Dated: 01/05/2026

To

Shri Akhilesh Kumar Trivedi,

Advisor (Networks, Spectrum and

Licensing), TRAI

Sub: Comments on TRAI Consultation Paper No. 08/2026 dated 30/04/2026: Regulatory Framework for Vehicle-to-Everything (V2X) Communication

Sir

While the Consultation Paper comprehensively addresses the technical and regulatory aspects of V2X communication for road safety, this analysis highlights two fundamental concerns that require urgent consideration before any rollout: (1) the significant privacy implications that potentially violate the fundamental Right to Privacy under the Indian Constitution, and (2) the substantial financial burden that will fall on both individual commuters and the public exchequer.

RIGHT TO PRIVACY CONCERNS

1. Constitutional Framework

The Supreme Court of India in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1 unequivocally held that the Right to Privacy is a fundamental right intrinsic to life and liberty under Article 21 of the Constitution. The nine-judge bench established that:

- Privacy is a constitutional value deserving protection

- Informational privacy is a core component of the right

- Any intrusion must satisfy the three-fold test: **legality, necessity, and proportionality**

2. V2X Architecture Inherently Violates Informational Privacy

The Consultation Paper itself acknowledges significant privacy risks at **paragraphs 3.48-3.50** (Page 77):

"V2X communication is inherently broadcast-based, with vehicles transmitting frequent messages to surrounding entities...Messages typically include location, speed, direction, and timing information, which can be used to track individual vehicles over time. Without adequate safeguards, this could enable persistent surveillance, profiling of user behaviour and misuse of personal data."*

This admission is damning. The V2X ecosystem described in the paper involves:

| Data Type | Frequency | Sensitivity |

|---|---|---|

| Real-time GPS location | Every 100ms or less | High |

| Speed and trajectory data | Continuous | High |

| Braking/acceleration patterns | Event-driven | Medium |

| Vehicle identification (VIN) | Persistent | Critical |

| Driver behavior patterns | Continuous | High |

3. Specific Privacy Breaches Not Adequately Addressed

3.1 Mass Surveillance Capability

Under the proposed framework, RSUs (Roadside Units) will be installed across highways, intersections, and urban corridors (**paragraph 2.8, Page 16**). These units will continuously collect vehicle data. The Consultation Paper does not address:

- Who will have access to this aggregated data?

- What prevents law enforcement from using this for dragnet surveillance without judicial oversight?

- How long will location histories be retained?

The Supreme Court has repeatedly held that dragnet surveillance violates fundamental rights. The *Puttaswamy* judgment specifically rejected the notion that the state can collect citizen data without procedural safeguards.

3.2 Pseudonym Certificates: Inadequate Protection

The paper proposes pseudonym certificates at **paragraph 3.53** (Page 79) as a privacy-preserving mechanism. However:

- These certificates are issued by a centralized PKI authority (**paragraph 3.57**, Page 81)

- The same authority can link pseudonyms to actual vehicle identities

- As demonstrated globally, "anonymous" vehicle tracking has been de-anonymized using simple statistical methods

International precedent: Studies in Europe have shown that despite pseudonym rotation every 5-10 minutes, vehicles can be tracked for over 95% of their journey using timing and location correlation attacks.

3.3 No Specific Data Protection Framework

The Paper mentions at **paragraph 4.2(ii)** (Page 199) that data privacy should comply with the Digital Personal Data Protection (DPDP) Rules 2025. However:

- The DPDP Act contains exemptions for State interests that could be broadly interpreted

- V2X data qualifies as "sensitive personal data" under any reasonable interpretation

- There is no explicit prohibition on: selling driving data to insurers, sharing with employers for fleet monitoring, or using for adverse actions against drivers

4. Failure to Satisfy the Three-Pronged Privacy Test

For any infringement of Article 21, the State must demonstrate:

| Test | V2X Compliance? | Analysis |

|------|-----------------|----------|

| **Legality** | Weak | The Telecommunications Act 2023 does not expressly authorize mass vehicle tracking. Section 3's "authorization" power does not override constitutional protections. |

| **Necessity** | Unproven | The Paper admits at **paragraph 1.5** that 92% of accidents are due to human error. V2X is not the only solution; improved driver training, road engineering, and basic ADAS features (cameras, radar) could achieve similar results without surveillance. |

| **Proportionality** | Fails | Mass collection of location data from every vehicle is disproportionate to the goal of preventing specific accidents. Less intrusive alternatives exist (e.g., local intersection sensors, voluntary safety systems). |

5. Comparison with Global Privacy Safeguards

The Consultation Paper fails to adopt robust privacy protections present in other jurisdictions:

| Jurisdiction | Privacy Safeguard | India's Position |

|---|---|---|

| EU (GDPR + ePrivacy) | Opt-in consent required for non-safety data, mandatory DPIAs | Not proposed |

| US (SCMS) | Distributed trust architecture - no single entity can link identity to messages | Centralized PKI proposed at **para 3.57** |

| South Korea | Data minimization by law - only what is strictly necessary | No such principle stated |

PART B: FINANCIAL BURDEN ON COMMUTERS AND EXCHEQUER

1. Direct Cost to Vehicle Owners

The Consultation Paper's analysis of financial aspects in **Chapter IV** (Pages 107-134) fails to quantify the inevitable pass-through costs to consumers.

