WRITTEN TESTIMONY OF DAVID LEDUC

VICE PRESIDENT, PUBLIC POLICY

THE NETWORK ADVERTISING INITIATIVE

BEFORE THE WASHINGTON STATE LEGISLATURE

HOUSE CIVIL RIGHTS & JUDICIARY COMMITTEE

January 24, 2023

H.B. 1155

Washington My Health My Data Act

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
(The NAI)

I. Introduction & About the NAI

On behalf of the Network Advertising Initiative ("NAI"), thank you for the opportunity to provide feedback on H.B. 1155, the Washington My Health My Data Act. While the NAI shares the goals of H.B. 1155 to provide additional protections for sensitive consumer health data, as currently drafted the legislation is overly broad in several areas and would unnecessarily prevent beneficial uses of consumer data for marketing, advertising, and analytical purposes.

The NAI is the leading self-regulatory organization dedicated to responsible data collection and use by advertising technology companies engaged in digital advertising. For over 20 years, the NAI has promoted a robust digital advertising industry by maintaining and enforcing the highest voluntary standards for the responsible collection and use of consumer data for Tailored Advertising and Ad Delivery and Reporting. Our nearly 100 member companies range from large multinational corporations to small startups, and play an integral role in maintaining the free internet, driving economic growth, and encouraging competition in the marketplace.

NAI members's business models positively impact consumers by connecting them with content they find most relevant in a privacy-friendly manner. In the health-space, the NAI has promoted the highest voluntary industry standards around the use of sensitive health data. As a result, NAI members play an important role in educating consumers about various medications and treatments that may be relevant to them and providing them resources to actively participate in their own healthcare, all while promoting strong privacy practices.

In an effort to address potential harms and retain the availability of the positive use cases associated with geolocation information, the NAI developed a set of Voluntary Enhanced Standards for Precise Location Information Solution Providers ("Standards") in June 2022.[1] These Standards created restrictions on the use, sale, or transfer of location data correlating to Sensitive Points of Interest, including places tied to religious worship, sensitive healthcare services, military bases, and LGBTQ+ identity.[2] The Standards also created a set of restrictions on the use, sale, or transfer of Precise Location Information for law enforcement, national security, or bounty-hunting purposes, except as needed to comply with a valid legal obligation.[3] In addition, the NAI has also published imprecise location guidance for members, which encourages and provides meaningful parameters on how member companies could render Precise Location Information (PLI) imprecise.[4] We urge the legislature to consider the approach

---

[1] *See* Network Advertising Initiative, NAI Precise Location Information Solution Provider Voluntary Enhanced Standards (2022), https://thenai.org/wp-content/uploads/2022/06/Precise-Location-Information-Solution-ProviderVoluntary-Enhanced-Standards.pdf.

[2] *Id*.

[3] *Id*.

[4] *See* Network Advertising Initiative, Guidance for Members: Determining Whether Location is Imprecise (2020), https://thenai.org/wp-content/uploads/2021/07/nai_impreciselocation2-1.pdf.

provided by these Enhanced Standards and the NAI's various guidance documents for critical amendments to H.B. 1155.

The NAI shares the legislature's interest in protecting the most sensitive forms of consumer data, particularly in light of the *Dobbs v. Jackson Women's Health* decision and the implications associated with inappropriate use and disclosure of citizens' reproductive health data. However, the NAI is concerned with various provisions in the legislation as drafted. Below are our principal recommendations for the Subcommittee to address before advancing this legislation.

II. H.B. 1155's Definition of "Consumer Health Data" is Overly Broad, Prohibiting a Wide Range of Legitimate and Valuable Practices That Benefit Consumers; the Legislation Should be Amended to Align with Similar Definitions in Other Recently Enacted State Privacy Laws

The NAI strongly believes that sensitive health data should *never* be used as the basis for targeted advertising without a consumer's affirmative consent, informed by clear and conspicuous notice.[5] However, we also recognize that health advertising can be extremely valuable to consumers when authorized with their consent. When done in a privacy-protective manner, health advertising has the potential to make consumers aware of new treatments and can be crucial in helping to fill clinical trials, especially for rare conditions like those covered by the Orphan Drug Act.[6] Through our advocacy and compliance program efforts, the NAI has been able to successfully strike a balance between privacy protections while retaining the benefits of targeted advertising. This balance is reflected in the way a number of state privacy laws define and treat sensitive consumer health information.

As drafted, H.B. 1155's definition of "Consumer Health Data" is far broader than the approaches taken in the comprehensive privacy laws recently enacted across five U.S. states. By including not only all search data regarding health services and supplies, in addition to the use or purchase of medicine, bodily functions, vital signs or symptoms, but also "*[a]ny information* … that is derived or extrapolated from nonhealth information[,]"[7] H.B. 1155 extends beyond the scope of what is required for the meaningful regulation of sensitive health data. In fact, this ambiguous and exceedingly expansive definition of Consumer Health Data would prohibit virtually all health-related targeted advertising or analytics based on a*ny kind of information* – likely stripping consumers of the benefits associated with these practices and creating problematic outcomes for both consumers and businesses.

