STATE OF NEW YORK

2313

2019-2020 Regular Sessions

IN ASSEMBLY

January 22, 2019

Introduced by M. of A. RODRIGUEZ, BLAKE, PEOPLES-STOKES, VANEL -- Multi-Sponsored by -- M. of A. COOK -- read once and referred to the Committee on Codes

AN ACT to amend the criminal procedure law, in relation to establishing the EMAIL privacy act (electronic messaging and individual location)

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. This act shall be known and may be cited as the "EMAIL privacy act (electronic messaging and individual location)".

§ 2. Paragraph (c) of subdivision 1 of section 690.15 of the criminal procedure law is amended and a new paragraph (d) is added to read as follows:

(c) A designated or described person[~~.~~]*;*

(d) Designated or described electronic customer data or electronic location information held in electronic storage, including the contents of and records and other information related to a wire communication or electronic communication held in electronic storage. For purposes of this paragraph, "electronic communication" has the meaning assigned by section 250.00 of the penal law, "electronic storage", "wire communication", "electronic customer data" and "electronic location information" have the meaning assigned by section 690.05 of this article.

§ 3. Subdivision 2 of section 690.05 of the criminal procedure law, as amended by chapter 504 of the laws of 1991, the opening paragraph as amended by chapter 424 of the laws of 1998, is amended and a new subdivision 3 is added to read as follows:

2. A search warrant is a court order and process directing a police officer to conduct:

(a) a search of designated premises, or of a designated vehicle, or of a designated person, for the purpose of seizing designated property or kinds of property, and to deliver any property so obtained to the court which issued the warrant; or

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD07279-01-9

(b) a search of a designated premises for the purpose of searching for and arresting a person who is the subject of: (i) a warrant of arrest issued pursuant to this chapter, a superior court warrant of arrest issued pursuant to this chapter, or a bench warrant for a felony issued pursuant to this chapter, where the designated premises is the dwelling of a third party who is not the subject of the arrest warrant; or

(ii) a warrant of arrest issued by any other state or federal court for an offense which would constitute a felony under the laws of this state, where the designated premises is the dwelling of a third party who is not the subject of the arrest warrant[~~.~~]**; or**

(c) a search of designated or described electronic customer data or electronic location information held in electronic storage or mobile device, including the contents of, and records and other information related to a wire communication or electronic communication held in electronic storage or mobile device.

3. The following definitions are applicable to this article:

(a) "Electronic storage" means any storage of electronic customer data in a computer, computer network, or computer system, regardless of whether the data is subject to recall, further manipulation, deletion, or transmission, and includes any storage of a wire or electronic communication by an electronic communications service or a remote computing service.

(b) "Wire communication" means an aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception, including the use of such a connection in a switching station, furnished or operated by a person authorized to engage in providing or operating the facilities for the transmission of communications as a communications common carrier. The term includes the electronic storage of a wire communication.

(c) "Electronic customer data" means data or records that:

(i) are in the possession, care, custody, or control of a provider of an electronic communications service or a remote computing service; and

(ii) contain: (1) information revealing the identity of customers of the applicable service;

(2) information about a customer's use of the applicable service;

(3) information that identifies the recipient or destination of a wire communication or electronic communication sent to or by the customer;

(4) the content of a wire communication or electronic communication sent to or by the customer; and

(5) any data stored by or on behalf of the customer with the applicable service provider.

(d) "Electronic location information" means any information that relates to: (i) the location of a cellular telephone, mobile or other wireless communications device; and (ii) is wholly or partly generated by or derived from the operation of the device.

§ 4. The criminal procedure law is amended by adding a new section 690.60 to read as follows:

§ 690.60 Search warrants; government access to stored customer data, communications and electronic location information.

1. An authorized police officer may require a provider of electronic communications service or a provider of a remote computing service to disclose electronic customer data or electronic location information that is in electronic storage by obtaining a warrant.

