ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

July 26, 2017

VIA email MyLanh.Graves@Vermont.gov

My-Lanh Graves
Vermont Attorney General's Office
109 State St.
Montpelier, VT 05609

Re: **Data Broker Legislation Working Group Public Meeting**

Amul Kalia's Testimony:

My name is Amul Kalia, and along with my colleague Priscilla Guo, we represent the Electronic Frontier Foundation (EFF), which is a digital rights non-profit based in San Francisco. We are an organization of experts, deeply interested in privacy issues with our team of activists, attorneys, and technologists.

Thank you to the Vermont Attorney General's office and the Data Broker Regulation Working Group for convening experts to testify about this very important issue.

I will be mainly covering two specific topics: 1) how we should think of and define data brokers as entities that fall within the purview of any proposed legislation; and 2) the nature of the data that these entities are collecting, and consequently, why there should be legislation that increases transparency and disclosure in this industry.

1) Defining Data Brokers

First, let's consider what entities should qualify as data brokers and how they should be defined. From the EFF's perspective, we need to take a narrow view of who qualifies as a data broker. Similar to other privacy advocates, our view is that data brokers should be narrowly defined, with a focus on entities, whose dominant purpose is to shuffle and sell data back and forth without any direct contact with people about whom data is being collected.

To be more specific, when we talk about data brokers, we are not talking about technology companies, i.e. companies like Facebook and Google that have products and services that customers use. Nor, are we talking about companies that broker or share lists of their own customers—retailers like Target, Walmart, and other merchants would fall fall into this category.

This distinction is important for a few different reasons:

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 *fax* +1 415 436 9993 *web* www.eff.org *email* information@eff.org

People don't know that much about data brokers. When we are using online services like Facebook and Google, we know who we are interacting with. As the FTC report from 2014 entitled *Data Brokers: A Call for Transparency and Accountability* describes, data brokers are collecting detailed and specific data about consumers, and consumers are unaware of them.[1] Consumers do not have direct relationships with the data brokers. Like many others in the room, I do not know which data broker companies have information on me, nor do I have a way of finding this information, unless I'm intimately familiar with each company's practices. Contrast this with my Google account for my Gmail, I know that I'm entering into a relationship with Google.

Users enter into contracts and agree to terms of use with tech companies, and have some understanding, or can refer to the terms of services, to figure out the practices of the company pertaining to data collection and dissemination. This is in stark contrast to data brokers, with whom consumers have no direct relationship; let alone being able to enter into a contract.

Lastly, another important aspect of lack of protection for consumers is the absence of control that consumers have once data brokers amass data on them. Again, as the FTC report noted, most of the data that data brokers aggregate actually comes from these entities trading it back and forth with each other.[2] Consumers are unaware of this market's existence, and without any ability to know how their potentially sensitive information is being traded. Nor can they discover how to control this dissemination. From a policy perspective, the data broker industry is a special case that could benefit from some sunlight. There's a definite lack of accountability and transparency.

2) Nature of Data and Its Implications for the Data Broker Industry

The second point I'd like to address is the nature of data itself that's valuable to the data broker industry, and the implications of collecting such data.

Data is often a wasting asset that depreciates over time. As a result, data brokers are always interested in gathering the latest data about consumers. But even "stale" data is in demand for identity verification or similar products. Moreover, data brokers' incentives for accuracy do not match well with consumers' interests in accuracy—a consumer who is inaccurately identified as having a criminal record will not be comforted by knowing that the data broker's list was accurate as a whole.

---

[1] Data Brokers: A Call for Transparency and Accountability, Federal Trade Commission (FTC), May 2014. Pg. 46. Available at https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

[2] *Id,* Executive Summary, Pg. IV

Additionally, as the FTC reported, some data brokers store data indefinitely, which obviously creates incentives for criminals to infiltrate and use the data for nefarious purposes, for instance identity theft.[3] And this is not a vague and undefined danger, 2016 was a record year for data breaches with an increase of 40% from 2015, according to the nonprofit Identity Theft Resource Center, which tracks these numbers.[4]

Thus, we are concerned that the data broker industry has incentives to collect as much information about consumers as possible without adequate regard to its accuracy.

From a policy standpoint, we have to create disincentives for this behavior. Increasing transparency within the industry is a good step forward in that regard.

[3] *Id.* Pg. 48

[4] Data Breaches Increase 40 Percent in 2016, Identity Theft Resource Center, January 2017. Available at http://www.idtheftcenter.org/2016databreaches.html

Priscilla Guo's Testimony:

I'd like to thank the Attorney General's Office, the members of this working group, and all those who have submitted testimony and public comments.

As an addendum to my colleague's remarks, the intent of my public comment is two-fold: 1) to articulate a clear need for data broker legislation by illustrating the myriad of harms associated with an unregulated market of data; and 2) to advise the Attorney General on the initial crafting of legislation in the area, specifically in regards to the narrowing of scope and the treatment of data aggregation techniques.

In the interests of protecting vulnerable populations, our priorities are to add accountability back into the system, via regulatory oversight. Take for instance your religion, whether you've had an abortion, your projected sexual orientation, your plans to have a baby, your addiction level, or even whether you're into Elvis memorabilia. Perhaps individually, these pieces of information seem disparate and random and don't strike you as remarkably harmful.

But the power of data brokers lies in the combination and analysis of this information. By piecing it all together, they've learned much about your personal data, your preferences, and your interests, bundled to sell to any buyer.

Unfortunately, the buyer is not always screened. For instance, domestic violence victims could face threats from their former abusers, who can use people search products to figure out what their new addresses are and a way to contact them. This is just the tip of the iceberg, and the reason why we have a duty to protect consumers in this dangerously crafted data broker market.

To be clear, EFF currently supports a light regulatory lift to be imposed on data brokers, specifically disclosure and transparency. And these disclosure obligations would only apply to the companies that are under the purview, which my colleague Amul Kalia has specified. Our current interest is not in questioning whether or not data brokers can sell data or requiring these data brokers to gain consent of consumers. It is to propose what should be considered as necessary disclosure.

Finally, we advocate for greater transparency behind data aggregation techniques and de-identification techniques of the industry. To advise the Working Group in their report on this matter, we would like to provide clarity that we don't trust data aggregation as the sole means of privacy protection. Aggregation is only valuable if the resultant data meets sufficient standards of de-identification. Stripping the last four numbers off a phone or simply removing names only shrinks the bucket of potential individuals down to a queryable data set.

First, we would like data brokers to disclose their de-identification technique so that it is understandable. This is important for accountability. Given the sensitive nature of the data that data brokers handle and the grave threat of data breaches, it's critical that the public receive assurances that their data remains private. Second, there needs to be a clear link established in how this degree of de-identification will actually protect privacy. Why does the data broker believe it protects privacy? What is the perceived risk of re-identification? These are critical questions that data brokers should be answering to.

In closing, I'd like to once again reiterate the desperate need for disclosure and transparency within the industry, so that the citizens of Vermont are better informed.