Testimony of Jon Potter
Connected Commerce Council

Before the Vermont Senate Committee on Economic Development, Housing and General Affairs
Hearing on H.121, Regarding Data Privacy
April 10, 2024

Chair Ram-Hinsdale and Committee members:

Thank you for the opportunity to speak about H.121, relating to consumer privacy. I'm Jon Potter of the Connected Commerce Council.

In the years since our organization was founded, we have met with hundreds of small businesses and dozens of small business consultants regarding the challenges and opportunities presented by the transition from physical to digital commerce and marketing. The Council, known as 3C, is supported by Amazon and Google, but our mission is to support small businesses that work with all digital platforms and I'm not here today to advocate on anyone's behalf. I'm here to explain in great detail why the House bill's internal drafting conflicts will hurt small businesses if the Senate does not address them.

Today's top-performing local businesses simultaneously operate online and offline. Restaurants, service providers, manufacturers, and retailers combine physical locations, wholesale relationships, and online platforms to maximize reach, optimize marketing dollars, and lower costs and prices in an effort to win a little more business and provide a little more for their families, employees, and communities. I think your goals are to help Vermont small businesses succeed and also protect consumers from invasive data collection and misuse of sensitive information. This bill is very close to accomplishing both goals.

I could sing rhapsodic about the benefits of targeted ads compared to mass media ads, both for small businesses and the great majority of consumers who would rather see ads about things that interest them than about irrelevant products and services. But you already understand the delicate balance between commerce and privacy, and your bill is so close to hitting the mark. Unfortunately, when this balance is slightly off, as is the House-passed bill, the weight of the imbalance comes down hard on small businesses. I'll explain why.

H.121 carefully and appropriately defines data processing prohibitions and permissions associated with targeted advertising. Unfortunately, section 2419(a)(2) conflicts with and supersedes the targeted advertising provisions by limiting data processing to only what is necessary to provide a consumer's specifically requested product or service. As a result, H.121 will restrict data processing well beyond limiting abusive practices and will instead require business owners to process less data than what has historically been permissible and acceptable among traditional businesses. Here are some hypothetical examples:

- Example 1: In 1983, a Rutland High School teacher bought a holiday-themed bowtie at McNeil & Reedy, Rutland's third-generation men's clothing store. Three years later, he received a postcard when the store started selling holiday-themed socks. He had never provided a mailing address - because it wasn't necessary to accomplish the specific task of purchasing bowties - and never told the store that he liked or was interested in holiday-themed socks. But the salesperson knew him, looked up his address, and sent him a postcard because she was permitted to collect and process data beyond what was minimally required for a specific purchase. If today I purchase bowties online and H.121 is law, McNeil & Reedy will not be permitted to email me about holiday-themed socks or about an upcoming sale - because the data they collect could be processed only to deliver my bowties. Even if I browse every pair of holiday-themed socks on the website, the store would not be permitted to email me or advertise to me about the socks. Moreover, if I opt-in to receive notices of upcoming sales, the store could not process the fact that I bought bowties or digitally examined every pair of socks to personalize the marketing email they send me, even though a 1980s salesperson would know this information and could have called or sent me a personalized postcard.

- Example 2: In another perhaps inadvertent conflict, the bill's data advertising processing limitations have specific exceptions (at section 2415 (50)(B)(iv)) to enable website and advertising effectiveness measurement, but section 2419(a)(2) prohibits the processing of data for those same purposes because they are not the purpose requested by the consumer.

- Example 3: This same drafting conflict will prohibit a farmer from processing website data that would inform her that she should rent space at the weekend market 40 miles away because 300 people from that zip code have been on her website this month.

To be fair, the small business owner could potentially solve this drafting conflict by getting individual consent to collect and process every individual piece of data for every individual purpose imaginable. But that will lead us to the European experience where virtually every website you visit - if they comply with the law - presents a dozen or more permission requests for *standard uses of nonsensitive data*, frustrating consumers who then do one of two things - opt-in or opt-out of everything without reading further. That's a terrible result for small business owners and consumers. Instead, this Committee can ensure with a modest amendment - presented below - that the data processing limitation aligns with the balanced and carefully crafted targeted advertising rules and consumer expectations instead of superseding them. You can let small businesses process the data for the very purposes that you have explicitly permitted.

Private Right of Action: Thank you for modifying the Private Right of Action in the latest draft bill. Our preference would be to eliminate the PRA. However, if the Committee chooses to narrow the PRA to apply only to data brokers, then it seems the most recent draft needs a bit more work to reflect your intent.

Our concern is that the definition of “sale of personal data,” for purposes of plaintiffs’ lawyers aggressive litigation, will be contorted in ways you do not intend that will open the PRA much more broadly. For example, it is absurd, but history tells us it is likely, that a lawyer would argue that an exchange or sharing of personal data occurs when a small business website works with optimization services to present consumers with individualized shopping experiences, e.g., that reflect previous purchases. These behind-the-scenes optimizations are not “data brokering” or “data selling” in the manner you may wish to scrutinize, but rather are the types of marketing we discussed that works well for consumers and small businesses. Sincet the definition includes this optimization activity within “data sharing” and “data exchanges” that have commercial value, the activity falls within the PRA as data sales and could subject every small business with a website to the litigation you intend to prevent.

