QUESTIONS POSED:

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

    a. Electronic communication data is all the information relating to our everyday digital interactions with the world, including text messages, emails, and interaction through social media. The entity that facilitates that communication, such as Google, is called an electronic communication service (ECS). Maine law protects the content of communications being sent by an ECS and storage of data by a remote computing storage (RCS), such as a Dropbox account or Google photos. Current law requires law enforcement to obtain a search warrant to obtain anything beyond "subscriber information" from these entities.

    b. Metadata is generally defined as "data about data." Depending on the definition, metadata can as narrow as the information about a single data file, or it can be as expansive as scanned testimony regarding a specific LD under consideration. An example of metadata would be the information about the size of a specific file, when it was created, who created it, and when it was last modified.

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

    In Maine, a search warrant is used to obtain information from an ECS or RCS, except that a subpoena may be used for "subscriber information," which is defined below. A search warrant must be used for location information.

    a. A search warrant is required to obtain "content information" from a service provider. This applies to "any wire, oral or electronic communication" and includes any information "concerning the substance, purport or meaning of that communication." 18 USC §2510(8); 16 M.R.S. §641(2).

    b. Only "subscriber information" held by service provider can be obtained with a subpoena. Although it relates more to the user's account, some may consider it metadata. The material available include, pursuant to 18 U.S.C. §2703(c)(2):

        i. Name
        ii. Address
        iii. Telephone connection records
        iv. Call times and durations
        v. Length of service (including start date)
        vi. Services used
        vii. Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address
        viii. Payment information, including any credit card or bank account number

    c. Under Maine law any location information concerning where an electronic device is or was, requires a search warrant. 16 M.R.S. §648.

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

    a. What is the third-party doctrine?

        i. Third-party doctrine arises from case law determining the limits of the 4th Amendment's protections for citizens against unreasonable searches. If a person either makes a statement or provides an item to another person, the original person has lost control over what the other person chooses to do with it. Therefore, the person has no reasonable expectation of privacy once the communication is made or the item is provided to the other person.

        ii. Currently, the third-party doctrine allows law enforcement to access certain records by a grand jury subpoena, including call detail records (who called and when) or financial records. These records have fewer legal protections because they are information that the individual has already shared with a third-party entity, such as a bank or phone provider. This is based on the United States Supreme Court's decisions in *Smith v. Maryland* (telephone records) and *U.S. v. Miller* (bank records).

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

The concerns regarding implementation will be addressed in a separate memo.