PROPOSED 28TH AMENDMENT TO THE UNITED STATES CONSTITUTION

The Right to Privacy and Protection Against Mass Surveillance
Discussion draft - October 2026

Purpose

To recognize a fundamental right to privacy and protect people against indiscriminate surveillance, including the collection and combination of data to track movements, identify associations, or create detailed behavioral profiles. The proposal is technology-neutral and would apply to present and future surveillance methods.

PROPOSED CONSTITUTIONAL TEXT

AMENDMENT XXVIII

The Right to Privacy and Freedom from Unreasonable Surveillance

Section 1. Fundamental Right to Privacy

The right of the people to privacy in their persons, communications, movements, associations, personal information, and activities shall not be infringed by the United States or by any State, except as provided by this article.

The exercise of this right shall not depend solely upon whether such information or activities are observable in public or disclosed to third parties.

Section 2. Protection Against Mass Surveillance

Neither the United States nor any State shall establish, operate, authorize, or knowingly utilize systems of indiscriminate or persistent surveillance of the people without individualized legal justification.

The systematic collection, retention, aggregation, or analysis of information concerning an individual for the purpose or effect of tracking their movements, identifying their associations, reconstructing their activities, or creating a comprehensive profile of their behavior shall constitute a search within the meaning of the Fourth Amendment.

Section 3. Protection Against Automated Profiling

No government authority shall employ artificial intelligence, automated recognition systems, biometric identification, automated license plate readers, or comparable technologies to systematically identify, track, classify, or profile individuals without lawful authorization consistent with this article.

The use of automated technology shall not diminish the constitutional protections afforded to the people.

Section 4. Judicial Authorization

Surveillance that constitutes a search under this article shall require a warrant issued upon probable cause, supported by oath or affirmation, and particularly describing the person, information, and duration of the surveillance authorized.

No warrant shall authorize indiscriminate surveillance of the general population.

Congress may provide narrowly tailored exceptions for emergencies involving imminent threats to life or serious bodily injury, subject to prompt judicial review.

Section 5. Prohibition Against Circumvention

Neither the United States nor any State may evade the protections of this article by purchasing, requesting, receiving, or otherwise obtaining information from private entities that the government would be constitutionally prohibited from collecting directly.

No government authority shall compel or induce a private entity to conduct surveillance on its behalf in violation of this article.

Section 6. Enforcement and Remedies

Any person whose rights under this article have been violated shall have access to judicial relief.

Congress shall have power to enforce this article by appropriate legislation, including legislation providing for the suppression of unlawfully obtained evidence, the deletion of unlawfully collected information, and remedies for violations.

Section 7. Preservation of Other Rights

Nothing in this article shall be construed to diminish the protections guaranteed by the First, Fourth, Fifth, Ninth, or Fourteenth Amendments to this Constitution.

EXPLANATORY NOTES (NOT PART OF THE AMENDMENT)

Why this is proposed

Existing Fourth Amendment law protects against certain forms of government tracking, but the constitutional treatment of widespread automated collection and data aggregation is not comprehensively settled. This draft would explicitly address surveillance profiles created from public observations, purchased information, and interconnected databases.

Illustrative applications

Practice	Intended treatment under proposal
Targeted investigation with a valid warrant	May proceed within the warrant's scope.
Mass license-plate collection and searchable movement histories	Would face constitutional limits on collection, retention, and use.
AI analysis of movements or associations over time	Would generally require individualized judicial authorization.
Government purchase of location histories from data brokers	Could not bypass constitutional limits on direct collection.
Indiscriminate facial recognition of people at a demonstration	Would face restrictions on population-wide identification and profiling.

Questions for further refinement

Should the amendment restrict private companies that independently create personal profiles? Should indiscriminate data collection itself be prohibited, even when no one searches the database? How should the text distinguish ordinary security cameras from interconnected tracking systems? These policy choices would affect the amendment's reach.

Legal context and process

In Carpenter v. United States (2018), the Supreme Court held that government acquisition of certain historical cell-site location records is generally a Fourth Amendment search. In United States v. Jones (2012), attaching and using a GPS tracker on a vehicle was held to be a search. Neither decision creates a blanket prohibition on all public-space surveillance. Under Article V, proposing a constitutional amendment generally requires two-thirds of both houses of Congress, or a convention called upon application of two-thirds of state legislatures; ratification requires three-fourths of the states.

References: Carpenter v. United States, 585 U.S. 296 (2018); United States v. Jones, 565 U.S. 400 (2012); U.S. Constitution, Article V.

This document is a proposed discussion draft, not an adopted amendment or a statement of current constitutional law.