MAINE CHIEFS OF POLICE ASSOCIATION

P.O. Box 2431 • South Portland, Maine 04116-2431

Chief Edward J. Tolan (ret.), Executive Director, Tel: (207) 838-6583
email: mcopa@maine.rr.com Web site: www.mainechiefs.com

Statement in Opposition to L.D. 1056 and LD 1576,
An Act to Update the Laws Governing Electronic Device Information as Evidence
September 25, 2023

Senator Carney, Representative Moonen, and members of the distinguished Committee on Judiciary. My name is William Bonney. I am the Chief of the Waterville Police Department. I am joined by my colleague, Jack Clements who is the Chief of the Saco Police Department. We are submitting testimony on behalf of the Maine Chiefs of Police Association against LD 1056, an Act Restricting State Assistance in Federal Collection of Personal Electronic Data and Metadata, and LD 1576, an Act to Update the Laws Governing Electronic Device Information as Evidence.

The Mission of the Maine Chiefs of Police is to secure a closer official and personal relationship among Maine Police Officials; to secure a unity of action in law enforcement matters; to enhance the standards of police personnel, police training and police professionalism generally; to devise ways and means for equality of law enforcement throughout the state of Maine; to advance the prevention and detection of crime; to prescribe to the Law Enforcement Code of Ethics; and to promote the profession of law enforcement as an integral and dedicated force in today's society sworn to the protection of life and property.

We were glad to hear that these two bills were carried over so that the Committee could have more time to properly weigh the concerns raised about the bill. And we are happy to be here today to provide more information about our concerns and to answer the questions the committee asked for us to answer. We first wanted to provide a little background on our concerns about each of these bills and then we wanted to take time to answer the four questions raised by the committee members.

First, as to the background, we submitted testimony during the public hearing for each of these bills detailing the reasons why we were opposed to their passage.

For LD 1056, we noted that it "would prohibit us working with our federal partners on very serious criminal matters. For example, matters like school threats, child abductions, and child pornography. These are matters that require close collaboration with our partners in federal law enforcement, and we welcome every chance that we get to broaden our resources so that we can resolve a matter quickly and efficiently. This way the victim finds peace more

quickly and the public stays safe from further harm that the person might cause the community." Chief Clements will discuss this concern more later on in our testimony.

Additionally, the Association would like to add that although this bill appears to affirm the basic tenants of criminal law, the reality is that the language is extremely broad and vague and so it would be difficult for us to enumerate all of the ways that this would affect our current work but a significant impact would be that we would not be able to share tips with federal partners to report child pornography transmissions or report social media threats to federal partners. We will discuss this more later.

For LD 1576, we addressed our concerns with restricting our ability to investigate crimes and noted that "the courts have been the leader in interpreting the constitution and structuring the circumstances in which a search warrant should be obtained." And that "we should allow them to continue to balance the rights of the individual and the rights of the community to be safe."

Additionally, the Association would like to add to our concerns that this bill would limit our ability to receive information outside of the search warrant. As noted by DSP, we typically receive a cyber tip from an Electronic Service Provider (ESP). These tips do not have enough for a search warrant, but it does allow an investigator to start the process to determine if there is enough probable cause to proceed with an investigation.

If these bills were to pass it would, in our opinion, restrict most of Maine law enforcement agency's ability to investigate some of the more heinous crimes around child sex abuse material (CSAM) commonly referred to as "child pornography." We heard from some small to mid-sized agencies that would not have been able to conduct these types of investigation without the training and equipment provided by the U.S. Secret Service. One of our officers was allowed to expand his training at the National Computer Forensic Institute because they were in partnership with the US Secret Service which in turn allowed the Secret Service to justify to Congress the expenditure of taxpayer dollars to train U.S. Law Enforcement to combat cyber criminals.

Furthermore, though federal law enforcement might seem like a large agency, spread out throughout the country and territories of the U.S. they often are stretched too thin to work every case. This allows for Task Force Officer to be a part of various federal agency and assist them as well as get assistance from these agencies in complex cases where a state agency would not have the resources or the reach to fully investigate and bring about charges, whether at the state of federal level. Which of course allows offenders to continue to victimize people with little or no consequence.

Second, we would like to provide a brief response to the Committee's questions. I will turn over to my colleague, Chief Clements, to answer those questions.

Before we get into the specific questions, we want to note that we are answering the questions asked by the Committee in the expertise from our role, but we

would ultimately defer to the experts on this specific subject in the room, like the Department of Public Safety, Maine Prosecutors' Association or the Office of Attorney General.

1. **What is electronic communication data vs. metadata?**

According to the definition provided in LD 1576, "'Electronic communication' means the transfer of information, including but not limited to signs, signals, writings, images, sounds, data or intelligence, in whole or in part by a wire or a radio or an electromagnetic, photoelectric or photo-optical system." This matches the definition provided in the United States Code. *See* 18 U.S.C. § 2510 (12). This is essentially all information that you have stored on your electronic device – your search history, emails, messages, photos etc.

According to the Department of Justice, "Put simply, metadata is 'data about data.' Metadata provides a description and important facts about material that is posted online and is itself machine-readable and can be searched by other computers."[1] This is essentially all the data about the electronic communications – who wrote it, when was it sent, was the file changed at all etc. It tells the story behind your electronic communication.

2. **How can Maine law enforcement access electronic communication data vs. metadata under current state and federal law?**

We defer to federal law enforcement experts about federal law, but under current state law, a government entity may obtain electronic information through two main ways.

