sentence of at least four years, and even within those exceptions, deployment requires a completed fundamental rights impact assessment, registration in an EU database, and compliance with temporal, geographic and personal limitations set by enabling national law.

Separately, the Council of Europe's Convention 108+ Guidelines on Facial Recognition require explicit, specific, free and informed consent for use of facial recognition, hold that mere passage through a monitored space cannot constitute consent, and would prohibit private-sector identification uses for marketing purposes outright. **Lesson for India: the EU model demonstrates that a legislature can authorise narrowly defined, high-necessity law enforcement exceptions to a general prohibition, binding impact assessment and registration requirements a considerably more codified approach than India's current reliance on executive discretion and post-hoc data protection exceptions.**

6.3 UNITED STATES

US practice is comparatively permissive for non-citizens and border contexts but preserves an opt-out for citizens, backed by extensive public documentation. A December 2025 DHS final rule authorises CBP to collect facial biometrics from all non-citizens on entry and exit at airports, land ports, and seaports, removing prior exemptions for diplomat's, most Canadian visitors, and age-based limits; DHS has published more than ten Privacy Impact Assessments covering policies for collection, storage, retention and deletion. US citizens may opt out and undergo manual passport inspection instead, with their photos discarded within 12 hours, whereas non-citizen images are retained for up to 75 years in the DHS Biometric Identity Management System. Independent oversight bodies have flagged risks even within this documented framework: EPIC's senior counsel warned of "mission creep," particularly given efforts to connect datasets across government agencies, and oversight reports have previously criticised inadequate signage informing citizens of their right to opt out.

Lesson for India: even a system built on extensive published privacy documentation and differentiated citizen/non treatment faces persistent oversight criticism regarding opt-out enforceability and cross/database linkage concerns that would be magnified, not diminished, in a system (like the CISF proposal) offering no citizen opt out at all and explicitly designed for cross/database fusion.

6.4 SINGAPORE

Singapore illustrates the "convenience-first" model, distinguishable from CISF's security-first model but instructive on governance design. Changi Airport has fully implemented passport-free biometric clearance across all four terminals using facial and iris recognition, cutting average time to 10 seconds. Critically, this is consent-based and opt-in for enrolment: foreign travellers departing Singapore must first register biometric data (facial, iris, fingerprint) at manual counters before accessing passport-free clearance, and the enabling legislation was passed by Parliament: Singapore's Immigration Amendment Bill specifically enabled end-to-end biometric clearance, and Parliament members raised concerns about data privacy during the bill's passage, resulting in restrictions limiting IT contracts to Singapore companies, mandatory non-disclosure agreements and security screening for vendor staff, and encrypted data transport.

Lesson for India: Singapore's model shows that airport-scale biometric identity infrastructure can be built with parliamentary authorisation, vendor security vetting, and encryption commitments none of which currently attach to the CISF/NATGRID proposal, which would also differ in kind from Singapore's model by pairing biometric capture with a law-enforcement watchlist-matching function rather than pure identity verification for immigration clearance.

6.5 AUSTRALIA

Australia demonstrates the risks of governing biometric surveillance through executive rule-making rather than legislation, closely paralleling India's current posture. Parliamentary committees reviewing Australia's proposed national facial biometric matching capability and Identity-Matching Services Bills found the scheme had not been designed with privacy in mind, lacked adequate safeguards such as a warrant requirement before enforcement agencies could access the database, and would give the Home Affairs Minister a rule-making power to expand the biometric markers covered—potentially including gait or odour analysis without effective limits, extending even to identifying faces in crowds for "gathering intelligence" purposes. Separately, Australia's SmartGate system for one-to-one passport verification at airport arrivals is considered a comparatively low-risk, proportionate use because it is targeted, single-purpose, and replaces a manual check already routinely performed, illustrating a workable middle path. The Human Rights Law Centre and University

of Technology Sydney researchers have proposed a dedicated Model Law requiring impact assessments, oversight mechanisms, and prohibition of law-enforcement/intelligence use of FRT absent a minimum seriousness threshold alongside a recommended moratorium on such use pending legislative reform. **Lesson for India:** Australia's cautionary experience with unlegislated, ministerially-expandable biometric matching schemes closely mirrors the risk profile of NATGRID's executive-order basis, and its unsuccessful legislative attempt underscores that even mature democracies with robust human rights institutions have struggled to pass adequate statutory safeguards for exactly this category of infrastructure.

7. INTERNATIONAL STANDARDS AND GUIDANCE

Several bodies of international soft law and standards bear directly on the design of any Indian framework:

- **Council of Europe Convention 108+ Guidelines on Facial Recognition:** these guidelines note that integrating facial recognition into existing surveillance systems poses a serious risk to privacy and data protection precisely because such use often does not require the awareness or cooperation of the individual concerned, and require regular, periodic impact assessments, with referral to ethics committees and supervisory authorities where risk is identified.

- **UN High Commissioner for Human Rights:** UN guidance holds that domestic legal frameworks governing mass-surveillance tools must be grounded in necessity and proportionality, and that indiscriminate, untargeted surveillance particularly in the context of assemblies and peaceful protest should not be permitted.

