HOUSE OF REPRESENTATIVES
2 STATE HOUSE STATION
AUGUSTA, MAINE 04333-0002
(207) 287-1400
TTY: MAINE RELAY 711

Margaret O'Neil
21 Sheila Circle
Saco, ME 04072
Phone: (207) 590-1679
Margaret.O'Neil@legislature.maine.gov

May 22, 2023

Testimony of Rep. Maggie O'Neil sponsoring

LD 1705, An Act To Give Consumers Control over Sensitive Personal Data by Requiring Consumer Consent Prior to Collection of Data

Before the Joint Standing Committee on Judiciary

Good morning, Senator Carney, Representative Moonen, and members of the Judiciary Committee. My name is Maggie O'Neil. I represent House District 129, which is in Saco. Thank you for the opportunity to present **LD 1705, "An Act To Give Consumers Control over Sensitive Personal Data by Requiring Consumer Consent Prior to Collection of Data."**

Our personal information is collected, used, and monetized at an alarming rate. As people subject to data collection, we often aren't given a choice. This bill requires companies to get our consent before collecting and using our most sensitive data--our faces, voices, and fingerprints. It creates guardrails for how this sensitive data can be used and protects against uses of data that disproportionately harm people of color and low-income communities.

The idea for this bill came from my privacy law classes at Maine Law. We learned about a similar law in the state of Illinois has been important for changing big tech company behavior. I drafted the bill with input from law faculty and national consumer privacy experts. Some of those folks are here today, including the Electronic Privacy Information Center (EPIC), a public interest research center dedicated to protecting privacy and democracy. Over the past two years, I have also consulted with a range of stakeholders, including the Attorney General's office, cosponsors from both parties, young people, organizations protecting older adult consumers, and local business leaders. AG Frey has also submitted a letter of support for the bill because of his office's dedication to protecting consumers.

Consumer privacy law is an area where large businesses have enjoyed limited regulation until recent years. That regulation has been limited to certain sectors and the strength of protection varies. Because this bill seeks to increase protections for a kind of data where protections do not currently exist, I expect you will hear pushback. Last year, I sought input from all parties who testified and worked to incorporate their input. I am committed to doing that again this year.

1. Biometric Data

Today's public hearing has been structured so that Sen. Keim's bill and my bill will be heard together. LD 1705 is targeted to a narrow category of vulnerable data. Sen. Keim's bill is a general privacy law that makes rules for all kinds of personal data. LD 1705 makes safeguards for a certain kind of data, called biometric identifiers. If we made a pie chart of different types of personal data, biometric identifiers would be one small slice of the pie.

a. What are biometric identifiers?

Biometric identifiers are a type of our personal data that is used to identify individuals based on unique, unchangeable parts of our bodies, such as our fingerprints, face prints, and our eyes.[1] We call them biometric identifiers because they can be used to identify a person from a group of people. Biometric identifiers are unique to an individual and tend not to change over time.

Biometrics are generated by measuring either a person's distinctive (a) physiological attributes, including fingerprints, voice, facial features, and retinas or ear features, or (b) behavioral characteristics, such as our gestures, voice, typing rhythm, and the way we walk.

There are two main ways to use biometric identifiers. The first way is *authentication*. Many of us are familiar with this technology through smartphones or computers that use our face or thumbprint as a password to unlock our device or to unlock passwords stored on our phone. The second way is *surveillance*. Biometric identifiers can also be used to track us because our faces or other characteristics such as gait are often visible in public.

Biometric identifiers do not include plain photos or videos. We are talking about scans of your face and scans of your fingerprint that can be used to identify you.

As an example, Clearview AI has created the world's largest facial recognition database. In December of 2021, Clearview announced to investors that it would approach 100 billion facial photos in its database within a year—enough to ensure "almost everyone in the world will be identifiable."[2] To create its face recognition database, Clearview uses an automated tool that scrapes internet photos containing our faces and associated data, stores our information in its servers, and extracts our biometric identifiers, using face measurements from the scraped mages.[3] Each faceprint consists of 512 data points corresponding to unique measurements that identify the person's face.[4] After extraction, the company's software associates that person's

---

[1] *New NIST Biometric Data Standard Adds DNA, Footmarks and Enhanced Fingerprint Descriptions*, NAT'L INST. OF STANDARDS & TECH. (Dec. 6, 2011), https://www.nist.gov/newsevents/news/2011/12/new-nist-biometric-data-standard-adds-dna-footmarks-and-enhanced [https://perma.cc/9ME2-R9GF]. Via https://ssrn.com/abstract=3929645

[2] Drew Harwell, *Facial Recognition Firm Clearview AI Tells Investors It's Seeking Massive Expansion Beyond Law Enforcement*, WASH. POST (Feb. 16, 2022), https://www.washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition/.

