ACLU
AMERICAN CIVIL LIBERTIES UNION
Maine

PO Box 7860
Portland, ME 04112
(207) 774-5444
www.aclumaine.org

TESTIMONY OF MEAGAN SWAY, ESQ.

Ought to Pass - LD 1705

An Act to Give Consumers Control over Sensitive Personal Data by Requiring Consumer Consent Prior to Collection of Data

JOINT STANDING COMMITTEE ON JUDICIARY

May 22, 2023

Senator Carney, Representative Moonen, and distinguished members of the Joint Standing Committee on Judiciary, good morning. My name is Meagan Sway, and I am the Policy Director at the ACLU of Maine, a statewide organization committed to advancing and preserving civil rights and civil liberties guaranteed by the Maine and U.S. Constitutions. On behalf of our members, we urge you to support LD 1705.

If enacted, this bill would require that companies obtain individuals' consent before collecting, using, or disclosing those individuals' sensitive biometric identifiers. This is a crucial yet reasonable protection that will allow people and companies to enjoy the benefits of advances in technology while helping to prevent abuse. Illinois has had a similar law on the books for more than a dozen years. Maine should follow suit.

Biometric identifiers, including fingerprints, iris and retina scans, facial recognition scans, and voiceprints, are unique to each individual. They can be used to instantaneously identify and track people, and if they are disseminated or leaked, the harm may be irreparable because, unlike a credit card number or social security number, they cannot be changed. Without strong and enforceable legal protections, Maine people will be left vulnerable to violations of their privacy, security, and civil rights. Everyone will experience these risks, but members of marginalized and vulnerable communities—including people of color, LGBTQ people, immigrants, survivors of intimate partner abuse, and others—will experience some of the greatest harms. Abusive collection and use of biometric identifiers is becoming increasingly widespread, and the time for the Legislature to act is now.

This bill would provide the following protections, which are currently lacking under Maine law:

- Require companies to provide notice and obtain written consent before collecting, using, or disclosing a person's biometric identifier (including iris, face, voice, palm, and finger prints);
- Prohibit companies from withholding services from people who choose not to consent to collection or use of their biometric identifiers;

- Require businesses to delete a Maine resident's biometric identifiers one year after the individual's last interaction with the business;

- Require safeguards against unauthorized disclosure when an individual's biometric identifier is collected, stored, and used;

- Prohibit companies from disclosing or sharing an individual's biometric identifiers without consent, except under very specific circumstances as required by law; and

- Provide individuals with the ability to sue companies that have violated their rights under the law.

Without these safeguards, people in Maine will remain unprotected from privacy, security, and civil rights harms stemming from collection, use, and dissemination of their personal biometric identifiers without consent.

Maine has already recognized problems with unconstrained use of people's biometric identifiers. Last session, you passed a bipartisan bill regulating the use of face recognition technology by government officials.[1] The legislature now has the opportunity to protect Maine people against harms from private sector use of biometric technologies as well.

Collection and use of biometric identifiers without consent violates Maine peoples' privacy.

Recent developments in technology have given corporations incredible powers to quickly identify, track, and surveil people through collection and analysis of biometric identifiers. These capabilities can be used both to identify people in an instant, and to pervasively track their movements in the physical world and online, such as by using face recognition to automatically track a person across a network of video surveillance cameras. The ability of these technologies to capture biometrics at a distance, or from video and photos, can evade detection and can easily be carried out without knowledge or consent of affected individuals. Even biometric identifiers that traditionally had to be collected from individuals in-person, such as fingerprints and iris scans, can now be captured remotely. Without this bill's protections, people may never know they have been identified or tracked, much less have the ability to refuse consent.

These concerns are not hypothetical. The face recognition company Clearview AI has amassed a database of more than 10 billion faceprints captured from photos of people it has downloaded from their social media pages and other websites—all without providing notice to those people or obtaining their consent. Clearview's customers can upload an individual's photo and use the company's face recognition software to match the photo against other photos of the same person in the database, providing a chilling ability to identify people and create a record of their activities and associations online. Clearview has made it clear that it intends to grow its biometric database to include more than *100 billion* faceprints, with the goal of making "almost

---

[1] *See* LD 1585, In the in the 130th Legislature, *An Act To Increase Privacy and Security by Regulating the Use of Facial Surveillance Systems by Departments, Public Employees and Public Officials*, *enacted at* 25 MRSA Pt. 14, available at www.mainelegislature.org/legis/bills/display_ps.asp?ld=1585&PID=1456&snum=130.

everyone in the world" identifiable.[2] Until recently, Clearview's thousands of users included retailers like Best Buy, Macy's, Kohl's, Walmart, and Home Depot; banks including Bank of America and Wells Fargo; private investigators and law firms; the NBA; and wealthy socialites. One New York billionaire used Clearview's app to surreptitiously identify his daughter's new boyfriend when he came across them on a date; he later bragged that he used the app to capture people's faceprints "as a hobby."

