

Attachment #21

Consumer Data Industry Association, 3/25/19 letter and related material



Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

P 202 371 0910

CDIAONLINE.ORG

March 25, 2019

The Honorable Evan P. Shanley
Chair, RI Online Data Transparency and Privacy Protection Commission
State House
Providence, RI 02903

Re: Relating to the Regulation of Data Brokers

Dear Members of the Commission:

I write on behalf of the Consumer Data Industry Association (CDIA) to express our strong opposition to the draft data broker legislation that you are currently considering. Although, this legislation strives to regulate the data broker community, it falls short of providing new regulations on the entire data broker community by narrowing its definition of a data broker to those that are already heavily regulated by the federal government.

The Consumer Data Industry Association (CDIA) is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals, and to help businesses, governments and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity, helping ensure fair and safe transactions for consumers, facilitating competition and expanding consumers' access to financial and other products suited to their unique needs.

While we are concerned about protecting personal and sensitive information, this legislation narrows the definition of a data broker and mandates unnecessary requirements that are unwarranted and impractical. The Vermont law, if adopted in Rhode Island, would require a data broker to register with the state. However, there is nothing inherently unique to a data broker's operation that should require a state registration. There is no policy reason for a data broker to register because of what they do. Imposing a registration on a business that has been buying and selling marketing data or publicly available information, does not in any way protect the consumers of Rhode Island.

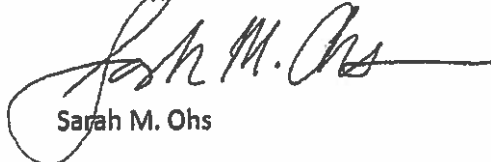
This legislation also requires data brokers to implement a customer ID program to verify that the customer is purchasing the information for legal purposes. Businesses buy and sell marketing information all of the time. Retailers, restaurants, plumbers are not required to have customer identification programs. This is because there is no reason to have a customer ID plan to protect

consumers. The same is true with data brokers. There is nothing unique to a data broker that requires a need for such a program. Mandating such a program on a business only consumes time and money, without offering any additional protections to the citizens of Rhode Island.

More importantly, this legislation ignores that businesses are currently heavily regulated on privacy concerns at the federal level. Federal statutes such as the Fair Credit Reporting Act (FCRA), which regulates how consumer reporting agencies use personal information. The Gramm-Leach-Bliley Act, which requires financial institutions and companies that offer consumers financial products or services, to explain their information-sharing practices to their customers and to safeguard sensitive data. This bill ignores the Children's Online Privacy Protection Act, which places requirements on operators of websites or online services directed to children under 13 years of age. All of these federal statutes exist to regulate business practices where personal information is collected and protects the consumer. This bill fails to appreciate that businesses are already operating under these tight regulations.

In conclusion, the Vermont data broker bill fails to regulate in a meaningful way. There is a long history of privacy regulations at the sectoral level that takes into account the unique needs of each industry. A bill that attempts to create one regulation, that is applied across all sectors, fails to distinguish the unique uses of data, and the existing federal statutes that regulate differing industries. Moreover, the way this bill is drafted it is only regulating those in the data broker community that are already heavily regulated at the federal level. If the concern is that there is a need for transparency to regulate the data broker industry, we believe you should consider regulating those data brokers that are not currently regulated at the federal level. This would hold the entire data broker community to the same standard rather than narrowing the definition, as this bill does, and only focuses on a portion of the industry that is already heavily regulated federally. For the reasons above, we believe the Vermont data broker bill should not be used as a model for Rhode Island. Thank you for your consideration of our comments. I would be happy to answer any questions the Committee might have.

Sincerely,

A handwritten signature in black ink, appearing to read "Sarah M. Ohs", written over a printed name.

Sarah M. Ohs

Director of Government Relations

Rhode Island H-7111 Sub A/3:**Section 7 FCRA Exemption language Needed:**

This chapter does not apply to:

Personal data provided to, from, or held by a consumer reporting agency as defined by 15 U.S.C. Sec. 1681a(f), and use of that data is governed by the federal fair credit reporting act (15 U.S.C. Sec. 1681 et seq.);

Fraud Prevention Language Needed:

EXEMPTIONS. (1) The obligations imposed on controllers or processors under this chapter do not restrict a controller's or processor's ability to:

- (a) Comply with federal, state, or local laws, rules, or regulations;
- (b) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;
- (c) Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local law;
- (d) Investigate, exercise, or defend legal claims;
- (e) Prevent, or detect, or respond to identity theft, fraud, or other malicious or criminal illegal activity, or verify authenticate identities; or assist another entity with any of the activities set forth in subsections (a) through (e)