2. In executing a search warrant directing a provider of an electronic communications service or a provider of a remote computing service to

disclose only electronic customer data that is information revealing the identity of customers of the applicable service or information about a customer's use of the applicable service a police officer need not give notice to the subscriber or customer:

(a) by obtaining an administrative subpoena authorized by statute;

(b) by obtaining a grand jury subpoena;

(c) by obtaining a warrant;

(d) by obtaining the consent of the subscriber or customer to the disclosure of the data;

(e) by obtaining a court order; or

(f) as otherwise permitted by applicable federal law.

3. A provider of telephonic communications service shall disclose to an authorized police officer, without any form of legal process, subscriber listing information, including name, address, and telephone number or similar access code that:

(a) the service provides to others in the course of providing publicly available directory or similar assistance; or

(b) is solely for use in the dispatch of emergency vehicles and personnel responding to a distress call directed to an emergency dispatch system or when the information is reasonably necessary to aid in the dispatching of emergency vehicles and personnel for the immediate prevention of death, personal injury, or destruction of property.

4. A provider of telephonic communications service shall provide an authorized police officer with the name of the subscriber of record whose published telephone number is provided to the service by an authorized police officer.

5. Electronic location information may be obtained by an authorized police officer without any form of legal process, if:

(a) the device is reported stolen by the owner; or

(b) there exists an immediate life-threatening situation.

§ 5. The criminal procedure law is amended by adding a new section 690.65 to read as follows:

§ 690.65 Search warrants; warrant issued in this state for stored customer data, communications or electronic location information.

1. This section applies to a warrant required under section 690.60 of this article to obtain electronic customer data, including the contents of a wire communication, electronic communication or electronic location information.

2. On the filing of an application by an authorized police officer, a district judge may issue a search warrant under this section for electronic customer data held in electronic storage, including the contents of and records and other information related to a wire communication or electronic communication held in electronic storage or electronic location information, by a provider of an electronic communications service or a provider of a remote computing service described by subdivision eight of this section, regardless of whether the customer data is held at a location in this state or at a location in another state. An application made under this subdivision must demonstrate probable cause for the issuance of the warrant and must be supported by the oath or affirmation of the authorized police officer.

3. A search warrant may not be issued under this section unless the application required by section 690.35 of this article sets forth sufficient and substantial facts to establish probable cause that:

(a) a specific offense has been committed; and

(b) the electronic customer data or electronic location information sought:

(i) constitutes evidence of that offense or evidence that a particular person committed that offense; and

(ii) is held in electronic storage by the service provider on which the warrant is served under subdivision seven of this section.

4. Only the electronic customer data or electronic location information described in the application required by section 690.35 of this article may be seized under the warrant.

5. The police officer shall execute the warrant not later than the tenth day after the date of issuance, except that the officer shall execute the warrant within a shorter period if so directed in the warrant by the district judge. For purposes of this subdivision, a warrant is executed when the warrant is served in the manner described by subdivision seven of this section.

6. A warrant under this section may be served only on a service provider that is a domestic entity or a company or entity otherwise doing business in this state under a contract or a terms of service agreement with a resident of this state, if any part of that contract or agreement is to be performed in this state. The service provider shall produce all electronic customer data, contents of communications, electronic location information, and other information sought, regardless of where the information is held in the United States and within the period allowed for compliance with the warrant, as provided by subdivision eight of this section. A court may find any designated officer, designated director, or designated owner of a company or entity in contempt of court if the person by act or omission is responsible for the failure of the company or entity to comply with the warrant within the period allowed for compliance. The failure of a company or entity to timely deliver the information sought in the warrant does not affect the admissibility of that evidence in a criminal proceeding.

7. A search warrant issued under this section is served when the authorized police officer delivers the warrant by hand, by facsimile transmission, or, in a manner allowing proof of delivery, by means of the United States mail or a private delivery service to:

(a) a person specified by section three hundred five of the business corporation law;

(b) the secretary of state in the case of a company or entity to which section three hundred six of the business corporation law applies; or

(c) any other person or entity designated to receive the service of process.