[3] *See Joint investigation of Clearview AI, Inc., PIPEDA Findings #2021-001*, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (Feb. 2, 2021) https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/#fn5-rf

[4] *Id.*

faceprint with the original scraped images stored on Clearview's server.[5] Then Clearview offers this database to any customers who buy its face recognition software. When a Clearview customer uploads a person's photo to the app for identification, the software extracts a new faceprint, compares it against all faceprints stored in Clearview's database, and shows the user a list of results containing any matching images, associated metadata, and links to original sources.[6]

b. Biometric identifiers are extremely sensitive.

Any efficiencies offered by technology must be considered alongside risks and impacts.

The same features that make biometrics convenient authenticators also pose serious risks to members of the public. Because biometrics are unique to each person and immutable, they are also an extremely sensitive subset of personal data. Collection and use of biometric identifiers raise concerns about data security, lack of transparency, misidentification, privacy intrusions, personal autonomy, free expression, and exacerbation of existing racial and social inequity. Surveillance poses the most extreme risks, whether employed by government or private actors.

Regarding data security, consumer protection advocates caution that a breach of biometric data may cause unmitigable harm. Data breaches are a fact of modern life. Once a person's personally identifiable information is stored in a database, they have little control to prevent a breach. Biometric identifiers are extremely sensitive to identity theft and abuse: they are unique to you, they identify you, they are easy to collect, and you can't change your biometric identifiers in the event of a breach. The harm is done once your data is compromised. Once it is out there, there is no recourse because you can't change your face or your fingerprint. When cyber-thieves access biometric data (whether fingerprint, retina, faceprint, or voiceprint) they gain information that can be linked to a victim's identity forever.[7]

Think about how scary it is when you get a notification alerting you that someone stole your password or bank information. With biometric identifiers, the consequences are even more permanent. Unlike a credit card, password, or even a social security number, our biometric data can't be changed or re-issued. Once we lose control, we are identifiable forever. Our stolen identifiers could be used to gain access to our sensitive accounts, our devices, and more.

As an example, a recent BioStar 2 breach compromised 28 million records of over a million people worldwide, exposing fingerprint data, facial recognition data, user face photos, unencrypted usernames and passwords, logs of facility access, security levels and clearance, and personal details of staff.[8] In another example, a company named PayByTouch had 3.7 million fingerprints on file. When they went bankrupt, those fingerprints (linked to financial accounts)

---

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] Steve Symanovich, *Biometric Data Breach: Database Exposes Fingerprints, Facial Recognition Data of 1 Million People*, NORTON BLOG (Aug. 18. 2019), https://us.norton.com/blog/emerging-threats/biometric-data-breach-database-exposes-fingerprints-and-facial-recognition-data#

were considered assets that could be sold.[9] In another example from 2015, hackers stole 5.6 million fingerprints from the federal government.[10] Those kinds of data compromises make us incredibly vulnerable. It goes without saying that biometric data must be treated with exceptional care. Its misuse can expose us to significant harm including increased risks for fraud, scams, and identity theft.

Biometric identifiers can also be used to track us, posing serious civil liberties concerns, with more pronounced impacts for communities of color and other over-surveilled communities. Biometric identifiers are unique and unchanging, enabling both government and private actors to detect, single out, and track individuals using their face, gait, voice, personal appearance, or any other unique bio-identifier. Face recognition and other biometric surveillance allow tracking from a distance, without detection, and on large numbers of people.[11] Face recognition technology has been particularly "supercharged" in scope and precision due to ever-increasing capabilities of machine learning algorithms and the vast number of photographs of our faces online.[12] This capability furthers both mass surveillance—dragnet collection and analysis of information on everyone, rather than merely those under suspicion—and targeted discriminatory surveillance.[13]

Face recognition is a prominent example. Because our faces are often publicly visible at a distance, face recognition allows for precise identification in real time; including in public spaces such as city parks, schools, workplaces, and transportation stations.[14] Out of concern for harms to our civil liberties, the Maine legislature unanimously banned the use of face recognition surveillance by government. Our law has a significant loophole because it allows private entities to use face recognition surveillance. Those entities impact our rights and lack oversight.

c. Imperfect technology and disparate impacts.

In addition to data security concerns, biometric surveillance technology is prone to make mistakes. These mistakes could impact anyone — any of us could be wrongly identified, wrongly ejected from a business, or have the police wrongly called on us for a crime we did not commit. Even if this technology was perfectly accurate, it would still be a nightmare for our civil liberties. Face recognition technology and other biometric surveillance gives governments, companies, and individuals the power to follow us wherever we go — tracking our faces at protests, political rallies, festivals, places of worship, the doctor, and more.

