Senator Anne Carney
Chair, Judiciary Committee
3 State House Station
Augusta, Maine 04333

Representative Matt Moonen
Chair, Judiciary Committee
2 State House Station
Augusta, Maine 04333

Re: The Maine Data Privacy and Protection Act

Dear Chairs Carney and Moonen,

We write today to express our support for the Maine Data Privacy and Protection Act (HP. 1270) ("DPPA"), which would provide critical privacy protections for residents of Maine. Maine is not alone in considering truly consumer-friendly legislation this legislative cycle, and we support similarly strong proposals in other States. Unfortunately, a number of State laws on the books simply rubber-stamp existing privacy violations. These laws should not be replicated in Maine.

Owned by a not-for-profit foundation and founded as a community open source project in 1998, Mozilla is the mission-driven technology company that advocates to keep the internet open and accessible for all. We are the maker of the open-source web browser Firefox, as well as a suite of privacy and security-enhancing products. A foundational principle of Mozilla's guiding Manifesto[1] demands that individual privacy and security online must not be treated as optional. This is why privacy comes first in our products,

[1] Mozilla Manifesto. https://www.mozilla.org/en-US/about/manifesto/

like Enhanced Tracking Protection (ETP)[2] and our end-to-end encrypted Firefox Sync service.[3]

The protections in HP. 1270 are essential for consumers and are reasonable guardrails on industry

Data minimization. Data minimization is based on two fundamental principles. First, the less data companies hold, the harder it is for malicious actors to breach that data. Second, that consent cannot be the sole basis of privacy guardrails. Consumers are often being presented with extremely complex and often contradictory information about how their data is being collected and used; they should not have the primary burden of defending their own privacy. Instead, data collectors should have an obligation in parallel to consumer consent that requires them to only collect data in a manner that is required to provide a service requested by a consumer, subject to certain exceptions such as those in the DPPA.

Mozilla's Lean Data Practices (LDPs) are our way of implementing data minimization. Our experience with these practices (and the LDP trainings we run) show that data minimization is possible for organizations of any size, and that rather than being a burden on business, data minimization increases consumer trust.

Far from becoming obsolete since the recent AI wave, data minimization is even more important as companies consider whether they are collecting highly personal data to fuel AI models.

For these reasons, the DPPA's minimization language is critical for creating a safer privacy experience. Weaker language, such as Connecticut's language linking minimization to *any* disclosed purpose, does little to protect consumers and makes a data minimization requirement nearly worthless. In fact, data handlers are *already* required by State and Federal consumer protection laws to limit their processing to disclosed purposes – to do otherwise would be deceptive.

---

[2] Deckelmann, Selena. "Latest Firefox rolls out Enhanced Tracking Protection 2.0." August 4, 2020. https://blog.mozilla.org/en/products/firefox/latest-firefox-rolls-out-enhanced-tracking-protection-2-0-blocking-redirect-trackers-by-default/

[3] Ritter, Tom. "Private by Design: How we built Firefox Sync." November 13, 2018. https://hacks.mozilla.org/2018/11/firefox-sync-privacy/

And, as history has shown us, companies have every incentive to game this framework and disclose broad processing purposes.

Connecticut's minimization provision therefore cements the status quo of dangerously broad data collection that leads to more severe data breaches, enables harms such as intimate partner violence, and steepens digital discrimination.

We urge you to reject Connecticut-style "minimization" in favor of meaningful safeguards for your constituents' data.

Definition of covered data. The modern online tracking ecosystem is built on troves of highly personal data. That data is often pseudonymized, which sounds like a privacy protective process. In reality, pseudonymised data can and does still enable invasive tracking of location and browsing, including re-identification. For example, tracking mechanisms such as Mobile Device Identifiers – a type of pseudonymized identifier – are a fundamental part of the advertising ecosystem today.

For that reason, the DPPA's definition of covered data is appropriately scoped to include data such as Mobile Device Identifiers. Attempts to narrow the set of covered data by excluding pseudonymised data from coverage would risk completely defanging privacy protections for residents of Maine.

Similarly, in order to be exempted from coverage by privacy legislation, data should be de-identified in a manner that makes it extremely difficult to link to an individual. De-identification is not magic: much of the technical and interaction data that Mozilla collects through telemetry to improve our products and services is not linkable to individuals. In fact, a significant portion of that data is collected only as aggregated statistics (and is therefore even less linkable to users). Other industry players are certainly capable of implementing similar safeguards for consumer data.

Finally, while data that is already covered by health or financial privacy laws should be excluded from coverage by a comprehensive privacy law in Maine, the entities themselves should not be wholesale excluded. For example, if a for-profit hospital is purchasing data for advertising purposes, it should still have to provide the basic data rights established in a comprehensive privacy law – because HIPAA does not cover this advertising data.

