June 16, 2023

Senator Spiros Mantzavinos
Chair, Senate Banking, Business, Insurance & Technology
spiros.mantzavinos@delaware.gov

Senator David P. Sokola
President Pro Tempore
david.sokola@delaware.gov

Senator Bryan Townshend
Senate Majority Leader
bryan.townshend@delaware.gov

Senator Gerald W. Hocker
Senate Minority Leader
gerald.hocker@delaware.gov

Senator S. Elizabeth Lockman
Senate Majority Whip
elizabeth.lockman@delaware.gov

Senator Brian Pettyjohn
Senate Minority Whip
brian.pettyjohn@delaware.gov

Legislative Hall
411 Legislative Ave.
Dover, DE 19901

Via email

CC: trey.paradee@delaware.gov; russell.huxtable@delaware.gov; sarah.mcbride@delaware.gov; nicole.poore@delaware.gov; john.walsh@delaware.gov

Re: Serious Concerns with HB 154

Chair Mantzavinos and Delaware Senate Leadership,

The Software & Information Industry Association (SIIA), the principal trade association for those in the business of information, writes to encourage you to align HB 154 more closely with consumer privacy best practices found in comparable state laws, as well as correct a likely drafting error that nevertheless implicates serious constitutional concerns within the bill's exemption for "publicly available information."

SIIA represents over 450 companies reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information; creators of software and platforms used by millions worldwide; and companies specializing in data analytics and information services. Our mission is to protect the three prongs of a healthy information environment essential to that business: creation, dissemination and productive use.

SIIA supports meaningful data privacy protections for consumers and the overall intentions of HB 154. We are concerned, however, that HB 154 contains several outlier definitions and substantive requirements while lacking key exemptions present in similar state privacy laws. These provisions would not only needlessly raise compliance costs for those entities serving residents of several states, but confuse Delaware consumers while creating their own impracticalities for businesses operating in the state. Furthermore, a technicality in the current language exempting "publicly available information"

renders the definition an unworkable—and likely unconstitutional—departure from nearly every comparable state privacy law.

I. HB 154 includes several outlier definitions that muddy its scope and additionally burden businesses while adding few corresponding protections for Delaware consumers.

The bill includes definitions that are at odds with similar state privacy laws. These novel definitions do not improve the consumer protections under HB 154 and, in fact, will undermine the objectives of HB 154 by increasing costs to businesses and consumers, creating confusion, and restricting socially beneficial practices.

First, the definition of "sensitive data" adds a variety of new categories that would prove operationally problematic. For example, including data revealing a person's "sex life," in addition to their sexual orientation, is both vague and unnecessary, and only renders compliance more difficult by blurring the line around where sensitive data starts and stops. Similarly, a person's "status as transgender or nonbinary" would unworkably force businesses to treat all categorically gender-related data as "sensitive." Even a woman routinely selecting "female" on a form speaks to the question of her nonbinary status, yet this selection would then qualify as "sensitive data."

Second, leaving out an exemption from the bill's definition of "sale" for disclosures to data processors, as exists in other state privacy laws, is also unnecessary to protect consumers. There is no need to limit the activities of processors via this definition, since HB 154 already restricts processors' handling of consumer data via contract. Including this language would only complicate the routine sharing of data between controllers and processors by actively treating this activity as a "sale" – yet HB 154 already deliberately regulates this type of transaction differently in § 12D-107. We recommend revising these definitions to align with best practices present in every similar state privacy law.

Finally, the bill contains various provisions that define requirements present in similar state privacy laws slightly differently, needlessly complicating compliance efforts across state lines with minimal consumer benefits. Like other states, for example, HB 154 provides additional protections for teens, yet defines this group as those between 13-18 years of age. Similar state privacy laws, including even California's, limit this definition to 13-16 years of age. In addition, the standard timeline for ceasing to process data when a consumer revokes consent is 45 days. A 45-day period enables controllers to better handle what are often multiple systems throughout the entity that may contain personal data. Reducing this to 15 days, as HB 154 proposes, would do very little to protect consumers and would likely force controllers to be less thorough, while also multiplying the difficulties associated with speedily implementing compliance protocols in the state.

