ACLU of Massachusetts
211 Congress Street, Suite 301
Boston, MA 02110
617-482-3170
www.aclum.org

April 29, 2019

Joint Committee on Consumer Protection and Professional Licensure
Sen. Paul Feeney & Rep. Tackey Chan, Chairs

SUPPORT: H.287/S.98

UPDATING CHAPTER 93H TO PROTECT PERSONAL BIOMETRIC INFORMATION

Dear Senator Feeney, Representative Chan, and members of the committee:

The ACLU of Massachusetts strongly supports H.287/S.98, and urges the committee to give this legislation a favorable report again this session, as it did in 2017. This is a simple bill to update the statutory definition of "personal information" under Chapter 93H, our state data breach and security law, to include biometric information.

Chapter 93H is intended to safeguard residents' personal information to prevent identity theft or similar fraudulent and illegal activity. The law requires businesses and government entities to treat personal information in their possession with particular care: they must safeguard it with physical and technological security measures, and follow basic notification procedures in the case of a security breach.

The problem? The existing definition of "personal information" reflects 20th century concerns, and leaves Massachusetts residents vulnerable to 21st century dangers.

Under current law, personal information protected by Chapter 93H is limited to a resident's name in combination with his or her social security number, driver's license or state-issued ID number, or financial account information. But today, people regularly use biometric information to authenticate their identities for all manner of commercial applications, including access to financial accounts. For example, millions of people use fingerprints and faceprints in place of passwords to login to computers and smartphones, and to authorize payments using "Apple Pay" and similar services.

Biometric information is more intimate than a social security number. An individual's biometric characteristics are unique, making them usable as authenticators in some circumstances. But when our biometric indicators are scanned and digitized, they can be stolen and abused. And while you can easily change a stolen password, or even change your social security number if you're the victim of identity theft, you cannot change your face or your fingerprint. If it's stolen or misused, your security could be compromised for life.

Researchers have demonstrated time and again that, with the right know-how, anyone can use another person's biometric identifiers to hack into their private accounts and devices. One research group used an image of a person's fingerprint to create a 3D printed mold that was capable of unlocking that person's smartphone. Another researcher used this method to create a model of a German government official's fingerprint.[1]

Now that we use biometric information as keys to unlock financial accounts, security breach laws must cover these sensitive and immutable identifiers.[2]

The risks aren't hypothetical. In 2015, the Office of Management and Budget was hacked by a foreign government, and the personal information of nearly 22 million federal government employees—including spies and intelligence officers—was stolen. As recently as last year, reports indicated that fraudsters were using the stolen government records to apply for loans in an identity theft bonanza. Among the stolen data was a cache of fingerprints from every federal official that has applied for and passed a background check.[3]

In 2007, when Chapter 93H was passed, we didn't foresee just how quickly commercial applications would integrate biometrics capabilities. But now we know. We should therefore amend the law to close this growing loophole.

We welcome the opportunity to answer questions and work with the committee to move this legislation forward. Thank you.

---

[1] Russell Brandom, "Your phone's biggest vulnerability is your fingerprint; Can we still use fingerprint logins in the age of mass biometric databases?" May 2, 2016, the Verge. https://www.theverge.com/2016/5/2/11540962/iphone-samsung-fingerprint-duplicate-hack-security/.

[2] Other states have begun to recognize the importance of protecting biometric data from identity theft and pass similar legislation. See, e.g., Wyoming: https://legiscan.com/WY/text/SF0036/id/1137322/Wyoming-2015-SF0036-Enrolled.pdf.

[3] Daniel Cooper, "Fraudsters caught using OPM hack data from 2015; She and her team used the information to open fraudulent loans," June 2018, Engadget. https://www.engadget.com/2018/06/19/fraudster-caught-using-opm-hack-data-from-2015/.