Thomas Weiss
P. O. Box 512
Montpelier, Vermont 05601
January 27, 2026

House Committee on Commerce and Economic Development
Sate House
Montpelier, Vermont

Subject: H.211, data brokers and personal information.

Dear Committee:

These comments are based on draft 1.2 of 1/14/2026.

Background. It is a while since I have testified on data brokers and data privacy. I testified in support of the original data broker bill which became Act 171 of 2018. I see H.211 as advancing the ability of Vermonters to control the uses and distribution of their personal data and as addressing some of the deficiencies that had not been addressed by the original data broker act.

One of my concerns then, and still is, that data elements, as I call them, might be protected in one subchapter and not in another. I figure if a data element is worth protecting in one subchapter, it is worth protecting on all the subchapters. The legislature made significant strides in this regard over the years. H.211 proposes succeeding the long list of data elements for brokered personal information with a description of the characteristics of brokered personal information. This we do not have to keep adjusting the list as technology changes. I think this will be a benefit.

The first data broker registry was dismaying and proved points made during the testimony on Act 171. There were so many data brokers that it would take an inordinate amount of time for me or any individual to keep track of them and figure out which allowed opt outs and the conditions the data broker imposed in order to opt out. Then we have heard here this year that data brokers change identities, so that even keeping track of them is difficult. We opt out from one data broker. It changes itself into another business and we have to start over, I guess. I appreciate the addition of the Accessible Deletion Mechanism to make it easier to give consumers more control over the use of their data.

The introduction of a second section on notices of data breaches can cause some confusion. The original (sec. 2435) is for data collectors and covers personally identifiable information and login credentials.. The other (sec. 2436) is for data brokers and covers brokered personal Information. We need to remember that a data broker also meets the definition of a data collector. When a data broker has a data breach that involves both personally identifiable information and brokered personal information, does the data broker have to follow both sets of notice requirements? I believe that all the listed elements of personally identifiable information (data collectors) meet the definition of brokered personal data (data brokers). My comments recommend a way to make it clear that all the elements of personally identifiable information also meet the proposed revision to the definition of brokered personal information, so a data broker need follow only the notice provisions for a data broker security breach.

The definition of a direct relationship has some potential ambiguities that I ask you to consider and resolve. I do make some recommendations. One example is the recordings of this committee that are posted on YouTube. The only way I can see them, I believe, is to go to the YouTube site. Does that mean that I have a direct relationship with YouTube even though I never post anything on YouTube? I think it should not, making any data that YouTube collects on me brokered personal information.

One of my concerns with the original data broker act and subsequent bills is that definitions are not uniform throughout chapter 62. I notice that there are some definitions in subchapter 6 that are duplicated in H.211's subchapter 1. Definitions in subchapter 6 apply only to subchapter 6. The definitions in subchapter 1 apply to all of chapter 62. I suggest that the definitions subchapter 6 that are the same as proposed in subchapter 1 be removed from subchapter 6. Also some definitions in subhapter 6 would be better if applied to all of chapter 62. I suggest they be moved into section 2430.

I appreciate that H.211 proposes that data brokers register within 30 days of collecting data on Vermonters. That is superior to allowing them to operate a full year before registering. I think they ought to register before they start collecting data on Vermonters. Most professionals, including professional engineers, must register before beginning practice in Vermont. Thirty days is better than 365 and not as good as zero days until being required to register.

I have reviewed the amendments that I had proposed in 2018 when the original data broker bill was being created. Many have been addressed, either in Act 171, subsequent bills, and now in H.211. Unfortunately some of the most significant have not been addressed.
- The crime of data trafficking was not created. It would be for information too sensitive to be sold or transferred; information that should only be obtained directly from a consumer.
- There is no prohibition on the re-purposing of data from the purpose for which it was originally collected.
- There are still too many paths for consumers never to be notified of data breaches and the delay between breach and notification is too long in too many paths.

The enclosure provides specific recommendations that I believe will improve H.211 by strengthening Vermonters' control over the use and distribution of their personal data.

I ask that you find that the recommendations have merit, and that you incorporate them into H.211.

