P. O. Box 512
Montpelier, Vermont
April 10, 2019

House Committee on Commerce and Economic Development
State House
Montpelier

Subject: S.100, data privacy and consumer protection

Dear Committee:

Good morning, I am Thomas Weiss, a resident of Montpelier who meets the definition of a consumer. I am testifying on S-110, data privacy and consumer protection. I think that protection of a consumer's information is important, and I thank you for allowing me to present my thoughts on this subject. These comments are from my point of view as a consumer. I bring my experience as a civil engineer to this testimony. As a civil engineer, I have had to read and to know and to understand laws, regulations, and contracts my entire career in order to do the engineering that I do. I use that background to help me figure out and understand what this bill does and does not do. I find this bill and the underlying statutes to be confusing. I find that the bill and the underlying statutes could do more to protect consumers.

My testimony today will cover sections 2 and 4 of the bill, (adding data elements to the category of personally identifiable information; and increasing the amount of direct notice to consumers in the event of a data breach).

Adding data elements to the definition of personally identifiable information (section 2 of the bill)

I'll cover three topics in section 2.

First, I ask that you expand the definition of of "data collector" to make it clear that the other handlers of data covered in chapter 62 on protection of personal information are also data collectors.

Second, I ask that you review the definition of a student's "covered information".

Third, I support the expansion of the definition of personally identifiable information to include the five data elements on page 3 of the bill as passed by the Senate.

Expand the definition of "data collector"

I believe that the existing chapter 62 is confusing because it focuses on the categories of handlers rather than on data elements. I think that a data element should be treated the same, no matter the category of the handler. This bill gives you an opportunity to reduce some of that confusion.

I suggest that you add a sentence amending the definition of a "data collector". The sentence would be something like "The definition of a data collector includes the other entities included in this chapter that handle other sets of data described in this chapter to the extent that they handle information included in the definition of personally identifiable information." I request the amendment because only data collectors are required to report a data breach. This amendment will make it clear that when other entities in the chapter handle data elements that are personally identifiable information they are also data collectors and bound by those requirements, too.

I think it is important to understand the scope of chapter 62; of how this bill fits into that chapter. So I'm going summarize the various categories of information contained in the chapter. Exhibit 1 indicates the data elements in each category of information and the name given to the entities that handle those categories of information.

Personally Identifiable Information is handled by data collectors. Loss of control of personally identifiable information is a security breach and must be reported to the offices of the Attorney General and of the Department of Financial Regulation. The people whose information has been breached might receive a direct notice, might have to learn about a breach through some kind of substitute notice requiring them to take steps to learn if their data have been breached., or might be prohibited from ever learning about a security breach. (I have summarized the notice requirements in Exhibit 2, which I'll come back to later.)

Brokered Personal Information is handled by data brokers, which are entities that collect, sell, or license this information about consumers with whom it has no direct relationship. Loss of control of brokered personal information by a data broker is not a data breach and is not required to be reported to anyone.

Personal information is handled by destroyers of records. Loss of control of personal information by a destroyer of records is not a data breach and is not required to be reported to anyone.

Social security numbers and limitations on their use by businesses are covered in the subchapter on the social security number protection act. The subchapter also places redaction requirements on town clerks and clerks of court for certain other information listed in the subchapter and on exhibit 1. The clerks are not required to redact those categories of information from documents placed on the internet unless there is a specific written request for each document to redact information.

Covered information is certain student information handled by operators. This bill proposes this new definition, which is not covered in exhibit 1.

Part of my confusion with the statute is that the responsibilities regarding protection of certain data elements depend on which of the four entities is handling the data. Let's look at a driver's license number. It is included in all four categories of information. If a data broker or a destroyer of records loses control of driver's license numbers, is that reportable? If a town or court clerk fails to redact driver's license numbers, is that reportable?

Only a data collector is required to report the loss of control over a driver's license number to the Attorney General or the Commissioner of Financial Resources or consumers. A data broker, a destroyer of records, or a town or court clerk has no responsibility to report a data breach as one of those three types of entities. That is why I request that the definition of "data collector" be expanded to make sure that it covers these other types of data handlers when they lose control of data elements included in the definition of personally identifiable information..