II. The bill mandates controller responsibilities and consumer rights that create impracticalities for well-intentioned businesses, instead gifting malicious actors opportunities to manipulate these requirements in bad faith.

As currently drafted, HB 154 would require a controller that receives an opt-out request believed to be fraudulent to explain to a potential cybercriminal why this request raises red flags. This does little to help consumers acting in good faith, but actively aids bad actors by jeopardizing fraud detection methods. This is because these explanations naturally give fraudsters a roadmap for how to outflank institutional safeguards while making a subsequent request. For this reason, no other state inserted this language – it threatens crucial cybersecurity priorities.

The bill's requirement that a consumer may obtain "a copy of the consumer's personal data" should similarly be clarified to read "personal data provided by the consumer." Requiring controllers to respond to requests by porting data provided by a different consumer is not only often operationally impracticable; it would also lead to non-privacy protective outcomes that again reward bad actors. For example, an abusive spouse could harass their partner with access requests for that partner's personal data as long as this data is "reasonably linkable" to them—per the bill's definition of "personal data"—even if they did not provide this data. In fact, this technicality could even lead to intractable conflicts when a deletion request conflicts with a portability request as multiple consumers assert claims over the same pool of information.

The right to delete also lacks an important practical provision. As in the Connecticut, Montana, Tennessee, Virginia, and Texas laws, a controller must be able to comply with a consumer deletion request by "opting the consumer out of the processing of such personal data for any purpose except for those exempted pursuant to the provisions of this chapter."[1] This both protects consumers and enables businesses to comply with deletion requests. Otherwise, the data subject to the request can be repopulated by supplemental data received in the future. This is especially problematic if there is no evidence left of a deletion, thus controllers cannot prevent this data from repopulating. For this reason, consumer advocates inserted this language in Virginia as a necessary fix for this consumer right.

III. HB 154 lacks routine exemptions and would limit positive and uncontroversial uses of data, opening up Delaware businesses to liability for societally beneficial activity.

The bill's Gramm-Leach-Bliley Act (GLBA) exemption would exempt entities regulated by the GLBA rather than data regulated by the GLBA. This creates a potentially enormous problem because the GLBA provides the governance framework for data whether or not held by a GLBA-related entity such as a bank, insurer, or financial institution. We strongly believe the exemption should be clarified to cover all data regulated by the GLBA. Every state law passed to date has properly addressed and included an exemption covering GLBA-regulated data. Even the Federal Trade Commission (FTC) considers providers that are not financial institutions nevertheless subject to their regulation if they possess and process GLBA information.[2] Exempting data regulated by the GLBA would not merely create a loophole; it would ensure that federal regulations do not preempt Delaware's regulatory structure via two regulatory schemes governing how businesses process this specific subset of information.

Furthermore, no other state limits the ability of controllers to use data they have received from other sources, or their own data generated internally, to improve or repair products, effectuate a product recall, or repair technical errors. It is entirely possible that these functions might require using internal data the consumer did not provide. These legitimate uses should not be limited based on whether the data comes "directly from consumers," especially since the improvements will ultimately benefit these consumers – and regardless do not implicate a significant privacy interest.

Meanwhile, all other states recognize that a business should not be vicariously responsible for the activities of business partners who violate contracts without actual knowledge of such a violation. This

[1] Va. Code Ann. § 59.1-577(B) (2023).
[2] Lesley Fair, "4 Gramm-Leach-Bliley tips to take from FTC's TaxSlayer case," August 29, 2017, https://www.ftc.gov/business-guidance/blog/2017/08/4-gramm-leach-bliley-tips-take-ftcs-taxslayer-case.

bill would render business partners wholly responsible for the violations of others if the disclosing party ever violates HB 154, chilling such partnerships due to the unpredictable and asymmetric risk.

The language applying to deidentified and pseudonymous data is confusingly duplicative with existing requirements. HB 154 already requires that deidentified data cannot be reidentified, and that pseudonymous data does not enjoy the exclusion if it is reunited with data that would reidentify it. Including an assessment on top of this based on a hypothetical that the data may be reidentified is simply unnecessary, and creates excess documentation that runs counter to HB 154's goal to minimize data proliferation and protect consumers' privacy interests.