Sincerely,
Thomas Weiss, P. E.

Enclosure:

Recommendations on H.211 data brokers and personal information
Presented to House Commerce and Economic Development
Thomas Weiss
January 27, 2026

These comments follow the order of the bill.

Section 2449a, definitions.
There are a number of definitions in section 2449a that apply to the same term as definitions in section 2430. Section 2430 applies to all of chapter 62. There is no need to repeat the definition in subchapter 6. These duplicated definitions in 2449a are for: biometric data, identified or identifiable individual; the combination of process and processor; and publicly available information. If I missed any, add them to this list.

There are other definitions in section 2449a that define terms used in other parts of chapter 62. These are for: affiliate, collect, consumer (9)(B), genetic data; and third party. If I missed any, add them to this list. It would be useful to have these definitions apply to all of chapter 62.

Recommendations:
- Remove all the duplicate definitions from subchapter 6, section 2449a, retaining them in section 2430.
- Move the definitions of terms also used outside subchapter 6 into section 2430.

Page 3, lines 12 through 16. Sec. 2430 (3)(A). Definition of brokered personal information. It is likely that the definition of brokered personal information contains all the data elements of personally identifiable information. Adding this to the definition will help when it comes to the two sections, 2435 and 2436, on security breach notices.

Recommendation: Add the following sentence at the end of line 16.
"Brokered personal information includes all elements of personally identifiable information."

Pages 4 line 20 through page 5 line 10. Sec. 2430 (6)(B). Definition of a direct relationship between a consumer and a business.

A part of the definition is that a direct relationship is formed when a consumer is "obtaining information about the business's products or services." Obtaining information should not create a direct relationship. When obtaining information, the consumer does not intend to form a relationship with the business. The consumer is merely trying to decide whether to form a relationship with any business, and if so, which one best suits the consumers needs. An example is an individual looking at the inventory on an auto dealer's internet site or an individual browsing in a store. Neither should be considered to have formed a direct relationship.

Is a direct relationship with Google formed when a consumer with a non-gmail address gets an e-mail from an individual with a gmail address? The individual with the gmail address has a direct relationship. The recipient does not. Or does that make a direct relationship with the recipient?

Conversely, is a direct relationship formed when a consumer with a non-gmail address replies to an individual with a gmail address?

Is a direct relationship with YouTube formed when a consumer views a video of a legislative committee, which is the only way to view a video?

I hope the answer to all three is "no" and that the bill be modified to state that directly. The legislature has the direct relationship and the consumer has no option as far as I know of viewing the video some other way.

Recommendation: Amend these lines as follow.

As used in this subdivision (6), "direct relationship" means that a consumer has intentionally interacted with a business for the purpose of accessing, purchasing, using, or requesting, ~~or obtaining information about~~ the business's products or services. A consumer does not have a direct relationship with a business if the consumer is interacting with another consumer who has a direct relationship with the business. A consumer does not have a direct relationship with a business if the purpose of the consumer's engagement is to exercise a consumer right or for the business to verify the consumer's identity. A business does not have a direct relationship with a consumer simply because the business collects brokered personal information directly from the consumer; the consumer must intend to interact with the business. A business is still a data broker and does not have a direct relationship with a consumer as to the brokered personal information the business sells about the consumer that it collected outside of a first-party interaction with the consumer.

Page 10, lines 16 and 17. Sec. 2430 (16)(B)(i). definition of what is not publicly available information. It should not matter whether the biometric data are collected with or without the consumer's knowledge. Biometric data are sensitive enough that they actually should be covered by a data trafficking statute.

Recommendation: Change (16)(B)(i) to
(i) biometric data ~~collected by a business about a consumer without the consumer's knowledge;~~

Page 11, lines 13 and 14. Sec. 2430(16)(B)(ix) intimate images excluded from publicly available information. How does the data broker know it is nonconsensual? It would be better to err on the side of privacy by requiring intimate images to be public only if known by the data broker to be consensual and that consent includes wider dissemination..