---

[9] https://trustarc.com/blog/2008/04/02/truste-recommends-destruction-of-more-than-37-million-fingerprint-records/

[10] https://money.cnn.com/2015/09/23/technology/opm-fingerprint-hack/index.html?iid=EL

[11] Garvie, et al., *Perpetual Line Up*, *supra* note 43.

[12] *Face Surveillance and Biometrics*, ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), https://epic.org/issues/surveillance-oversight/face-surveillance/

[13] *Id.* See, e.g., Patrick Reevell, *How Russia is Using Facial Recognition to Police its Coronavirus Lockdown*, ABC NEWS (Apr. 30, 2020), https://abcnews.go.com/International/russia-facial-recognition-police-coronavirus-lockdown/story?id=70299736; *Face Recognition Map*, FIGHT FOR THE FUTURE, last accessed Dec. 20, 2022 https://www.banfacialrecognition.com/map/.

[14] Garvie, et al., *Perpetual Line Up*.

We know the burdens of biometric surveillance are not borne equally. Throughout history, powerful surveillance tools have threatened institutional and individual abuse, and discriminatory targeting, disproportionately violating the civil liberties and human rights of people of color, political dissidents, religious minorities, LGBTQ+ people, people with disabilities, and people with low incomes.[15]

The precision of biometric surveillance amplifies these systemic risks, especially when combined with other forms of data collection and surveillance. Through biometric surveillance, our faces and bodies have become unique markers that we cannot change or hide.[16] Biometrics enable sophisticated tracking without a person's knowledge that can pick us out from a crowd and track our movements including where we go, who we are with, and what we do.

Face recognition technology is especially dangerous because the technology misidentifies certain populations more frequently than others, posing risk of wrongful arrest or ejection from businesses. Face surveillance algorithms tend to be worse at accurately analyzing the faces of people who have darker skin, women, older adults, LGBTQ+ community members, and children.[17]A 2020 NIST study found that face recognition used in police investigations tends to produce more false positive results when processing facial images of Native Americans, Black women, Asian women, women generally, older people, and the very young.[18] NIST warned that technological inaccuracies can result in invasive searches, "false accusations," and wrongful "detentions, interrogations, and deportation" when used by government agents, exacerbating existing disproportionate impacts to people of color.[19]

---

[15] Turner Lee & Chin, *Report: Police Surveillance and Facial Recognition: Why Data Privacy is Imperative for Communities of Color, supra* note 39. *See also* Barton Gellman & Sam Adler-Bell, *Report: The Disparate Impact of Surveillance*, THE CENTURY FOUND. (Dec. 2017), https://tcf.org/content/report/disparate-impact-surveillance/

[16] Garvie, et al., *Perpetual Line Up*. See also "Resisting the Menace of Face Recognition" Electronic Frontier Foundation (EFF) (Oct. 26, 2021), https://www.eff.org/deeplinks/2021/10/resisting-menace-face-recognition.

[17] https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/

[18] Patrick Grother, *et al., Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NIST 2 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf (testing law enforcement images, the highest false positives occur for Native Americans, followed by African American and Asian test subjects; relative ordering depends on sex and varies with algorithm—e.g., compared to images of white men, images of Native American women were 68 times more likely to produce false positive, and Native American men were 47 times more likely to produce false positive.). *See also* Joy Buolamwini & Gebru Timnit, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Conference on Fairness, Accountability and Transparency (2018). https://proceedings.mlr.press/v81/buolamwini18a.html; *see also* Hachim El Khiyari & Harry Wechsler, *Face Verification Subject to Varying (Age, Ethnicity, and Gender) Demographics Using Deep Learning*, 7 J. of Biometrics & Biostatistics 1-5 (2016), https://doi.org/10.4172/2155-6180.1000323. Data from the National Academy of Sciences reflects that each false arrest of a Black person carries an elevated risk of excessive or even deadly police force. *NIST report, supra* note 96 at 5. *See also* Nicole Turner Lee, *Mitigating bias and equity in use of facial recognition technology by the U.S. Customs and Border Protection*, BROOKINGS INSTITUTION (July 27, 2022). https://www.brookings.edu/testimonies/mitigating-bias-and-equity-in-use-of-facial-recognition-technology-by-the-u-s-customs-and-border-protection/

[19] *NIST report, supra* note 96 at 5. *See also* Nicole Turner Lee, *Mitigating bias and equity in use of facial recognition technology by the U.S. Customs and Border Protection*, BROOKINGS INSTITUTION (July 27, 2022). https://www.brookings.edu/testimonies/mitigating-bias-and-equity-in-use-of-facial-recognition-technology-by-the-u-s-customs-and-border-protection/

Simply put: the technology is dangerous when it works — and when it doesn't. Facial recognition and other biometric surveillance tech infringe on our freedom to live, work, and act without being watched, followed, or tracked. That's why Maine has already banned government use of face recognition technology. That bill passed unanimously through both bodies of the legislature last session. LD 1705 continues that work. It goes to the root of the problem by giving us control over whether this sensitive data gets collected in the first place.

