HOUSE DOCKET, NO. 4038 FILED ON: 1/17/2025

HOUSE . . . . . No. 2687

The Commonwealth of Massachusetts

PRESENTED BY:

David M. Rogers

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act relative to protecting Massachusetts residents against federal government surveillance.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	DATE ADDED:
David M. Rogers	*24th Middlesex*	*1/17/2025*
Patrick Joseph Kearney	*4th Plymouth*	*1/17/2025*

HOUSE DOCKET, NO. 4038 FILED ON: 1/17/2025

HOUSE . . . . . No. 2687

By Representative Rogers of Cambridge, a petition (accompanied by bill, House, No. 2687) of David M. Rogers and Patrick Joseph Kearney relative to personal data access by criminal justice agencies. Public Safety and Homeland Security.

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Fourth General Court
(2025-2026)

An Act relative to protecting Massachusetts residents against federal government surveillance.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. Section 1 of chapter 66A of the General Laws, as appearing in the 2020 Official Edition, is hereby amended by inserting after the definition of "Automated personal data system," the following definition:-

"Commonwealth fusion center", an entity established in executive order no. 476 within the criminal information section of the department of state police, established in section 38 of chapter 22C, and under the direction of the executive office of public safety and security, or any successor entity.

SECTION 2. Said section 1 of said chapter 66A, as so appearing, is hereby further amended by inserting after the definition of "Criminal intelligence agency," the following 2 definitions:-

"Criminal intelligence information", data collected on an individual or organization that is reasonably suspected of involvement in criminal activity for the purpose of their identification

or for acquiring evidence of their criminal activity. Reasonable suspicion is established when information exists that establishes sufficient facts to give a trained law enforcement or criminal justice agency officer, investigator or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

"Criminal intelligence system", the arrangements, equipment, facilities and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information, including the commonwealth fusion center, the Boston Regional Intelligence Center, any successor entities and any other entities in the commonwealth bound by the provisions of 28 CFR Part 23.

SECTION 3. Said section 1 of said chapter 66A, as so appearing, is hereby further amended by striking out the definition of "Personal data," and inserting in place thereof the following definition:-

"Personal data", any information concerning an individual that, because of a name, identifying number, mark or description, can be readily associated with a particular individual; provided however, that personal data shall not include information that would reasonably be expected to: (i) interfere with an ongoing criminal investigation or other law enforcement proceeding; (ii) constitute a clearly unwarranted invasion of personal privacy; (iii) disclose the identity of a confidential source; or (iv) endanger the life or physical safety of any individual.

SECTION 4. Said section 1 of said chapter 66A, as so appearing, is hereby further amended by adding the following definition:-

"Protected information", information about the political, religious or social views, associations or activities of any individual, group, association, organization, corporation, business or partnership or other entity.

SECTION 5. Said chapter 66A is hereby further amended by inserting after section 2 the following 6 sections:-

Section 2A. At least once annually, every criminal intelligence system shall conduct an internal audit and publish a report based on the results. This audit shall include:

(i) for each database that contains personal data: (1) the number of authorized users; (2) each user's level of access; (3) the quantity of data accessed by each user on a weekly basis; (4) the number of transactions performed of each specified transaction type for each unique user and access location; (5) the quantity of data collected and maintained from each unique source; and (6) the frequency of use in an investigation of data from each source;

(ii) the numbers of investigations authorized and denied under paragraph (4) of subsection (b) of section 2C, and the dates of initiation and closure for each of these investigations;

(iii) the number of investigations authorized under said paragraph (4) of said subsection (b) that remain open, the date of initiation of the investigation for each open investigation, the length of time the investigation has remained open and a justification for continued collection or maintenance of protected information;

(iv) the number of investigations authorized under said paragraph (4) of said subsection (b) that have led to indictments or prosecutions, and the names and docket numbers of resulting court proceedings; and

(v) the number of authorized disseminations under paragraph (3) of said subsection (b), and to which entity each dissemination was made.

Section 2B. Every criminal intelligence system shall provide assistance and unrestricted access to the office of the inspector general, who shall submit to the clerks of the house of representatives and the senate, the house and senate committees on post audit and oversight, and the joint committee on public safety and homeland security a report every 2 years on the compliance of criminal intelligence systems with section 2C. The report shall include recommendations for corrective action and shall be a public record.