1.1 OBU Costs

While OBUs are proposed to be "license-exempt" (**paragraph 3.6(iii)**, Page 54), the Paper does not specify:

- Who bears the cost of OBU manufacturing and installation?

- Will OBUs be mandatory for all new vehicles?

Projected cost estimate (based on international deployments):

| Component | Estimated Cost (INR) |

|---|---|

| C-V2X chipset | 5,000 - 8,000 |

| Antenna and RF module | 2,000 - 4,000 |

| Integration with vehicle systems | 3,000 - 6,000 |

| Security module (secure element) | 1,500 - 3,000 |

| Certification and testing | 2,000 - 5,000 |

| **Total per vehicle** | **13,500 - 26,000** |

For India's ~4 crore annual vehicle production, this represents **₹54,000 - ₹104,000 crore** in upfront costs to consumers annually.

1.2 RSU Costs – Taxpayer Burden

Paragraph 3.4(e) (Page 51) and 3.5 (Page 51-52) state that RSUs will be deployed by State Governments, NHAI, or authorized agencies. The Paper nowhere quantifies:

- Number of RSUs required for meaningful coverage

- Installation and maintenance costs

- Power and backhaul connectivity expenses

Estimated infrastructure costs:

| Highway Type | Length (India) | RSU density | Total RSUs |

|---|---|---|---|

| National Highways | 1.46 lakh km | 1 per 2 km | 73,000 |

| State Highways | 1.80 lakh km | 1 per 5 km | 36,000 |

| Urban intersections (major) | ~50,000 locations | 1 per intersection | 50,000 |

| **Total** | | | **~1,59,000 RSUs** |

At an estimated ₹5-10 lakh per RSU (including installation, backhaul, power), total capital cost = **₹7,950 - ₹15,900 crore**.

Annual operating costs (power, maintenance, connectivity) estimated at 15% of capital = additional **₹1,200 - ₹2,400 crore per year**.

2. Spectrum Charges – Unclear but Potentially Significant

The Paper discusses spectrum charges at **paragraphs 4.12-4.37** (Pages 111-122) but is deliberately ambiguous:

- **Q12** asks whether charges should be levied at all

- **Q13** asks which service category should apply for charging

- **Q14** proposes AGR-based charging

If spectrum charges are imposed (either on RSU operators or eventually passed to consumers), the dissenting note at **Page 166** provides a crucial warning:

"The recent 2024 spectrum auction reserve price for the 3300 MHz band was set at Rs. 355.04 crores per MHz for a 20-year period. If this were applied to the 5.875-5.925 GHz band, then the cost for 50 MHz of spectrum would be approximately Rs. 900 crores per annum."

Even if concessional rates apply (as suggested for safety services), any recurring spectrum charge will ultimately be borne by:

- Taxpayers (if central/state governments pay)

- Toll payers (if NHAI passes costs)

- Consumers (if private operators deploy RSUs)

3. Double Financial Burden Identified by Dissenting Member

The dissenting note at **Page 166** (Santosh Sam Koshy, Scientist E, C-DAC) explicitly raises the financial burden concern:

"Vehicle manufacturing and selling is a commercial activity, and it is anticipated that customers will be additionally charged for vehicles equipped with OBUs under V2X technology, marketed as a premium feature. It is likely that private entities or public-private partnerships (PPP) will handle the installation, making the service similar to mobile cellular services, potentially involving user fees."

This confirms that:

1. Mandatory OBUs will increase vehicle prices

2. RSU deployment may ultimately be monetized through user fees

3. No business model ensures free access to safety features

4. Opportunity Cost – Funds Diverted from Proven Safety Measures

India's road safety crisis (1.73 lakh fatalities in 2023, per **paragraph 1.3**, Page 5) deserves attention. However, V2X is an unproven solution at scale, while cost-effective alternatives exist:

| Intervention | Cost per life saved | Proven effectiveness |

|---|---|---|

| Speed bumps/calming measures | Low | High (30-40% reduction) |

| Illuminated pedestrian crossings | Low | High |

| Mandatory ABS (already required) | Low | High |

| Improved driver licensing tests | Very low | Medium |

| Highway rumble strips | Low | High (40-50% reduction) |

| Emergency response optimization | Medium | High |

| **V2X (projected)** | **Very high** | **Unproven at scale** |

The ₹60,000+ crore projected cost of V2X could instead fund hundreds of thousands of proven safety interventions across India's accident-prone areas.