The solution for this is in the amendment below, which simply removes “other commercial purpose” from the definition of sale as applied to the PRA. That term - “other commercial purpose” - is in the definition of “sale” for other reasons, but when applied to the PRA makes it overbroad and overrides your intent to narrow the PRA to data brokers and data sellers.

Data Protection Assessments: Data protection assessments are a new concept that will inevitably require expensive lawyers and consultants. The requirement that small businesses produce “data protection assessments” for every data processing activity “that creates a heightened risk of harm” will crush small businesses.

- “Heightened risk” processing includes ***all data related to targeted advertising*** and “sensitive data,” including data identifying a consumer’s race, religion, or health.
- With regard to targeted advertising, imposing the data protection assessment on small businesses is a backdoor way to raise the costs of advertising so high that small businesses simply stop doing the very advertising that this bill otherwise permits. Once again, this bill gives with one hand and takes away with another. I hope that is not the bill’s intent.
- With regard to the sensitivity of health data, small businesses will fear—and be sued—because a purchase of makeup or hair products could identify race, a purchase of religious products could identify religion, and a purchase of Tylenol could be considered health data or reveal health status. Failing to produce data protection assessments for processing these data points should not be the goal of this bill.

More broadly, there is simply no reason to ask law-abiding small businesses to hire lawyers or consultants to provide the government with detailed assessments of how they use basic non-sensitive consumer data to operate and grow. Perhaps this requirement could start with the largest companies, and then in several years the legislature could decide if assessments have value and their cost is reasonable when undertaken by small businesses.

Small Business Exemption: A month ago, I brought the owner of a 3-person business to Albany to meet with the sponsor of the NY Privacy Act, a similar proposal to H.121. The website of that business, which has received no outside investment and is working very hard to grow, gets 300,000 hits annually. H.121 would exempt only small businesses with fewer than 25,000

records, though it is clear that this will subject hundreds or thousands of small businesses to extraordinary compliance obligations.

Aligning the small business exemption with a novel percentage of Vermont's population suggests that Vermont businesses deal only with Vermont consumers. But the legislature's economic goal, and the success of so many small businesses, is based on attracting out-of-state consumers, tourists, and other money-spenders into Vermont. Why would the legislature hobble "made in Vermont" businesses by imposing challenging, expensive compliance costs on those who successfully reach non-Vermont consumers? In contrast, the goals of this bill must align with broader goals of empowering Vermont small businesses to effectively attract out-of-state consumers, and not punish those that do this successfully.

We suggest aligning the small business exemption with the small business definition in other sections of Vermont law. If a small business is eligible for a loan or grant from the Department of Economic Development, then it should be a small business under this law also and exempt from burdensome regulations.

In closing, I thank the Committee for your extraordinary attentiveness to Vermont small business owners who previously were not invited to participate in this bill's development. Please let me know if I can be of any assistance to you in the future. Attached are our suggested amendments to the bill.

Connected Commerce Council

Small Business Amendments to Vermont Privacy Bill (H.121)

1. <u>Amend data minimization limitation provision</u>

§ 2419. DUTIES OF CONTROLLERS (a) A controller shall:

(1) specify in the privacy notice described in subsection (d) of this section the express purposes for which the controller is collecting and processing personal data;

(2) process personal data only:

(A) as reasonably necessary and proportionate to ~~provide the services~~ **achieve the disclosed purpose** for which the personal data was collected, consistent with the reasonable expectations of the consumer whose personal data is being processed;

(B) for another disclosed purpose that is compatible with the context in which personal data was collected; or

(C) for a further disclosed purpose if the controller obtains the consumer's consent;

2. <u>Amend data protection assessment provision</u>

§ 2423. DATA PROTECTION ASSESSMENTS FOR PROCESSING ACTIVITIES THAT PRESENT A HEIGHTENED RISK OF HARM TO A CONSUMER (a) A controller **with annual gross revenue in excess of $250 million** shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer, which, for the purposes of this section, includes:

(1) the processing of personal data for the purposes of targeted advertising; (2) the sale of personal data;

(3) the processing of personal data for the purposes of profiling, where the profiling presents a reasonably foreseeable risk of:

(A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

(B) financial, physical, or reputational injury to consumers;

(C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where the intrusion would be offensive to a reasonable person; or

(D) other substantial injury to consumers; and

(4) the processing of sensitive data.

<u>3. Amend Private Right of Action</u>

§ 2427(a)(3) The private right of action available under this subsection shall only be available for an action brought against a person that during the preceding calendar year derived more than 50 percent of the person's gross revenue from the sale of personal data, except that for purposes of this § 2427(a)(3) the exchange of personal data for other commercial purposes as defined by § 2415(48) shall not be considered a sale.