Testimony of Social Sentinel, Inc.
Vermont Senate Economic Development, Housing, and General Affairs Committee
H.764, An act relating to data brokers and consumer protection

April 10, 2018

Introduction: Mr. Chair and members of the Committee, I am Liz Kleinberg, General Counsel for Social Sentinel, Inc. Thank for the opportunity to present testimony on behalf of Social Sentinel.

While Social Sentinel supports the general idea of increased transparency for Data Brokers, we cannot support H.764, An act relating to data brokers and consumer protection (the "Bill"), given the current definition of "Data Broker." That definition arguably includes Social Sentinel, and we do not believe that the Bill is intended to or should include Social Sentinel as a Data Broker. We request certain modifications to the Bill that would make it more narrowly tailored to include organizations that are data brokers while excluding companies that are not, such as Social Sentinel.

Who we are: Social Sentinel helps organizations better understand and protect their communities by alerting them to threats shared publicly on social media. The majority of our clients are educational institutions (both K12 school districts and institutions of higher education) in 24 states (including Vermont), and they use our service to help protect approximately 7,000,000 students. We are a start up company with approximately 30 employees, about 25 of whom are located in Vermont.

How our service works: Our Service identifies publicly available social media posts that are threat alerts relevant to our clients. Upon receiving an Alert, clients are able to assess the potential safety and security threat in context by going directly to the publicly accessible content on the social media platforms. We have carefully configured our service to provide meaningful results to our clients while respecting the rights of individuals and groups. Our Service identifies a post as an Alert only if it contains sufficient indicia of a threat and is reasonably affiliated with a client. We have taken preventative measures to ensure that our service cannot be used to surveil/monitor/track individuals or groups. Our service assesses only publicly available social media. Once we identify a post as a threat, we deliver the post to a client in the same form as we receive it from the social media, and we deliver each alert to our clients in as near to real time as we can.

Social Sentinel is not a Data Broker: Regarding whether Social Sentinel should be considered a Data Broker within the meaning of the Bill, it is important to note the following points, which distinguish Social Sentinel from organizations we believe are intended to be considered Data Brokers:

- Our service assesses only publicly available social media posts that are made by people who have made a choice to post publicly.
- Our service does not let users obtain information about any particular individual, because our service will not identify a post as an alert unless it (1) contains language of harm and (2) is associated with our clients.
- The post's author's social media handle may be included, but our service does not intentionally target that information; that information is incidental to the information that our service intentionally seeks.
- We do not extract data from SM posts; we do not scrub or alter SM posts that we receive from the SM platforms.

Each of these points contrasts sharply with the characteristics of Data Brokers as outlined in the Findings

and Intent section of the Bill.

We note that people who choose to post on publicly available social media make an informed decision to make their posts public. They could post on *private* social media but opt to do so publicly. This contrasts with the information in the data points that Data Brokers obtain, such as Internet browsing history, online purchases, loyalty programs, and subscription information – in those situations, individuals may provide information in what they think are non-public ways, resulting in their unwitting disclosure of information that becomes public.

When people make publicly available social media posts, they have readily available opportunities to opt-out regarding use of their public social media posts. Before making the post, they could decide not to make their post on publicly available social media. After they make such a post, many social media platforms provide the opportunity for an author to modify or delete the post.

Proposed Revisions: As we support the spirit of the Bill, we recommend the following revisions that would make the Bill more narrowly tailored to include only persons that are intended to be included as Data Brokers.

1. Definition of "Data Broker" section 3(A): We propose the following changes to the definition of Data Broker:

   "Data broker" means a business that **intentionally and as its primary purpose** collects and licenses or sells to one or more third parties the **personally identifiable** information of a consumer with whom the business does not have a direct relationship.

2. Definition of "personally identifiable information" in Section 7(B): We propose the following changes:

   (B) "Personally identifiable information" does not mean publicly available information that is lawfully made available to the general public from federal, State, or local government records**, or lawfully made available to the general public by the consumer on publicly available social media**.

Thank you for your consideration.