Finally, the waiver protection for attorney-client privilege or privileged work product should not depend on its being "conspicuously identified" during a DPA. This vague standard is not found in any other state's DPA requirements, and is at odds with the policy goal of eliminating the waiver of these protected data categories – which exists regardless of conspicuous headings.

IV. As written, the bill's exemption for publicly available information requires this data to be made available not only by government records but also the consumer. Requiring both for this data to be exempted is unworkable and likely unconstitutional.

HB 154's exemption for publicly available information currently reads:

> "'Publicly available information' means information that is lawfully made readily available to the general public through federal, state, or local government records or widely distributed media, *and* a controller has a reasonable basis to believe a consumer has lawfully made available to the general public" (emphasis added).

Due to the many state privacy laws that include similar language—except with an "or" in place of the "and," thus permitting either category to qualify as publicly available information—it is possible this is a scrivener's error. We strongly urge the Assembly to consider that it makes little sense to require information exempt from HB 154's consumer rights requests on the basis of public availability to be *both* a public government record and "lawfully made available" by the consumer. This would render public government records as well as information publicly released by consumers insufficient to enjoy the exemption if the other condition is not also met.

Such a dual requirement is neither logical nor workable, and would lead to absurd results. For example, this technicality could enable bad actors attempting to hide criminal records to veto their inclusion in databases and publications that government entities provide to businesses and non-profits, who in turn use them for legitimate purposes such as public safety, fraud detection, and public health. For this reason, the definition of "publicly available information" in almost every other state privacy law has permitted either government records *or* consumer release to qualify for the exemption.[3]

[3] In fact, the only legislation that includes the same language as HB 154 is the Connecticut Data Privacy Act (CTDPA). Yet this appears to be a similar mistake: this language is not only inconsistent with established public records policy, but Connecticut's own public records laws. For example, the Connecticut Freedom of Information Act (FOIA) guarantees access to most government records at the request of state residents. Conn. Gen. Stat. § 1-210(a) (2013). Yet this runs headfirst into the CTDPA's language, which would, like HB 154, give these same residents the right to request the deletion of information about them found in public government records if they were not also made available to the public by that consumer.

In fact, the only legislation that includes the same language as HB 154 is the Connecticut Data Privacy Act (CTDPA). Yet this appears to be a similar mistake: this language is not only inconsistent with established public records policy, but Connecticut's own public records laws. For example, the Connecticut Freedom of Information Act (FOIA) guarantees access to most government records at the request of state residents. Yet this runs headfirst into the CTDPA's language, which would, like HB 154, give these same residents the right to request the deletion of information about them found in public government records if they were not also made available to the public by that consumer.

Further, restricting either "information that is lawfully made readily available to the general public through federal, state, or local government records or widely distributed media" or information "a controller has a reasonable basis to believe a consumer has lawfully made available to the general public" would unconstitutionally restrict both categories of data. The Supreme Court has made clear that "the creation and dissemination of information is speech for First Amendment purposes."[4] The State may not infringe these rights to protect generalized interests such as consumer privacy.[5]

The constitutionally protected public domain consists not only of information released by the government, but also that which is widely available in private hands. Restrictions on the dissemination of publicly available information violate the First Amendment rights of both the businesses whose speech they burden and the users of the information who are entitled to receive it.[6] Yet HB 154 as written would restrict information in the public domain via government records based on whether it was made available by the consumer, and conversely restrict public data released by consumers that does not happen to exist within government records. This language would almost certainly fail to pass constitutional muster, and the associated challenges would needlessly frustrate the bill's intent.

* * *

Protection of privacy is a legitimate legislative priority, and SIIA supports efforts to provide meaningful protections for consumers while clarifying compliance requirements and protecting constitutionally guaranteed speech interests. We thank you very much for your consideration, and would be happy to discuss any of these issues further with you, if helpful.

Respectfully submitted,

Chris Mohr, President
Paul Lekas, Senior Vice President for Global Public Policy and Government Affairs
Anton van Seventer, Counsel for Privacy and Data Policy
Software & Information Industry Association

[4] *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011).
[5] See generally *E. Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 Stan. L. Rev. 1049, 1081 (2000).
[6] *See California v. LaRue*, 409 US 109, 133 (1972).