SENATE DOCKET, NO. 1217 FILED ON: 1/19/2023

SENATE . . . . . No. 27

The Commonwealth of Massachusetts

PRESENTED BY:

James B. Eldridge

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 to protect private electronic communication, browsing and other activity.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	
James B. Eldridge	*Middlesex and Worcester*	
Jason M. Lewis	*Fifth Middlesex*	*2/9/2023*

SENATE DOCKET, NO. 1217 FILED ON: 1/19/2023

SENATE . . . . . No. 27

By Mr. Eldridge, a petition (accompanied by bill, Senate, No. 27) of James B. Eldridge and Jason M. Lewis for legislation to protect private electronic communication, browsing and other activity. Advanced Information Technology, the Internet and Cybersecurity.

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Third General Court
(2023-2024)

An Act to protect private electronic communication, browsing and other activity.

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. Chapter 276 of the General Laws, as appearing in the 2020 official edition, is hereby amended by striking Section 1B and inserting in its place the following new sections:-

Section 1B. (a) As used in this section, the following words shall have the following meanings:

"Adverse result", the following situations:

(i) danger to the life or physical safety of an individual;

(ii) a flight from prosecution;

(iii) the destruction of or tampering with evidence;

(iv) the intimidation of a potential witness or witnesses; or

(vi) serious jeopardy to an investigation or undue delay of a trial.

“Electronic communication,” the transfer of signs, signals, writings, images, sounds, or data of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system. This term does not include wire and oral communications as defined in section 99 or chapter 272.

“Electronic communication information”, any information pertaining to an electronic communication or the use of an electronic communication service, including, but not limited to the content of electronic communications, metadata, sender, recipients, format, or location of the sender or recipients at any point during the communication, the time or date the communication was created, sent, or received, or any information pertaining to any individual or device participating in the communication. Electronic communication information does not include subscriber information as defined in this section.

"Electronic communication services,” a service that provides to its subscribers or users the ability to send or receive electronic communications, including any service that acts as an intermediary in the transmission of electronic communications, or stores electronic communication information. This definition shall not apply to corporations that do not provide electronic communication services to the general public.

“Electronic device” or “device”, any device that stores, generates, or transmits information in electronic form and that enables access to, or use of, an electronic communication service, remote computing service, or location information service.

“Electronic device information”, electronic communication information and location information stored in a device.

“Electronic information”, electronic communication information and location information stored by a service provider on behalf of a subscriber or user of an electronic communication service, location information service, or remote computing service.

"Foreign corporation", any corporation or other entity that makes a contract or engages in a terms of service agreement with a resident of the commonwealth to be performed in whole or in part by either party in the commonwealth. The making of the contract or terms of service agreement shall be considered to be the agreement of the foreign corporation that a search warrant which has been properly served on it has the same legal force and effect as if served personally within the commonwealth.

“Location information”, information derived from a device or from interactions between devices, with or without the knowledge of the user and regardless of the technological method used, that pertains to or directly or indirectly reveals the present or past geographical location of an individual or device within the Commonwealth of Massachusetts.

“Location information service”, a service that generates location information or is otherwise used to provide location information to the user or subscribed or the service. This term includes global positioning system services and other mapping, locational, or directional information services.

"Massachusetts corporation", any corporation or other entity that is subject to chapter 155 or chapter 156B.

“Metadata”, information, other than communications content, which is necessary to or associated with the provision of electronic communication services, remote computing services, or location information services, including but not limited to information about the source or

destination of electronic communications, date and time of electronic communications, delivery instructions, account information, internet protocol address, quantum of data, data or file type, or data tags.

"Properly served", delivery of a search warrant by hand, by United States mail, by commercial delivery service, by facsimile or by any other manner to any officer of a corporation or its general manager in the commonwealth, to any natural person designated by it as agent for the service of process, or if such corporation has designated a corporate agent, to any person named in the latest certificate filed pursuant to section 15.03 of chapter 156D.

"Remote computing service", the provision of remote computer processing services or remote computer storage of digital assets. This definition shall not apply to corporations that do not provide those services to the general public.

“Service provider”, a person or entity offering electronic communication services, location information services, or remote computing services.

“Subscriber information”, the name, street address, telephone number, email address, or similar contact information provided by the subscriber to a service provider to establish or maintain an account or communication channel, a subscriber or account number or identifier, the length of service, and the types of services used by a user of or subscriber to a service provider.

