HOUSE OF REPRESENTATIVES
2 STATE HOUSE STATION
AUGUSTA, MAINE 04333-0002
(207) 287-1400
TTY: MAINE RELAY 711

Margaret O'Neil
21 Sheila Circle
Saco, ME 04072
Phone: (207) 590-1679
Margaret.O'Neil@legislature.maine.gov

May 22, 2023

Testimony of Rep. Maggie O'Neil sponsoring

LD 1576, An Act to Update the Laws Governing Electronic Device Information as Evidence

Before the Joint Standing Committee on Judiciary

Good afternoon, Senator Carney, Representative Moonen, and members of the Judiciary Committee, I am Maggie O'Neil. I represent House District 129 in Saco. Thank you for the opportunity to present **LD 1576, An Act to Update the Laws Governing Electronic Device Information as Evidence**.

I. Background

This bill is about clarifying when a warrant is required. I started working on this idea while taking classes at Maine Law's privacy program. This idea came out of conversations with a fellow law student and former law enforcement officer about how clear warrant requirements should be established given the scale and kinds of data being searched in today's world. Over the past few years, I have explored this issue with faculty members at Maine Law and legislators from both parties. Rep. Faulkingham has submitted an analogous proposal aimed at closing the same loophole I am working on in this bill. These issues speak to the core of who we are and how we live our lives as Mainers. In preparation for presenting the bill, I have been in touch with both law enforcement and the attorney general's office. If the committee would permit it, I would like to have the months of the off-session to work this concept with them and get the language right.

II. Today's Economy and Implications for our Privacy.

Throughout history, societal threats to privacy have arisen unpredictably from emerging technology—from the instant photograph to wiretapping to apps on our smartphones. In today's society, collection and use of data is built into the business models of companies of all sizes—from tech giants Google, Meta, and Amazon to smaller businesses based in Maine.

Harvard business professor Shoshana Zuboff has identified a global economic shift comparable to the industrial revolution. Companies like google design products to obtain "behavioral

surplus" or data generated from your primary activity—e.g., search terms, links you click, how many results you view, how quickly you type. That information is then used to create value via targeted advertising and making predictions about behavior. In the face of this shift, we need to fundamentally rethink our old frames to recognize what's at stake and create protections.

Because there is so much money to be made in this new economy, companies are incentivized to create new technology that creates new ways of gathering data: from apps that your collect locational data or perfect facial recognition technology by putting bunny ears on your head, to digital watches that monitor your health information and collect data as "exhaust," to smart home devices like Alexa that have an active microphone and are connected to a network. The privacy risks faced by Mainers and people around the world are more complex, more systemic, and potentially more harmful than ever before. By making clear "rules of the road," this law could be used to help protect Mainers from privacy harm stemming from big tech and social media.

III. Fourth Amendment Protections in the Digital Age.

If privacy protections were a pie, LD 1576 would be one slice of the pie. One element of privacy protections is our Fourth Amendment protection against unreasonable searches and seizures. The Fourth Amendment provides that:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

Both the Fourth Amendment in the U.S. Constitution and Maine's Article I equivalent require that where a search is undertaken by law enforcement officials to uncover criminal wrongdoing, a warrant generally must be obtained based upon probable cause and that they define the scope of a search or seizure with particularity. The goal of that protection is to safeguard our privacy and security against arbitrary invasions by government officials.

In 1979, the Supreme Court created a gap in our Fourth Amendment protections. In *Smith v. Maryland*, the Court ruled that the Fourth Amendment didn't protect the privacy of the numbers we dial on our phones because we voluntarily share those numbers with the phone company when we dial them. This principle, known as the Third-Party Doctrine, suggests that when we share data with a communications service provider like a telephone company or an email provider, we know our data is being handed to a third party, and we can't reasonably expect it to be private anymore.[1] After *Smith*, the government took this small gap created by *Smith v. Maryland* and blew it wide open, arguing that *Smith*'s narrow 1979 decision about phone dialing