---

[5] *See* Network Advertising Initiative, 2020 NAI Code of Conduct (2020) § II.C, 1.e [hereinafter "NAI Code"], https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf.

[6] Orphan Drug Act, Pub. L. 97-414 (1983).

[7] H.B. 1155 § 3(7) (proposed).

In contrast, recently enacted U.S. state privacy laws take different and more practical approaches to protecting consumer health information. The NAI encourages you to consider aligning H.B. 1155 with these laws. For example, the Virginia Consumer Data Protection Act requires businesses to obtain opt-in consent before processing "personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status. . . [or] [p]recise geolocation data."[8] Differently, the Colorado Privacy Act defines sensitive data as "personal data revealing … a mental or physical health condition or diagnosis …"[9] and includes "sensitive data inferences" which explicitly provides that while geolocation on the whole is not always sensitive, "geolocation data which shows an individual visited a reproductive health clinic and is used to indicate an individual's health condition or sex life is considered Sensitive Data."[10]

Despite these differing definitions, the existing state laws provide a strong and tailored approach to protect the most vulnerable types of consumer health information, without completely eliminating positive data uses and legitimate business practices.

III. H.B. 1155's Prohibition on Geofencing is Overly Broad and Should be Amended to Prohibit Specific, Sensitive Use Cases

Despite the laudable goal of H.B. 1155 to protect the sensitive location data of Washington citizens, the current prohibition on implementing geofences around facilities that provide "in-person health care services" is overly broad and would make it unlawful to utilize a geofence around any facility that provides health care services, regardless of the downstream use-case or end-user of the practice.[11] This broad prohibition would apply to practices that are beneficial to these institutions and citizens, inadvertently disrupting important projects and initiatives that rely upon creating geofences around medical facilities. Further, we believe that the definition of in-person health care facilities is too broad, focusing on all medical facilities rather than those that are sensitive in nature, like reproductive clinics, mental health facilities, and others where citizens rightfully expect and deserve a higher level of privacy.[12] Finally, the bill's definition of "geofence" is ambiguous, leading to potential issues with understanding how far from a given location the prohibition would extend. We urge the legislature to address these concerns based on the following.[13]

---

[8] VA. Code Ann. § 59.1-575.

[9] Colo. Rev. Stat. § 6-1-1303(24)(a).

[10] Rule 2.02, 4 Colo. Code Regs. § 904-3 (proposed).

[11] H.B. 1155 § 10 (proposed).

[12] H.B. 1155 § 3(14) (proposed).

[13] H.B. 1155 § 3(13) (proposed).

Today, a variety of location data companies support both private businesses as well as municipalities in understanding foot traffic, supply chains, and commuting patterns in connection with the places of interest that make up the communities and neighborhoods we live in. This naturally includes hospitals and other medical facilities. As an example, most major infrastructure developments undergo years of pre-construction research where stakeholders leverage location data to ensure that a project is being built where it will best serve the interests of a given community. This is especially true for hospitals, as limited community resources require that these multi-billion dollar infrastructure projects are correctly placed in locations that will maximize their economic value and ensure social equity.

The NAI's Voluntary Enhanced Standards for the processing and sharing of precise location information associated with sensitive locations, including reproductive clinics and others where consumers expect and deserve heightened protections is an extremely valuable resource, and one we urge the legislature to consult in addressing concerns the breadth of the current geofencing prohibition.[14] Additionally, our imprecise location guidance offers helpful tools for defining "geofence" with greater precision, creating a more workable compliance obligation for covered businesses.[15]

The NAI therefore respectfully requests that H.B. 1155 be amended to prohibit specific use cases of citizens' precise location information around sensitive medical facilities, as well as prohibit voluntary sharing or selling precise location information for law enforcement or to infer an individual's pregnancy status. We also request the definition of geofence be clarified.

IV. H.B. 1155 Extends a Prohibition on Sales of All Covered Data; the Legislation Should be Amended to Allow for Sales of Most Health Data with Opt-In Consent from Consumers, Applying a Prohibition on Sales Only for the Most Highly Sensitive Health Data, Such as Reproductive Health Data

As drafted, H.B. 1155 allows for consumers to opt-in for the "collection" and "sharing,"[16] of Consumer Health Data, while flatly prohibiting its "sale."[17]As discussed above, the bill's current definition of Consumer Health Data is overly broad, prohibiting sales or sharing of virtually all health data where there is valuable consideration. While the NAI recognizes that certain highly sensitive subsets of Consumer Health Data should be prohibited from sale, such as reproductive health data, a prohibition on sales of Consumer Health Data more broadly as defined by H.B.