Last year, the ACLU won a settlement against Clearview under the Illinois Biometric Information Privacy Act. The ACLU represented organizations that work with undocumented immigrants, survivors of sexual assault and domestic violence, current and former sex workers, and individuals who regularly exercise their right to protest. By capturing and selling access to people's biometric identifiers without consent, Clearview threatened to empower abusive ex-partners and serial harassers, exploitative companies, and others to track and target members of these vulnerable communities. Under the terms of the settlement, Clearview is permanently banned, nationwide, from making its faceprint database available to most businesses and other private entities. The company will also cease selling access to its database to any entity in Illinois, including state and local police, for five years. Illinois law protects against these abuses. Maine law should too.

Although Clearview's conduct is particularly egregious, it is far from the only company to have secretly collected people's biometric identifiers and used them in ways most people would never have agreed to had they known about it. One company that marketed an online digital photo storage service secretly used people's uploaded photos to train a face recognition system that it sold to police. Numerous retailers, concert venues, and stadiums have begun quietly using face recognition technology to identify and track shoppers and event attendees. Few of these companies are willing to disclose their use of biometric technologies; when the ACLU asked 20 top American retailers whether they used face recognition cameras on their customers, only two would answer. Landlords have started installing face recognition systems in apartment buildings, granting themselves the power to automatically track the comings and goings of every resident, and to identify their guests and romantic partners as they arrive and depart. The notice and consent requirements in LD 1705 would be critical protection against such abuse.

Collection and storage of biometric identifiers without consent puts Maine people at risk of data breaches and identity theft.

LD 1705 also helps people keep control over their biometric identifiers, thus securing them against inclusion in companies' databases that may be subject to breaches or other damaging dissemination. Unlike many forms of sensitive data, such as a passport number, credit card number, or even social security number, we cannot change our biometric identifiers after they have been stolen or misused. Unfortunately, breaches of databases containing people's biometric identifiers are all too common, putting people at risk of identity theft and similar harms. Examples include:

---

[2] Drew Harwell, *Facial recognition firm Clearview AI tells investors it's seeking massive expansion beyond law enforcement*, Feb. 16, 2022, WashPo, available at https://www.washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition/

- The security company Suprema, which sells biometric lock systems to control access to secure areas, left the "fingerprints of over 1 million people, as well as facial recognition information" exposed in a publicly accessible database.

- Students who were required to use the remote exam proctoring company ProctorU have sued alleging that their biometric identifiers were exposed in a data breach that affected the records of almost 500,000 students.

- A ransomware attack on the Personal Touch Holding Corporation exposed the data of dozens of Maine people in 2021.[3] Fingerprints were among the data exposed.

- A cyber-attack on a private company contracting with the federal government compromised approximately 184,000 images of travelers from a facial recognition pilot program operated by U.S. Customs and Border Protection.

LD 1705's requirements of notice and consent, its requirement that companies delete people's biometric identifiers after a specified time period, and its limitations on how biometric identifiers are stored, used, and disseminated will help minimize the risk of sensitive biometric identifiers being lost to hacks or data leaks like these.

Collection and use of biometric identifiers without consent subjects Maine people to discrimination and other civil rights harms.

Multiple studies by the federal government, academic researchers, and the ACLU show that face recognition algorithms have markedly higher misidentification rates for Black people, people of color, women, and children. Face classification algorithms, which seek to identify people by demographic category, have likewise been shown to be significantly less accurate when used on people of color, transgender and gender nonconforming people, and women. Other biometric technologies that purport to be able to infer information beyond identity, such as face scanning to determine a person's emotional state or eye scanning to detect whether they are telling the truth, are similarly, if not more, flawed.