---

[1] In *United States v. Miller*, 1976 (bank records not subject to Fourth Amendment protections) and *Smith v. Maryland*, 1979 (telephone call logs of numbers a person dials held by the company not subject to Fourth Amendment protections), the Court affirmed that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Though the Supreme Court has never considered directly whether stored electronic communications are entitled to Fourth Amendment protection, the Court has assumed (without concluding) that individuals have a reasonable expectation of privacy in stored messages. *Quon v. City of Ontario, CA*, 560 U.S. 746, 748 (2010).

applied to the vast amount of data we now share with online service providers -- everything from email to cell phone location records to social media.

In recent years, the Supreme Court has acknowledged that this rule does not make sense in the digital age. The Court has moved toward limiting the Third Party Doctrine with *Carpenter* in 2018, concurrences and dissents leading up to that decision, and general sentiment that search and seizure protections must be adapted to protect privacy in the digital age.

When we write an email message in Gmail to deliver on our behalf or create notes in a Google document, we do so with an intention that our private communications and thoughts will be respected and kept in confidence. Just like with a letter in the mail, we would expect that no one else will review the message other than the intended recipient. But governments have argued that because we handed our communications to a service provider, the Fourth Amendment does not require a warrant before conducting a search. In the digital age, this gap in Fourth Amendment law has become a chasm because everything that used to live in a letter, a filing cabinet, or our desk drawer now lives in the cloud.

My goal is to extend the Supreme Court's ruling regarding cell site location information, or CSLI, in *Carpenter* to apply to other types of electronic data. Prior to the digital age, privacy was protected by the difficulty and cost of surveillance. Before smartphones and other technology changes, for example, observing a person's movements on public roads for a month would be costly, burdensome, and difficult to execute. Officer staff time would need to be dedicated to observe a person over that monthlong period, and the observation would be in real time and potentially detectible by the subject of observation or community members. It's a completely different ballgame when agencies can tap into our electronic data: surveillance can be remote, instantaneous, and undetected.

In 2012, Justice Sotomayor warned that data monitoring is (1) inexpensive when compared with conventional surveillance, (2) it proceeds surreptitiously, not checked by resource constraints, community hostility, and opportunity to observe surveillance activity; and (3) it can generate incredibly sensitive information about family, work, politics, religion, sexual life, and association. As such, these powers of observation are susceptible to abuse, and the awareness that agencies may be watching chills associational and expressive freedoms. Unless we are off the grid like Ron Swanson, in the age of new technology we all reveal an incredible amount of information about ourselves to third parties just by carrying out mundane tasks.

That is why Maine law currently goes beyond Fourth Amendment case law and federal statute to require a warrant for certain situations. A warrant requirement balances privacy rights against competing interests of public safety. LD 1576 will clean up gaps in the law and create a clear process, both for law enforcement and for members of the public.

IV. Current warrant requirements in federal and Maine Statute.

As electronic communication started to become more prevalent, Congress passed the Electronic Communications Privacy Act (ECPA) in 1986. The ECPA somewhat improved the privacy rights around certain electronic communications. However, the law reflects the technology of

1986, and it has aged poorly. It doesn't address documents stored in the cloud, information revealing our personal associations, or the vast quantities of location data our mobile devices collect on us every day. See Figure I for more information about the ECPA.

Maine statute closes some of the gaps left open by Fourth Amendment case law and the ECPA. It requires a clear process for certain kinds of data: a warrant is required to search location data (both real time and historic), to search the content of communication on portable electronic devices, and to attach a location tracking device. (I mapped the current law as I read it at the end of my testimony, under Figure II.) To use a pie analogy again, Maine's law and the ECPA together protect some slices of the pie, but leave significant slices of the pie without protection. LD 1576 closes those gaps.