---

[14]*See* Network Advertising Initiative, NAI Precise Location Information Solution Provider Voluntary Enhanced Standards (2022), https://thenai.org/wp-content/uploads/2022/06/Precise-Location-Information-Solution-ProviderVoluntary-Enhanced-Standards.pdf.

[15] *See* Network Advertising Initiative, Guidance for Members: Determining Whether Location is Imprecise (2020), https://thenai.org/wp-content/uploads/2021/07/nai_impreciselocation2-1.pdf.

[16] H.B. 1155 § 5 (proposed)

[17] H.B. 1155 § 9 (proposed).

1155 would prevent valuable advertising and marketing uses of this data, resulting in the elimination of common and legitimate practices.

As previously noted in this testimony, when done properly and with the right protections in place, health-related targeted advertising is extremely beneficial and plays an important role in connecting consumers with medical treatments, medications, or information they genuinely need or want, as well as the provision of coupons and discounts for medications. Consequently, prohibiting the sale of Consumer Health Data outright – particularly when defined as broadly as it is in this bill – effectively deprives consumers of this opportunity. The NAI therefore proposes that H.B. 1155 be amended to provide consumers the ability to opt-in to the sale of Consumer Health Data in accordance with the strong requirements for providing notice and consent established in the legislation.

In addition, H.B. 1155's current consent requirements are ambiguous. As currently worded, it is unclear whether consent is required for sharing only when that sharing is "separate and distinct" from the purpose for which the consumer provided consent for its collection, or whether the requirement calls for this additional consent requirement to be "separate and distinct" from the initial consent for collection. This latter interpretation would be cumbersome and undesirable for consumers in many cases where a singular notice and consent interface could provide for collection and sharing practices that are consistent.

As currently drafted, Section 5 of the legislation requires similar consent requirements for both "collect" and "share"[18]. In both instances, consent must be obtained prior to the activity, and notice must disclose the categories of consumer health data involved, the purpose of the activity, the entities with whom it will be shared, and the means by which the consumer may withdraw consent.[19]

To avoid a consent process that is inefficient and undesirable for consumers, the NAI proposes that H.B. 1155 be amended to clarify that separate consent requirements could be provided within the same interface. Businesses and consumers alike would benefit from amendments to the bill to clarify in which cases a separate consent is required for sharing, and to provide for consolidated notice in consent in cases where the collection and sharing of the data are for similar purposes. Not only would this change streamline compliance for covered businesses, but it would also make the consumer experience easier to navigate and understand.

V. H.B. 1155 Provides for a Private Right of Action, Which Would Be Crippling to Businesses and the Court System Without Benefiting Consumers; H.B. 1155 Should be Amended to Provide Enforcement Vested Solely with the Attorney General

---

[18] Covered businesses are restricted from both collecting and sharing Consumer Health Data except with consent from the consumer, or to the extent necessary to provide a product or service. *See* H.B. 1155 § 5(1)-(2) (proposed).

[19] H.B. 1155 § 5(3) (proposed).

As presently drafted, H.B. 1155 enables private citizens to bring actions against covered entities for violations of the bill – an unprecedented approach as compared to other state or federal privacy laws. Including a private right of action in legislation such as this is likely to have a crippling impact on state courts and businesses alike.

Principally, a broad private right of action risks attracting frivolous lawsuits driven by opportunistic trial lawyers searching for technical violations rather than focusing on actual consumer harm or providing tangible privacy benefits for consumers. Further, even when companies are found to be in compliance, the litigation costs of numerous unfounded suits are crippling, particularly for small and medium-sized businesses. What is more, this approach is also likely to flood the state's courts, absorbing valuable state resources that could otherwise be used to advance consumer privacy efforts in other, more productive ways.

Consumer privacy laws are extremely nuanced, and implications often turn on the knowledge and interpretation of the regulatory body charged with enforcing them. As is reflected in the other state privacy regimes, the office of the state attorney general is the best and most practical location for consistent and meaningful enforcement to play out. While the California Privacy Protection Act does contain a private right of action, it is tailored narrowly to data security, an area where companies can more reasonably be held accountable than for minor violations that do not lead to consumer harms but could be subject to spurious private causes of action. Therefore, the NAI urges you to amend H.B. 1155 to provide for enforcement of violations exclusively by the Washington Attorney General.

VI. Conclusion

The NAI appreciates the opportunity to provide comments on this important legislation, and we would welcome the opportunity to provide further input and discuss specific amendment language to address the concerns highlighted. Thank you in advance for your attention to these recommendations, and please do not hesitate to contact me at david@thenai.org with any questions or to discuss.