- Employees of color whose companies use facial recognition to monitor their activity at work are kicked out of the system more than their white colleagues.
- In Detroit, a 14-year old was kicked out of a skating rink, even though she had never been there, because the skating rink's facial recognition system wrongly identified her as someone else.[20]
- Apple wrongly accused a black teenager of shoplifting in New York, in part based on facial recognition.[21]
- Rite Aid installed more facial recognition collecting cameras in areas that were less wealthy and less white. In areas where people of color, including Black or Latinx residents, made up the largest racial or ethnic group, Reuters found that stores were 3x more likely to use the technology. After negative media exposure, Rite Aid stopped that practice.[22]
- Nijeer Parks, a 31-year-old Black man from Patterson, New Jersey, was falsely identified and subsequently arrested, jailed for over 11 days, and faced charges for nearly a year after being misidentified.[23]
- Michael Oliver, a 25-year-old Black man from Detroit, was wrongly charged with a felony after being misidentified[24]

Finally, commercial biometric identification software blurs lines between corporations and government.[25] Private companies provide surveillance technology to customers including private businesses and governmental clients, often compiling databases of suspicious individuals, aggregating massive amounts of highly personal data, and sharing that data with multiple clients, including government authorities.[26] Databases are compiled by staff without public oversight. Misidentification can result in wrongful arrests and detentions, denial of service, ejection from necessary infrastructure including grocery stores, transportation hubs, and pharmacies, and other

---

[20] https://www.fox2detroit.com/news/teen-kicked-out-of-skating-rink-after-facial-recognition-camera-misidentified-her

[21] https://www.theregister.com/2021/05/29/apple_sis_lawsuit

[22] https://www.reuters.com/investigates/special-report/usa-riteaid-software/

[23] John General & Jon Sarlin, *A False Facial Recognition Match Sent This Innocent Black Man to Jail*, CNN (Apr. 29, 2021). https://www.cnn.com/2021/04/29/tech/nijeer-parks-facial-recognition-police-arrest/index.html

[24] Elisha Anderson, *Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit*, DETROIT FREE PRESS (July 10, 2020), https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/.

[25] See EPIC, *Face Surveillance and Biometrics, supra* note 85; *see* also *Open Letter Calling for a Global Ban on Biometric Recognition Technologies That Enable Mass and Discriminatory Surveillance*, (June 7, 2021), https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Statement-English.pdf [hereinafter Open Letter].

[26] *Open Letter; see, e.g.*, Matt Burgess, *Some UK Stores Are Using Facial Recognition to Track Shoppers*, WIRED MAG (Dec. 20, 2020), https://www.wired.com/story/uk-stores-facial-recognition-track-shoppers/.

unexplained discrimination against individuals who appear on watchlists in all premises using such databases.[27] Even when lawmakers ban or create guardrails for government use of biometric identification, private use continues to generate vast amounts of data. For that reason, individuals and lawmakers seeking to regulate surveillance should look to the companion source of mass surveillance: private entities that provide and employ biometric identification.

d. Right now, there are no rules.

Despite how sensitive biometric data is, there are no restrictions for the ways corporations can collect, use, and even sell our biometric identifiers. In Maine, we allow companies to collect our biometric identifiers without our consent, and we have no rules regarding how long they can keep our data or what they can do with it. Corporations don't have to tell us how or when they are collecting, using, or even selling our data. They don't even have to tell us who will have access to it. We deserve to know and to have choices.

Most people would be surprised to learn that this data is not protected already. A recent poll across the country actually showed that 88% of voters think that lawmakers should act to protect our biometric data.[28]

2. What the bill does: Guardrails for biometric identifiers

a. Requires companies to get our consent.

If a company wants to collect biometric identifiers such as our faceprint or fingerprints, the company must (1) tell us what they want to do with our biometric identifiers and (2) get our express consent before collecting them. This provides notice to us that something serious is being asked for, and it gives us a choice about whether we want to give away our information. This consent can be digital. As a compromise last year, I amended the bill so that in an employment context, an employee's consent can be conditioned on employment.

b. Discrimination prohibited.

Companies would not be allowed to treat us differently or deny us service if we do not consent. As an example, you could use a password instead of your face for unlocking your phone. This protects consumer choice. The power to say no vanishes if companies can treat us differently if we say no.

c. Ban on sale of biometrics.

The bill would ban companies from selling our biometric data.

---

[27] *Open Letter; see, e.g.*, Dennis B. Desmond, Bunnings, *Kmart and The Good Guys Say They Use Facial Recognition for 'Loss Prevention.' An Expert Explains What It Might Mean for You*, THE CONVERSATION (June 15, 2022), https://theconversation.com/bunnings-kmart-and-the-good-guys-say-they-use-facial-recognition-for-loss-prevention-an-expert-explains-what-it-might-mean-for-you-185126.

