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

October 17, 2023

Testimony of Rep. Maggie O'Neil sponsoring

LD 1977, An Act to Create the Data Privacy and Protection Act

Before the Joint Standing Committee on Judiciary

Good afternoon Senator Carney, Representative Moonen, and members of the Judiciary Committee, I am Maggie O'Neil. I represent House District 129 in Saco. Thank you for the opportunity to present **LD 1977, An Act to Create the Data Privacy and Protection Act**.

I. Background: A bipartisan compromise formed through years of negotiation and stakeholder input.

This bill protects Mainers against unwanted and unexpected uses of our personal data.

Mainers value privacy. We want to choose who has our personal information, who it gets shared with, and how it is used. In the absence of Congressional action, Maine has led the country in passing a face recognition ban, warrant protections for data, and a landmark law requiring internet service providers to get our consent before sharing our data. There is more work to do to protect Maine consumers.

LD 1977 will create coherent privacy protections across the board, whether we are searching Google, wearing a watch that gathers health data, or operating an Alexa device in our living room. Residents of other states and countries currently enjoy these protections, but Mainers are stuck without protections until we act. LD 1977 will reign in the amount of our personal data that companies collect and use, give us certain rights to control our personal data, and deter abuses by creating meaningful consequences when the law is violated.

I submitted this bill alongside the other bills on your calendar today about specific kinds of data so that the committee would have the option of working on either (a) a general consumer privacy law that covers *all* kinds of data or (b) *specific* protections for extremely vulnerable kinds of personal data. If consumer privacy protections were a pie, the biometric and health data bills would be slices of a pie. This bill would cover most of the pie, including biometric and health data.

LD 1977 is drafted based on a bipartisan compromise bill at the national level that was formed with years of stakeholder input. Because it is a compromise bill, it does not contain everything that a consumer advocate would want, but it has strong protections and years of industry input and buy-in. It is a strong starting point for us to create a bill that works for Maine.

Over the past few years, I have explored data privacy issues with faculty members at Maine Law and legislators from both parties. These issues speak to the core of who we are and how we live our lives as Mainers. Leading up to today, I have been in touch with consumer protection advocates, members of industry, the Attorney General's office, and Sen. Keim. I am committed to working this concept with interested parties to get the language right for Maine.

II. Risks and harms for today's consumers.

The privacy risks faced by Mainers and people around the world are more complex, more systemic, and potentially harmful than ever before. In today's society, collection and use of data is built into the business models of many of the major companies we interact with, including tech giants Google, Meta, and Amazon. A few examples include apps that your collect phone activity and locational data; digital watches and health websites that monitor your health information; and smart home devices like Alexa that operate an active microphone in your home. Collection and processing of personal data at this massive scale is the root cause of many problems online from discrimination to threats to democratic society.

Unrestricted data collection has eroded consumer privacy, and Congress has failed to act on this issue for decades, allowing data-driven abuses and harms to flourish. Consumers are surveilled through constant monitoring, profiling, and targeting online. Online firms have been allowed to collect and commodify every bit of consumer data, depriving consumers of control over their personal information, heightening security risks, and leading to data misuse, the loss of autonomy, manipulation, and discrimination. Our lack of protections even *incentivizes* these harmful practices because there is so much money to be made without boundaries on what these companies can do.

The excessive data collection and processing that fuels commercial surveillance systems is inconsistent with the expectations of consumers, who reasonably believe that the companies they interact with will safeguard their personal information. These exploitative practices don't have to continue. By making clear rules of the road, this law will help protect Mainers from privacy harm stemming from Big Tech and social media.

III. How LD 1977 protects Maine consumers.

1. Data Minimization

Data minimization is a valued practice that reduces the amount of unnecessary personal data floating around online reduces the potential for that data to be abused. The trend and training for data management should be privacy by design. For companies not engaging in privacy by design, this requirement will protect consumers.

When companies collect our data, this bill will require them to match our expectations as consumers by limiting the scope of the personal information that they collect, use, share, and keep. Companies may not collect any covered data unless it is reasonably necessary and

proportionate to provide or maintain a specific product or service requested by the individual. Companies are more restricted when handling our sensitive data, including social security numbers, biometrics, and health data: they may not collect, process, or transfer the data unless strictly necessary to provide or maintain a specific product or service requested by the individual.

Data minimization is a common tool in data privacy frameworks employed to protect consumers. For example, if you search the International Association of Privacy Professionals (IAPP) website, you will find many articles about accomplishing data minimization.

From a data security standpoint, there is less risk of data compromise if a company does not collect more data than is needed. To illustrate, a data security issue occurs when companies fail to safeguard personal data against unauthorized access – e.g., when a social media company collects nonpublic information beyond what is needed to run the app and hackers steal that data due to lapses in the company's data security practices. Data minimization is a responsible professional practice because a company doesn't have to protect data that it doesn't collect. Practicing data minimization makes businesses less attractive targets for data thieves and hackers and limits the harm to consumers when breaches do occur.

