Maine State Legislature
OFFICE OF POLICY AND LEGAL ANALYSIS
www.mainelegislature.gov/opla
13 State House Station, Augusta, Maine 04333-0013
(207) 287-1670

BILL ANALYSIS

TO: Members, Joint Standing Committee on Judiciary

FROM: Janet Stocco, Legislative Analyst

DATE: September 25, 2023

RE: **LD 1576, An Act to Update the Laws Governing Electronic Device Information as Evidence (Rep. O'Neil)**

CURRENT STATE LAW

The following laws govern state and local government access to specific types of information held by an "electronic communication service"—*e.g.,* a cellular, email or social media company—or a "remote computing service"—a computer storage or processing service, *e.g.*, a cloud storage company.

1. **<u>Portable</u> electronic device <u>content</u> information – warrant generally required.** Title 16, chapter 3, *subchapter 10* generally requires state and local governments to obtain a search warrant and provide subsequent notice to the user or owner of the portable electronic device in order to access portable electronic device "content information"—information about the substance or meaning of an electronic or wire communication. The law also specifies (a) circumstances in which a warrant is not required—including when law enforcement has consent, the information is public or there is an emergency—and (b) circumstances in which notice is not required—when providing the required notice within 3 days of accessing the information would lead to an adverse result, for example, flight from prosecution. If a state or local government violates the provisions of this law, the information it obtains is inadmissible in any proceeding and a court may enjoin future violations by the government.

2. **<u>Location</u> of an electronic device – warrant generally required.** Title 16, chapter 3, *subchapter 11* generally requires state and local governments to obtain a search warrant and provide subsequent notice to the user or owner of the electronic device in order to access information about the current or prior location of the device. The law also specifies (a) circumstances in which a warrant is not required—including the circumstances above as well as when the user calls for help or is thought to be dead or missing—and (b) circumstances in which notice is not required—when providing the required notice within 3 days of accessing the information would lead to an adverse result (defined the same as in the law above). A search warrant for location information must be limited in time and location information obtained in compliance with this law is admissible in a hearing only if advance notice is provided to the other party, unless such notice is not possible.

SUMMARY OF LD 1576

Note: The attached chart summarizes and compares LD 1575 and current state law.

LD 1576 amends Title 16, chapter 3, subchapter 10, the law governing state and local government access to portable electronic device content information, by:

1. **Type of device**: Extending its protections to "electronic devices" —*i.e.,* all devices that store, generate or transmit electronic information—not just portable electronic devices.

2. **Type of information:** Extending the warrant and notice requirements (and their exceptions) beyond content information to a much broader category of "electronic device information" that includes:
   - Information "transferred through electronic communication"—presumably ***content information***
   - Information "transferred . . . through the use of an electronic communication service," including the format, time and date of a communication, the location of a sender or recipient during the communication or the IP address of a device involved in the communication—*i.e.,* ***additional communication information***
   - Current and prior locations of the electronic device—*i.e.,* ***location information***; and
   - ***Other information*** "stored on, generated or transmitted through the operation of the device"—likely including photos/videos stored on the device or in the cloud, browser search history, etc.

3. **Type of access:** Extending the warrant and notice requirements (and their exceptions) to state and local government entity access to electronic device information through the following means:
   - Obtaining information directly from an electronic communication service or remote computing service (the type of access regulated by current law);
   - Compelling production of information by any person who is not the device owner or user (new);
   - The government entity physically interacting with the electronic device (new); or
   - The government entity communicating electronically with the electronic device (new).

4. **Voluntary recipient disclosure**: Clarifying that a recipient of an electronic communication may voluntarily disclose information about the electronic communication to a government entity.

ISSUES FOR CONSIDERATION

1. **Fourth Amendment**. The Fourth Amendment to the U.S. Constitution protects persons from unreasonable searches and seizures by the government. While the Fourth Amendment expressly recognizes the reasonableness of a government search pursuant to a valid search warrant based on probable cause, the courts have also recognized the reasonableness of several types of *warrantless* searches, including those (a) based on valid consent; (b) incident to lawful arrest; (c) where there are exigent circumstances and probable cause; (d) where law enforcement is legally present and apparent evidence of a crime is in plain view; or (e) where special law enforcement circumstances exist, for example, to control an international border; or (f) where the person voluntarily gives the information to a third party. When applying these decisions to new technologies, the U.S. Supreme Court has focused on preserving a person's legitimate and reasonable expectations of privacy. For example, in *Riley v. California*, 573 U.S. 373 (2014), the Court held that the justification for allowing a warrantless search incident to arrest—officer safety and presenting evidence destruction—does not justify a warrantless search of the contents of an arrestee's cell phone. In reaching this decision, the Court noted the arrestee's significant privacy interest in the immense amount of information that can be stored on a phone, including several years' worth of text messages, pictures, videos and other data.

2. **Third party doctrine**. The U.S. Supreme Court has held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties . . . even if the information is revealed on the assumption that it will be used only for a limited purpose." The government may therefore obtain such information "without triggering Fourth Amendment protections." *Carpenter v.*

United States, 138 S. Ct. 2206, 2216 (2018). In *United States v. Miller*, 425 U.S. 435 (1976), the Court held that the government could validly subpoena banks (and not seek a search warrant from a court) to obtain a person's canceled checks, deposit slips and account statements, all of which contain information the person voluntarily shared with the bank. Similarly, in *Smith v. Maryland*, 442 U.S. 735 (1979), the Court held that use of a pen register to record all outgoing numbers dialed on a telephone did not require a search warrant because customers voluntarily share the numbers they dial with the telephone company. The Court emphasized in both decisions that, by choosing to share these types of information with a third party, the defendants had "taken the risk" that those third parties would convey that information to the government. *See Carpenter*, 138 S. Ct. at 2216.

