May 11, 2026

The Honorable Michael Marcotte
Chair, House Committee on Commerce and Economic Development
Vermont State House
115 State Street
Montpelier, VT 05633

Dear Chair Marcotte:

I write on behalf of the Software & Information Industry Association (SIIA) regarding S.71, the Vermont Data Privacy and Online Surveillance Act, currently before the House Committee on Commerce and Economic Development. SIIA is the principal trade association for companies in the business of information, including its aggregation, dissemination, and productive use. Our members include nearly 400 companies reflecting a diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used worldwide and companies specializing in data analytics, identity verification, fraud prevention, and information services.

SIIA supports comprehensive privacy legislation and appreciates Vermont's continued effort to provide meaningful protections for Vermont consumers. SIIA engaged on Vermont H.121 in the 2023-2024 session, and at that time we recognized constructive amendments that brought the definition of "publicly available information" closer in line with the First Amendment. We understand the Committee is now actively reviewing draft committee language with legislative counsel, and SIIA believes thatS.71, as passed by the Senate, reintroduces precisely the kinds of categorical carveouts from the definition of "publicly available information" that were identified as constitutionally problematic in the prior session. As detailed below, these provisions would burden lawfully obtained public information in ways that the First Amendment does not permit, and they would undermine the State's strong interest in identity verification, fraud prevention, and other risk-management services on which Vermonters and businesses operating in the state rely.

Proposed 9 V.S.A. § 2415(50)(B), as passed by the Senate, would carve five categories out of the definition of "publicly available information," each of which raises constitutional concerns:

- subdivision (ii): information collated and combined to create a consumer profile that is made available to a user of a publicly available website, whether in exchange for payment or free of charge;
- subdivision (iii): information made available for sale;
- subdivision (iv): inferences generated from the foregoing categories;
- subdivision (vi): inferences made exclusively from multiple independent sources of publicly available information that reveal sensitive data; and
- subdivision (vii): personal data created through the combination of personal data with publicly available information.

Each provision would treat lawfully obtained public information as regulated personal data — subject to deletion, opt-out, and other downstream obligations — based on what is done with the information rather than on whether it is, in fact, public. To the extent the Committee's working draft retains equivalent carveouts, these concerns set out below apply with equal force to those provisions.

As the Supreme Court articulated in *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570-71 (2011), and *Bartnicki v. Vopper*, 532 U.S. 514, 527, 534-35 (2001), the creation and dissemination of information constitutes speech for First Amendment purposes and any statute burdening that speech is subject to heightened judicial scrutiny. The State may not burden the dissemination of lawfully obtained public information based on a generalized privacy interest, particularly where the information is already in the public domain. Furthermore, public information does not lose constitutional protection because it is compiled into a profile, used to generate an inference, or offered for sale as part of an information product.

Businesses, courts, and public agencies rely on lawfully obtained public-record information and inferences drawn from public sources for identity verification, fraud prevention, investigative journalism, anti-money laundering and sanctions screening, due diligence, underwriting, lending, and consumer protection. Reclassifying those outputs as nonpublic data subject to deletion or opt-out rights would create ambiguity for regulated entities, undermine existing compliance programs, and invite litigation. It would also create a perverse result: bad actors could attempt to suppress or delete identity and risk indicators used to detect synthetic identities, fraud, and other unlawful activity.

Each of the carved-out categories presents serious constitutional flaws. Consumer profiles built from public information are routinely used in lawful and socially valuable contexts. Counsel preparing for litigation or representing a client in due diligence frequently uses public records products to identify a counterparty's residence, assets, prior litigation, and other information bearing on the merits of a claim or transaction. Once information is released by the State as a public record, the State cannot reclaim a privacy interest in it; the First Amendment prohibits the State from interfering with the downstream dissemination of that information as if it were private.

Public data also does not become private simply because it is combined with other data, or because an inference is drawn from it. Anyone who lawfully reviews property records, liens, bankruptcy filings, licensing records, claims history, or geographic data and draws a risk inference from those sources is engaging in analysis and speech that the First Amendment protects. Subdivision (vi) of § 2415(50)(B) is particularly difficult on this score: by its terms, it would treat as personal data any inference that "reveals sensitive data" even when drawn exclusively from multiple lawful, public sources. That is regulation of speech based on what the speech says about a person — exactly the kind of content-based burden on speech that triggers heightened scrutiny under *Sorrell*.

Subdivision (iii), which excludes information "made available for sale" from the protected category of publicly available information, fares no better. The First Amendment draws no distinction between information disseminated commercially and information disseminated without charge, as the sale of speech does not strip it of constitutional protection. Treating sale

as the operative trigger for deletion and opt-out obligations punishes speech because it is offered in commerce — a content and speaker-based distinction that the Supreme Court has repeatedly rejected.

Subdivision (vii), which would convert any combination of personal data with publicly available information into regulated personal data, has the further consequence of swallowing the rule. In ordinary practice, virtually every information product combines public and nonpublic elements. Read literally, subdivision (vii) would extinguish the publicly available information exclusion in nearly every commercial context in which it would meaningfully apply, leaving Vermont's definition narrower than that of every other state with a comprehensive privacy statute and importing significant constitutional risk in the process.

SIIA recognizes Vermont's well-intentioned goal to protect consumers from genuine privacy harms. But that interest must be balanced against constitutionally protected speech and against Vermont's strong interest in allowing lawful identity verification, fraud prevention, due diligence, and other risk-management services to function. Accordingly, SIIA respectfully urges the Committee to ensure that any final version of S.71 does not include the carveouts in proposed 9 V.S.A. § 2415(50)(B)(ii), (iii), (iv), (vi), and (vii), or any equivalent provisions in the Committee's working draft. Striking these subdivisions would leave intact the bill's narrower carveouts for nonconsensually collected biometric data, obscene visual depictions, genetic data, restricted audience information, and nonconsensual intimate images — categories that present distinct concerns and do not implicate the same constitutional issues.

We appreciate your consideration, and would welcome the opportunity to discuss this issue further with the Committee and with the Attorney General's Office, as well as to provide additional information on how lawful public records products are used by businesses, courts, and government agencies in Vermont and elsewhere for fraud prevention and other risk-management applications.

Sincerely,

Abigail Wilson
Director of State Policy
Software & Information Industry Association
awilson@siia.net
859.760.7648

cc/ members of House Committee on Commerce and Economic Development