A MODEL TO PREVENT GEOLOCATION DATA FROM BEING WEAPONIZED

State Location Privacy Act

BY MATT SCHWARTZ AND JUSTIN BROOKMAN

JANUARY 28, 2026

CR Consumer Reports

SECTION 1

Consumer Protections

(a) A controller that collects a consumer's precise geolocation data shall, in its publicly accessible privacy notice, inform consumers of the following:

(1) The fact that the consumer's precise geolocation data is being collected.

(2) The type of precise geolocation data collected, including the precision of the data.

(3) The goods or services requested by the consumer for which the controller is collecting, processing, or disclosing the precise geolocation data and a description of how the controller will process the precise geolocation data to carry out those purposes.

(4) Whether the controller is collecting, processing, or disclosing precise geolocation to prevent or respond to security incidents, fraud, harassment, malicious or deceptive activities, or any illegal activity and a description of how the controller will process the precise geolocation to carry out those purposes.

(5) Any disclosures of the precise geolocation data necessary to provide the goods or services requested by the consumer and the identities of the third parties to whom the precise geolocation data is disclosed.

(b) In addition to the provisions set forth in (a), a controller that collects a consumer's precise geolocation shall prominently display, at or before the point of collection, a notice that informs the consumer that the consumer's precise geolocation is being collected.

(c) A controller or processor shall not do any of the following:[1]

(1) Collect or process precise geolocation data more than necessary to provide the goods or services requested by the consumer.

(2) Retain precise geolocation data longer than necessary to provide the goods or services requested by the consumer or longer than one year after the consumer's last intentional interaction with the controller, whichever is earlier.

(3) Sell, trade, or lease precise geolocation data to a third party.

(d) Notwithstanding subsection 5(c) of this section, a controller or processor may collect or process precise geolocation data that is necessary to prevent or respond to security incidents, fraud, harassment, malicious or deceptive activities, or any illegal activity targeted at the consumer, the controller or processor to investigate, report, or prosecute those responsible for any of those actions. Precise location information collected and processed under this

[1] In states that already have privacy laws, drafters may need to specifically supersede existing protections for sensitive data that are more lenient (e.g. opt-in consent for processing of sensitive data) than the proposal here.

subdivision shall not be retained for longer than 90 days except as required under law and shall not be used for any other purpose.

(e) Notwithstanding subsection 5(c) of this section, a controller or processor may use precise geolocation data to perform services on behalf of the controller or processor, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing storage, or providing similar services on behalf of the controller or processor. Precise location information collected and processed under this subdivision shall not be used for any other purpose.

SECTION 2

Enforcement

(a) A violation of Section 1 with respect to the precise geolocation data of a consumer constitutes an injury to that consumer. The injured consumer may bring a civil action against the party that commits the violation. In a civil action brought under this subsection in which a plaintiff prevails, the court may award the plaintiff any of the following:

(1) Damages in an amount not less than $5,000 per individual per violation, as adjusted annually to reflect an increase in the Consumer Price Index, or actual damages, whichever is greater;
(2) punitive damages;
(3) injunctive relief, including an order that an entity retrieve any personal data transferred in violation of this title;
(4) declaratory relief; and
(5) reasonable attorney's fees and litigation costs.

SECTION 3

Severability

(a) If any provision of this Act or the application thereof to any person or circumstance is held invalid for any reason in a court of competent jurisdiction, the invalidity does not affect other provisions or any other application of this Act that can be given effect without the invalid provision or application, and for this purpose, the provisions of this Act are declared severable.

SECTION 4

Definitions

(1) “Collect” means buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring personal data by any means.

(2) “Controller” means a person who, alone or jointly with others, determines the purpose and means of collecting or processing personal data.

(3) “Consumer” means an individual who is a resident of this state. “Consumer” does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency.

(4) “De-identified data” means data that does not identify and cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data:

(A) takes reasonable physical, administrative, and technical measures to ensure that such data cannot be associated with an individual or be used to re-identify any individual or device that identifies or is linked or reasonably linkable to an individual,
(B) publicly commits to process such data only in a de-identified fashion and not attempt to re-identify such data, and
(C) contractually obligates any recipients of such data to satisfy the criteria set forth in subparagraphs (A) and (B) of this subdivision.

(5) “Device” means any physical object that is capable of connecting to the internet, directly or indirectly, or to another device.

(6) “Personal Data” means any information, including derived data and unique persistent identifiers, that is linked or reasonably linkable, alone or in combination with other information, to an identified or identifiable individual or a device that identifies or is linked or reasonably linkable to an individual. “Personal data” does not include de-identified data or publicly available information.

(7) “Process” and “processing” mean any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the use, storage, disclosure, analysis, deletion or modification of personal data.

(8) “Processor” means a person who collects, processes, or transfers personal data on behalf of, and at the direction of, a controller or another processor.

(9) “Precise geolocation data” means information derived from technology, including, but not limited to, latitude and longitude coordinates from global positioning system mechanisms or other similar positional data, that reveals the past or present physical location of an individual or device that identifies or is linked or reasonably linkable to 1 or more individuals with precision and accuracy within a radius of one thousand seven hundred fifty feet.

“Precise geolocation data” does not include the content of communications, or a photograph or video unless used to identify an individual or device’s precise geolocation.

(10) “Sale of personal data” means the exchange of personal data for monetary or other valuable consideration by the controller to a third party.

“Sale of personal data” does not include:

(A) the disclosure of personal data to a processor that processes the personal data on behalf of the controller;
(B) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;
(C) the disclosure or transfer of personal data to an affiliate of the controller;
(D) with the consumer’s affirmative consent, the disclosure of personal data where the consumer affirmatively directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party; or
(E) the disclosure of personal data that the consumer:
(i) intentionally made available to the general public via a channel of mass media; and
(ii) did not restrict to a specific audience

(11) “Third Party” means a person that collects personal data from another person that is not the consumer to whom the data pertains and is not a processor with respect to such data

Acknowledgements

The State Location Privacy Act was drafted and published by Consumer Reports.

Endorsements

The State Location Privacy Act has been endorsed by the Electronic Privacy Information Center (EPIC), the Consumer Federation of America (CFA), Public Knowledge, Privacy Rights Clearinghouse, the Center for Democracy and Technology (CDT), Public Interest Research Group (PIRG), and Tech Equity.