April 22, 2026

Chair Cyndie Romer
House Technology and Telecommunications Committee
Delaware General Assembly
411 Legislative Avenue
Dover, DE 19901

Re: *H.B. 380 (An Act to Amend Title 6 of the Delaware Code Relating to Personal Data Privacy) - SUPPORT*

Dear Chair Romer and Members of the Committee,

Consumer Reports[1] and the Electronic Privacy Information Center (EPIC)[2] write in support of H.B. 380 and sincerely thank you for your consideration of advancing consumer privacy in Delaware. H.B. 380 would build on the Delaware Personal Data Privacy Act (DPDPA) by extending to Delaware consumers important new protections, including expanding consumers' rights around the use of profiling, improving key terms like "sensitive data," expanding the law's coverage, and more. These important amendments largely reflect the last several years of work on privacy legislation across the states and would raise the baseline of protection for consumers and should be adopted. However, there are a few additional areas of Delaware's privacy law that should also be further amended to better protect consumers and their data.

We particularly appreciate that the bill includes the following elements:

- ***Expanded Definition of Sensitive Data.*** We support the expansion of the definition of sensitive data to include categories such as social security numbers, financial information, neural data, and health treatment or status. These updates pull categories that other states have included in their definition of sensitive data and are common-sense additions of personal data that necessitate heightened protections.

[1] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.
[2] The Electronic Privacy Information Center (EPIC) is an independent nonprofit research organization founded 30 years ago to protect privacy, freedom of expression, and democratic values in the information age.

- ***Lower Thresholds.*** H.B. 380 would lower the threshold for coverage so that the bill would apply to any businesses that control or process the personal information of 10,000 consumers; businesses that control or process the personal information of 5,000 consumers and that derive more than 20 percent of their revenue from the sale of personal data; or third parties that acquire personal data from a controller. This change will expand protections for consumers, ensuring that large national companies with a moderately sized footprint in Delaware will be required to abide by the law. We similarly support lowering the threshold for businesses required to conduct data protection assessments to those that process the personal data of 50,000 consumers.

- ***Narrowing of Entity-Level Exemptions.*** Delaware's privacy law currently exempts from coverage any financial institution or an affiliate of a financial institution, as defined in the Gramm-Leach-Bliley Act (GLBA). This carveout arguably makes it so that large tech companies (Apple, Amazon, Google, Facebook, and Microsoft) would be exempted from the entire law if one arm of their business receives enough financial information from banks, a line many of them are already currently skirting.[3] H.B. 380 would narrow this entity-level exemption somewhat by exempting specific types of businesses (e.g., banks, insurers, credit unions, etc.) rather than any financial institution or affiliate under GLBA. While we support any efforts to close potential loopholes, this exemption should be tightened further to instead exempt only the *information* that is collected pursuant to GLBA, applying its protections to all other personal data collected by such entities that is not currently protected by other laws.

- ***Protections for Personal Data Used in Profiling Rights.*** We commend the bill sponsor for focusing in H.B. 380 on protecting personal data used in profiling decisions. Profiling is often used in high-stakes contexts, including in determining people's access to housing, employment, health care, and other life necessities, so this particular use of data should have additional safeguards. We support the new definitions for "adverse action" and "report," the addition of a consumer right to know whether a controller is engaging in profiling, and the requirement that controllers conduct impact assessments if they engage in profiling. While we support the addition of consumer rights to be notified of an adverse action in a decision based on profiling, access the personal data used in that profiling decision, correct inaccuracies in their personal data, and request meaningful human review of the profiling decision, as drafted, H.B. 380 seems to provide consumers with more rights if a third party conducts the profiling than if a controller does. The bill should be amended to ensure that a consumer can exercise all these rights regardless of the entity engaging in the profiling.

- ***Right to Access Inferences.*** In our experience assisting consumers making privacy requests, many businesses do not respond to access requests by providing *all* of the personal information they've amassed about consumers, including inferences they have generated about consumers based on existing personal data. We appreciate that H.B. 380 would clearly require businesses to respond to any access request with any such inferences. This information can be highly material to a consumers' decision to interact with a business, as it can reveal whether they are being placed into sensitive marketing segments, such as "parents of preschoolers," "rural and

[3] See e.g., The Economist, "Big Tech Pushes Further into Finance," (Dec. 15, 2022), https://www.economist.com/business/2022/12/15/big-tech-pushes-further-into-finance

barley making it", "Christian church goers," or "wealthy and not healthy" (all of which are real marketing categories used by data brokers and others).[4]

- ***Right to Request List of Third-Party Recipients of Data.*** We appreciate that this proposal would allow consumers to request the list of third-parties to which their personal information has been sold or shared. This is a critical protection that provides much needed transparency into the otherwise opaque data sharing ecosystem. In addition, it allows consumers to trace the movement of their personal data and more meaningfully leverage their privacy rights in the event that they wish to access or delete personal information shared with third-parties.