Review the definition of a student's "covered information"

The definition of covered information includes "personal information". Now §2445 already defines "personal information" in relation to destruction of records. That definition is limited to that section. However, it is potentially confusing to have an undefined "personal information" in §2443 and a defined version in §2445 applicable only to §2445. I ask that you consider changing the phrase "personal information" in either §2445 or §2443. Because §2443 will be new, it seems the likelier place to make the change.

Support for adding data elements to personally identifiable information

I support the addition of the five new data elements to the definition of personally identifiable information. These are the five elements on page 3 of the bill as passed by the Senate.

One of the reasons I support this addition is that I believe data protection should focus more on the data elements than on the entities handling the data. I think that a data element should be treated the same, no matter what entity handles the data. My long term goal is to convince you to focus on the data elements. For example, if it is

worthwhile to protect a student's covered information, any entity that holds that information (not just an operator) should be required to treat it in the same way as the bill proposes for an operator. And the same holds true for the other data elements, those listed in exhibit 1.

Another example is the data element of financial account number, credit card number, or debit card number that requires passwords, access codes, or additional identifying information. Destroyers of records are required to protect those data. Town and court clerks are allowed to put that information on an internet site unless the person whose number it is requests that it be redacted. If a data collector loses control of the data, that is not a security breach and is not reportable. I do not see why that information is protected when being destroyed and not protected when merely being held by an entity.

Adding the five data elements already in the bill moves us in that direction. These five elements are now included in brokered personal information and are not reportable if there is a loss of control of the data. Adding the elements to personally identifiable information will require that a loss of control be reported.

I also ask you to look at the data elements in exhibit 1 to see if there are some which you would now be willing to change to "yes" in the column of personally identifiable information (reportable data elements).

Increasing the amount of direct notice to consumers in the event of a data breach (section 4 of the bill)

This bill proposes a minor expansion of direct notice to consumers of a data breach. I support that as a baby step in the direction of increasing the number of data breaches requiring direct notice to consumers. However, the bill proposes decreasing direct notice in the case of e-mail.

This bill proposes to reduce the amount of direct notice by e-mail to consumers. Right now, if the data collector normally communicates with consumers by e-mail, the collector is required to notify them directly by e-mail, no matter what the cost. This bill will no longer require direct notice by e-mail if the total cost of direct notice by all forms exceeds $10,000. Let's consider the case of a company that communicates in a variety of methods: (some by e-mail, others by telephone, and still others by letter). If the cost of direct notice to the customers using mail and telephone exceeds $10,000, then the company may provide substitute notice to all, including those who could be reached by e-mail at a very small cost compared to telephone or mail.

I ask that you remove "e-mail" from the list in (B)(i)(I) on page 13 of the bill. This will retain the current condition of requiring direct notice by e-mail in all security breaches.

I think that $10,000 is too low a threshold for avoiding direct notice. However, raising it to $10,000 is better than not raising it at all. I also support the removal of any limit on the the class of affected consumers who are to be notified directly as in the bill.

My long range goal is to convince you to increase the number of ways that individuals will be notified directly of a data breach.

Exhibit 2 shows the ways that a loss of control of information will be handled under the Security Breach Notice Act. There are 10 possible paths to follow. The bill proposes to reduce the number of paths to nine. (It does this by removing the limit on direct notice to consumers based on the number of consumers whose data were breached. (This is the path in the orangish color with the crossed-out text.)

In four of the remaining nine paths (brown boxes) the consumer never learns of the loss of data. Two of those four (data loss is non-digital; data loss is encrypted) aren't even considered to be breaches. In one path (green box), the consumer can only learn about the security breach through a public records request.

In two paths (grey boxes), substitute notice is used to alert the public in general of a data breach. The consumer has to contact the company to find out if his or her data have been breached. In only two paths (white boxes) the consumer is notified directly of the loss of his or her data in a security breach.