[28] https://morningconsult.com/2021/04/27/state-privacy-congress-priority-poll/

d. Use reasonable data safeguards.

The bill says that companies can't keep our data forever. They can only hold onto our data for a limited amount of time once they collect it and they are finished using it. It also requires companies to use appropriate safeguards to protect our biometric data while they hold onto it and to make their data retention policy available to the public. The standard of care is the reasonable industry standard, and it must be at least as protective as safeguards for other sensitive information.

e. Upon request, companies must tell people what data they have about us.

This means you could contact Facebook or Amazon to ask what kind of biometric data they have about you. You could also find out where they got it and who they have shared it with. If a company doesn't collect biometric information, they don't have to worry about this requirement.

f. Allows regular people to pursue violations of the law.

The bill creates a private right of action for individuals harmed by violations of the statute. Statutory damages can reach $1,000 for each negligent violation, and $5,000 for each intentional or reckless violation.

To truly protect consumers, any state adopting a privacy law must include a private right of action. A privacy law is only as strong as its enforcement tools, and the best enforcement tool is a private right of action. Boston University law professor Woodrow Hartzog suggests that "only private causes of action seem capable of meaningfully deterring companies from engaging in practices with biometrics based on business models that inevitably lead to unacceptable abuses."[29]

In the absence of a private right of action, enforcement of consumer protection laws is generally assigned to state attorneys general. Although state attorneys general play an important role in protecting consumers, they are often selective in bringing enforcement actions because they have limited resources and balance a number of competing priorities.[30] In fact, many state attorneys general have not brought any enforcement actions under privacy laws that they are authorized to enforce.[31] A private right of action closes the enforcement gap. Regular people must be free to protect their own rights.

Including a private right of action is how legislators normally approach privacy laws. Many privacy statutes contain a private right of action, including federal laws on wiretaps,[32] stored

---

[29] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?* (Oct. 30, 2020). Regulating Biometrics: Global Approaches and Urgent Questions, ed. Amba Kak (AI Now 2020), 96, https://ssrn.com/abstract=3722053

[30] *Id. See* Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 755 (2016); Citron & Solove, *Privacy Harms*, 102 BOSTON UNIVERSITY L. REV., 793, 814-15 (2022).

[31] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 755 (2016).

[32] 18 U.S.C. § 2520

electronic communications,[33] video rentals,[34] driver's licenses,[35] credit reporting,[36] and cable subscriptions.[37] So do many other kinds of laws that protect the public, including federal laws on clean water, employment discrimination, and access to public records.

Big tech companies told Congress for years that they could self-regulate. They haven't been held accountable. Now public opinion has shifted, and our constituents of all political backgrounds agree that more protections should be in place. As a result, big companies have shifted from calling for no regulation to blocking protective laws like this one and asking us to pass weak laws that shield their companies. Their opposition indicates that this law will actually hold tech companies accountable.

History shows us that only a private right of action will protect Mainers. Texas and Washington have both passed biometric privacy laws similar to the Illinois law this bill draws on, with one key difference: they only authorize attorney general enforcement.[38] Those states have seen little to no enforcement of their privacy laws, and but-for Illinois's private right of action, there would likely be zero enforcement.

This should tell you all you need to know: The Illinois law passed in 2008 with a private right of action, and a similar Texas law passed in 2009 with only AG enforcement. Since then, people in Illinois have been able to bring cases to court and change the behavior of big companies like Facebook, Amazon, and Clearview AI. In Texas, after more than a decade, the AG has only filed *two* suits enforcing Texans' biometric privacy rights: (1) the first suit—filed in 2021—piggybacked *Patel*, BIPA's largest ever civil settlement regarding Facebook's tag suggestions feature;[39] and (2) the second suit was filed in October of 2022 again piggybacking the $100 million *Rivera* settlement regarding Google's photo app and alleging additional violations gleaned from BIPA litigation.[40] Texas never would have filed suit if not for the success of the IL law. Washington's recent law has not been enforced at all.

Without a private right of action, Mainers will not have accountability. AG's offices have limited resources to fight the biggest companies in the world. That's why people need to be able take these companies to court themselves.

---

[33] 18 U.S.C. § 2707
[34] 18 U.S.C. § 2710
[35] 18 U.S.C. § 2724
[36] 15 U.S.C. § 1681n
[37] 47 U.S.C. § 551
[38] WASH. REV. CODE ANN. § 19.375.020; TEX. BUS. & COM. CODE § 503.001. Washington's law is more limited in scope.
[39] *State of Texas v. Meta Platforms, Inc.*, No. 22-0121 (Tex. 2022) https://texasattorneygeneral.gov/sites/default/files/images/child-support/State%20of%20Texas%20v.%20Meta%20Platforms%20Inc..pdf
[40] *State of Texas v. Google LLC*, No. (filed 2002), https://www.texasattorneygeneral.gov/sites/default/files/images/press/The%20State%20Of%20Texas's%20Petition%20(Google%20Biometrics).pdf (regarding collection of voice and faceprints from a range of google products, including Google's photo app).