(b) Except pursuant to a warrant issued by a justice of the superior court or acting in accordance with a legally recognized exception under subsection (k), it shall be unlawful for a government office, law enforcement agency as defined in section 1 of chapter 6E, or public official to

(i) obtain or access electronic information or subscriber information from a service provider

(ii) access electronic device information from the electronic device, whether by physical or electronic means.

(c) A justice of the superior court may issue a search warrant upon a sworn application by the applicant showing there is probable cause to believe that:-

(i) particular identified records or information are in the actual or constructive custody of the Massachusetts or foreign corporation acting as a service provider; and

(ii) such records or information constitute evidence of or the means or instrumentalities of the commission of a specified criminal offense under the laws of the commonwealth.

(d) Search warrants issued under this section shall:-

(i) designate the person, corporation, or other entity, if any, in possession of the records or data sought;

(ii) describe, with particularity, the information sought and to be provided;

(iii) be directed to the law enforcement officer or government making the application for the warrant and authorize them to properly serve the warrant upon the corporation and to take all other actions prescribed by this section; and

(iv) be issued in the form and manner prescribed in sections 2A½ and 2B, insofar as they are applicable.

(e) The following provisions shall apply to any search warrant issued under this section:-

(i) when properly served with a search warrant, a corporation subject to this section shall provide all records sought pursuant to that warrant within 14 days of receipt, including those records maintained or located outside the commonwealth;

(ii) if the applicant makes a showing and the court finds that failure to produce records within less than 14 days would cause an adverse result, a warrant may require production of records within less than 14 days;

(iii) a court may reasonably extend the time required for production of the records upon finding that the corporation has shown good cause for that extension and that an extension of time would not cause an adverse result;

(iv) a corporation seeking to quash a warrant served on it pursuant to this section shall seek relief from the court that issued the warrant within the time required for production of records pursuant to this section. The court shall hear and decide such motion not later than 14 days after the motion is filed; and

(v) the corporation shall verify the authenticity of records that it produces by providing an affidavit from the person in custody of those records certifying that they are true and complete.

(f) A Massachusetts corporation that provides electronic communication services, remote computing services, or location information services, when served with a warrant or subpoena issued by another state to produce records that would reveal the identity of the customers using those services, data stored by, or on behalf of the customer, the customer's usage of those services, the recipient or destination of communications sent to or from those customers, or the content of those communications, shall produce those records as if that warrant or subpoena had been issued under the law of the commonwealth.

(g) No claim shall lie against any foreign or Massachusetts corporation subject to this section, its officers, employees, agents, or other persons for providing records, information, facilities, or assistance in accordance with the terms of a search warrant issued pursuant to this section.

(h) Not later than 7 days after information is obtained by a law enforcement officer or government office pursuant to a warrant under this section, that officer or office shall serve upon, or deliver by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective as specified by the court issuing the warrant, to the individual to whom the information pertains to, a copy of the warrant, a copy of the application for the warrant and notice that informs them of the following:-

(i) the nature of the law enforcement inquiry with reasonable specificity;

(ii) in the case of electronic information, that such information was requested by or supplied to that government office or public official, a description of the information, and the dates on which the request was made and on which the information was supplied;

(iv) whether notification of the customer, subscriber, or user was delayed under subsection (i); and

(v) which court made the certification or determination under which that delay was made, if applicable.

(i) A government office, law enforcement agency, or public official may include in its application for a warrant a request for an order delaying the notification required under subsection (h) for a period not to exceed 90 days, and the court may issue the order if it

determines there is reason to believe that notification of the existence of the warrant may have an adverse result. Upon expiration of any period of delay granted under this subsection, the government office, law enforcement agency as defined in section 1 of chapter 6E, or public official shall provide the customer or subscriber a copy of the warrant together with notice required under, and by the means described in, subsection (h).

(j) A government office, law enforcement agency as defined in section 1 of chapter 6E, or public official may include in its application for a warrant a request for an order directing a corporation or other entity to which a warrant is directed not to notify any other person of the existence of the warrant for a period of not more than 90 days, and the court may issue the order if the court determines that there is reason to believe that notification of the existence of the warrant will have an adverse result.

The court may, upon application, grant one or more extensions of orders delaying notification for an additional 90 days if the court determines that there is reason to believe that notification of the existence of the warrant will have an adverse result.

(k) Notwithstanding any general or special law to the contrary, a government office, law enforcement agency as defined in section 1 of chapter 6E, or public official may obtain or access the categories of information mentioned in subsection (b):-

(i) with the specific contemporaneous written consent of the individual to whom the information pertains as the owner or authorized user of the device or as user or subscriber of the remote computing services, electronic communications services, or location information services;

(ii) with the specific contemporaneous written consent of the recipient of an electronic communication.