8. The district judge shall indicate in the warrant that the deadline for compliance by the provider of an electronic communications service or the provider of a remote computing service is the fifteenth business day after the date the warrant is served if the warrant is to be served on a domestic entity or a company or entity otherwise doing business in this state, except that the deadline for compliance with a warrant served in accordance with section three hundred six of the business corporation law, may be extended to a date that is not later than the thirtieth day after the date the warrant is served. The judge may indicate in a warrant that the deadline for compliance is earlier than the fifteenth business day after the date the warrant is served if the officer makes a showing and the judge finds that failure to comply with the warrant by the earlier deadline would cause serious jeopardy to an investigation, cause undue delay of a trial, or create a material risk of:

(a) danger to the life or physical safety of any person;
(b) flight from prosecution;
(c) the tampering with or destruction of evidence; or
(d) intimidation of potential witnesses.

9. If the authorized police officer serving the warrant under this section also delivers an application form to the provider of an electronic communications service or the provider of a remote computing service responding to the warrant, and the police officer also notifies the provider in writing that an executed application is required, then the provider shall verify the authenticity of the customer data, contents of communications, electronic location information, and other information produced in compliance with the warrant by including with the information the application form completed and sworn to by a person who is a custodian of the information or a person otherwise qualified to attest to its authenticity that states that the information was stored in the course of regularly conducted business of the provider and specifies whether it is the regular practice of the provider to store that information.

10. On a service provider's compliance with a warrant under this section, an authorized police officer shall file a return of the warrant and a copy of the inventory of the seized property as required under section 690.50 of this article.

11. The district judge shall hear and decide any motion to quash the warrant not later than the fifth business day after the date the service provider files the motion. The judge may allow the service provider to appear at the hearing by teleconference.

12. A provider of an electronic communications service or a provider of a remote computing service responding to a warrant issued under this section may request an extension of the period for compliance with the warrant if extenuating circumstances exist to justify the extension. The district judge shall grant a request for an extension based on those circumstances if:

(a) the authorized police officer who applied for the warrant or another appropriate authorized police officer agrees to the extension; or

(b) the district judge finds that the need for the extension outweighs the likelihood that the extension will cause an adverse circumstance described by subdivision eight of this section.

§ 6. The criminal procedure law is amended by adding a new section 690.70 to read as follows:

§ 690.70 Search warrants; warrant issued in another state for stored customer data, communications or electronic location information.

Any domestic entity that provides electronic communications services or remote computing services to the public shall comply with a warrant issued in another state and seeking information described in subdivision two of section 690.65 of this article, if the warrant is served on the entity in a manner equivalent to service of process required by subdivision eight of section 690.65 of this article.

§ 7. The criminal procedure law is amended by adding a new section 690.75 to read as follows:

§ 690.75 Search warrants; back-up preservation for stored customer data, communications or electronic location information.

1. A subpoena or court order for disclosure of certain electronic customer data or electronic location information held in electronic storage by a provider of an electronic communications service or a

provider of a remote computing service may require that provider to create a copy of the customer data or electronic location information sought by the subpoena or court order for the purpose of preserving that data. The provider may not inform the subscriber or customer whose data is being sought that the subpoena or court order has been issued. The provider shall create the copy within a reasonable time as determined by the court issuing the subpoena or court order.

2. The provider of an electronic communications service or the provider of a remote computing service shall immediately notify the authorized police officer who presented the subpoena or court order requesting the copy when the copy has been created.

3. The authorized police officer shall notify the subscriber or customer whose electronic customer data or electronic location information is the subject of the subpoena or court order of the creation of the copy not later than three days after the date of the receipt of the notification from the applicable provider that the copy was created.

4. The provider of an electronic communications service or the provider of a remote computing service shall release the copy to the requesting authorized police officer not earlier than the fourteenth day after the date of the police officer's notice to the subscriber or customer if the provider has not:

(a) initiated proceedings to challenge the request of the police officer for the copy; or

(b) received notice from the subscriber or customer that the subscriber or customer has initiated proceedings to challenge the request.

5. The provider of an electronic communications service or the provider of a remote computing service may not destroy or permit the destruction of the copy until the electronic customer data or electronic location information has been delivered to the applicable law enforcement agency or until the resolution of any court proceedings, including appeals of any proceedings, relating to the subpoena or court order requesting the creation of the copy, whichever occurs last.