Data minimization is also a valued tool because it prevents harmful "secondary uses" of personal data that often cause harm to consumers. Frequently, consumers are harmed by out-of-context uses of personal data by (a) businesses that have collected it and (b) third parties with whom we never interacted and shared our data. Secondary uses of our personal data often expose our data to security risks and violate our expectations as consumers – e.g., a company uses a consumer's nonpublic account security information such as their location or cell phone for marketing purposes to target the consumer.

Nearly every online interaction can be tracked and cataloged to build detailed profiles and target us. Even offline, credit card purchases, physical movements, and smart devices in our homes create countless data points that are logged and tracked without our awareness or control. This data collection and surveillance can reveal or infer sensitive details about us. Companies build extremely detailed profiles about us that can alter what we see, what prices we pay, and whether we are able to find the information that we seek online (including information about job opportunities, health services, and relationships).[1]

Despite this bill being a compromise measure, consumer advocates will explain that this bill has stronger language than the competing measure (LD 1973). I hope we can keep the stronger language here to create good protections for Mainers.

2. Consumer Control: Consent and the Rights to Know, Correct, and Delete

a. Consent: Companies must get consent to (a) collect sensitive data and (b) to conduct targeted advertising. Further, sensitive data may not be used for targeted advertising.

b. Rights to Know, Correct, and Delete: If we make a consumer request, companies must allow us to know what data is collected about us or transferred to another party in the past 24 months. Companies must also allow us to correct inaccurate data about us. This protection is important because our data is used to make decisions about us in many ways that we are not aware of.

---

[1] EPIC, Data Minimization.

Finally, consumers may request that a company delete our data. The bill allows two free requests annually.

3. Non-retaliation

Companies may not treat a person differently for not consenting to share their personal data. As a compromise, the bill does not ban customer loyalty programs and creates certain protections for consumers within those programs.

4. Transparency about our data

Companies must disclose the type of data they collect, what they use it for, how long they retain it, and who they share it with. The disclosure must be in a publicly available privacy policy.

5. Protects Minors from Harm

Companies may not use targeted advertising on minors, making it easier to limit the addictive features of social media. Companies also may not share a minor's data without consent of the minor or a guardian.

Advocates point to the rising mental health crisis as one reason for this protection. Over half of teens have reported that giving up social media would be difficult.[2] Leaked reports of Facebook's internal research on its app Instagram concluded it was making body image issues worse for 1 in 3 teen girls.[3] A recent study found that 13% of teenage girls struggling with mental health drew a direct line between Instagram and a desire to kill themselves.[4] The whole system of targeted advertising is about getting people use their phones and shop more. It is more important that we protect the mental wellbeing of young people.

6. Prevents Civil Rights Abuses

The bill prohibits the use of personal data to discriminate or otherwise make unavailable the equal enjoyment of goods or services based on protected characteristics (note: the list enumerated in this bill is more limited than Maine law and should likely be updated to match the work this committee has done; the state of MA is considering a very similar proposal with additional characteristics protected). This will address data practices and automated decision-

---

[2] PIRG https://pirg.org/articles/why-bidens-call-to-ban-targeted-advertising-to-kids-teens-matters/#:~:text=During%20the%20State%20of%20the,anxiety%2C%20depression%20and%20social%20isolation.

[3] "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show" Wall Street Journal (Sept. 14, 2021) https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739

[4] PIRG https://pirg.org/articles/why-bidens-call-to-ban-targeted-advertising-to-kids-teens-matters/#:~:text=During%20the%20State%20of%20the,anxiety%2C%20depression%20and%20social%20isolation.

making systems that have led to discrimination in housing,[5] employment,[6] credit,[7] education, finance, and other economic opportunities, which has negatively impacted communities of color. As the use of individuals' most personal information becomes more pervasive, it is critical that an individual's data not be used in ways that harm them. Privacy rights are civil rights. In addition to the protections here, well-drafted consumer privacy legislation will protect civil and human rights, empower communities of color, and ensure opportunities are open for marginalized populations.

7. AI Ethics and Harm Reduction

Large data holders like Google and Facebook must conduct algorithm impact assessments and submit an audit report to the Attorney General. To illustrate with a real-life example, this requirement would help identify and prevent an algorithm that allows digital redlining, such as a targeted ad that offers a predatory student loan product or a sham degree just to young people who live in a low-income rural area or a urban neighborhood but not to young people living in wealthier communities. As a result, the young people are more likely to get trapped in cycles of debt.

Digital redlining severely alters the reality we see and the services offered to us. Without audits of what is under the hood of a company's practices, consumers often experience unequal treatment. Algorithm assessments will help identify biases that reproduce patterns of discrimination and, thus, minimize risks of harm. Everyone has a right to engage in the online economy free from algorithmic bias, digital redlining, and pervasive surveillance.

Finally, the bill also considers algorithmic impacts on minors to promote safety and wellbeing.