(iii) in order to respond to a call for emergency services; or

(iii) in response to an emergency involving immediate danger of death or serious physical injury to any person requires obtaining without delay information relating to the emergency; provided, however, that the request is narrowly tailored to address the emergency and subject to the following limitations:-

(a) the request shall document the factual basis for believing that an emergency involving immediate danger of death or serious physical injury to a person requires obtaining without delay of the information relating to the emergency; and

(b) not later than 48 hours after the government office obtains access to records, it shall file with the appropriate court a signed, sworn statement of a supervisory official of a rank designated by the head of the office setting forth the grounds for the emergency access.

(iv) in case of electronic device information, if the government office, law enforcement agency, or public official, in good faith, believes the device to be lost, stolen, or abandoned; provided, however, that the entity shall only access electronic device information in order to attempt to identify, verify, or contact the owner or authorized possessor of the device.

(l) Within five business days after issuing or denying a warrant, the court shall report to the office of court management within the trial court the following information:-

(i) the name of the agency making the application;

(ii) the offense specified in the warrant or application therefore;

(iii) the nature of the information sought;

(iv) if the warrant application sought authorization to obtain or access information from a corporation or other entity, the name of that entity;

(v) whether the warrant was granted as applied for, was modified, or was denied;

(vi) the period of disclosures or access authorized by the warrant;

(vii) the number and duration of any extensions of the warrant; and

(viii) any order directing delayed notification of the warrant's existence.

In June of each year, the court administrator in the office of court management within the trial court shall transmit to the legislature a full and complete report concerning the number of applications for warrants authorizing or requiring the disclosure of or access to information under this section. The reports shall include a summary and analysis of the data required to be filed with that office. The reports shall be filed with the offices of the clerk of the house and the senate and shall be public records. The court administrator in the office of court management within the trial court shall issue guidance regarding the form of the reports.

(m) The requirements of this section shall apply to all state and local law enforcement officers operating in the commonwealth, whether said officers are assigned to state and local law enforcement operations exclusively, or to a joint task force or other collaborative operations with federal law enforcement agencies.

Section 1C. (a) As used in this section, the following words shall have the following meanings:

"Reverse-keyword court order, any court order, including a search warrant or subpoena, compelling the disclosure of records or information identifying any unnamed persons, by name or other unique identifiers, who electronically searched for particular words, phrases, or websites, or who visited a particular website through a link generated by such a search, regardless of whether the order is limited to a specific geographic area or time frame.

"Reverse-keyword request", any request, in the absence of a court order, by any government entity for the voluntary provision of records or information identifying any unnamed persons, by name or other unique identifiers, who electronically searched for particular words, phrases, or websites, or who visited a particular website through a link generated by such a search, regardless of whether or not the request is limited to a specific geographic area or time frame. Such requests shall include offers to purchase such records or information.

"Reverse-location court order", any court order, including a search warrant or subpoena, compelling the disclosure of records or information pertaining to the location of previously unidentified electronic devices or their unnamed users or owners and whose scope extends to an unknown number of electronic devices present in a specified geographic area at a specified time, irrespective of whether such location is identified via global positioning system coordinates, cell tower connectivity, wi-fi positioning, or any other form of location detection.

"Reverse-location request", any request, in the absence of a court order, by any government entity for the voluntary provision of records or information pertaining to the location of unidentified electronic devices or their unnamed users or owners and whose scope extends to an unknown number of electronic devices present in a specified geographic area at a specified time, irrespective of whether such location is identified via global positioning system

coordinates, cell tower connectivity, wi-fi positioning, or any other form of location detection. Such requests shall include offers to purchase such records or information.

"Subpoena", a grand jury or trial subpoena issued in the course of a criminal proceeding or an administrative subpoena issued pursuant to section 17B of chapter 271.

(b) It shall be unlawful for a government office, law enforcement agency as defined in section 1 of chapter 6E, or public official to:-

(i) seek, from any court, a reverse-location court order or a reverse-keyword court order.

(ii) seek, secure, obtain, borrow, purchase, or review any information or data obtained through a reverse-location court order or a reverse-keyword court order.

(c) No court subject to the laws of the commonwealth shall issue a reverse-location court order or a reverse-keyword court order.

(d) No person or entity in the commonwealth, as a result of any law, regulation, or agreement adopted by the commonwealth or any political subdivision thereof, shall be obligated to comply with a reverse-location court order or a reverse-keyword court order issued by the commonwealth or a political subdivision thereof.