Language in the Connecticut Data Privacy Act exempts entire covered entities that are subject to HIPAA and GLBA, not just the data covered by those laws. This amounts to a vast carveout for these industries, and leaves unprotected the marketing data they are collecting.

Consent and universal opt-out signals. We are pleased to see that Maine's DPPA would require data controllers to respect browser-based universal opt-out signals for data collection. Multiple jurisdictions have now implemented laws that require data controllers to abide by these easy-to-implement technical signals, the most prominent of which is the Global Privacy Control (GPC).

This method of expressing consent preferences is gaining significant legislative and regulatory momentum because browser-based signals are much more consumer-friendly than a barrage of cookie banners or forcing consumers to opt out of sales one-by-one. One study, for example, found that 94% of respondents would turn on GPC if given the opportunity and 81% correctly understood what GPC does – and this latter number would likely only increase with higher adoption.

We have supported the inclusion of browser-based opt-outs in Federal Privacy legislation as well as in states such as California. Individuals using Firefox can already turn on GPC, and thousands of websites have the technical capacity to receive GPC signals. Global privacy signals should have simple requirements, similar to the California Privacy Rights Act's requirements, rather than confusing provisions such as that in Connecticut, where opt-out signals cannot "unfairly disadvantage" other controllers.

Furthermore, the DPPA uses an appropriately scoped definition of data transfers. Narrower definitions, such as those including only direct sales of data for monetary compensation, would exclude vast swaths of the privacy-violating ecosystem.

Finally, we suggest for your consideration a provision that would require browsers to implement browser-based opt-outs so that all people on the internet can take advantage of these easy-to-use mechanisms. (While we have integrated an opt-out preference signal into Firefox, other major browsers have not integrated this mechanism yet.) The board of California's Privacy Protection Agency recently proposed just such a requirement.

Prohibition on AI-based discrimination. Years of research (including by Mozilla and its fellows) and litigation by Federal agencies has shown that algorithmic discrimination is all-too-common across the digital ecosystem. Many State and Federal laws already prohibit discrimination on- and offline, so businesses should already be minimizing bias and discrimination in algorithms they develop and deploy. But having a clear Maine statute laying out anti-discrimination requirements would provide compliance clarity for businesses who are trying to understand their obligations in this critical area.

These anti-discrimination requirements are even more vital given the increased integration of AI in consumer tools. We encourage you to ensure that consumers are just as protected from discrimination by generative AI and other algorithmic systems (such as those that set prices for goods or determine access to commercial services) as they are from discrimination via any brick-and-mortar business practice.

Prohibitions on deceptive design (i.e., dark patterns). Lessons from privacy laws across the world show that unscrupulous or unwitting actors will use deceptive designs to nudge consumers to give up their privacy. For example, consent banners are often difficult to navigate, hiding or obscuring the option to reject tracking. In one recent study in the EU, hundreds of websites were found to be using deceptive design patterns in their data consent processes.

These deceptive practices defeat the entire purpose of establishing consent. Indeed, recent research[4] among Mozilla newsletter subscribers surveyed in 5 languages (N=14,096) found that fully 55% of those asked said that they did not understand when they had given consent for apps to share their data. Since the study was self-assessed, those respondents that said that they did understand when they gave consent may have had varying or mistaken views on what constituted their consent. Furthermore, because participants came from a pool of individuals who already subscribed to a privacy-related newsletter, this statistic may overestimate the understanding of consent by the general population.

In this survey, the vast majority of respondents said they wanted companies to: “Ask me before I’ve given the company any of my personal information;” “Ask me in clear,

[4] Internal qualitative study of Mozilla newsletter subscribers, June 13-21 2023.

easily understandable language;" and "Give me the chance to say "no" or opt out." (74%, 75%, 80%, respectively.)

In free-form fields, respondents suggested other things companies should make sure to do when they ask for consent: "Don't make saying 'no' so difficult." "They should make it clear what they are asking for and why." "Give me [a] choice to opt out of all options given…"

We therefore applaud the inclusion of prohibitions on deceptive design in the DPPA.

Sensitive data definitions. Similarly, given the opacity of the data ecosystem, the DPPA's robust list of sensitive types of data is vital to protecting consumers. Mozilla's experience fighting cross-site tracking, for example, shows just how important it is to ensure that browsing data over time is protected as sensitive.

Data security. At Mozilla, we're committed to securing user data against unauthorized access, and we have a robust security program – including bug bounties – that works to keep our community members safe. Because so many actors in the space are already following best security practices, it is even more important that the law sanctions bad or negligent actors when it comes to data security.

Please do not hesitate to contact us if you have any further questions.

Jennifer Taylor Hodges
Head of US Public Policy
jhodges@mozilla.com

Noam Kantor
Sr. Public Policy and Govt. Relations Analyst
nkantor@mozilla.com