The only way to actually have biometric privacy is to enforce biometric privacy laws. Big companies know that, and that's why they oppose the private right of action. They don't want to be accountable to you and me.

In Illinois, companies are accountable for both technical and egregious violations of the law, preventing harm before it occurs. Likewise, this bill's private right of action will be triggered when a private entity fails to adhere to the statutory procedures because our right to maintain our biometric privacy vanishes when the law is violated. We seek to prevent violations of the law.

g. The Attorney General can also enforce the law.

The AG's Office can also step in to defend consumers. Over the past two years, the Office has provided feedback on language. To be clear, the Maine AG's office does not have adequate resources to battle the world's biggest companies every day (including Facebook, Amazon, and Google). However, this is a good option to supplement the private right of action. Other laws contain precedent for multiple ways of enforcement—e.g., the telephone consumer protection act has three ways of enforcement (PRA, FCC, AGs).

h. Exemptions

1. Medical research.
2. Personal health information subject to HIPAA.
3. Personal information collected, processed, and disclosed subject to GLBA.
    a. GLBA does not require consent before collecting biometrics. Last year, Maine Bankers' Association conducted a member survey regarding use of biometric technology. Voice recognition for banking by phone was the most common use of the technology. A local institution shared that it was standard practice to obtain consent for using voice recognition, despite having no legal requirement.
    b. It will apply to other uses such as face recognition surveillance of sidewalks outside the building and building lobbies. The same survey did not indicate that any members used face recognition surveillance. This is consistent with Maine's concern regarding the use of face recognition surveillance.
4. Biometric identifiers used to complete a financial transaction.
5. Employment settings: consent to biometric technology may be required as a condition of employment and an entity is permitted to only disclose the policy internally.

3. Opponents make these protections sound scary.

You will hear from opponents today. They will drag out tired arguments about our civil legal system, saying that we should leave enforcement to government regulators and that this bill will only be good for lawyers. Corporate lobbyists have attacked our civil legal system for a long time because they know that it is one of the only places that a regular person like you or me can hold them accountable. That's why they came here from DC and spent their money organizing other businesses to speak on their behalf. Their opposition speaks to how effectively this law will empower us to choose whether our data is collected. It speaks to how important the IL law has been for holding companies accountable.

a. The Illinois law has forced big tech companies to change their behavior.

In 2022, Clearview AI was forced to restrict its activities when it settled an Illinois suit brought on behalf of survivors of domestic violence and sexual assault and other vulnerable communities uniquely harmed by face recognition surveillance. The settlement terms permanently ban Clearview AI from selling its faceprint database to most businesses and other private entities—nationwide.[41] Clearview will also (a) stop selling access to its faceprint database to any entity in Illinois, including state and local police, for five years; (b) create an opt-out request form for Illinois residents on its website; (c) cease its practice of offering free trial accounts to individual police officers; and (d) remove photos in its database uploaded from Illinois. Plaintiff Attorney Nate Wessler suggested the nationwide protections contained in the settlement demonstrate that "strong privacy laws can provide real protections against abuse."[42]

For almost 10 years TX has had a similar law on the books that does not let regular people bring a claim in court. After 10+ years, the AG in Texas has finally filed the first enforcement action against a company. The action Texas filed is a direct replica of a suit that was originally brought against Facebook under the IL law via the private right of action. In that suit, *Patel v. Facebook*, Facebook settled for $650 million (more than what Equifax paid to settle its $330m suit), and Facebook agreed to change their practices globally and get opt-in consent before collecting biometrics. Facebook was harvesting and storing users' facial data from photos without asking for our consent or providing notice. That Illinois case made Facebook change their actions, not government regulators.

b. LD 1705 requires entities adopting biometric technology to internalize their externalities.

In economics, an externality is an indirect cost or benefit to third party that arises as an effect of another party's activity.[43] That impact—whether positive or negative—is caused by an entity producing or consuming a good or a service when that causing entity does not bear the cost or receive the benefit of their actions. A common example of a negative externality is a business that causes pollution that diminishes property values or public health in the surrounding area: the polluter does not bear the cost of its pollution on its balance sheet. Because externalities can lead to market deficiencies, government may seek to curb negative externalities either by regulating an activity or by forcing parties conducting business to bear the external costs of their activities, thus internalizing their externalities. Tort law and private causes of action require injurers to internalize such harms by making them liable for harms that are incurred related to risky products and services.[44] Strict liability is employed for especially risky or dangerous activities.