(e) It shall be unlawful for a government office, law enforcement agency, or public official to:-

(i) make a reverse-location request or a reverse-keyword request;

(ii) seek, secure, obtain, borrow, purchase, or review any information or data obtained through a reverse-location request or a reverse-keyword request.

(iii) seek the assistance of any agency of the federal government or any agency of the government of another state or subdivision thereof in obtaining information or data from a reverse-location court order, reverse-keyword court order, reverse-location request, or reverse-keyword request if the government entity would be barred from directly seeking such information under this section.

(f) For the purposes of this section, a record, information, or evidence is “derived from” a reverse-location court order, reverse-keyword court order, reverse-location request, or reverse-keyword request where the government entity would not have originally possessed the information or evidence but for the violative court order or request, and regardless of any claim that the record, information, or evidence is attenuated from the unlawful order or request, would inevitably have been discovered, or was subsequently reobtained through other means.

Section 1D. (a) As used in this section, the following words shall have the following meanings:

"Cell site simulator device", any device that functions as or simulates a base station for commercial mobile services or private mobile services in order to identify, locate, or intercept transmissions from cellular devices for purposes other than providing ordinary commercial mobile services or private mobile services.

(b) It shall be unlawful for a government office, law enforcement agency, or public official to use a cell site simulator device for any purpose other than to locate or track the location of a specific electronic device, pursuant to a warrant consistent with subsection (d), or if exigent circumstances exist requiring swift action to prevent imminent danger to the safety of an individual or the public.

(c) Any warrant application seeking to intercept the substance of a wire or oral communication from an electronic device may only be granted pursuant to section 99 of chapter 272.(d) An application for a warrant to use a cell site simulator device must include:

(i) a statement of facts establishing probable cause to believe that the use of a cell site simulator will aid in the apprehension of a person who the applicant has probable cause to believe has committed, is committing, or is about to commit a felony; and

(ii) sufficient facts demonstrating that less invasive methods of investigation or surveillance to the privacy of non-targeted parties have been tried and failed or reasonably unlikely to succeed if tried; and

(iii) a description of the nature and capabilities of the cell site simulator device that will be used and the manner and method of its deployment, including whether the cell site simulator device will obtain data from non-target communications devices; and

(iv) a description of the procedures that will be followed to protect the privacy of non-targets during the investigation, including the deletion of data obtained from non-target communication devices.

(v) the name of the government agency that owns the cell site simulator device.

(e) All non-target data must be deleted immediately upon collection, but no later than once every 24 hours.

(f) All target data must be deleted within thirty days if there is no longer probable cause to support the belief that such information or metadata is evidence of a crime.

(g) The warrant shall permit the use of a cell site simulator for a period not to exceed fifteen days. Any time prior to the expiration of a warrant, the applicant may apply to the issuing judge for a renewal thereof with respect to the same electronic device, person, and location of surveillance. An application for renewal must incorporate the warrant sought to be renewed together with the application and any accompanying papers upon which it was issued. The application for renewal must set forth the results of the investigation thus far conducted, as well as present grounds for extension in conformity with subsection (d). Upon such application, the judge may issue an order renewing the warrant and extending the authorization for a period not exceeding fifteen days.

(h) For the purposes of this section, a record, information, or evidence is "derived from" unauthorized use of a cell site simulator where the government entity would not have originally possessed the information or evidence but for the violative court order or request, and regardless of any claim that the record, information, or evidence is attenuated from the unlawful order or request, would inevitably have been discovered, or was subsequently re-obtained through other means.

Section 1E. (a) Any individual whose information was obtained by a government entity in violation of sections 1B, 1C, and 1D shall be notified of the violation, in writing, by the government office, law enforcement agency, or public official who committed the violation and of the legal recourse available to that person pursuant to this section.

(b) Except in a judicial, administrative or legislative trial, hearing, or other proceeding alleging a violation of sections 1B, 1C, and 1D, no information acquired in violation of said sections, and no evidence derived therefrom, may be received in evidence in any trial, hearing, or

other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the commonwealth, or a political subdivision thereof.

(c) Any individual alleging harm caused by a violation of sections 1B, 1C, and 1D may bring a civil action against the government office, law enforcement agency, or public official who violated those sections in the Superior Court or any court of competent jurisdiction. Venue in the Superior Court shall be proper in the county in which the plaintiff resides or was located at the time of the violation.

(d) An individual protected by this section shall not be required, as a condition of service or otherwise, to file an administrative complaint with the attorney general or to accept mandatory arbitration of a claim arising under this chapter. Chapter 258 shall not apply to a claim brought under this section.