As I said, it is a long-term goal of mine to change more of the colored boxes to the white boxes of direct notice. And to reduce the delays between discovery of a security breach and notice to consumers. Data collectors have a month-and-a-half to two months until they have to notify consumers of a data breach.

Consumers are the last to learn of a security breach. The order of receiving information is: data collector; attorney general (or department of financial regulation); law enforcement; and eventually consumers. By making the consumers the last to know, the consumers lose valuable time before they can begin to take steps to prevent (or at least reduce) damage from the breach. This is disrespectful of a consumer's need to know of an unauthorized acquisition.

Proposed amendments to the bill

My testimony has been wide-ranging with a mix of long term-ideas and what to do here and now with this bill. Sections 2 and 4 of the bill will increase the ability of consumers to receive direct notice in case of a data breach (rather than a substitute (indirect) notice or no notice at all), so I support those sections. I ask that you go a little bit farther in this bill by making the following amendments.

- amend the definition of a "data collector".
- change the phrase "personal information" as part of the description of covered information
- remove "e-mail" from the list in (B)(i)(I) on page 13 of the bill

Conclusion

Thank you for giving me the time to testify this morning. You have an opportunity to increase the protection of consumers' information. I urge you to take advantage of this opportunity by amending this bill in the ways that I have suggested in this testimony.

Sincerely,

Thomas Weiss

Exhibit 1 - data elements classified in 9 V. S. A. chapter 62

S-110- data privacy and consumer protection

Thomas Weiss

April 10, 2019

data element	PII	BPI	PI	SSN
name (for PII, name plus any other(s))	yes	yes	no	no
address	no	yes	no	no
name or address of immediate family or household member	no	yes	no	no
social security number	yes	yes	yes	yes
driver's license number	yes	yes	yes	yes
non-driver ID number	yes	yes	yes	yes
passport number	no*	yes	yes	yes
employer taxpayer ID number	no	yes	no	yes
other government issued ID number	no	yes	no	no
biometric record	no*	yes	no	no
physical characteristics or description	no	no	yes	no
date of birth	no	yes	no	no
place of birth	no	yes	no	no
mother's maiden name	no	yes	no	no
financial account number, credit card number, or debit card number that can be used without passwords, access codes, or additional identifying information	yes	no	yes: bank acct. number only	yes
financial account number, credit card number, or debit card number that requires passwords, access codes, or additional identifying information	no	no	yes	yes
financial account PIN's, passwords or other access codes	yes	no	yes	yes
credit card or debit card PIN's, passwords or other access codes	no*	no	yes	yes
any other financial information	no	no	yes	no
insurance policy number	no?	no?	yes	no
signature	no	yes	yes	no
any other information that, alone or in combination, is linked or linkable to the consumer that would allow a reasonable person to identify the consumer with reasonable certainty	no	no	yes	no
credit report	no	no	no	
internet browsing history	no	no	no	
online purchases	no	no	no	
location data	no	no	no	
loyalty programs	no	no	no	
subscription information	no	no	no	
Additions proposed by bill S-110 as passed by the Senate				
biometric information, including a finger print, retina scan, and facial recognition data	yes	no	no	no
genetic information	yes	no	no	no
health information	yes	no	no	no
login credentials including a username or password	yes	no	no	no

Vermont requires notice to consumers only for the unauthorized acquisition of PII (personally identifiable information) , and only in some cases. Vermont does not require notice to consumers for unauthorized acquisition of all other information.

PII - personally identifiable information (data collectors) - non-encrypted-digital only (§2430)
BPI - brokered personal information (data brokers) - non-encrypted-digital only (§2430)
PI - personal information - physical destruction of records (§2445)
SSN - social security number protection - digital or paper (§2440)

*Bill S.110 proposes to add these three data elements to the definition of PII.

Exhibit 2
Notice to consumers of unauthorized acquisitions of personally identifiable information
S.110 - data privacy and consumer protection
Thomas Weiss, April 10, 2019

References are to subsections of 9 V. S. A. 2435 unless otherwise noted.