- **nist (US):** while a technical standards body rather than a rights body, NIST's ongoing FRVT/FRTE programme and its proposed equity measures are being considered for incorporation into ISO/IEC 1975–10, an international standard on measurement and reporting of demographic effects in biometric systems providing a ready-made technical benchmark India could require of any vendor.

- **OECD Privacy Guidelines and AI Principles:** referenced by civil society (e.g., EPIC's call for lawmakers to implement OECD AI Principles and adopt prohibitions on mass surveillance and secret scoring) as a baseline for necessity, purpose specification, and

> accountability that India's own DPDP framework only partially reflects given its state-security carve-outs.

These instruments converge on a common minimum architecture: legality, necessity/proportionality assessed before deployment (not after), mandatory and periodic impact assessment, independent algorithmic testing against demographic bias, and accountability to a body independent of the deploying agency.

8. PRACTICAL SAFEGUARDS AND GOVERNANCE MECHANISMS

Drawing on the comparative and domestic legal analysis above, the following safeguards would materially reduce the privacy and security risks identified in Sections 3–5, while preserving the initiative's legitimate security objectives:

1. **Enabling primary legislation**. Facial recognition-based identification integrated with NATGRID should proceed only under a designated statute (not executive notification) that specifies: permissible purposes, categories of persons who may be placed on a watchlist, retention limits for both matched and non-matched images, and the agencies authorised to query the system. This directly addresses the "legality" prong repeatedly found deficient across NCRB/AFRS, NATGRID, and Digi Yatra.

2. **Judicial or independent pre-approval for bulk/real-time queries**, modelling on the UK's Investigative Powers Act requirement of Fundamental Rights Impact Assessments

3. **Mandatory, published Data Protection/Fundamental Rights Impact Assessments** before deployment at each airport, updated periodically, following the EU AI Act and Convention 108+ models including explicit necessity analysis of less intrusive alternatives (e.g., intelligence-triggered rather than continuous scanning).

4. **Independent algorithmic testing and public disclosure of accuracy and demographic-differential metrics**
benchmarking against NIST FRVT/FRTE or an equivalent 108+ models including explicit necessity analysis of less intrusive alternatives (e.g., intelligence-triggered rather than continuous scanning).

5. **Strict data minimisation and retention limits**, with non-matched images deleted within a defined, short, and audited window (the UK's sub-second and US citizen 12-hour benchmarks provide useful reference points), and matched images/logs retained only as long as necessary for the specific investigative purpose, subject to independent audit.

6. **An independent regulator with audit powers**, distinct from CISF, MHA, and the deploying agencies, empowered to conduct the UK's sub-second and US citizen 12-hour benchmarks provide useful reference points), and matched images/logs retained only as long as necessary for the specific investigative purpose, subject to independent audit.

7. **Defined and narrow watchlist criteria**, excluding categories such as protest participants, journalists, or persons subject only to minor/non-serious offences, addressing the UK experience of/watchlist scope-creep and the Indian AFRS "N:N search" ambiguity.

8. **A transparency and redress mechanism** allowing individuals to learn whether their biometric data was captured or matched, and to seek correction, consistent with (though currently under specified even by) the GDPR Act's grievances provisions, adapted for the security context where full disclosure may need to be deferred but not permanently denied.

9. **Explicit prohibition on private/database matching without statutory authorisation**, given the initial proposal's ambiguous reference to matching against "private databases" a feature none of the comparative models reviewed permit without express legislative sanction.

10. **Sunset and periodic parliamentary review clauses**, ensuring the scheme (and any future expansion of its scope, as occurred with NATGRID's NPR linkage) requires renewed legislative or parliamentary committee scrutiny rather than indefinite executive discretion.

9. TOWARD A BALANCED POLICY FRAMEWORK

India's security agencies face genuine and evolving threats at airports specifically, and at the wider critical infrastructure CISF protects that make some degree of technological modernisation reasonable and, in narrowly targeted forms, proportinate. At the same time, the **Puttaswamy** line of jurisprudence establishes clear, judicially mandated boundaries that a scheme of this scale cannot lawfully bypass through administrative convenience.

A balanced framework would decouple two objectives that the current proposal conflies:

- **Verification/convenience objectives** (confirming a traveller is who their travel document says they are) can be pursued through consent-based, opt-in systems as Digi Yatra was originally conceited, and as Singapore's and Australia's SmartGate models demonstrate with comparatively lighter-touch governance, provided genuine consent, data minimisation, and short retention are honoured.

- **Law-enforcement identification objectives** (matching a traveller's face against a suspect or fugitive watchlist without their knowledge or consent) are categorically more intrusive and, per both Indian constitutional doctrine and the comparative examples above, require the fuller statutory, judicial, and independent oversight architecture set out in Section 8. This is the category into which the CISF Data Fusion Centre proposal falls, and it is this category that current Indian law including the soon-to-be-operative DPPD Act does not yet adequately govern.