(e) In a civil action in which the plaintiff prevails, the court may award actual damages, including damages for emotional distress, of one thousand dollars per violation or actual damages, whichever is greater, (punitive damages; and any other relief, including but not limited to injunctive or declaratory relief, that the court deems to be appropriate. In addition to any relief awarded, the court shall award reasonable attorney's fees and costs to any prevailing plaintiff.

(i) In assessing the amount of punitive damages, the court shall consider:-

(a) The number of people whose information was disclosed;

(b) Whether the violation directly or indirectly targeted persons engaged in the exercise of activities protected by the Constitution of the United States of America or the Massachusetts Declaration of Rights, and

(c) The persistence of violations by the government office, law enforcement agency, or public official.

(f) Non-waivable rights. Any provision of a contract or agreement of any kind, including a private corporation terms of service or policies, that purports to waive or limit in any way an individual's rights under this section, including but not limited to any right to a remedy or means of enforcement, shall be deemed contrary to state law and shall be void and unenforceable.

(g) No private or government action brought pursuant to this chapter shall preclude any other action under this chapter.

SECTION 2. Chapter 276 is hereby amended by inserting after section 2A the following section:-

Section 2A½. (a) A warrant issued pursuant to section 1B for records or data from a corporation providing electronic communication services, remote computing services, or location information services shall be in substantially the following form:-

THE COMMONWEALTH OF MASSACHUSETTS.

(COUNTY), ss. (NAME) COURT.

To the Sheriffs of our several counties, or their deputies, any State Police Officer, or a Police Officer of any city or town in the Commonwealth.

Proof by affidavit having been made this day before (name and office of person authorized to issue warrant) by (names of person or persons whose affidavits have been taken) that there is probable cause for believing that certain records or data are in the in the possession of (identify corporation or other entity) and that those records or data constitute evidence of or

the means or instrumentalities of the commission of (specified criminal offense under the laws of the commonwealth).

We therefore authorize you to present this warrant to (identify corporation or other entity), which warrant shall operate as an order for immediate disclosure of the following records or data:

(description of particular records or data), and if any such records or data are disclosed to bring it before (court having jurisdiction) at (name of court and location).

Dated at (city or town) this _____ day of _____, (insert year).

Justice of the Superior Court

(b) A warrant issued pursuant to section 1D authorizing the use of a cell site simulator device shall be in substantially the following form:

THE COMMONWEALTH OF MASSACHUSETTS.

(COUNTY), ss. (NAME) COURT.

To the Sheriff, or their deputy, State Police Officer, or municipal Police Officer who has made this complaint on oath.

Proof by affidavit having been made this day before (name and office of person authorized to issue warrant) by (names of person or persons whose affidavits have been taken) that there is probable cause for believing that the use of a cell site simulator device will lead to evidence of or the means or instrumentalities of the commission of (specified criminal offense under the laws of the commonwealth) or the location of a person whom there is probable cause

to believe has committed, is committing, or is about to commit (specified criminal offense under the laws of the commonwealth).

We therefore authorize you to obtain or access by means of a cell site simulator device, the following records or data:

(description of particular records or data), and if any such records or data are disclosed to bring it before (court having jurisdiction) at (name of court and location).

Dated at (city or town) this _____ day of _____, (insert year).

Justice of the Superior Court

SECTION 3. Section 2B of said chapter 276 is hereby amended by striking clauses 3 and 4 of the model affidavit and inserting in place thereof the following:-

3. Based upon the foregoing reliable information (and upon my personal knowledge) there is probable cause to believe that the property, records or data hereinafter described (has been stolen, or is being concealed, or constitutes evidence of a particular offense, etc.) and may be found (in the possession of A. B. or any other person or corporation) at premises (identify).

4. The (property, records, or data) for which I seek issuance of a search warrant is the following: (here describe the property, records, or data as particularly as possible).

SECTION 4. Section 7 of chapter 78 of the General Laws is hereby amended by striking the third sentence.

SECTION 5. Said chapter 78 is hereby amended by inserting after section 7 the following section:-

Section 7A.

(a) For the purposes of this section, “library user private data” shall mean that part of the records of a public library which reveals the identity and intellectual pursuits of a person using such library.

(b) Library user private data shall not be a public record as defined by clause Twenty-sixth of section seven of chapter four.

(c) The rights contained within sections 1B, 1C and 1E of chapter 276 shall apply to a library user as if that person were in possession of their library user private data.