Session of 2016

HOUSE BILL No. 2715

By Committee on Federal and State Affairs

3-2

AN ACT enacting the electronic communications privacy act; relating to electronic communications; search warrants.

Be it enacted by the Legislature of the State of Kansas:

Section 1. (a) Sections 1 through 4, and amendments thereto, shall be known and may be cited as the electronic communications privacy act.

(b) As used in the electronic communications privacy act:

(1) "Adverse result" means any of the following:

(A) Danger to the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

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

(2) "Authorized possessor" means the possessor of an electronic device when that person is the owner of the device or has been authorized to possess the device by the owner of the device.

(3) "Electronic communication" means the transfer of signs, signals, writings, images, sounds, data or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric or photo-optical system.

(4) "Electronic communication information" means any information about an electronic communication or the use of an electronic communication service, including, but not limited to, the contents, 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, including, but not limited to, an IP address. Electronic communication information does not include subscriber information.

(5) "Electronic communication service" means 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.

(6) "Electronic device" means a device that stores, generates or transmits information in electronic form.

(7) "Electronic device information" means any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device.

(8) "Electronic information" means electronic communication information or electronic device information.

(9) "Governmental entity" means a department or agency of the state or a political subdivision thereof, or an individual acting for or on behalf of the state or a political subdivision thereof.

(10) "Service provider" means a person or entity offering an electronic communication service.

(11) "Specific consent" means consent provided directly to the governmental entity seeking information, including, but not limited to, when the governmental entity is the addressee or intended recipient or a member of the intended audience of an electronic communication. Specific consent does not require that the originator of the communication have actual knowledge that an addressee, intended recipient or member of the specific audience is a governmental entity.

(12) "Subscriber information" means the name, street address, telephone number, email address or similar contact information provided by the subscriber to the 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.

Sec. 2. (a) (1) Except as provided in this section, a governmental entity shall not:

(A) Compel the production of or access to electronic communication information from a service provider;

(B) compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device; or

(C) access electronic device information by means of physical interaction or electronic communication with the electronic device.

(2) This section does not prohibit the intended recipient of an electronic communication from voluntarily disclosing electronic communication information concerning that communication to a governmental entity.

(b) A governmental entity may compel the production of or access to electronic communication information from a service provider, or compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device only under the following circumstances:

(1) Pursuant to a warrant issued pursuant to K.S.A. 22-2502, and amendments thereto;

(2) pursuant to an order issued pursuant to K.S.A. 22-2515 or 22-2516, and amendments thereto;

(3) pursuant to a request for cellular location information in an emergency situation pursuant to K.S.A. 2015 Supp. 22-4615, and amendments thereto; and

(4) pursuant to a subpoena issued pursuant to existing state law, provided that the information is not sought for the purpose of investigating or prosecuting a criminal offense, and compelling the production of or access to the information via the subpoena is not otherwise prohibited by state or federal law. Nothing in this paragraph shall be construed to expand any authority under state law to compel the production of or access to electronic information.

(c) A governmental entity may access electronic device information by means of physical interaction or electronic communication with the device only as follows:

(1) Pursuant to a warrant issued pursuant to K.S.A. 22-2502, and amendments thereto;

(2) pursuant to an order issued pursuant to K.S.A. 22-2515 or 22-2516, and amendments thereto;

(3) with the specific consent of the authorized possessor of the device;

(4) with the specific consent of the owner of the device, only when the device has been reported as lost or stolen;

(5) if the governmental entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information;

(6) if the governmental entity, in good faith, believes the device to be lost, stolen or abandoned, provided 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; or

(7) except where prohibited by state or federal law, if the device is seized in a correctional facility under the jurisdiction of the department of corrections in accordance with rules and regulations or internal management policies and procedures of the department of corrections.

(d) Any warrant for electronic information shall comply with the requirements of this subsection.

(1) The warrant shall describe with particularity the information to be seized by specifying the time periods covered and, as appropriate and reasonable, the target individuals or accounts, the applications or services covered and the types of information sought.

(2) The warrant shall require that any information obtained through the execution of the warrant that is unrelated to the objective of the warrant shall be sealed and not subject to further review, use or disclosure

without a court order. A court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use or disclosure is required by state or federal law.

(3) The warrant shall comply with all other provisions of state and federal law, including any provisions prohibiting, limiting or imposing additional requirements on the use of search warrants. If directed to a service provider, the warrant shall be accompanied by an order requiring the service provider to verify the authenticity of electronic information that it produces by providing an affidavit that complies with the requirements set forth in the rules of evidence. Admission of that information into evidence shall be subject to the rules of evidence.

(e) When issuing any warrant or order for electronic information, or upon the petition from the target or recipient of the warrant or order, a court may, at its discretion, require that any information obtained through the execution of the warrant or order that is unrelated to the objective of the warrant be destroyed as soon as feasible after the termination of the current investigation and any related investigations or proceedings.

(f) A service provider may voluntarily disclose electronic communication information or subscriber information when that disclosure is not otherwise prohibited by state or federal law.