The policy choice is not between security and privacy in the abstract, but between two paths to security: one built on durable statutory authorisation and independent verification (which tends, per the UK and EU experience, to survive legal challenge and retain public confidence over time), and one built on executive discretion and post-hoc justification (which, per the AFRS, NATGRID, and Digi Yatra experience to date, has repeatedly generated legislation, civil society challenge, and periods of operational uncertainty). The former path is more likely to deliver durable, legally resilient security capability; the latter risks the scheme being challenged, curtained, or discounted precisely when it might be operationally needed.

10. CONCLUDING RECOMMENDATIONS

1. **Do not operationalise the CISF Data Fusion Centre—NATGRID integration until dedicated enabling legislation is enacted.**

   Administrative notification, as with NATGRID's original 2012 clearance, is legally insufficient in light of Puttuswary's legality requirement and invites the same legal vulnerability that has attended AFRS and Digi Yatra.

2. **Commission and publish an independent, pre-deployment fundamental rights and data protection impact assessment**, addressing necessity (why continuous scanning rather than intelligence-triggered deployment is required), proportionality, and algorithmic accuracy across demographic groups, using NIST FRVT/FRTE-equivalent benchmarks.

3. **Establish an independent oversight body**, separate from CISF and the Ministry of Home Affairs, with statutary audit powers over both the airport FRC deployment and NATGRID more broadly, empowered to publish periodic compliance findings, modelling on the UK ICO's FRT audit programme.

4. **Exclude private-database matching from the scheme absent explicit parliamentary authorisation**, and clarify publicly and unambiguously what "private databases" the initial proposal contemplated, if any.

5. **Fix binding, short retention periods for non-matched biometric captures**, with independently audited deletion logs, and clearly differentiated (and longer, but still finite and reviewable) retention for confirmed matches connected to an active investigation.

6. **Require vendor algorithm certification against an independent demographic-bias benchmark** before deployment at any airport, with public disclosure of test results, and a mechanism for periodic re-testing as algorithms are updated.

7. **Build in a transparency and grievement mechanism** enabling an individual to learn, through a defined process (which may involve appropriate delay for active investigations but not indefinite denial), whether their data was captured and matched, and to seek correction of erroneous matches.

8. **Bring forward the operational deadline for a fully constituted and independently functioning Data Protection Board of India**, and resolve the ambiguity currently the subject of Kerala High Court proceedings regarding Digi Yatra as to whether the Board is presently equipped to exercise meaningful oversight over any biometric surveillance system, airport-based or otherwise.

9. **Subject the scheme to periodic parliamentary review**, including a mandatory sunset clause requiring renewed statutory authorisation for any expansion of scope (additional airports, additional data sources, or new analytical capabilities such as predictive matching), directly addressing the "scope creep"相应 identified in the Australian comparative experience.

10. **Decouple convenience-oriented biometric services (Digi Yatra-style) from law enforcement identification services within airport infrastructure)**, ensuring that consent obtained for the former is never treated as authorisation for the latter, and that passengers are given clear, affirmative notice of which category of biometric processing they are subject to at each stage of their airport journey.

11. REFERENCES

- https://www.medianama.com/2026/06/223-cisf-facial-recognition-cameras-airports-natgrid/
- https://www.decanherald.com india/why-cisf-wants-to-link-facial-recognition-cameras-at-six-key-airports-to-data-fusion-centre-in-delhi-4050290
- https://www.biometricupdate.com/202606/india- considers-nationwide-facial-recognition-network-for-airports
- https://www.khaleejtimes.com/world/asia-india-links-airport-facial-recognition-to-intelligence-grid-for-national-security
- https://the420.in/cisf-ai-surveillance-network-airports-natgrid-data-fusion-centre/
- https://www.meitv.com/static/uploads/2024/06/2b11
- 0e9f04e6f6b4f8f3582c24aa5.pdf
- https://panoptic.in case-study/ncrbs-national-automated-facial-recognition-system
- https://en.wikipedia.org/wiki/Automated_Facial_Recognition_System (India)
- https://wwwMedianama.com/2019/11/223-ncrb-afrs-legality/
- https://www.gov.uk/government/publications/police-use-of-facial-recognition-factsheet
- https://www.biometricupdate.com/20258/ico-encouraged-by-uk-police-facial-recognition-compliance-with-data-protection-law
- https://bigbrotherwatch.org.uk/wp-content/uploads/202504/4briefing_–Facia-recognition-QA-briefing_Police-update
- https://artificialintelligence.eu/article/5/
- https://digital-strategy.eu.eu/en/policies/regulatory framework ai
- https://www.fpf.org/blog/the-digital-personal-data-protection_act-of-india-explained/
- https://www.lexology.com/library/detail.aspx?g=06a5c11c-6f5d-4aec-8d07-851c89d92d2
- https://www.en.wikipedia.org/wiki/Puttaswamy_v_Union_of_India
- https://www.barandbench.com/columns/proportionality-test-for-aadhaar-the-supreme-courts-two Approaches
- https://globalalfreedomofexpression.columbia.edu cases/puttaswamy-v-union-of-india-ii/

CyberPeace

CISF's PROPOSED FACIAL RECOGNITION NETWORK

Balancing Airport Security Modernisation with Privacy and Civil Liberties Safeguards in India

Author: Ritika Goswami, Intern, Policy & Advocacy, CyberPeace