Section 2C. (a) No state or local law enforcement agency, as defined in section 1 of chapter 6E, prosecutorial office, criminal intelligence system, as defined in section 1, police or peace officer or agent thereof shall track, collect, maintain or disseminate protected information, unless such information directly relates to an investigation of criminal activities, and there are reasonable grounds to suspect the subject of the information is involved in criminal conduct.

(b) (1) No protected information obtained in violation of any applicable federal, state or local law, ordinance or regulation shall be knowingly accessed, received, maintained or disseminated.

(2) All protected information shall be evaluated for the reliability of its source and the accuracy of its content prior to being included in any investigation file, whether temporary, interim or permanent in nature.

(3) Protected information shall be disseminated only to law enforcement agencies, contingent upon review and prior written authorization by the head of the originating law enforcement agency or criminal intelligence system. The originating law enforcement agency shall maintain a record of any such written authorization, specifying the reasons the dissemination is necessary, for a minimum of 5 years. The originating entity shall record each instance of dissemination in a log containing: (i) the method of dissemination; (ii) the name of the subject; (iii) the name of the entity with whom the information was shared; and (iv) the date of dissemination.

(4) All investigations undertaken on the basis of any protected information shall first be authorized in writing by the head of the investigating law enforcement agency or criminal intelligence system. A record of any such written authorization, specifying the reasons for such investigation, shall be maintained in the corresponding investigation file for a minimum of 5 years.

(5) A law enforcement agency or criminal intelligence system shall review all information included in its investigation files at least once every 5 years, and shall destroy any information that is not reliable, accurate, relevant and timely; provided, that any documents related to the authorization for and termination of investigations based in whole or in part on protected information collected under this section, and any authorization to disseminate such protected information, shall be retained. Information retained in an investigation file after a review shall be accompanied by the following documentation: the name of the reviewer, the date of review and an explanation of the decision to retain the information.

(6) Any violation of this section constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief or writ of mandamus in the superior court. An action instituted under this paragraph may be brought against any agency with possession, custody or control of personal data, and any person whose data is included in the violation may institute proceedings and shall be entitled to recover actual damages not exceeding $2,000 or $200 per day for each day of violation, whichever is greater. A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under this paragraph. Violations of this section by a government employee shall result in consequences that may include retraining, suspension or termination, in accordance with any memorandums of understanding with employee bargaining units.

Section 2D. The executive office of public safety and security shall engage an independent auditor to select and audit a random sample of the suspicious activity reports held by the Boston Regional Intelligence Center, the commonwealth fusion center and the New England State Police Information Network, relating to current or former residents of the commonwealth. If the auditor finds any of these suspicious activity reports to lack indicia of reasonable suspicion of a crime as outlined in 28 CFR part 23.20, the department of state police shall suspend cooperation with the entity that produced the report until such time as all records held by these agencies pertaining to Massachusetts residents have been reviewed for compliance with 28 CFR part 23.20, and such records purged from these agencies' systems if noncompliant.

Section 2E. (a) The commonwealth fusion center shall publish the names of the members of its privacy oversight committee. The meetings of the privacy oversight committee shall take place at least quarterly, and shall be open to the public.

(b) For entities retaining criminal intelligence information, training manuals related to the handling of personal data shall be available to the public.

Section 2F. Personal data held in a criminal intelligence system shall not be exempt from disclosure to the individual concerned, or to their attorney or their heirs, by reason of being held in a criminal intelligence system; provided, that disclosure is otherwise proper.

Section 2G. After notice and opportunity for a hearing, the office of the inspector general may impose a monetary penalty on any person or group found to be in violation of any of the provisions of sections two A to two F, inclusive, or of any rules or regulations promulgated thereunder. The monetary penalty shall not exceed five hundred dollars for each act or violation. The amount of any such monetary penalty shall be paid to the inspector general for general use.

SECTION 6. After notice and opportunity for a hearing, the office of the inspector general may impose a monetary penalty on any person or group found to be in violation of any of the provisions of SECTION 5, inclusive, or of any rules or regulations promulgated thereunder. The monetary penalty shall not exceed five hundred dollars for each act or violation. The amount of any such monetary penalty shall be paid into the general fund.