LD 1705

MAINE LAW | Faculty of Law
UNIVERSITY OF MAINE SCHOOL OF LAW

May 21, 2023

Dear Committee Members,

My name is Scott Bloomberg and I am an Associate Professor at the University of Maine School of Law. I teach and research in the area of information privacy law and am the Director of Maine Law's Information Privacy Law Program. In that capacity, I am writing to give my support to three bills designed to protect the privacy of Mainers' personal information:

- LD 1945, An Act to Regulate the Use of Biometric Identifiers.
- LD 1576, An Act to Update the Laws Governing Electronic Device Information as Evidence.
- LD 1902, An Act to Protect Personal Health Data.

As I shall explain, each of these bills is designed to fill a gap where existing law fails to adequately safeguard individual privacy. Moreover, each bill—in my view—merely codifies a privacy protection that most Mainers' likely assume they already have.

The testimony that I provide below reflects my own personal views and not the views of the University of Maine School of Law as a faculty or institution.

LD 1945, An Act to Regulate the Use of Biometric Identifiers.

When it comes to the privacy of information, there is perhaps no personal information more sensitive than data about your body: Your fingerprints or handprints. Your faceprint. Your voiceprint. Your eyescan. Your gait (the way you walk). This information—this biometric data—is unique in that it cannot be changed. It is immutable. If your biometric data falls into the wrong hands you cannot get a new finger or face or voice (as opposed to, say, a new credit card number). The data could be used to your detriment for the remainder of your life.

That is exactly why some states began to regulate companies' collection, handling, and sharing of biometric data. To date, three states have specific biometric data privacy laws (Washington, Texas, and Illinois). Other states, such as California, have comprehensive privacy laws that classify biometric data within a broader category of "sensitive information" that are subject to heightened privacy protections. And biometric data that is captured in the medical setting is, of course, generally subject to significant privacy protections under HIPAA.

Of the three states with specific biometric data privacy laws, Illinois' Biometric Information Privacy Act ("BIPA") has proven to be by far the most impactful. That is so for a very simply reason: BIPA contains a private right of action, allowing classes of plaintiffs to sue in federal or state court when a company mishandles their biometric data in a way that violates the law. That private right of action has given BIPA real teeth, whereas the laws in Washington and Texas have gone under-enforced.

Upon reviewing LD 1945, I can see that it is similar to Illinois' BIPA, including most importantly containing a private right of action. Indeed, the Bill has several desirable features of a biometric data privacy law (or any privacy law for that matter). It includes a data minimization requirement to ensure that companies do not store biometric data indefinitely and without purpose. It creates a standard of care around how companies store biometric data. It gives individuals a right to know about the biometric data companies collect about them. And, it prevents companies from collecting or disseminating biometric data without first obtaining informed consent. The Bill is, in short, very thoughtfully crafted, providing protections that most Mainers likely believe they already have (or at least should have) around one of the most sensitive types of information they share with businesses.

As a final thought on this bill, I would like to highlight an ambiguity in the draft that may prove to be consequential. The draft defines the term "biometric identifier" as "information generated by measurements of an individual's unique biological characteristics . . . that *can be used to identify* that individual. . . ." (Emphasis added.) This definition's emphasis on identification may allow companies that collect biometric data that is not, or cannot be, used to identify an individual to circumvent the law. Specifically, marketers could use biometric data like face and eye movements to gain insight into consumers' preferences. And they may do so without having to identify the individual consumer—indeed, a marketer may be far more interested in understanding what a consumer's face or eye movements reveal about the consumer's likes and dislikes than they are in knowing the consumer's name and address. Does the consumer smile or frown when they see a company's advertisement? Do they stare or look away? Given the term "biometric identifier" and its definition's focus on identity, companies would likely argue that such uses of biometric data are not covered by the bill. A reviewing court may or may not agree with that argument in a given case, but legislators should be aware of, and account for, the prospect that the issue will come up in future litigation.

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

LD 1576 likewise codifies a right that most Mainers probably believe they already have. The Fourth Amendment to the U.S. Constitution prevents the government from engaging in "unreasonable searches and seizures" and, with only narrow exception, requires the

government to obtain a warrant before searching a person, their house, their papers, or their effects.[1] Article 1, Section 5 of the Maine State Constitution provides the same protection.[2]

Hundreds of years ago, the requirement for government agents to obtain a warrant before searching a person, their house, their papers, or their effects covered virtually all information a person possessed about themselves. After all, that information was contained in paper letters and documents, which people kept inside of their homes or (when out and about) on their persons. The secluded desk drawer in the Colonial home's study is, of course, no longer the place where people store most of their information. Instead, people store troves of personal information online, through services offered by third-party businesses, which the businesses can themselves access. The paradigmatic example is cloud-based storage services (think Google Drive), but any online app, service, or platform that you use may be a place where you store your personal information.

LD 1576 would, simply put, take the same protection that the nation's founders provided to letters in the desk drawer and extend it to data that you store online with a third-party business. That protection is presently lacking due to a rule called the "third-party doctrine." Beginning with a pair of cases in the 1970s,[3] the Supreme Court has held that a person loses a reasonable expectation of privacy in their information when they share that information with a third party. In other words, the Supreme Court has required *secrecy* and a precondition for *privacy*. While the soundness of this principal is hotly contested, the result when applied to today's world is quite clear: Put your information in the hands of a third-party business, and the government can (generally[4]) compel that business to divulge the information without obtaining a warrant based on probable cause.

LD 1576 patches this gap in the law, requiring the government to obtain a warrant based on probable cause to search such information. Moreover, it does so in a manner that balances individual privacy interests with law enforcement and public safety needs. The bill includes an exception for emergency situations and allows law enforcement to request an order directing businesses to keep the existence of a warrant secret, where their investigation so requires. The bill also does not apply when the information in question is publicly available or when it is obtained with the subject's consent.

---

[1] U.S. CONST., amend. IV.

[2] MAINE. STATE CONST., art. 1, § 5.

[3] United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979).

[4] There are a few notable exceptions. The Supreme Court, in a narrow 5-4 decision, held that the government must obtain a warrant to search a type of data called historical cell site location information. Carpenter v. United States, 138 S. Ct. 2206 (2018). It is also widely accepted that the government must obtain a warrant to access the content of emails, even though they are stored with third-party businesses. *See, e.g.*, United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

LD 1902, An Act to Protect Personal Health Data.

I am willing to bet that the one privacy law that all of your constituents have heard of is HIPAA. However, your constituents would likely be surprised to learn that HIPAA does not, in fact, apply to all of their health information. It only protects health information handled by entities that deal with health insurance—basically, providers, insurers, and certain of their service providers. Health information that other businesses collect falls outside of HIPAA's scope.

Part of your constituents' surprise would stem from a misconception about the law's title. Most people think the law is called the Health *Information* Privacy and Protection Act (or something similar) when it is actually called the Health *Insurance* Portability and Accountability Act. But more fundamentally, most people have an expectation that if they share health information with a company, that company is prohibited from further disclosing it without consent. They're surprised to learn that the law does not meet their expectation of privacy. And, in a world where people share health information with a growing range of companies (think genetic testing, fitness apps, WebMD) more and more health information is falling outside of HIPAA's ambit.

LD 1902 simply applies HIPAA-like protections to Mainers' health information regardless of what type of business holds that information. The State of Washington recently passed a similar bill, HB 1155, and in my view Maine would be wise to follow suit.

***

As I have explained, each of these bills provides a form of privacy protection that Mainers likely assume they already enjoy, and would be surprised to learn that they do not. I hope the Committee will push them forward.

Best Regards,

Scott Bloomberg