PRIVACY RIGHTS CLEARINGHOUSE

August 11, 2017

Via email to MyLanh.Graves@Vermont.gov

The Honorable Thomas J. Donovan, Jr.
Attorney General of Vermont
109 State Street
Montpelier, VT 05609-1001

The Honorable Michael S. Pieciak, Commissioner
Vermont Department of Financial Regulation
89 Main Street
Montpelier, VT 05620-3101

**RE: State of Vermont Data Broker Legislation Working Group**

**Dear General Donovan, Commissioner Pieciak and colleagues:**

We at the Privacy Rights Clearinghouse (PRC) appreciate this opportunity to submit the following comments as you deliberate on the issue of data broker regulation.

The PRC is a nationwide nonprofit consumer education and advocacy organization based in San Diego, California. The organization was established 25 years ago in 1992. We invite individuals to contact us with their questions and complaints about a wide range of informational privacy issues. For the past decade, the topic of data brokers has been at or near the top of the list of complaints we receive from the public.

I had the opportunity to listen to a good bit of the data brokers public meeting, held July 25-26, 2017. I commend you for holding this two-day forum. You covered the topic in significant depth and breadth, and added a tremendous amount to the public discussion on this issue. I thank you for your comprehensive coverage of the data broker issue.

**Harms:**

I made a brief presentation to your working group via telephone on July 26th, focusing on the types of harms that individuals experience as a result of the absence of regulation of the data broker industry.

At the top of the list is the ability of stalkers and batterers to locate victims of stalking and domestic violence who have moved to new residences in order to evade those bent on locating


3033 Fifth Avenue, Suite 223, San Diego, CA 92103
Phone: 619.298.3396 • Fax: 619.298.5681 • www.privacyrights.org

and harming them. Victims are not able to ensure their personal safety so long as their addresses can be discovered via the online databases of data brokers. Victims of domestic violence and stalking must be able to protect the privacy of their homes in order to escape those determined to harm them.

Individuals who work in law enforcement and the judicial system face similar risks to their personal safety if their residential addresses are exposed via data brokers. These include law enforcement officers, judges, and parole officers. I vividly recall a phone call from a law enforcement officer who served on gang detail in a major city on the east coast. She had just discovered that online data brokers exist, and had been able to find her name and home address on several websites. She asked how she could be removed from all such online databases and asked if there were a single website she could visit to request that she be opted out of all at once.

She was understandably dismayed when I told her: one, there is no comprehensive list of data brokers; two, not all data brokers offer an opt-out because, three, there is no law requiring an opt-out; and four, even if she were to opt out of as many as she could, data brokers can change their opt-out policies whenever they wish.

I recall another phone call, this from a citizen activist who had taken a public stance on a controversial environmental issue in his community. He spoke out frequently at public meetings and was regularly quoted in the local newspaper. He was concerned that his personal safety could be at risk because his home address was easy to find online.

We were contacted by a victim of identity theft who described her particular ordeal in some detail to me. An imposter had obtained enough information about her to open up several new credit card accounts and make many purchases before being apprehended. She explained that the fraudster was able to obtain both her current and former addresses in order to make credit card applications look particularly legitimate. I asked her how the identity thief obtained all this information, in particular, her *prior* addresses. She said she found out from the detective on her case that the identity thief had purchased information about her from an online data broker.

Individuals don't need to be in the kinds of situations I've described above in order to want to prevent their personal information from being posted on the web by online data brokers. A majority of the complaints we receive from individuals about data brokers are not from victims of stalking and are not law enforcement officers or court officials. They are individuals who simply value their privacy and want to exert control over their personal information.

**Legislation:**

The Privacy Rights Clearinghouse favors data broker legislation that includes the following provisions:

- The right of access to one's personal information.
- The right to correct one's data profile.

- The ability to opt out of one's data profile being sold to or shared with third parties.
- The requirement that data brokers publicly identify themselves in a central clearinghouse in order to simplify the process of opting out.
- And the further requirement that opting out be available to individuals in a one-step process encompassing all data brokers listed in the clearinghouse.

In addition, we would like to see these additional provisions in data broker legislation:

- No personal information provided to a data broker for the purpose of opting out can be used by the data broker to add to its data profile on that individual.

- Individuals need to be able to communicate with someone within the company. A common complaint we have received is that many if not most data brokers are "black boxes" – that is, impenetrable. I recall talking with one victim of stalking who resorted to hiring an attorney to contact data brokers via postal letter because she herself (the victim) was unable to get responses from them, including assurances that they would indeed remove her from their public websites.

- Some data brokers charge a fee to opt out. This should be prohibited.

California statutes include a law that gives a limited number of individuals the ability to require they be opted out of online websites containing their personal information, in particular, their home address. The following description of the statute is from the California Attorney General's compendium of privacy laws (https://oag.ca.gov/privacy/privacy-laws -- Scroll down to "Safe at Home Participants, Online Privacy".)

> This law provides participants in the Secretary of State's confidential address program, Safe at Home (for victims of domestic violence or stalking and reproductive health care providers, employees, and volunteers) with the right to demand the removal if their personal information, including home address and phone number, from online search engines or databases, and imposes related obligations on the operators of such search engines and databases.

As with a great deal of consumer protection legislation that is passed into law in California, this law illustrates that the Legislature has dealt with the issue of data brokers incrementally. In many such instances, the Legislature has revisited privacy issues in subsequent years, adding to the body of law in additional increments. We are not at all opposed to such an incremental approach.