6. An authorized police officer who reasonably believes that notification to the subscriber or customer of the subpoena or court order would result in the destruction of or tampering with electronic customer data or electronic location information sought may request the creation of a copy of the data. The police officer's belief is not subject to challenge by the subscriber or customer or by a provider of an electronic communications service or a provider of a remote computing service.

7. (a) A subscriber or customer who receives notification as described in subdivision three of this section may file a written motion to quash the subpoena or vacate the court order in the court that issued the subpoena or court order not later than the fourteenth day after the date of the receipt of the notice. The motion must contain an affidavit or sworn statement stating:

(i) that the applicant is a subscriber or customer of the provider of an electronic communications service or the provider of a remote computing service from which the electronic customer data or electronic location information held in electronic storage for the subscriber or customer has been sought; and

(ii) the applicant's reasons for believing that the customer data or electronic location information sought is not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this article in some other respect.

(b) The subscriber or customer shall give written notice to the provider of an electronic communications service or the provider of a

remote computing service of the challenge to the subpoena or court order. The authorized police officer requesting the subpoena or court order must be served a copy of the papers filed by personal delivery or by registered or certified mail.

8. (a) The court shall order the authorized police officer to file a sworn response to the motion filed by the subscriber or customer if the court determines that the subscriber or customer has complied with the requirements of subdivision seven of this section. On request of the police officer, the court may permit the response to be filed in camera. The court may conduct any additional proceedings the court considers appropriate if the court is unable to make a determination on the motion on the basis of the parties' initial allegations and response.

(b) The court shall rule on the motion as soon after the filing of the officer's response as practicable. The court shall deny the motion if the court finds that the applicant is not the subscriber or customer whose electronic customer data or electronic location information held in electronic storage is the subject of the subpoena or court order or that there is reason to believe that the police officer's inquiry is legitimate and that the customer data sought is relevant to that inquiry. The court shall quash the subpoena or vacate the order if the court finds that the applicant is the subscriber or customer whose data is the subject of the subpoena or court order and that there is not a reason to believe that the data is relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this article.

(c) A court order denying a motion or application under this section is not a final order and no interlocutory appeal may be taken from the denial.

§ 8. The criminal procedure law is amended by adding a new section 690.80 to read as follows:

§ 690.80 Search warrants; preclusion of notification for stored customer data, communications or electronic location information.

1. An authorized police officer seeking electronic customer data or electronic location information may apply to the court for an order commanding the service provider to whom a warrant, subpoena, or court order is directed not to disclose to any person the existence of the warrant, subpoena, or court order. The order is effective for the period the court considers appropriate. The court shall enter the order if the court determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will have an adverse result.

2. In this section, an "adverse result" means:

(a) endangering the life or physical safety of an individual;

(b) flight from prosecution;

(c) destruction of or tampering with evidence;

(d) intimidation of a potential witness; or

(e) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

§ 9. The criminal procedure law is amended by adding a new section 690.85 to read as follows:

§ 690.85 Search warrants; reimbursement of costs for stored customer data, communications or electronic location information.

1. Except as provided by subdivision three of this section, an authorized police officer who obtains information under this article shall reimburse the person assembling or providing the information for all costs that are reasonably necessary and that have been directly incurred

in searching for, assembling, reproducing, or otherwise providing the information. These costs include costs arising from necessary disruption of normal operations of an electronic communications service or remote computing service in which the information may be stored.

2. The authorized police officer and the person providing the information may agree on the amount of reimbursement. If there is no agreement, the court that issued the order for production of the information shall determine the amount. If no court order was issued for production of the information, the court before which the criminal prosecution relating to the information would be brought shall determine the amount.

3. Subdivision one of this section does not apply to records or other information maintained by a communications common carrier that relate to telephone toll records or telephone listings unless the court determines that the amount of information required was unusually voluminous or that an undue burden was imposed on the provider.

§ 10. The criminal procedure law is amended by adding a new section 690.90 to read as follows:

§ 690.90 Search warrants; stored customer data, communications or electronic location information; no cause of action.

A subscriber or customer of a provider of an electronic communications service or a provider of a remote computing service does not have a cause of action against a provider or its officers, employees, or agents or against other specified persons for providing information, facilities, or assistance as required by a court order, warrant, subpoena, or certification under this article.

