Joint Committee on the Judiciary
Testimony of GLBTQ Legal Advocates & Defenders, Equality Maine, MaineTrans.Net, by Mary L. Bonauto
LD 1705, An Act to Give Consumers Control over Sensitive Personal Data by Requiring Consumer Consent Prior to Collection of Data – OTP
May 22, 2023

Senator Carney, Representative Moonen, and Distinguished Members of the Judiciary Committee,

I am Mary Bonauto, a resident of Portland, and an attorney with GLBTQ Legal Advocates & Defenders, or GLAD. Along with Equality Maine and MaineTrans.Net, GLAD strongly supports LD 1705, *An Act to Give Consumers Control over Sensitive Personal Data by Requiring Consumer Consent Prior to Collection of Data,* and appreciates Representative O'Neil's bringing forward this important bill.

We have supported other bills seeking to safeguard personal privacy.[1] We are enthusiastic about this bill's requirement of written, informed consent from individuals when private entities seek to collect or obtain, store, use and disseminate our "unique biological characteristics." We appreciate the bill's measured approach, careful definitions and targeted exemptions, and overall common sense. It would:

- require "affirmative written consent" before a "private entity" may collect or obtain biometric data, including our voiceprint and images of our faces, the iris and retina of the eye, fingerprints and hands, as well as "measurable biological characteristics that can be generated or captured from a photograph or video" and and specifically -
    - requires the entity to provide written notice and information to the individual about the specific purpose and length of time for which the identifier is being collected, stored, bought, traded, used, disclosed, or otherwise disseminated, and to obtain "affirmative, written consent" from the individual. and
    - prohibits the sale, lease or trade of that biometric identifier, including from those with or to whom the private entity transferred, shared or provided the biometric identifier, and
    - requires private entities not to discriminate by requiring consent in order to obtain goods or services, and at the same price as others (LD 1507, proposed §9607 (1-3));

---

[1] We have testified in support of other bills, e.g. LD 1585 – *An Act To Increase Privacy and Security by Prohibiting the Use of Facial Surveillance by Certain Government Employees and Officials*, in the Criminal Justice & Public Safety Committee (130th Leg., sess. 1). That bill is now law. We also supported Representative O'Neil's earlier iteration of this bill, LD 1945, in this Committee in the 130th Leg., 2d session.

- require private entities that possess biometric information (with defined exceptions) to develop and publicize its policies on retention and destruction of the material, with destruction date tied to accomplishment of its intended use, consumer request and within a specified time after the last intentional action between the customer and company (LD 1507, proposed §9603);

- when requested by an individual, require the private entity to disclose to the individual information such as what was collected, its sources for collection, its links to personal information, and what disclosures of the data and personal information have been made to third parties (LD 1507, proposed §9606);

- require the collector or holder of this information to take care in how it is stored and transmitted in order to prevent disclosure, in accord with reasonable standards of care in the industry, with the caveat that those standards must be at least as protective as those of the private entity in storing, transmitting and protects its own "confidential and sensitive data"[2] (LD 1507, proposed §9605);

- create a private right of action against private entities for violations of the law, with consequences calibrated to ensure at least minimum damages for negligent or reckless/intentional violations ($1,000 and $5,000 respectively), or actual damages if greater), along with reasonable attorney's fees, court, expert and litigation costs, and injunctive and other equitable relief, (LD 1507, proposed §9608 (1)); and

- find that a violation of this proposed chapter is also prima facie evidence of a violation of the Maine Unfair Trade Practices Act. Tit. 5 MRS, chap. 10. The Attorney General would also be empowered to enforce this measure, whose effective date of January 1, 2025 (LD 1507, proposed §9608 (2-4)).

This bill is not only timely, but imperative to meet our times. Without this bill, ordinary individuals do not even know what private entities have our biometric identifiers let alone to obtain information from them. This bill would require the safekeeping and eventual destruction of our most personal information while also, when we ask, telling us how that information was obtained and how it has been used. The power of the technology involved and the singularity of the information collected about individuals is far more consequential than the better known uses of technology, such as identifying the clothing brands we purchase, what we stream online or at home, or our political party.

The civil rights implications of this technology are staggering. Nearly 100 years ago, Justice Brandeis dissented in a case that allowed government wiretapping without judicial process. The vaunted "right to be left alone"[3] that Justice Brandeis championed became law later

---

[2] Confidential and sensitive information is defined to include genetic testing information, unique or personal identification numbers, account numbers and passcodes, and driver's license and social security numbers.