PART C: SPECIFIC RESPONSES TO CONSULTATION QUESTIONS

Response to Q6 (Pages 83, 136-137) – Security Framework Necessity

While a security framework is certainly necessary if V2X proceeds, the more fundamental question is whether the privacy risks can ever be adequately mitigated. To answer the specific question:

"Whether there is a need for prescribing a security framework for ITS/C-V2X in India?"

Response: Yes, if V2X is deployed. However, no security framework can fully address the inherent privacy violations of continuous vehicle tracking. The proposed centralized PKI architecture (**paragraph 3.57**) is particularly concerning as it creates a single point of trust capable of linking all pseudonyms to actual identities.

Alternative recommendation: Before any deployment, India should:

1. Explicitly amend the Telecommunications Act to include privacy protections for V2X data

2. Mandate distributed trust architecture (similar to US SCMS) rather than centralized CCA-controlled PKI

3. Require judicial authorization for accessing V2X location history

4. Prohibit insurance pricing or employer monitoring based on V2X data

Response to Q12 (Page 122) – Spectrum Charges

> *"Should there be spectrum charges levied on spectrum assigned to V2I communication service authorised entities?"*

Response: No, spectrum charges should NOT be levied, **but for different reasons than implied by the Paper.**

The Paper suggests waiving charges to encourage deployment. However, this response is based on a different rationale: if V2X proceeds despite privacy concerns, imposing spectrum charges would further increase the financial burden on commuters and taxpayers without advancing safety. However, the absence of spectrum charges is not a justification for proceeding with V2X.

Given the already-high costs and uncertain benefits, imposing additional spectrum charges would be arbitrary and against public interest.

Response to Q17 (Page 126) – Revenue Sources

"What are the potential sources of revenue for a V2I communication service authorised entity?"

Response: The Paper's discussion of revenue sources reveals a critical flaw in the V2X business case. As noted, safety applications "are not expected to generate any direct revenue" (**paragraph 4.38**, Page 124). This means:

Revenue source	Likelihood	Concern
Direct user fees for safety alerts	Unlikely – would undermine safety purpose	N/A
Traffic data monetization	Likely – as paper admits at **para 4.40**	Privacy violation
Insurance telematics	Very likely	Discrimination, higher premiums for safe drivers
Advertising/location-based services	Likely	Privacy violation, driver distraction
Government subsidy/taxpayer funding	Certain	Burden on exchequer

The inevitable conclusion is that to make V2X financially viable, entities WILL monetize driving data, directly violating privacy rights.

PART D: RECOMMENDATIONS

Recommendation 1: Constitutional Scrutiny Required

Before any V2X rollout, the government should:

- Submit the V2X framework to the Ministry of Law and Justice for constitutional review

- Specifically examine whether continuous vehicle tracking meets the Puttaswamy standard

- Publish a detailed Privacy Impact Assessment as required under DPDP Act

Recommendation 2: Opt-In, Not Mandatory

If V2X is deployed:

- OBUs must be optional, not mandatory

- No insurance, tax, or regulatory benefit for V2X-equipped vehicles

- Clear disclosure of data collection to vehicle purchasers

- Ability to permanently disable V2X functionality

Recommendation 3: Prioritize Alternative Safety Measures

Given the ₹60,000+ crore estimated cost and fundamental privacy concerns, the government should redirect resources to:

- Proven intersection safety improvements (cost: ₹10,000 crore nationally)

- Mandatory advanced driver training (cost: ₹5,000 crore)

- Highway engineering improvements at accident black spots (cost: ₹15,000 crore)

- Emergency medical services on highways (cost: ₹5,000 crore)

Recommendation 4: Pilot with Strict Privacy Safeguards

If V2X testing proceeds:

- Limit pilots to limited geographic areas (e.g., one highway corridor)

- Require opt-in consent from all participating vehicle owners

- Prohibit any law enforcement access to pilot data

- Mandate independent privacy auditing

- Sunset pilot after 2 years with mandatory evaluation

CONCLUSION

The TRAI Consultation Paper on V2X communication fails to adequately address two fundamental barriers:

First, the Right to Privacy. The continuous collection of location, speed, and behavioral data from every vehicle on Indian roads constitutes a massive intrusion into fundamental rights. The paper's proposed pseudonym certificates and centralized PKI do not prevent—and may facilitate—mass surveillance. No compelling justification has been provided why less intrusive alternatives cannot achieve similar safety benefits.

Second, the Financial Burden. The paper repeatedly admits that safety applications generate no direct revenue, which means every rupee of V2X deployment will ultimately be paid by vehicle purchasers (through mandatory OBUs) and taxpayers (through RSU infrastructure). Estimated costs exceed ₹60,000 crore, with unproven safety benefits at scale. This money would save more lives if invested in proven road safety interventions.

Therefore, I recommend that the Authority advise the government NOT to proceed with mandatory V2X deployment and instead focus on cost-effective, privacy-preserving road safety measures that respect fundamental constitutional rights.

Best Regards

Abhinav Vashisht

H.No. 201, Inner Akhara Bazar,

Kullu. HP - 175101

Mob: 9418022261