(g) If a governmental entity receives electronic communication information voluntarily provided pursuant to subsection (f), it shall destroy that information within 90 days unless one or more of the following circumstances apply:

(1) The entity has or obtains the specific consent of the sender or recipient of the electronic communications about which information was disclosed;

(2) the entity obtains a court order authorizing the retention of the information. A court shall issue a retention order upon a finding that the conditions justifying the initial voluntary disclosure persist, in which case the court shall authorize the retention of the information only for so long as those conditions persist, or there is probable cause to believe that the information constitutes evidence that a crime has been committed; or

(3) the entity reasonably believes that the information relates to child pornography and the information is retained as part of a multiagency database used in the investigation of child pornography and related crimes.

(h) If a governmental entity obtains electronic information pursuant to an emergency involving danger of death or serious physical injury to a person, that requires access to the electronic information without delay, the entity shall, within three days after obtaining the electronic information, file with the appropriate court an application for a warrant or order authorizing obtaining the electronic information or a motion seeking

approval of the emergency disclosures that shall set forth the facts giving rise to the emergency, and if applicable, a request supported by a sworn affidavit for an order delaying notification pursuant to section 3(b)(1), and amendments thereto. The court shall promptly rule on the application or motion and shall order the immediate destruction of all information obtained, and immediate notification pursuant to section 3(a), and amendments thereto, if such notice has not already been given, upon a finding that the facts did not give rise to an emergency or upon rejecting the warrant or order application on any other ground.

(i) This section does not limit the authority of a governmental entity to use an administrative, grand jury, trial or civil discovery subpoena to do any of the following:

(1) Require an originator, addressee or intended recipient of an electronic communication to disclose any electronic communication information associated with that communication;

(2) require an entity that provides electronic communications services to its officers, directors, employees or agents for the purpose of carrying out their duties, to disclose electronic communication information associated with an electronic communication to or from an officer, director, employee or agent of the entity; or

(3) require a service provider to provide subscriber information.

Sec. 3. (a) Except as otherwise provided in this section, any governmental entity that executes a warrant, or obtains electronic information in an emergency pursuant to section 1, and amendments thereto, shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, the identified targets of the warrant or emergency request, a notice that informs the recipient that information about the recipient has been compelled or requested, and states with reasonable specificity the nature of the governmental investigation under which the information is sought. The notice shall include a copy of the warrant or a written statement setting forth facts giving rise to the emergency. The notice shall be provided contemporaneously with the execution of a warrant, or, in the case of an emergency, within three days after obtaining the electronic information.

(b) (1) When a warrant is sought or electronic information is obtained in an emergency under section 1, and amendments thereto, the governmental entity may submit a request supported by a sworn affidavit for an order delaying notification and prohibiting any party providing information from notifying any other party that information has been sought. The court shall issue the order if the court determines that there is reason to believe that notification may have an adverse result, but only for the period of time that the court finds there is reason to believe that the notification may have that adverse result, and not to exceed 90 days.

(2) The court may grant extensions of the delay of up to 90 days each on the same grounds as provided in paragraph (1).

(3) Upon expiration of the period of delay of the notification, the governmental entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective as specified by the court issuing the order authorizing delayed notification, the identified targets of the warrant: (A) A document that includes the information described in subsection (a); (B) a copy of all electronic information obtained or a summary of that information, including, at a minimum, the number and types of records disclosed, the date and time when the earliest and latest records were created; and (C) a statement of the grounds for the court's determination to grant a delay in notifying the individual.

(c) If there is no identified target of a warrant or emergency request at the time of its issuance, the governmental entity shall submit to the attorney general, within three days of the execution of the warrant or issuance of the request, all of the information required in subsection (a). If an order delaying notice is obtained pursuant to subsection (b), the governmental entity shall submit to the attorney general, upon the expiration of the period of delay of the notification, all of the information required in subsection (b)(3). The attorney general shall publish all such reports on an official website within 90 days of receipt. The attorney general may redact names or other personal identifying information from the reports.

(d) Except as otherwise provided in this section, nothing in the electronic communications privacy act shall prohibit or limit a service provider or any other party from disclosing information about any request or demand for electronic information.

Sec. 4. (a) Any person in a trial, hearing or proceeding may move to suppress any electronic information obtained or retained in violation of the fourth amendment to the constitution of the United States or of the electronic communications privacy act.

(b) The attorney general may commence a civil action to compel any governmental entity to comply with the provisions of the electronic communications privacy act.

(c) An individual whose information is targeted by a warrant, order or other legal process that is inconsistent with the electronic communications privacy act, or the constitution of the state of Kansas or the constitution of the United States, or a service provider or any other recipient of the warrant, order or other legal process may petition the issuing court to void or modify the warrant, order or process, or to order the destruction of any information obtained in violation of the electronic communications privacy act, or the constitution of the state of Kansas or the constitution of

the United States.

(d) A Kansas or foreign corporation, and its officers, employees and agents, are not subject to any cause of action for providing records, information, facilities or assistance in accordance with the terms of a warrant, court order, statutory authorization, emergency certification or wiretap order issued pursuant to the electronic communications privacy act.

Sec. 5. This act shall take effect and be in force from and after its publication in the statute book.