§ 11. The criminal procedure law is amended by adding a new section 690.95 to read as follows:

§ 690.95 Search warrants; stored customer data, communications or electronic location information; cause of action.

Except as provided by section 690.90 of this article, a provider of an electronic communications service or a provider of a remote computing service, or a subscriber or customer of that provider, that is aggrieved by a violation of this article has a civil cause of action if the conduct constituting the violation was committed knowingly or intentionally and is entitled to:

1. injunctive relief;

2. a reasonable attorney's fee and other litigation costs reasonably incurred; and

3. the sum of the actual damages suffered and any profits made by the violator as a result of the violation or one thousand dollars, whichever is more.

§ 12. The criminal procedure law is amended by adding a new section 690.96 to read as follows:

§ 690.96 Search warrants; annual report of warrants and orders.

1. No later than January fifteenth of each year, a provider of an electronic communication service or a provider of a remote computing service doing business in this state shall report to the office of public safety the following information for the preceding calendar year, disaggregated by each law enforcement agency in this state making the applicable requests:

(a) the number of requests made for pen register or trap and trace information;

(b) the number of requests made for ESN reader information;

(c) the number of requests made for location information;

(d) the number of individuals whose location information was disclosed; and

(e) the amount that each law enforcement agency was billed by the communication common carrier or electronic communications service for each request made under paragraph (a), (b) or (c) of this subdivision.

2. No later than the thirtieth day after the date of expiration of a warrant or order issued under this article or an order extending the period of a warrant or order issued under this article, or no later than the thirtieth day after the date the court denies an application for a warrant or order under this article, the court shall submit to the office of public safety the following information, as applicable:

(a) the receipt of an application for a warrant or order under this article;

(b) the type of warrant or order for which the application was made;

(c) whether any application for an order of extension was granted, granted as modified by the court, or denied;

(d) the period of monitoring authorized by the warrant or order and the number and duration of any extensions of the warrant or order;

(e) the offense under investigation, as specified in the application for the warrant or order or an extension of the warrant or order; and

(f) the law enforcement agency or prosecutor that submitted an application for the warrant or order or an extension of the warrant or order.

3. No later than January fifteenth of each year, each prosecutor that submits an application for a warrant or order or an extension of a warrant or order under this article shall submit to the office of public safety the following information for the preceding calendar year;

(a) the information required to be submitted by a court with respect to each application submitted by the prosecutor for the warrant or order or an extension of the warrant or order;

(b) a general description of information collected under each warrant or order that was issued by the court, including the approximate number of individuals for whom location information was intercepted and the approximate duration of the monitoring of the location information of those individuals;

(c) the number of arrests made as a result of information obtained under a warrant or order issued under this article;

(d) the number of criminal trials commenced as a result of information obtained under a warrant or order issued under this article; and

(e) the number of convictions obtained as a result of information obtained under a warrant or order issued under this article.

4. Information submitted to the office of public safety under this section is public information and subject to disclosure.

5. No later than March first of each year, the office of public safety shall submit a report to the governor, the state attorney general, the speaker of the assembly, and the chairs of the standing committees of the senate and assembly with primary jurisdiction over criminal justice. The report must contain the following information for the preceding calendar year:

(a) an assessment of the extent of tracking or monitoring by law enforcement agencies of pen register, trap and trace, ESN reader, and location information;

(b) a comparison of the ratio of the number of applications for warrants or orders made under this article to the number of arrests and convictions resulting from information obtained under a warrant or order issued under this article;

(c) identification of the types of offenses investigated under a warrant or order issued under this article; and

(d) with respect to both state and local jurisdictions, an estimate of the total cost of conducting investigations under a warrant or order issued under this article.

§ 13. The criminal procedure law is amended by adding a new section 690.97 to read as follows:

§ 690.97 Search warrants; stored customer data, communications and electronic location information and use in a court of law.

Stored customer data, communications and electronic location information obtained without any form of legal process and not pursuant to section 690.60 of this article shall be inadmissible in a court of law.

§ 14. This act shall take effect immediately.