January 30, 2024

House Committee on Judiciary
Room 0112, Colorado State Capitol
200 East Colfax Avenue
Denver, CO 80203-1784

RE: HB 1058 "Protect Privacy of Biological Data" (Oppose unless amended)

Dear Chair Weissman and Members of the House Committee on Judiciary:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 1058.

CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For over 50 years, CCIA has promoted open markets, open systems, and open networks. The Association supports the enactment of comprehensive federal privacy legislation in order to promote a trustworthy information ecosystem characterized by clear and consistent consumer privacy rights and responsibilities for organizations that collect data. A uniform federal approach to the protection of consumer privacy is necessary to ensure that businesses have regulatory certainty in meeting their compliance obligations and that consumers are able to understand and exercise their rights.

We appreciate, however, that in the absence of federal privacy protections, state lawmakers have a continued interest in enacting local legislation to guide businesses and protect consumers. As you know, Colorado is out in front of this effort as one of the growing number of states with a comprehensive consumer data privacy law. CCIA commends lawmakers in their thoughtful approach in enacting legislation that supports meaningful privacy protections while avoiding interference with the ability of businesses to meet their compliance obligations and the opportunity for consumers to benefit from the innovation that supports the modern economy.

CCIA strongly supports the protection of consumer data and understands that Colorado residents are rightfully concerned about the proper safeguarding of their biological and neural data. However, as currently written HB 1058 would encompass almost every wearable technology device, beyond those directly related to health applications, which could result in degraded consumer services and experience.

We appreciate the committee's consideration of our comments regarding several areas for potential improvement.

Align key definitions with privacy standards to promote regulatory interoperability and mitigate unnecessary compliance burdens.

By introducing a broad definition and compliance obligations relating to "biological data", which encompasses and includes a new definition for "neural data", HB 1058's scope extends

beyond the subject of “biometric” and “health” data as defined in other privacy laws, with multiple implications. To meet compliance requirements under a new privacy regime, businesses inevitably face logistical and financial challenges. Given the significant costs associated with developing privacy management systems, even minor statutory divergences between frameworks for definitions or the scope of compliance obligations, can create significant burdens for covered organizations.[1] HB 1058’s definition of “neural data” includes “information that concerns the activity of an individual’s central nervous system or peripheral nervous systems, including the brain and spinal cord, and that can be processed by or with the assistance of a device” and therefore would encompass “potential use” rather than “actual”. As such, this definition should be more narrowly tailored to avoid unnecessary regulatory burdens, which may deter business from researching and developing solutions in healthcare and other important sectors. And, by extension, HB 1058 might result in Coloradoans being denied innovative products in the marketplace.

Sufficient time is needed to allow covered entities to understand and comply with newly established requirements.

HB 1058 fails to provide covered entities with a sufficient onramp to achieve compliance. A successful privacy framework should ensure that businesses have an appropriate and reasonable opportunity to clarify the measures that need to be taken to fully comply with new requirements. As you know, Colorado’s recently enacted privacy law, along with those in California and Virginia included two-year delays in enforcement of those laws. CCIA therefore recommends amending the current effective date of 90 days following the adjournment of the Colorado General Assembly to a later date.

* * * * * *

We appreciate your consideration of these comments and stand ready to provide additional information as the legislature considers proposals related to technology policy.

Sincerely,

Khara Boender
State Policy Director
Computer & Communications Industry Association

[1] A study commissioned by the California Attorney General estimated that in-state companies faced $55 billion in initial compliance costs for meeting new privacy requirements, with small businesses facing disproportionately higher shares of costs. Berkeley Economic Advising and Research, LLC, “Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations,” (August, 2019), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.