

SUBMISSION OF COMMENTS TO THE COMMITTEE ON PHYSICAL INFRASTRUCTURE ON THE DIGITAL/ ELECTRONIC NUMBER PLATE PROJECT

September 2026

A. Introduction

1. The digital/electronic number plate system, commonly known as the Intelligent Transport Monitoring System (ITMS), may support legitimate objectives, including vehicle recovery, traffic management, road safety and crime prevention. However, its reported capabilities, including vehicle identification, possible real-time tracking, integration with CCTV and other state databases, and centralised access to movement information, create substantial risks to privacy, data protection, freedom of movement, association and assembly.

2. Parliament should assess the ITMS not only as a number plate procurement project, but also as a potentially large-scale vehicle-monitoring and personal data processing system with significant surveillance implications.

3. The Committee cannot assess the legality, necessity, proportionality, accountability or value for money of the ITMS without access to its technical architecture, data flows, access rules, retention periods, contract terms, security controls and Data Protection Impact Assessment. The Committee should therefore require the responsible ministries and contractor to disclose:

- i. The technical specification and data-flow map.
- ii. The lawful basis and purposes for processing.
- iii. The DPIA and safeguards adopted.
- iv. Data retention, deletion and access-control rules.
- v. Data-sharing and international-transfer arrangements.
- vi. Security, audit and independent-oversight measures.

B. IMPACT OF THE DIGITAL/ ELECTRONIC NUMBER PLATE SYSTEM FOR PRIVACY AND DATA PROTECTION

4. The Data Protection and Privacy Act, Cap. 97 provides for the protection of personal data and the privacy of persons in accordance with Article 27 of the Constitution. Section 7 generally requires prior consent before personal data is collected or processed. However, section 7(2) permits collection or processing without consent where it is authorised or required by law, or where it is necessary for the proper performance of a public duty, national security, or the prevention, detection, investigation, prosecution and punishment of an offence or breach of law.

5. These grounds do not create a blanket exemption from the Act. Any processing carried out under them must still comply with the other applicable data protection requirements, including fair and lawful processing, collection of data that is adequate, relevant and not excessive, processing for a specified purpose, retention only for as long as necessary, appropriate security safeguards, and the applicable transparency and data subject rights requirements. Any limitation on constitutional rights must also comply with Article 43 of the Constitution, which permits limitations only where they are acceptable and demonstrably justifiable in a free and democratic society.

6. The ITMS has the potential to enable the identification of vehicles, the collection of vehicle movement information and, where linked with other databases or surveillance systems, the identification or profiling of individuals.

7. Recommendations

- i. Establish legal safeguards to govern scale, technical design, access arrangements. In particular, Parliament should require confirmation of whether the system allows real-time or historical vehicle-location tracking, which authorities may access the information, the purposes for which it may be used, the safeguards against misuse, and whether access is subject to independent or judicial oversight.
- ii. Where a system enables broad or continuous monitoring of vehicle movements, Parliament should assess whether the resulting interference with privacy and other rights is necessary and proportionate to the purposes for which the system is deployed. These questions must be answered through clear law, published safeguards, effective independent oversight and compliance with the Data Protection and Privacy Act.

C. IMPLICATIONS OF THE SYSTEM FOR DIGITAL RIGHTS AND THE RIGHTS OF MOTORISTS AND OTHER USERS

8. Mobility Surveillance Beyond Traffic Management

A system that records vehicle location, time and movement patterns can support legitimate traffic-management and security functions. However, where vehicle data are linked to CCTV, registration, identity, tax or other databases, the system may enable broader mobility surveillance that goes beyond traffic management.

9. Chilling Effect on the Exercise of Fundamental Human Rights and freedoms

The ITMS may affect the exercise of constitutional rights, including freedom of movement under Article 29(2)(a), peaceful assembly and demonstration under Article 29(1)(d), and freedom of association under Article 29(1)(e), particularly if movement data are used to identify, track or deter participation in political, civic or associational activity.

10. The risk is not that every use of vehicle data will necessarily interfere with these rights. Rather, a system that makes it easy to reconstruct movements, identify associations or link vehicle records to other personal-data systems may create a chilling effect, particularly where access rules, oversight arrangements and limits on political or non-traffic uses are unclear.

11. Recommendation

- i. To check on mobility in paragraph 8 above, surveillance beyond traffic management, Parliament should require clear legal limits on the purposes for which ITMS data may be accessed and used.

D. CONCERNS ARISING FROM THE IMPLEMENTATION AND OPERATIONALISATION OF THE SYSTEM

12. Data security, contractor and cross-border processing risks

The ITMS is implemented with the involvement of a foreign commercial contractor. The extent to which data of Ugandans is managed and processed may not be certain.

