Vermont House Data Broker Bill Testimony

Jim Halpert
General Counsel
State Privacy & Security Coalition
January 18, 20018

I am general counsel to the State Privacy & Security Coalition, which works across the states for clear and consistent privacy and security legal requirements. In this capacity, I have helped with drafting more than 250 state privacy, security and consumer protection laws.

While this bill is well-intentioned, we believe that it should be narrowed to avoid regulating a broad range of entities that are not understood to be data brokers, to avoid potential First Amendment problems, and to avoid confusing data breach notice requirements.

- The definition of "data broker" is confusing and circular and seems to depend on an overly narrow list of exceptions (for example, if a company simply transferred to a debt collection agency a few names on its subscriber list to collect unpaid subscription fees, it might be a data broker). The definition has a double negative in it, that makes its meaning confusing. It also depends critically upon an overly narrow definition of first party relationships and would apply sweep in Internet advertising functions that are not commonly understood to be data broker functions. We recommend that if the bill goes forward that this definition be narrowed significant and have a representative list of first party relationships, instead of the small list currently in the bill.

- Prohibitions against sale in order to further abusive use of data in Sec. 2433(a) are a very good idea in general.

    - But "discrimination" needs to be defined. It can be interpreted as applying to offering discounts to consumers or even minority scholarship programs. To avoid creating these unintended consequences, the prohibition against "discrimination" should be clarified to apply to "otherwise unlawful discrimination."

    - Also, there should be no AG rulemaking on use of data. Instead, the bill should state clearly what the law requires and not create uncertainty about potential changes in AG rules that many Vermont businesses would be unaware of.

- The data breach provisions in the bill are overbroad.

    - First, the law should not apply to breach of paper records.

        - Paper breaches are far less likely to cause harm because records cannot be transferred easily via the Internet, which is how data breach information can fall into the wrong hands.
        - Second, it is very difficult to know if a paper data breach has occurred.

        - Third, the current Vermont breach notice law contains guidance that a breach occurs whenever information is "lost". This occurs routinely without any harm occurring in the case of paper records, as they can simply be misfiled to left in another office and never have left the business' premises. Because Vermont already has one of the broadest breach notice laws in the country, this change is not necessary. Very few states have paper breach notice obligations and those that do, have higher harm triggers and do not require notice if paper records are missing, as Vermont's law would if they were added to the law

    - Second, as currently drafted, the bill would allow the AG's Office to share broadly with agents and states attorneys, among others, preliminary breach notification submissions that are required specially in Vermont within 14 days of learning of a data breach. This information is required to be submitted much sooner in Vermont than in other states, is highly sensitive and is often inaccurate. This information should never be shared. Even, as to 45 day breach notice to the AG's Office, this information should be shared with other agencies only if necessary for investigation of illegal activity relating to the breach.

    - Third, it is by no means clear why special data broker breach notice provisions are needed – in contrast to data broker data security obligations in § 2447. Vermont already has one of the most demanding breach notice laws in the country with 14 day notice to the State AG's Office, a requirements that already apply fully to data brokers today.

- Lastly, because the AG's Office is a very strong enforcer of privacy and security violations, the bill should make clear that the prohibitions in the bill do not create a basis for a private right of action.

    - The requirements in this bill are entirely new and key definitions are unclear. This is a recipe for frivolous litigation and given the AG's role in the State as a strong enforcer, there is no point in leaving open the possibility of private class action enforcement.

Respectfully submitted,

Jim Halpert