[3] The right to be left alone was articulated in the dissenting opinion of Justice Brandeis in *Olmstead v. United States*, 227 U.S. 438 (1928). Decades later, the Supreme Court reversed Olmstead and agreed that a search warrant is required before the government could wiretap a phone. *Katz v. U.S.*, 389 U.S. 347

and applies to government oversight and overreach. But without measured regulation, private companies can peer into what we do, where we go, and with whom, and then transfer or sell that information unconstrained by the constitutional safeguards applicable to the government. Just because technology has made this possible doesn't mean it is a good idea for all people in all contexts. Many of us still want to enjoy "the freedom of movement" that is "part of our heritage" and "to remain in a public place of [our] choice"[4] without private companies surveilling us and our comings and goings for private gain. This bill says that Maine should be smarter about this powerful technology so we can consent to collection or not, obtain information about what companies have and how out markers have been used, and require standards of care for safekeeping of information and destruction of that information.

Another important reason why we need safeguards is because facial recognition technology is known to misidentify people along racial and gender lines. With respect to race, there are simply high error rates, including but not limited to skin tone.[5] Relying on this technology has resulted in mistaken identity and false arrests.[6] The technology also sorts faces by "male" and "female" even though human diversity cannot be bounded by these generalizations. A review of four facial recognition programs concluded that the software failed to correctly identify the gender of transgender men in over one-third of cases, whereas the programs correctly identified other men almost all of the time, and was confounded by nonbinary people.[7]

(1967). That Court continues to require judicial intervention before the government can track our movements.

[4] *Chicago v. Morales*, 527 U.S. 41, 54 (1999) (internal citations omitted).

[5] *See, e.g.*, Larry Hardesty, *Study finds gender and skin-type bias in commercial artificial-intelligence systems*, MIT NEWS (Feb. 11, 2018), https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212#:~:text=artificial%2Dintelligence%20systems-,Study%20finds%20gender%20and%20skin%2Dtype%20bias%20in%20commercial%20artificial,percent%20for%20dark%2Dskinned%20women ; Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROCEEDINGS OF MACHINE LEARNING RSCH. 1 (2018) (demonstrating discrepancy of over 30% in error rates between identifying light-skinned men and dark-skinned women).

[6] For example, a Black man in Georgia was pulled over and arrested while driving and held in jail for nearly a week after he was misidentified as the perpetrator of thefts in Louisiana. He was not informed of what evidence led to his arrest, which was later reported to be the use of facial recognition of Clearview AI. He was released when the surveillance video of the thefts and other photos of this individual clearly showed he was not the culprit. K. Hill & R, Mac, *'Thousands of Dollars for Something I Didn't Do,'* NY Times (April. 6, 2023) available at: https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html?searchResultPosition=3. See also Tate Ryan-Mosley, *The new lawsuit that shows facial recognition is officially a civil rights issue*, MIT TECH. REV. (Apr. 14, 2021) (highlighting wrongful arrest of Black man based on erroneous placement of Detroit Police Department facial recognition system and similar false arrests against Black men).

[7] *See* accessnow, *Computers are binary, people are not: how AI systems undermine LGBTQ identity*, (updated Jan. 13, 2023), available at: https://www.accessnow.org/how-ai-systems-undermine-lgbtq-identity/ (noting errors arising from assumed characteristics of men and women); Lisa Marshall, *Facial recognition software has a gender problem*, UNIV. OF CO. AT BOULDER (Oct. 8, 2019), https://www.colorado.edu/today/2019/10/08/facial-recognition-software-has-gender-problem . *See also* Morgan Kalus Scheuerman et al., *How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis and Image Labeling Services*, UNIV. OF CO. AT BOULDER, 144:26 (Nov.

We understand that technology is part of what drives our modern world and this bill does not stop the use of biometric identifiers. This bill provides sensible guardrails as the collection and marketing of biometric identifiers proliferates. In addition, the dangers posed to Black and Brown communities, some of whom are also part of Muslim and/or immigrant communities, and parts of the LGBTQ community, also compel action here.

Thank you for your consideration, and we urge you to unanimously vote that LD 1705 ought to pass.

Sincerely yours,

Mary L. Bonauto, Esq.
(on behalf of GLAD, EqualityMaine, MaineTrans.Net_
Civil Rights Project Director
GLBTQ Legal Advocates & Defenders
mbonauto@glad.org
257 Deering Ave., #203
Portland ME 04103

2019), https://dl.acm.org/doi/pdf/10.1145/3359246 (finding that computer classifications in binary gender (male/female) performed worse with images of transgender images than cisgender images, could not correctly identify if someone did not have a non-binary (neither male/female) identity, and that while labeling in the programs could allow for gender neutrality, they still made use of coding gender performance (i.e., the expression of gender) as male and female only and with no accommodation of gender nonconforming or gender nonbinary people.