First, a search warrant must be obtained to "obtain *portable electronic device* content information directly from a provider of electronic communication service or a provider of remote computing service." 16 M.R.S. § 642(1); *see* 16 M.R.S. § 641(6) (stating that the definition of portable electronic device is "a device that is portable and electric that enables access to, or use of, an electronic communication service or remote computing service") and 16 M.R.S. § 641(2) (stating that the definition of content information is "any information concerning the substance, purport or meaning of that communication."). This means that law enforcement needs a search warrant to access the texts and emails on any portable device like a cell phone. However, there are exceptions provided in statute and the most relevant to this discussion is a search warrant is not needed if the information is disclosed by anyone in a publicly accessible domain. 16 M.R.S. § 644(2). This means that if someone shares a photo to another person and then that person puts that photo online, then law enforcement can obtain information about that content online.

[1] https://www.justice.gov/oip/blog/using-metadata-foia-documents-posted-online-lay-foundation-building-government-wide-foia.

This would be the case that is often exemplified by child pornography investigations - person A takes an illegal photo on their phone. Law enforcement would need a search warrant to access person A's phone to look at the photo and to gather any meta data about that photo like where it was taken and what time it was taken. However, if person A texts the photo to person B and person B puts the photo online, then law enforcement can investigate the photo including accessing the photo's metadata which can help solve the investigation to protect the victim and hold the proper people being accountable including person A who took the original photo.

Second, a search warrant must be obtained for "location information of an electronic device." 16 M.R.S. § 648; *see* 16 M.R.S. § 647(3) (stating that the definition of electronic device is "a device that is electric and that enables access to, or use of, an electronic communication service, remote computing service or location information service") and 16 M.R.S. § 647(5) (stating that the definition of location information "means information concerning the location of an electronic device, including 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"). This means that a law enforcement officer needs a search warrant to access a location information stored on *any* electronic device. However, there are certain exceptions including to respond to a user's call for emergency services. 16 M.R.S. § 650.

3. How does the third-party doctrine impact law enforcement access to data and metadata?

Both the Maine Constitution (Article 1, section 5) and the United States Constitution (Fourth Amendment) protect individuals from unreasonable searches and seizures by the government of your person, property, house, papers and effects. The courts have outlined the reasonable perimeters of these protections and have determined certain exceptions. The third-party doctrine is one of those exception and it holds that "police do not need a Fourth Amendment warrant to access information that an individual has voluntarily disclosed or conveyed to a third party, such as bank records or call histories."[2]

It is important to note that the United States Supreme Court has placed limits on this doctrine – in *Carpenter v. United States*, the Court determined that a person's location information archived on their phone was protected because this was an involuntary feature of their cell phone that their cell phone provider had access to the information. 138 S. Ct. 2206 (2018). As you probably note, this is like the statutory protections provided by the Maine Legislature described in question two. This indicates that the courts are willing to make changes to adapt to the technology changes and we should allow them to do so when it makes sense.

[2]https://scholarship.law.tamu.edu/cgi/viewcontent.cgi?article=2420&context=facscholar#:~:text=The%20third%2Dparty%20doctrine%20is,bank%20records%20or%20call%20histories.

If this legislation were to be passed, then it would go well beyond the perimeters established by the judicial branch. This doctrine is well established, supported by the courts, and this, and other exceptions, are important for law enforcement to balance the concerns of the individual's right to privacy and other's right to live safely in their community without harm from other people. If changes are needed, then it should be left to the Courts to abridge.

4. **What implementation issues for law enforcement, if any, do you anticipate from LD 1056 or LD 1576—e.g., expense? other difficulties?**

We would defer to the other groups in the room to speak to the specifics, but I wanted to add my own personal experience of working in partnership with federal agencies. I am not a computer crimes person in any way, shape, or form, but my background has been working with the federal government is traditional violent crime. I spent 25 years working at a Nevada police department and during my time there, I spent almost 9 years assigned to the FBI Safe Streets Task Force dealing with violent crime. There was a lot of information sharing between local law enforcement and federal law enforcement because I was with the task force before and after 9/11. Terrorism was, and still should be, a major concern for all law enforcement.

My last few years I was a Lieutenant assigned to Investigative Services where I oversaw Robbery investigations, the auto-theft task force, and the cyber-crimes unit. Again, I'm not a computer or cyber crimes person, however, the collaboration between local, state and federal law enforcement was key to mitigating all manner of cyber related crimes. These crimes include, but are not limited to:

- Child pornography investigations
- Cyber attacks
- Financial crimes, especially those targeting the elderly
- Interstate crimes, etc.

We live in a digital world. If we are prohibited from sharing information, this could potentially preclude us from sharing information on all other crime traditional crime categories such as Murder and Robbery. In addition, Federal law enforcement is tasked with investigating Hate Crimes which often have some internet/digital component that local, county or state law enforcement receives. How do we work with our federal partners to prosecute those who commit egregious crimes?

We are increasingly seeing a digital/electronic component to all crime categories. Restricting any sharing with federal partners will most certainly

result in our federal partners not sharing information with us. This is not a good idea.

These experiences have taught me that we need to be strengthening relationships with our federal partners and encouraging the sharing of information at every step. Our communities are safer because of it. On behalf of the Maine Chiefs of Police Association, we want to thank the committee members for your work on this Committee. And we would ask that you oppose LD 1056 and LD 1576 in this upcoming legislative session. We are happy to answer any questions today or that might arise in the future.