As outlined above, courts develop constitutional law in a piecemeal manner, on a case-by-case basis. Our Fourth Amendment law constantly plays catchup while new technology is constantly emerging in our economy that is saturated with the collection, storage, and use of our personal data. If Maine or the federal government has no explicit law in place, we rely on the constitution as a backstop to define the limits of whether a warrant is required. As new technology emerges and evolves at a lightning pace, Americans wait for the courts to catch up and define the contours of our Fourth Amendment rights. That gap creates a lack of clarity for both members of the public and law enforcement.

As a state legislature, we can take a proactive approach and define our warrant requirements in statute. That way, both law enforcement and community members know what to expect through clear guidelines provided by the Legislature.

V. Proposal: Reinforce Current Process and Close Gaps in Law.

LD 1576 would require the government to get a warrant before obtaining personal electronic data and communication, including cloud data, when it is held by a third-party service provider. There is agreement that the law should be moving in this direction, as noted by *Carpenter* in 2018, concurrences and dissents leading up to that decision, and general sentiment that search and seizure protections must be adapted to protect privacy in the digital age.

Fourth Amendment privacy jurisprudence has shown that the legislative branch lags behind emerging technology. We struggled to keep up 100 years ago, and it's especially difficult now. In 1928, Justice Brandeis, one of the fathers of privacy law, outlined that the purpose of the Fourth Amendment is to protect against government abuses of power, and the amendment must be able to adapt to a changing world. He warned that with technological advances, "subtler and more far-reaching means of invading privacy have become available to the government," and suggested that, as technology changes our world, the law must adapt to protect our privacy rights.

I met with Lieutenant Colonel Brian Scott over the past couple of years to learn more about current processes and identify gaps. Lt. Col. Scott assured me that although gaps currently exist in the law regarding cloud data, typical company policy requires a warrant to obtain that data. AAG Paul Rucha also assured me that DA Offices currently have a policy of requiring a warrant.

LD 1576 seeks to clarify that requirement in statute so that our Fourth Amendment protections are spelled out in Maine statute, rather than in a company's privacy policy or a prosecutor's policy. I also plan to discuss additional data that may demand protection.

To draft LD 1576, I incorporated elements of the state of California's Electronic Communications Privacy Act (2015). The CalECPA covers a broader range of issues than ECPA and offers protection over all electronic communication information. Under the CalECPA, the government must obtain a search warrant or subpoena before accessing "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." I have communicated with state police, the attorney general's office, and prosecutors that I used this language as a starting point, and I am interested in sitting down with them and crafting a process that works for Maine.

I hope to have the committee's approval to continue those conversations. Thank you for your consideration.

Figure I: ECPA

ECPA lays out guidelines for law enforcement access to data. Under the Stored Communications Act, the government is able to access many kinds of stored communications without a warrant.

The following table illustrates the different treatment of the contents of an email at various times:

Type of Communication	Required for Law Enforcement Access	Statute
Email in Transit	Warrant	18 U.S.C. § 2516
Email in Storage on Home Computer	Warrant	4th Amendment, US Constitution
Email in Remote Storage, Opened	Subpoena	18 U.S.C. § 2703
Email in Remote Storage, Unopened, Stored for 180 days or less	Warrant	18 U.S.C. § 2703
Email in Remote Storage, Unopened, Stored for more than 180 days	Subpoena	18 U.S.C. § 2703

Source: EPIC

In addition to the specific government exceptions outlined above, there is other information that the government is empowered to collect from communications providers in the form of customer records. Under § 2703, an administrative subpoena, a National Security Letter ("NSL"), can be served on a company to compel it to disclose basic subscriber information. Section 2703 also allows a court to issue an order for records. Whether an NSL or court order is warranted depends upon the information that is sought.

An NSL can be used to obtain the name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for service (including any credit card or bank account number) of a subscriber. Although the breadth of information that can be gathered with an NSL is quite large, and was dramatically expanded with the USA PATRIOT Act, none of this information is supposed to include content.