13. Section 19 of the Data Protection and Privacy Act regulates the processing or storage of personal data outside Uganda, while section 20 requires appropriate security safeguards for personal data. Parliament should therefore require disclosure of the location of primary and backup servers, the jurisdictions in which data may be processed, the identity of any sub-processors, who holds encryption keys, and whether the contractor or any foreign entity has remote or privileged access to the system.

14. Recommendation

- i. Under paragraph 12 above, Parliament should require the responsible public bodies to disclose the contractor's role in collecting, hosting, accessing, maintaining, securing and sharing personal data generated through the system.
- ii. In respect to paragraph 13 above, Parliament should undertake measures to ensure that data management arrangements are governed by written data-processing, confidentiality, security and audit obligations.
- iii. The Committee should also require confirmation that access to personal data is limited to authorised persons and that every access is logged, reviewable and subject to sanctions for misuse.

15. Transparency and Data Protection Impact Assessment

The public record does not appear to show that a Data Protection Impact Assessment has been published for the ITMS. Given the scale and nature of the processing, including the potential monitoring of vehicle movements and linkage with CCTV, vehicle-registration, tax and national-identity datasets.

16. Recommendation

- i. Parliament should require the responsible public bodies to confirm whether the processing was assessed under Regulation 12 and, if so, whether a DPIA was conducted before the relevant processing commenced.
- ii. If a DPIA was conducted, Parliament should require publication of a non-sensitive version and a statement of the safeguards adopted. If one was not conducted, Parliament should require the responsible bodies to explain why and to conduct an assessment before further compulsory rollout or expansion of the system.

17. Court proceedings and disclosure of ITMS documents

In proceedings concerning the ITMS, the High Court vide *Legal Brains Trust v Attorney General* (Miscellaneous Cause No. 225 of 2021) ordered the Government to produce specified documents and provide further particulars relating to the system, including the agreement with the contractor, financial and technical assessment material and information concerning the system's operating procedures and safeguards.

18. In subsequent proceedings seeking interim relief against implementation, the Court of Appeal declined to grant an injunction halting the ITMS.

19. Recommendation

- i. (i) In respect to paragraph 17, Parliament should seek access to those materials and require a public summary of their data-protection, human-rights, security and financial implications.
- i. (ii) Undertake measures in respect to paragraph 18, to treat the litigation as evidence of the need for scrutiny and disclosure, rather than as a judicial determination that the system is unlawful.

20. Public information about the device is inconsistent and incomplete

Public information about the technical components of the ITMS appears inconsistent. A July 2024 government communication described a full installation kit as including two aluminium registration plates, a tracker, a SIM chip, two Bluetooth beacons and snap locks. It also stated that the system would enable real-time vehicle tracking at Police Command Centres.

21. [CIPESA's own analysis of August 2024](#) similarly described trackers, SIM chips and Bluetooth beacons. [Investigative reporting in October 2025](#) described radio-frequency identification chips, quick-response codes and machine-readable text read by cameras. These sources should be distinguished from the Government's own technical disclosure, but they reinforce the need for a definitive public specification.

22. By contrast, the current ITMS public FAQ [describes](#) a digital number plate as an electronic plate containing a Bluetooth Low Energy tag. It does not state whether each installation includes a tracker, SIM card or continuous location-reporting capability.

23. These systems have materially different privacy implications. A passive identifier may be read only when it passes an authorised reader. A tracker with a SIM card may enable continuous or near-continuous location reporting.

24. Recommendation

- i. The Committee should distinguish between the capabilities of the plate itself, the roadside readers and the wider ITMS platform, since a location record may be generated either by a continuously transmitting device or by a reader detecting a vehicle at a particular location.
- ii. The Committee should require the Ministry and contractor to publish a definitive technical specification, data-flow diagram, list of sensors and communications interfaces, transmission frequency, storage locations, access arrangements and security controls.

E. COLLECTION, STORAGE, ACCESS, SHARING AND RETENTION OF INFORMATION GENERATED THROUGH THE SYSTEM

25. A plate read is not one fact. Each detection may record a vehicle, a time and a place. Accumulated over time, such records can create a detailed movement history. The ITMS may not initially identify the driver. However, repeated vehicle detections, especially where linked to vehicle-registration, CCTV, tax, identity or other databases, may enable the identification or inference of a person's routine, movements and associations.

