H.764--DATA BROKERS BILL

Charles Storrow, Leonine Public Affairs, LLP on behalf of RELX, Inc. (LexisNexis)

1. RELX collects data (largely from public records) and provides information to businesses and governments. For instance, it collects motor vehicle operating records (i.e., public record information about traffic offenses) from DMVs and provides information derived from those records to insurance companies for their use in underwriting automobile insurance policies (this activity is regulated under the federal Drivers Privacy Protection Act). Another example of an information service it provides is to help state tax authorities determine whether a request for a state income tax refund is fraudulent, i.e., being made by an identity thief. It also provides information to state Medicaid agencies to weed out fraud, to law enforcement agencies to assist in locating people and for a myriad of other commercial and governmental purposes.

2. Certain requirements of the bill are a major problem because: (a) they are unnecessary in light of existing law, (b) because many businesses who handle the same type of information implicated in the bill are not subject to the bill's requirements, and (c) because the information that is involved in a Data Broker Security Breach is already widely available.

3. *Existing Security Breach Notice law* (9 VSA chapter 62)--"Data Collectors" who collect, disseminate or otherwise handle "personal information" (undefined under existing law) have to give notice of a breach of "personally identifiable information" (PII) to the AGO and affected Vermonters (Security Breach Notice Act set forth at bottom of page 14) (9 VSA section 2435).

4. Under the bill a "Data Broker" must annually register with the Secretary of State and, in so doing, provide information concerning a number of topics (pages 29-31). One item of information it would have to disclose is whether it suffered a "data broker security breach" (page 30, line 15).

5. Operative Definitions and Their Relationships

a. *Data Collectors* (existing law): a person who collects, etc., personal information (undefined in existing law) (page 10, line 15) (9 VSA section 2430(3)).[1]

b. *Personally Identifiable Information (PII)* (existing law): Name *and* SSN *or* driver's license # *or* bank account/credit card #) (p.11, line 6) (9 VSA section 2430(5)(A)). Note: under existing law PII does not include information that can be lawfully obtained from public records (page 11, line 19).

c. Many businesses, such as on line and brick and mortar retailers, and businesses in the hospitality industry, to name a few, are data collectors as they collect PII.

d. *Data Brokers* (proposed law): a business that collects and sells "personal information" (page 9, line 2). Note: Under the bill the term "Data Brokers" does *not* include a business that collects and sells personal information if that business is consumer facing. Thus, many businesses that collect and sell personal information are not covered by the proposed law. Stated differently, the universe of data brokers is much more limited than the universe of businesses that collect and sell personal information.

e. *Personal Information (PI)* (proposed law): *one* or more of the following data elements: name, address, name or address of family member, personal identifier or other info that might ID a person) (page 12, line 1).

f. *Data Broker Security Breach* (proposed law): unlawful acquisition of two or more elements of PI from a data broker (page 9, line 13).

g. Under existing law RELX (and Equifax) are "data collectors." Under existing law Equifax had to give notice to the AGO and affected Vermonters about the breach it suffered last year because that breach involved PII.

[1] There is an incongruity in existing law in that the definition of "data collector" references the currently undefined term "personal information," but the AGO/consumer breach notice requirements in 9 VSA section 2435 are triggered if the data collector suffers a breach of "personally identifiable information," which is currently defined. The change to the definition of "data collector" on page 10, line 20 resolves that incongruity.

h. Under the bill RELX and EQF would also be data brokers. If they are breached and PI is obtained, but not PII, they would have to so indicate on their annual filing with the S of S.

6. Yahoo breaches

   a. September 2016 Yahoo announced a breach that happened in 2014. 500 million names, email addresses, telephone numbers, dates of birth, passwords and, in some cases, encrypted or unencrypted security questions and answers.

      http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/index.html

   b. In December 2016 Yahoo announced a breach that had happened in 2013. One *billion* names, email addresses and passwords.

      http://money.cnn.com/2016/12/14/technology/yahoo-breach-billion-users/index.html

   c. The breaches Yahoo suffered did not involve PII, as defined in existing law, but did involve PI as defined in the bill.

7. Under the bill, because it is consumer facing Yahoo is not a data broker and will not have to make an annual filing with the S of S much less indicate in such a filing that, if it suffers a breach similar to ones announced in 2016, that it suffered a breach of PI. But, because it is non-consumer facing RELX is a data broker and would have to annually register with the S of S and indicate whether it suffered a breach of PI.

8. Moreover, PI is already widely available. One can go to Whitepages.com and similar on line information providers and run the name of someone you know. It will give that person's address for free and if you pay a modest fee, a lot of other info such as names and addresses of relatives. Similarly, Ancestry.com acquires vital records from states (including Vermont) and one using that service can obtain the information on a person's birth certificate, i.e., the person's place of birth, the age of the person, and names of the person's parents. Clearly, PI is readily available.

9. At a minimum, the definitions of "data broker security breach" and "personal information" and the requirement to disclose a data broker security breach on the annual registration with the S of S should be deleted from the bill. Those definitions and that disclosure requirement apply only to a small subset of entities that collect and sell personal information, and personal information is otherwise widely available. Vermont's existing data security breach notice law is adequate.

10. Moreover, because the definition of "data broker" applies only to a small subset of businesses that collect and sell personal information, the value of requiring data brokers to register with the Secretary of State is very limited and imposes an unfair burden on them.

11. Lastly, the bill requires data brokers to meet certain standards relative to maintaining the security of the PII they hold. (*See* proposed section 2447 beginning at the bottom of page 31). Those standards are derived from existing Massachusetts law. As a practical matter RELX already complies with those standards. However, the MA law applies to *all* entities that hold PII, whereas this provision in H.764 applies *only* to data brokers.