All other non-content customer records must be obtained by a court order under § 2703(d). These include transactional records such as "addresses of web sites visited by the customer and e-mail addresses of other individuals with whom the account holder has corresponded." Although an order for these materials is issued by a court, the court is not issuing a warrant based upon probable cause. Instead, § 2703(d) requires only that there be "specific and particularly facts showing that there are reasonable grounds to believe" that the records requested are "relevant and material to an ongoing criminal investigation."

ECPA itself does not prohibit the disclosure of customer records to third parties. When the third party is the government, ECPA expressly permits the service provider to share customer records "if the provider reasonably believes than an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information." This authorization

is found in § 2702 and was added as part of the USA PATRIOT Act. In practice, it allows law enforcement to forgo even the minimal burden of a subpoena or a court order and claim there is an emergency that necessitates the records being turned over. Although it is voluntary for the provider to act under this provision, many do in practice.

Figure II. Maine Warrant Requirements

I. Warrant Required

1. Location

    a. Government cannot obtain real time or historical location information without a warrant. 16 M.R.S. §§ 647-650-B. (*Carpenter v. U.S.* plus real time location data; predated *Carpenter*.)

    b. Location information = "information concerning the location of an electronic device, incl. both the current location and any prior location of the device, that, in whole or in part, is generated, derived from or obtained by the operation of an electronic device."

    c. Covers *electronic devices*: "means a device that is electric and that enables access to, or use of, an electronic communication service, remote computing service or location information service." "Electronic communication service" means a service that provides to users the ability to send or receive wire or electronic communications.

    d. Exceptions: response to person's call for EMS, consent, threat of serious physical injury (broadened from previous language of immediate danger of death/serious injury). §650.

2. Content of Communication

    a. Government cannot obtain content information regarding communication conducted on a *portable electronic device* directly from a provider of electronic communication service or a provider of remote computing service without a warrant. 16 M.R.S. §§ 641-6

    b. Electronic communication service = "a service that provides to users the ability to send or receive spoken or electronic communications."

    c. Content information: "when used with respect to any wire, oral or electronic communication, includes any information concerning the substance, purport or meaning of that communication."

    d. Exceptions: (1) consent of device owner, (2) content otherwise publicly disclosed, or (3) in an emergency ("emergency" was amended to broaden this exemption: "involves or is believed to involve imminent danger of death or serious physical injury to any person." "Serious physical injury" means "bodily injury that creates a substantial risk of death, serious, permanent disfigurement or loss or substantial impairment of the function of a bodily member or organ or extended convalescence for recovery of physical health; or any harm potentially caused by a violation of Title 17-A, chapter 11 (sexual assault) or Title 17-A, section 282 (sexual exploitation of

a minor), 301 (kidnapping), 302 (criminal restraint) or 303 (criminal restraint by parent)."

3. Tracking Device Installation and monitoring

    a. A warrant is required to install a real-time tracking device. §§638 - 640. See also *United States v. Jones*.

    b. Time period: warrant must require the installation of the tracking device within 14 days of the issuance of the warrant and allow the tracking device to be monitored for a period of 30 days following installation. Monitoring period may be extended for an additional 30 days upon a finding of continuing probable cause.

II. Notice required

1. Location

    a. Notice required within 3 days of obtaining. §649

    b. Notice must include: (i) nature of law enforcement inquiry; (ii) info and date supplied/requested; and (iii) identity of third party if information was obtained from a provider of electronic communication service or other 3rd party. 16 M.R.S. § 649(1).

2. Content of Communication

    a. Broad: Notice required within 3 days whenever government obtains content. §643

        i. *State v. Evans*. Content §643. "When interpreting the statute as a whole, it is clear that section 643 requires notice to be provided to a [*3] cell phone user every time cell phone content has been obtained by a government entity." 2016 Me. Super. LEXIS 271.

    b. Notice must include: (i) nature of law enforcement inquiry, (ii) content supplied and date requested, and (iii) identity of third party if information was obtained from a provider of electronic communication service or other 3rd party. 16 M.R.S. § 643(1).

    c. Exceptions: (i) consent, (ii) content disclosed to public domain, or (iii) emergency.