**Definitions of Data Brokers:**

The website of the Office of the Vermont Attorney General provided an overview of the issues to be discussed by participants in the two-day public meeting, held July 25-26, 2017. In

addition to the agenda for this forum, the AG listed "Topics to Consider." First on the list is "An appropriate definition of the term 'data broker'".

The task of determining a definition of data brokers is not easy, to say the least. I have collected several definitions of data brokers over the years. These have been included in legislation and policy reports. I am not singling out any one such definition in these comments. Rather, I've provided this list as an addendum to these comments for your review and consideration.

**Data Broker Resources on PRC's Website:**

The website of the Privacy Rights Clearinghouse includes a consumer guide on data brokers and "people-search" sites. It is found here: https://www.privacyrights.org/consumer-guides/data-brokers-and-people-search-sites .

Following are the topics covered in this guide:

1. What are data brokers?
2. How do data brokers obtain information?
3. What types of information do data brokers collect?
4. What are the different types of data brokers?
5. Who uses data broker information?
6. How accurate is data broker information?
7. Are there any laws that regulate data brokers?
8. Do individuals have any rights to see, correct, or opt-out of the information that data brokers have compiled?
9. Resources

The Resources section of our guide includes links to materials provided by federal government agencies, news media, and nonprofit consumer advocacy organizations, including the Privacy Rights Clearinghouse. Our data brokers consumer guide and its Resources section might be of interest to you as you deliberate further on the topic of data brokers.

**Conclusion:**

On behalf of the Privacy Rights Clearinghouse, I thank you once again for the opportunity to submit our comments to your Data Broker Legislation Working Group. I wish you all the best in your deliberations. Feel free to contact me if you have questions about my comments or wish additional information.

Sincerely,

Beth Givens
Executive Director
Privacy Rights Clearinghouse
3033 5th Ave., Suite 223, San Diego, CA 92103

Website: www.privacyrights.org
Email address: bethg *at* privacyrights.org

## ADDENDUM:
## Definitions of Data Brokers from Introduced Legislation and from Policy Reports

The following definitions were included in comments submitted to the Federal Trade Commission by the PRC in response to its December 2010 report, *Preliminary FTC Staff Report, Protecting Consumer Privacy in an Era of Rapid Change.* (https://www.privacyrights.org/blog/comments-ftc-protecting-consumer-privacy-era-rapid-change-0 )

In 2009 Senator Leahy introduced the Personal Data Privacy and Security Act which defined data brokers as "business entities which, for monetary fees or dues, regularly engage in the practice of collecting, transmitting, or providing access to sensitive personally identifiable information on more than 5,000 individuals to nonaffiliated third parties on an interstate basis."

[From Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. (2009), summary available at http://www.govtrack.us/congress/bill.xpd?bill=s111-1490&tab=summary.]

In 2009 Rep. Rush introduced the Data Accountability and Trust Act which defined "information brokers" as:

> [An 'information broker' is] a commercial entity (or its contractor or subcontractor) whose business is to collect, assemble, or maintain personal information concerning individuals who are not current or former customers of such entity in order to sell or provide access to such information to any nonaffiliated third party.
>
> [S]uch definition does not include a commercial entity to the extent that such entity processes information collected by or on behalf of and received from or on behalf of a nonaffiliated third party concerning individuals who are current or former customers or employees of such third party to enable such third party to provide benefits for its employees or transact business with its customers.
>
> [From Data Accountability and Trust Act, H.R. 2221, 111th Cong. (2009), summary available at http://www.govtrack.us/congress/bill.xpd?bill=h111-2221&tab=summary.]

In 2009, a New York Governor's Program Bill, put forth for consideration by the legislature but never introduced, defines "individual reference services provider (IRSP)" as:

[IRSP] means any person, agent, business, entity, affiliate or subsidiary who primarily engages in the business of collecting, assembling, transmitting or maintaining sensitive personal information for the purpose of providing access to such information about individual data subjects to third parties for monetary compensation or other consideration. [IRSP] activities shall not include provision of information to the federal or state government or any political subdivision thereof. A person or entity that engages in [IRSP] activities shall be presumed to be primarily engaged in such practice if the revenue such person or entity derives from such practice represents more than twenty percent of such person's or entity's professional service-related revenue.

[From An Act to amend the general business law, in relation to the protection of sensitive personal information; NY Governor's Program Bill, 2009 Memorandum, Bill #26.] The definition did not include government entities, consumer reporting agencies, media, private investigators, and labor unions.

In 2005, California Senate Bill 550 contained the following definition of "data broker":

'Data broker' means any person other than a governmental entity that regularly engages in compiling or maintaining consumer data files used or expected to be used or collected in whole or in part for the purpose of providing consumer data files, or access to those files, to nonaffiliated third parties for monetary fees, dues, or on a cooperative nonprofit basis.

[From California Data Broker Access and Accuracy Act of 2005, S.B. 550 (Cal. 2005), *available at* http://leginfo.public.ca.gov/pub/05-06/bill/sen/sb_0501-0550/sb_550_bill_20050628_amended_asm.pdf (version amended in assembly June 28, 2005).] Not included were financial institutions subject to the California Financial Code, credit bureaus, "covered entities," and Internet Service Providers.

To this collection of definitions, I add one more – the definition crafted by the Federal Trade Commission in its 2012 report on privacy:

"...companies that collect information, including personal information, about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud."

[From Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (March 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf at 68].