Recommendation: Change the exclusion to:

(ix) intimate images, authentic or computer-generated, unless known to be ~~nonconsensual~~ consensual and that the consent includes wider distribution.

Page 12, lines 4 through 20. Sec 2430(17). Definition of sale.
(i) Disclosure to a processor. The disclosure agreement must have a condition that the processor may not disclose, sell, transfer that brokered personal information to any other entity. And the processor must destroy all disclosed brokered personal information at the earlier of the data no longer being used, the contract expires, or the processor goes out of business, merges, is sold.

(ii) Disclosure to a third party to provide something requested by a customer. This is confusing. If requested by a consumer, the entity providing the service is not a data broker, at least in terms of that transaction. This seems to have no reason for being here.

(iv) Disclosure with the consumer's consent. The use of data broker here is confusing. How can a consumer direct a data broker to release information? Doesn't that create a direct relationship, so no longer a data broker?

(iii) and (vi) Disclosure to an affiliate and disclosure as an asset. These seem to be a direct contradiction of the definition of sale. We have heard testimony that some data brokers change identity often and are difficult to trace. They are probably transferring the data from the outgoing data broker to the incoming data broker. The identity changes might be to an affiliate or through a merger or acquisition.

This as many of my other comments is intended to be all inclusive with no loopholes.

Recommendation: Amend the definition of sale.

(B) "Sale" does not include:

(i) the disclosure of brokered personal information to a processor that processes the brokered personal information on behalf of the data broker; only if the processor is prohibited from disclosing, selling, or transferring the brokered personal information to any other entity and the processor is required to destroy all disclosed brokered personal information at the earlier of the data no longer being used, the processing arrangement expires, or the process goes out of business, merges, or is sold..

~~(ii) the disclosure of brokered personal information to a third party for purposes of providing a product or service requested by the consumer;~~

~~(iii) the disclosure or transfer of brokered personal information to an affiliate of the data broker;~~

~~(iv) the disclosure, with the consumer's consent, of brokered personal information where the consumer directs the data broker to disclose the brokered personal information or intentionally uses the data broker to interact with a third party;~~

(v) the disclosure of publicly available information;

~~(vi) the disclosure or transfer of brokered personal information to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction, or a proposed merger, acquisition, bankruptcy, or other transaction, in which the third party assumes control of all or part of the data broker's assets.~~

Page 15 lines 12 through 20. Sec. 2436(b) Notice of data broker security breach

A data broker is also a data collector. Thus in the event of a data broker security breach, the data broker is also subject to the notice requirements that apply to data collectors when the data breach contains elements of personally identifiable information or login credentials. Stating in the definition of brokered personal information that all elements of personally identifiable information are part of brokered personal information reduces confusion over whether to use section 2435 or 2436.

Recommendations:

- This is resolved by the previous recommendation to clarify that all elements of personally identifiable information are included in the definition of brokered personal information.
- Apply recommendations to sec. 2436 to the corresponding provisions of sec. 2435.

Page 18 lines 13 and 14. Sec. 2436(b)(4)(D) notice to consumer

The notice requires a telephone number that the consumer may call for further information, We heard at an earlier hearing someone who raised the question of overseas data brokers.

Recommendation: Consider requiring that it be a toll-free number.

Page 18 line 18 through page 19 line 15. Sec. 2436(b)(5) forms of notice to consumers.

Some of the conversion of section 2435 into 2436 left a few odd situations.

One of them is that a consumer has no idea who the data broker is that is providing notice. It'll be some company calling or e-mailing out of the blue. The consumer likely will think it a scam and ignore it. Thus, require all notices to consumers to be direct notices in writing and delivered by certified mail. And prohibit telephonic or electronic notice unless there is some mechanism by which the consumer can be assured that the notice is legitimate and not a scam.

(B)(i) How can a data broker have a primary method of communication with a consumer? If there is a primary method of communication, that likely makes it a data collector, not a data broker.

(D) I do not think that Vermont has had a newspaper of statewide circulation in decades. Maybe Vermont has never had a newspaper of statewide circulation.

Recommendation: Amend (5) as follows.