This doctrine has its limits, however. In 2018, the Court held in *Carpenter v. United States* that the underpinnings of the third-party doctrine do not justify a warrantless search for detailed historic cell-site location information (CSLI), even though the information is held by a third party. Importantly, the Court concluded that "in no meaningful sense does the user voluntarily assume the risk of turning over a comprehensive dossier of his physical movements"—*i.e.,* information about the person's location "every day, every moment, over several years"—merely by using a cell phone. *Id.* at 2220. In reaching its decision about historic CSLI, the Court specifically did not decide whether a warrant is required for government access to "real-time" CSLI about a specific person or a "tower dump" of information about all devices connected to a particular cell site during a particular time. *Id*. at 2220.

3. **Federal statute.** The Stored Communications Act (SCA), 18 U.S.C. §2701 to §2713:

   - **Generally prohibits** an electronic communication service or remote computing service from knowingly divulging the ***contents of an electronic communication*** or other information about the service's customer or subscriber (a.k.a. ***subscriber information***) to any person or entity.

   However, the federal SCA:

   - **Allows** companies to disclose content information and subscriber information in specific circumstances including: with customer/subscriber consent, to make a cybertip about child sexual abuse material (CSAM) or in an emergency involving danger of death or serious physical injury.
   - **Requires** companies to divulge content or subscriber information if the government has:
     - ***A warrant based on probable cause***—for any content or subscriber information;
     - ***A court order based on reasonable grounds, with prior notice to the customer***—for content information stored for any length of time by a remote computing service or for content information stored for >180 days by an electronic communication service;
       - The SCA provides a mechanism for courts to delay notice if prior notice will lead to one of several specified adverse results (a list similar to the adverse results in Maine law).
     - ***A court order based on reasonable grounds without notice to the customer***—for all types of subscriber information; or
     - ***An administrative or federal or state court or grand jury subpoena***—for specific subscriber information, including the subscriber's name, IP address, session times and duration, etc.

4. **Sponsor's stated intent:** LD 1576 is designed to clarify that, regardless of the third-party doctrine and any lesser protections under the federal SCA, state and local government entities must, except in certain specifically enumerated circumstances, have a search warrant and provide subsequent notice the owner or user of an electronic device to obtain (a) past or current location information, (b) electronic communication content information, (c) electronic communication metadata and (d) other information stored on, transmitted through or generated by use of the electronic device.

5. **Concerns raised in testimony and potential amendments**:

- The Attorney General indicated that the bill's current language would "significantly imped[e]" computer crime, financial crime and homicide investigations. The Maine State Police's Computer Crimes Unit and the Maine Prosecutors' Association expressed several other concerns, including:
  - Although the bill includes an emergency exception to the warrant requirement, delays in receiving tips can often render this exception to the warrant requirement inapplicable.
  - The SCA currently allows law enforcement to subpoena limited subscriber information—*e.g.,* name, address, telephone records or records of session times and durations, telephone number or IP address, and means of payment. These subpoenas are often the only step available to commence an investigation in response to a tip about suspected internet criminal activity, for example a tip about an internet scam or a cybertip about online child sexual abuse material. It may be impossible for investigators to develop probable cause for a warrant to obtain content or other information without first obtaining this subscriber information.
  - Even when probable case exists, drafting search warrants for electronic information is a complex and time-consuming process that delays the commencement of these investigations.
- The sponsor requested that her bill be carried over to provide time for her to work with the Attorney General's Office and law enforcement to address their concerns.

6. **Drafting Issues**:

- **Subscriber information – definition**: This term is defined but not otherwise used in the bill.
- **Electronic communication information – definition.** This definition is somewhat vague.
  - Does "the information transferred through electronic communication" = content information?
  - What is "the information contained under a sender or recipients [sic] folder"?

  The sponsor noted that her definition is based on the definition in the California Electronic Communications Privacy Act, which reads:

  > "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 as defined in this chapter.

- **Location information – conflicts with current law**. Current law regarding government access to location information (subchapter 11) differs from the rubric in LD 1576 for government access to all device information, including location information, in the following ways (see attached chart):
  - Which methods of government access require a warrant (or an exception to the requirement);
  - Whether a warrant for location information must be limited in duration;
  - Which exceptions to the warrant requirement apply and whether the government must file a statement of facts with the court after the government uses the emergency exception; and
  - Whether pre-trial notice is required for location information to be admissible in evidence.

  Does the committee wish to exclude location information from LD 1576, leaving the current law regulating location information in place? Or, should the current law for location information be repealed, with or without incorporating some of that law's provisions in LD 1576?
- **Bill Section 14 – drafting error?** Is " electronic device information" correctly placed in this section of the bill or should it only include "electronic communication information"?

FISCAL IMPACT

The Preliminary Fiscal Impact Statement (dated 5/11/23) anticipates the bill will have "No fiscal impact."