At the same time, we urge the drafters to strengthen the bill by adding the following protections, which are necessary to provide Delaware consumers with the level of protection they deserve:

- ***Institute Meaningful Data Minimization Provisions.*** A strong privacy law should limit the data companies can collect and use to match what consumers expect based on the context of their interaction with the business. For example, a mobile flashlight application should not be permitted to collect a consumer's precise geolocation information because such information is not necessary to provide the service requested, and the collection of that data is unlikely to be in the consumer's interest.

  In contrast, the core of the framework currently found in the DPDPA is "notice-and-choice," which focuses on disclosures in privacy policies. The law allows businesses to continue collecting whatever personal data they want and using it for any reason they want as long as they disclose those practices in their privacy policies and allow consumers to opt out. However, very few consumers have the time to read privacy policies in practice, and would likely struggle to decipher their lengthy legalese even if they did. Moreover, the opt-out framework offloads all of the burden of consumer protection onto consumers themselves, while absolving companies of the responsibility to engage in responsible data collection. As the Connecticut Attorney General's Office has written[5]:

  > *Unfortunately, the CTDPA's current notice-and-consent model sets an exploitable standard— businesses can seek to justify unnecessary data collection by deeming such collection "adequate, relevant and reasonably necessary" to the purposes disclosed to consumers. This standard contravenes data minimization principles outright— it allows businesses to collect data they simply do not need so long as it is disclosed in privacy notices that are often bulky, confusing, or worse, misleading.*

  Rather than continue with this approach that harms consumers, H.B. 380 should implement a data minimization rule that businesses can only collect and use data when it is "reasonably necessary" to provide the services the consumer asks for. Unfortunately, the new data

---

[4] Federal Trade Commission, FTC Order Will Ban InMarket from Selling Precise Consumer Location Data, (January 18, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data

[5] Connecticut Office of the Attorney General, Updated Enforcement Report Pursuant to Connecitcut Consumer Data Privacy Act, (April 17, 2025), https://portal.ct.gov/-/media/ag/press_releases/2025/updated-enforcement-report-pursuant-to-connecticut-data-privacy-act-conn-gen-stat--42515-et-seq.pdf

minimization standard proposed in H.B. 380 is still ultimately pegged to "the purposes disclosed to the consumer." Company privacy policies often list open-ended and ambiguous processing purposes that allow them to essentially do whatever they want with consumer data, which means any limitation that is based on them will be illusory. We therefore propose the following redline:

> *(1) Limit the processing of personal data to what is reasonably necessary and proportional to provide or maintain the product or service requested by the consumer. ~~in relation to the purposes for which such data is processed, as disclosed to the consumer~~*

- ***Create Stronger Protections for Sensitive Data.*** The bill should ban the sale of sensitive data outright, as was done in the Maryland Online Data Privacy Act. As currently written, H.B. 380 would require companies to obtain consent before selling sensitive data, but this is already the case under the DPDPA. Under Section 12D-106(a)(4) of the DPDPA, controllers must obtain consent before processing sensitive data; the definition of "processing" encompasses "sales". H.B. 380 would go a step further by requiring this consent to be standalone, though that is unlikely to meaningfully address the inherent flaws in consent-based privacy laws, which are that consumers do not have the time to meaningfully assess hundreds of individual company privacy policies and are already bombarded with constant consent requests on every website. Adding an additional one is not going to move the needle.

  A prohibition on the sale of sensitive data would reduce the outward flow of data about our most personal characteristics, including our health, precise geolocation, race, religious beliefs, and data from children. This change would also shift the burden of privacy protection away from consumers and toward companies that otherwise have every incentive to exploit consumer data for their own benefit and profit. The less sensitive information companies collect and sell about us in the first place, the less that can be used against us or exposed in a data breach.

  If the idea of banning the sale of all sensitive data is further than the Legislature is willing to go, Delaware could instead follow in the footsteps of Oregon and Virginia, which have prohibited the sale of precise geolocation data. Connecticut is also currently considering this idea and the bill sits on the Senate floor. Ultimately, banning businesses from trafficking in our most sensitive personal information would be a significant step toward a more protective online world.

Thank you again for your consideration, and for your work on this legislation. We look forward to working with you to ensure that Delaware residents have the strongest possible privacy protections.

Sincerely,

Matt Schwartz
Senior Policy Analyst, Consumer Reports

Kara Williams
Counsel, EPIC