(5) A data broker may provide notice of a security breach involving brokered personal information to a consumer only by ~~two or more of the following methods:~~
~~(A)~~ written notice ~~mailed~~ by certified mail to the consumer's residence; and
~~(B) electronic notice, for those consumers for whom the data broker has a valid email address, if:~~
~~(i) the data broker's primary method of communication with the consumer is by electronic means, the electronic notice does not request or contain a hypertext link to a request that the consumer provide personal information, and the electronic notice conspicuously warns consumers not to provide personal information in response to electronic communications regarding security breaches; or~~
~~(ii) the notice is consistent with the provisions regarding electronic records and signatures for notices in 15 U.S.C. § 7001;~~
~~(C) telephonic notice, provided that telephonic contact is made directly with each affected consumer and not through a prerecorded message; or~~
~~(D)~~ notice by publication in ~~a newspaper~~ newspaper of general ~~of statewide~~ circulation covering the entire state from the Secretary of State's list ~~in the event the data broker cannot effectuate notice by any other means~~.

Page 21 lines 15 through 19. Sec. 2446(a). Data Brokers Annual Registration

Thank you for reducing the time that a functioning data broker has before registering. Waiting a full year was too long. Professionals must register in Vermont before practicing here.

Recommendation: Retain the shorter period before first registration. Better yet, require that data brokers must register before collecting data on residents.

Page 22 lines 6 through 18. Sec. 2446 (a)(3). Registration requirements.

Recommendations: Require the registration to include the corporate structure of the previous five years. This will help track those that change often.

Page 23, line 12. Sec. 2446(a)(3)(E)(i)(III). Whether the data broker collects biometric data

Actually this relates to sec. 2443 (1)(B)(iii).

Recommendation: Change "biometric information" to "biometric data" in sec. 2443 change "biometric information" to "biometric data" in sec. 2443 (1)(B)(iii)..

Page 24, lines 12 through 21. Sec. 2446(a)(3)(E) Data broker registration requirements.

(E)(ii)(IV) Information on sharing or selling to law enforcement should be listed in all events, in the interest of transparency.

Recommendations: I almost always use "data" as a plural noun. I acknowledge that many individuals use "data" as a singular noun.
- E(ii)(IV) Change to: "(IV) to law enforcement, ~~unless~~ even though the data ~~was~~ were shared pursuant to 12 a subpoena or other court order; or"

Page 28 lines 10 through 20. Sec. 2446a(a). Accessible deletion mechanism
(a)(2) and (a)(5) seem to be the same.

Recommendation: If (a)(2) and (a)(5) are the same, delete one of them. If they are different expand one or both to clarify the difference.

Page 34 lines 5 through 10. Sec. 2446c Credentialing.
Thank you for adding more information on credentialing.

Recommendation: Add to (b) and (c) that the prospective user is registered as a data broker with the Secretary of State. The prospective user shall so certify in (b) and the selling data broker shall confirm in (c).

Issues that still need to be resolved.
I have reviewed the amendments that I had proposed in 2018 when the original data broker bill was being created. Many have been addressed, either in Act 171, subsequent bills, and now in H.211. Unfortunately some of the most significant have not been addressed.

The crime of data trafficking was not created. It would be for information too sensitive to be sold or transferred; information that should only be obtained directly from a consumer. H.764 is the bill that developed into Act 171. It contained a proposed section 2433 that began to address this issue.

There is no prohibition on the re-purposing of data from the purpose for which it was originally collected. This issue relates more to data collectors than to data brokers.

There are still too many paths for consumers never to be notified of data breaches. The delay between breach and notification is too long in too many paths. There are ten paths in section 2435 that control whether consumers receive notice of security breaches. Five paths result in no notice to consumers at all. Only two paths result in direct notice to consumers. Three paths result in indirect notice, meaning that consumers must search to find out what might have been breached and whether the might have affected them.

The proposed section 2436 has the same problem. It has six paths that control whether consumers receive notice of security breaches. Two paths result in no notice to consumers at all. Two result in indirect notice. And two result in direct notice.

Recommendation: Consider amending H.211 to address these three issues.