---

[41] *ACLU v. Clearview AI, Inc.*, 2020 CH 04353 (Ill. Cir.), https://www.aclu.org/legal-document/exhibit-2-signed-settlement-agreement?redirect=exhibit-2-signed-settlement-agreement.

[42] IN BIG WIN, SETTLEMENT ENSURES CLEARVIEW AI COMPLIES WITH GROUNDBREAKING ILLINOIS BIOMETRIC PRIVACY LAW May 9, 2022, https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois

[43] *See generally*, Louis Kaplow & Steven Shavell, *Economic Analysis of Law*, HARV. CENTER FOR L. ECON. & BUS. (Feb. 1999), https://ssrn.com/abstract=150860.

[44] *Id.*

Economic theory suggests that liability creates an incentive for businesses to mitigate risk in design, manufacturing, and delivery of services.[45]

LD 1705 will help internalize externalities in two ways: (1) its powerful private right of action ensures that plaintiffs will be able to enforce violations of their rights under the law; and (2) the liquidated damages provision avoids in-court battles regarding the monetary value of privacy invasions. By instituting recovery for violations of the law, this law will create a strong incentive for businesses to reduce risk. To avoid liability or restrictive settlement terms, would-be implementors of biometric technology must consider the impact of adopting the technology and take responsibility for following proper procedure. Further, the strong private right of action also creates a strong incentive to engage in economically efficient levels of activity: LD 1705 will require would-be adopters of biometric systems to consider whether the benefits of a biometric system outweigh the risks, rather than simply whether the technology is convenient. The bill's private right of action creates a strong financial incentive for data collectors to protect biometric data and minimize its use.

c. Thanks to a strong private right of action, businesses in Illinois are now respecting consumer privacy.

Industry lobbyists say that the Illinois BIPA has caused a litigation nightmare and that Maine will be the same. Why is that wrong?

First, Illinois's population (12.67m) is nearly ten times larger than Maine's. Even putting population differences aside, there are a number of reasons why Maine is likely to see only a fraction of that number of lawsuits once LD 1945 is enacted.

For a period of time, businesses in Illinois violated the Illinois law. After Illinois first passed its law in 2008, industry initially argued that language in the private right of action permitting a "person aggrieved" by a violation of the law to sue meant that only people who could show they had suffered monetary or other tangible loss could bring suit. Demonstrating such injury can be extremely difficult in the context of privacy violations, where tangible harms may not be discoverable for years, if ever. Many private entities did not take compliance with BIPA seriously at first, perhaps because they thought it was unlikely that they could ever be subject to a successful lawsuit. It took a decade before litigation in the lower courts ripened into the state supreme court ruling in *Rosenbach* making clear that a person is "aggrieved" by a violation of the law—and therefore can sue—whenever their rights under BIPA are violated. The court reasoned that a person is aggrieved with a "real and significant" injury when that person's right to maintain privacy and control over biometric data has been violated.[46] When a business violates a person's statutory rights, their right to maintain privacy and control "vanishes into thin air."[47]

---

[45] *Id.*

[46] *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186 ¶ 34, 129 N.E.3d 1197, 1206 quoting *Patel*, 290 F. Supp. 3d at 953.

[47] *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186 ¶ 34, 129 N.E.3d 1197, 1206 quoting *Patel*, 290 F. Supp. 3d at 953.

Following that ruling, individuals filed a number of lawsuits against businesses that they alleged to have violated their rights under BIPA. Illinois businesses could and should have taken advantage of the preceding decade since enactment of BIPA to get themselves into compliance with the law, but some of them chose to wait to get sued before doing so. Now that businesses have an incentive to comply with BIPA, the volume of lawsuits in Illinois is likely to decline steeply.

In Maine, the dynamics will be very different. The private right of action in LD 1705 is drafted more clearly, so both Maine residents and Maine businesses will be clear from the moment of enactment about their rights and obligations. Private entities in Maine will thus have the information and the incentive to start complying with the law immediately. Additionally, the lengthy implementation period will give Maine businesses more than enough time to bring themselves into compliance with the law. Trade associations, business groups, and state agencies will have time to produce informational materials and model notice-and-consent forms that will make compliance easy. Because businesses in Illinois, Texas, and Washington have been complying with biometric privacy laws for years, there are numerous examples of retention schedules, consent forms, and other resources available for Maine businesses to use. Moreover, national businesses operating in Maine are already complying with the Illinois, Texas, and Washington laws, and so will have no trouble complying in Maine (and no reason to fear continuing to do business in Maine either).