The harms of using these faulty biometric technologies are very real. In Michigan, a 14-year-old Black girl was ejected from a skating rink after a face recognition system incorrectly matched her to a photo of someone who was suspected of previously disrupting the rink's business. The rink made the girl, who had never been to the rink before and whose mother had already left after dropping her off, leave the building. During the Covid-19 pandemic, students of color have reported that face recognition technology in remote exam proctoring software has failed to recognize them, threatening to lock them out of important academic and professional-licensing exams.

When biometric technologies are disproportionately deployed in communities of color, the harms are compounded. When Rite Aid quietly deployed face recognition cameras to look for

[3] Data Breach Notifications, Office of Maine Attorney General, *available at* https://apps.web.maine.gov/online/aeviewer/ME/40/79e73e85-40e7-4c4f-aa0d-206e0d0cc530.shtml

shoplifters, it installed them almost exclusively in stores in low-income communities of color, subjecting shoppers in those neighborhoods—but not nearby higher income and whiter neighborhoods—to biometric tracking. Predictably, because the technology worked relatively poorly on people of color, it resulted in at least one case of a Black shopper being told to leave a store based on an incorrect match to a photo of a suspected shoplifter.

Companies are now using face recognition technology in numerous other troubling ways. Walgreens, for example, is deploying "face-detection technology that can pick out a customer's age and gender" and show them tailored ads.[4] This invasive practice raises concerns about shoppers being steered to discounts or products based on gender stereotypes. Even more consequentially, face and voice recognition technology is being used to collect and analyze biometric data during employment interviews. Vendors of predictive interview hiring tools dubiously claim to measure an applicant's skills and personality traits through automated analysis of verbal tone, word choice, and facial expressions. This technology raises an enormous risk of amplifying employment discrimination against people due to accents, disabilities, skin color, or because they are transgender, nonbinary, or gender nonconforming.

A private right of action is essential to ensuring Maine peoples' rights.

One of the most important aspects of LD 1705 is its enforcement mechanism, a private right of action for individuals whose rights have been violated. The scale and scope of potential harms associated with exploitation of people's sensitive biometric identifiers are too extensive to be left to overburdened state agencies, or to promises of self-policing by companies.

Without a private right of action, people have little practical ability to seek relief in cases where their biometric identifiers are unscrupulously collected or misused. This eliminates a powerful tool that can incentivize companies to comply with the law in order to avoid lawsuits. Where companies nonetheless choose to ignore the law, the private right of action allows affected individuals to obtain redress for the harm they have suffered.

A private right of action is also important because government agencies often do not have the resources to investigate and take action in every case—or sometimes any case—where people's rights are violated. The experience of the three states that have enacted biometric privacy laws is instructive. In Illinois, where the law includes a private right of action, state residents have been able to sue technology companies like Clearview AI, Facebook, and Google for collecting and using their biometric identifiers without consent, and this has led to those companies changing their practices. In Texas and Washington State, on the other hand, where there is no private right of action, enforcement actions by those states' attorneys general against companies that violated their laws are virtually nonexistent. The Washington Attorney General has never sued to enforce its law, and just last week the Texas attorney general brought its first lawsuit to enforce the Texas law in the 21 years since it was enacted. State regulators simply have not kept up with companies' practices. A biometric privacy law that is not enforced is unlikely to deter companies from committing violations.

---

[4] Adam Levin, Basic biometrics: Why this emerging technology must be regulated now, Sep. 24, 2019, The Hill, available at https://thehill.com/opinion/cybersecurity/462719-basic-biometrics-why-this-emerging-technology-must-be-regulated-now/

A private right of action both conserves state resources, and ensures that state residents can vindicate their own rights. As the California Attorney General put it when supporting a private right of action in a recently enacted consumer privacy law, "The lack of a private right of action, which would provide a critical adjunct to governmental enforcement, will substantially increase the [Attorney General's Office's] need for new enforcement resources. I urge you to provide consumers with a private right of action."

Also critical is LD 1705's statutory damages provisions, which permits individuals who prevail in their lawsuits to recover reasonable money damages without needing to document tangible damages. Because nonconsensual capture of biometric identifiers often happens in secret, the resulting harms can be extraordinarily hard to quantify and trace. Statutory damages provide a way to meaningfully enforce the law. Numerous privacy and consumer protection statutes at the state and federal level include statutory damages provisions.

As technology capturing biometric information grows in use, it becomes increasingly more dangerous without guardrails in place. Legislators should act now to protect Maine residents' privacy. Please vote "ought to pass" on this important legislation.