8. Privacy by Design

Covered entities have a duty to implement reasonable policies, practices, and procedures for collecting, processing, and transferring covered data. These should correspond to the entity's size, complexity, activities related to covered data, the types and amount of covered data the entity engages with, and the cost of implementation compared to the risks posed. Privacy by design must also take into account the particular privacy risks related to individuals under 17 years of age.

9. Small business protections

Small businesses (as defined) are exempt from compliance with many provisions of the bill. We will need to look at the contours of this exemption and determine what is right for Maine to protect consumers. The goal here is to create a strong consumer privacy law that balances

---

[5] Valerie Schneider, "Locked Out by Big Data: How Big Data, Algorithms, and Machine Learning May Undermine Housing Justice." https://blogs.law.columbia.edu/hrlr/files/2020/11/251_Schneider.pdf

[6] Kochling & Wehner, "Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development." Business Research. https://link.springer.com/article/10.1007/s40685-020-00134-w#Abs1

[7] Rice & Swesnik, "Discriminatory Effects of Credit Scoring on Communities of Color." https://cpb-us-e1.wpmucdn.com/sites.suffolk.edu/dist/3/1172/files/2014/01/Rice-Swesnik_Lead.pdf

burdens of small business compliance and protects consumers from harm. I have already requested input on this item from the business community and await their feedback.

10. Data Broker Registry

Companies that sell data must register annually with the Attorney General and clearly tell the public that they sell data.

11. Enforceable protections

The bill is enforceable both by (a) the Attorney General and (b) a consumer private right of action, ensuring that both can act to protect consumers. Individuals may enforce violations of their rights under the Act by bringing a case seeking liquidated damages, punitive damages, injunctive relief, reasonable attorney's fees and litigation costs, and any other appropriate relief. Small businesses are exempt from this provision.

It is typical practice for consumer protection statutes to contain a private right of action. Many privacy statutes contain a private right of action, including federal laws on wiretaps, stored electronic communications, video rentals, driver's licenses, credit reporting, and cable subscriptions. So do many other kinds of laws that protect the public, including federal laws on clean water, employment discrimination, and access to public records.

Maine's law needs teeth to be enforceable. Otherwise, the protections will exist on paper only. A right without a remedy is no right at all to someone who has been harmed.

Consumer advocates suggest that a strong private right of action is the most important tool to deter privacy violations that are otherwise difficult to enforce.[8] State attorneys general are often constrained by limited resources and tend to be selective regarding enforcement.[9] In fact, many state attorneys general have not brought any enforcement actions under privacy laws that they are authorized to enforce.[10] With so many huge data collectors covered by this law, it is not practical to expect Maine's consumer protection division to enforce this law. That is why Big Tech lobbyists will advocate against it.

To fill the enforcement gap, private rights of action provide an incentive for individuals to enforce the law and deter violations, acting as "private attorneys general."[11] Companies oppose this because it creates real consequences for breaking the law. This is the most important part of the bill, especially because it only applies to large companies.

Finally, from an economic standpoint, a strong private right of action requires companies to internalize their externalities. Externalities are things a company does or causes that the company doesn't bear the cost of on their balance sheet. Right now, Big Tech can harm people without any cost and there is even a financial incentive to do so. By putting the cost of privacy harms on

---

[8] Hartzog, *supra* note 172, at 101.

[9] Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV., 793, 815-15 (2022).

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

[11] Citron & Solove, *Privacy Harms*, at 797, 821.

Big Tech's balance sheet, we will create a financial incentive for those companies to follow the law and protect our data.

IV. Don't let Big Tech write Maine's privacy law.

There are powerful economic incentives for businesses to collect, track and commodify consumer data far beyond what is necessary or expected by consumers. Unsurprisingly, industry self-regulation has failed to meaningfully protect consumer privacy online. Industry is supportive of a measure that they helped craft and which is modeled on other weak privacy laws across the country. For years tech companies pushed for no regulation in this arena. Now that other countries and other states are passing strong laws, they are working to get ahead of the "problem" by pushing weaker, industry-written laws. The attached article details these industry efforts, including the history on the Connecticut bill that industry lobbyists have used as their model for a Maine bill. Don't allow Big Tech to write our consumer privacy law here in Maine.

V. Don't repeal Maine's landmark Internet Service Provider Law.

Maine has a best-in-the country law that protects us from having our data used and sold by internet service providers (ISPs) without getting out consent. In my privacy law classes, we learned about how it is a crucial protection for consumers. As a consumer we might be able to use DuckDuckGo instead of Google to search, but we cannot choose whether we use our internet service provider. ISPs have access to everything we do online, so they have a perverse incentive to make money by selling information about us and what we do online. Maine-based providers like GWI spearheaded this law because they do not use these exploitative practices and they know that Mainers don't like it. Please maintain this important protection for Mainers.

Thank you for your time. I am committed to working with the committee and stakeholders to get this right for Maine.