Joint Committee on the Judiciary
Testimony of GLBTQ Legal Advocates & Defenders, Equality Maine, Maine TransNet,
by Mary L. Bonauto
LD 1945, An Act to Recognize the Use of Biometric Identifiers – OTP
February 22, 2022

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

Good Morning. I am Mary Bonauto, a resident of Portland, and an attorney with GLBTQ Legal Advocates & Defenders, or GLAD. Along with Equality Maine and Maine TransNet, we support LD 1945, An Act to Regulate the Use of Biometric Identifiers.

We testified in the last session to support 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. That bill is now law. We now ask you to support LD 1945 to provide safeguards for all of us when it comes to how private companies obtain, store and use our "unique biological characteristics." We appreciate the bill's measured approach, as it would:

- require "affirmative written consent" before a private entity may collect or obtain biometric data, including images of our faces, the iris and retina of the eye, fingerprints and hands, that can identify an individual, and to provide information to the individual of the purpose and duration of the collection or possession;

- require those possessing this information to create and publish policies about retention of this information, and creating a default end date (the earlier of completion of the purpose for which the data was obtained, or a year since the individual's "last intentional interaction" with the private entity possessing the information (with limited exceptions));

- 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, which standards must be at least as protective as those applied to other confidential and sensitive information. Failure to act with reasonable care is deemed to violate the Maine Unfair Trade Practices Act;

- require the collector, upon an individual's request, 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. Failure to provide the information is deemed to violate the Maine Unfair Trade Practices Act;

- requires notice, an individual's affirmative, written consent, and information disclosures before an entity may collect, purchase, receive through trade or otherwise obtain, use, disclose or otherwise disseminate a person's biometric identifier from an individual. This section is enforceable via a private right of action, with monetary penalties, reasonable attorney's fees, and expert and court costs, and other relief as the court determines.

This bill is coming just in time. Ordinary individuals are not equipped to push back against the large technology companies that sell the surveillance technology the companies that use it, and those that store or disseminate it. The quest to collect and monetize people's personal information would extend far beyond what technology companies can track now, such as 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"[1] that Justice Brandeis championed became law later 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, 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. This bill says that Maine should be smart about this powerful tool, requiring consent, standards of care, disclosures and transparency.

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.[2] Relying on this technology has resulted in mistaken identity and false arrests.[3] The technology also sorts faces by "male" and "female" even

---

[1] 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 (1967). That Court continues to require judicial intervention before the government can track our movements.

[2] *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).

[3] E.g. 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).

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.[4]

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 1945 ought to pass.

Sincerely yours,

GLAD
Equality Maine
Maine TransNet

By Mary L. Bonauto, Esq.
Civil Rights Project Director
GLBTQ Legal Advocates & Defenders
mbonauto@glad.org
257 Deering Ave., #203
Portland ME 04103

[4] *See* 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. 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.