26. The Uganda Police have stated that the ITMS will be integrated with the closed-circuit television network, motor vehicle registration, the Uganda Revenue Authority electronic tax system and the national identity database held by NIRA. Each linkage can make a vehicle record more readily attributable to an identified or identifiable person. When combined over time with registration, CCTV, tax, identity or other datasets, the resulting records may enable detailed inferences about a person's movements, routines and associations.

27. The following questions are necessary to assess whether the system has adequate legal, privacy and security safeguards. The Committee should require clear public answers.

- i. What is generated? Whether plates transmit continuously or are read only at fixed points, what readers capture besides the plate, and whether images of occupants are retained.
- ii. Where is it stored? The location of primary and backup storage, the jurisdiction over it, and who holds the encryption keys.
- iii. Who may query it? Whether access requires judicial authorisation, administrative approval, or only valid credentials, and whether a query must state a purpose.
- iv. What is recorded about access? Whether every query is logged, whether the log is tampered evident, and whether anyone outside the operating agency may inspect it.
- v. With whom are records shared? Whether data flows to security agencies, the revenue authority or the contractor, and whether such transfers are themselves recorded.
- vi. In terms of the period records are kept, no public retention schedule has been identified for ITMS data. Parliament should require the responsible agencies to disclose the retention periods for plate reads, location records, images, access logs, alerts and linked identity data, together with the legal basis for each period. Without this information, Parliament and the public cannot assess compliance with section 18 of the Act or whether retention is necessary and proportionate.

28. Recommendations

- i. The Committee should consider whether further compulsory rollout or expansion should proceed before these questions are answered, the DPIA is confirmed, and the required safeguards are publicly established.

F. CYBERSECURITY RISKS AND MEASURES TO MITIGATE THEM

29. In addition to earlier mentioned risks and vulnerabilities, a centralised national movement database may be vulnerable to hostile state actors, organised crime, malicious insiders and other unauthorised parties. It is attractive to potential cyber criminals given the sensitivity and scale of the information it could contain. The device itself includes positioning hardware, SIM cards, Bluetooth components or other radio-based technologies. This even makes it more vulnerable.

30. Recommendation

- i. Parliament should require publication of the applicable security standard, software-update process, vulnerability-disclosure procedure and incident-response plan. The technical specification should state what information is broadcast, whether it is encrypted or pseudonymised, which devices can read it, and whether third parties can collect or correlate the identifier.

G. RECOMMENDATIONS ON MEASURES THAT MAY ENHANCE THE PROTECTION OF DIGITAL RIGHTS WHILE ACHIEVING THE INTENDED OBJECTIVES OF THE PROJECT

31. In addition to the above-mentioned recommendations, the following should be undertaken by the Parliament to ensure robust digital rights protection

- i. Specifically require the companies involved in the digital/electronic number plate system to strictly comply with the Data Protection Act Cap 97 and the Data Protection and Privacy Regulations 2021 especially in compliance with data protection rights and principles to ensure maximum protection of the data subject.
- ii. Amend the existing pieces of legislation especially the Data Protection Act Cap 97 to provide clear boundaries and safeguards in respect to:

- a. Demarcation of warranties, periods and dockets for vehicle tracking including specification of national security, political activities, judicial or civil enforcement as opposed to blanket justifications
- b. Establishment and specification of judicial oversight over deployment and implementation of the ITMS
- c. Establishment of clear data control sovereignty safeguards of Ugandan citizens' data such as through the establishment of infrastructure to ensure exclusive hosting of citizens' data within Uganda such as by the National Information Technology Authority Uganda (NITA-U) as opposed to use of foreign private entities or actors who often control their infrastructure.
- d. Empower the Personal Data Protection Office to issue administrative fines for the errant data controllers and processors including companies that man citizens' data by amending the Data Protection and Privacy Act, Cap 97, specifically section 33. Section 33 entitles the data subject to applying to a court of competent jurisdiction for compensation from the data collector, data processor or data controller for the damage or distress despite a finding in liability of the data collector, data processor or data controller for the damage or distress in section 32.

H. A NOTE ON PROPORTIONALITY

32. The Committee should assess whether the intrusion created by the ITMS is necessary and proportionate to its demonstrated benefits. That assessment should be based on reliable evidence of effectiveness, cost, error rates, alternative measures, impact on rights and the adequacy of safeguards. Where that evidence is unavailable or insufficient, the Committee should require the responsible authorities to provide it before determining whether further compulsory rollout or expansion is justified.



CIPESA

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

Plot 10B Katalima Crescent, Naguru. | P.O.Box 122311, Kampala (U)

+256 414 289 502 | programmes@cipesa.org | [f](#) [x](#) [in](#) @cipesaug

www.cipesa.org