Of course, there will be lawsuits if businesses abuse Mainers' trust by collecting and using personal biometric data without consent, failing to take reasonable steps to safeguard that information once collected, or deciding to put Mainers' biometric identifiers up for sale. The Attorney General's office will never be able to investigate or take action against every business that violates our rights under the law. The private right of action is necessary to ensure that Maine residents are able to obtain meaningful relief. That is why private rights of action are commonly provided in privacy and consumer protection laws.

The truth is, businesses have been asking lawmakers to not regulate their data practices for a very long time. We can see where that has gotten us: civil liberties, human autonomy, and democracy are all threatened.

This bill is targeted to (a) very specific and (b) incredibly vulnerable data. To corporate lobbyists in the room today: if you are in the data collection business, you are in the data protection business. The stakes for individuals who consent to the use of their biometric data is extremely high, and the consequences for mismanagement of our data should be equally high. Companies already have a choice: if they can't take adequate steps to protect biometric data, they should not be collecting it in the first place. Period.

Why are they so opposed to us having a choice? It's about money--big data is big business. If a company can't protect our biometric data, they should not be collecting it in the first place. We don't need to our faces tracked or fingers scanned when we go to RiteAid. If a company finds it burdensome to comply, there's an easy solution: don't collect sensitive biometric data.

A note about financial institutions: testimony from the banking lobby suggests that this law should not apply to them because an existing federal law pertaining to financial institutions called Gramm-Leach-Bliley (GLB) already protects consumers. Financial institutions often come to public hearings for consumer privacy bills and ask for a total exemption on everything they do just because of this law. It is important for us to have a conversation about how the law is not protective of consumers. That said, I won't die on that hill and am coordinating with them on their data collection policies.

Here's a little bit about Gramm-Leach-Bliley (GLB), the federal law mentioned: GLB does not preempt state laws that offer stronger protections, as this bill does. GLB has been criticized for being a weak privacy law. A longtime Congressional staffperson who drafted HIPAA and other landmark privacy legislation has commented that "the privacy provisions of Gramm-Leach-Bliley for financial institutions are so weak that consumers would actually be better off if Congress repealed the law."[48] The privacy part of GLB provides only two provisions for consumers: (1) First, financial institutions must have a privacy notice. That's something but not much. Consumers don't read privacy notices, although others do—e.g., regulators, consumer groups, and reporters. Notices used to be an annual requirement, but banks lobbied Congress to dilute that obligation. In any event, in 2022 banks have privacy notices with or without this law. (2) Second, GLB provides that a financial institution that wants to share your personal information with a non-affiliated third party—anyone outside the corporate family—must give consumers the chance to "opt out" under some circumstances. Even if a consumer doesn't opt out, the law prevents sharing of account and credit card numbers for third-party marketing uses. But the opt-out does not apply to joint marketing agreements with other financial institutions. That means that if one financial institution wants to share consumer information with another financial institution, it can do so through a joint marketing agreement, and consumers have no opt-out rights. That's the "strong" federal law banks say protects you here. Limited opt-out rights and a privacy policy are clearly not the same as this bill. That said, I've reached out to our local banks to meet. I'm willing to accommodate their concerns within reason.

Lobbyists suggest working this bill side-by-side with another one, LD 1973. Respectfully, that bill (LD 1973) is written to benefit industry, not Mainers. Sen. Keim is dedicated to ensuring privacy protections, and I will work with her on next steps. It was not her intent to benefit industry—she is a strong privacy advocate. I have seen a number of Trojan Horse bills written by tech lobbyists. They are submitting them around the country to prevent legislatures from enacting real protections. In my testimony, I linked an article entitled "Big Tech is pushing states to pass privacy laws, and yes, you should be suspicious."[49] As written, LD 1973 would enact watered down protections and repeal our important law that protects our privacy with internet service providers. Lobbyists have been trying to get rid of that law for a while. It's like whack-a-mole keeping up with them. Good local internet providers like GWI supported that internet privacy bill, and it's important that we protect it. Leading up to this bill, I met with Fletcher Kittredge, CEO at GWI, and he opposes removing our strong ISP protections for Mainers. He's submitting written testimony because his schedule did not allow him to be here today. GWI is a

[48] https://iapp.org/news/a/protect-consumer-privacy-repeal-the-glbas-privacy-provisions/
[49] https://thenextweb.com/news/big-tech-is-pushing-states-to-pass-privacy-laws-and-yes-you-should-be-suspicious-syndication/amp

good example of businesses building privacy into their business model. Not all businesses are fighting these laws. They know privacy is important to their customers.

Young people have also taken the time to tell you why this is important to them. I encourage you to take the time to read their testimony. They bear the weight of our inaction, and they don't have a vote to cast.

In closing, there are few rules governing the use of biometric identifiers despite the explosion of technology gathering them. Other states such as Illinois have laws like LD 1945, and they have successfully protected consumers. I urge you to pass this bill so that Mainers can have the same protections.