Consumer Federation of America
1620 I Street, N.W., Suite 200 * Washington, DC 20006

August 3, 2018

Via email to rowan.cornell-brown@vermont.gov

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

June E. Tierney, Commissioner
State of Vermont
Department of Public Service
112 State Street
Montpelier, VT 05620-2601

RE: Protecting the Privacy of Vermonters

Dear General Donovan and Commissioner Tierney:

Consumer Federation of America (CFA),[1] applauds the State of Vermont for its interest in protecting the privacy of its residents. We hope that the following information will be helpful as you consider the options before you. It is crucial for states to act in this area, as they did in regard to data breach notification, since Congress has not done so and the authority of the Federal Trade Commission (FTC) to address privacy issues is very limited.[2]

Vermont Should Enact Broadband Privacy Rules

As the internet has become an essential tool for modern life, concerns about privacy have increased. Internet service providers (ISPs) are in a unique position to see everywhere customers go and everything they do online that is not encrypted. That information can reveal a lot about us – our race and ethnicity, our sexuality, our health conditions, our interests, our habits, with whom we associate, our political beliefs, the composition of our families, and much more. We wouldn't want our telephone companies to listen in on our calls or compile a list of whom we call and disclose that information to others or use it on their behalf in order to advertise to us, determine our eligibility for things or the prices that we should

[1] Consumer Federation of America is an association of more than 250 nonprofit consumer organizations across the United States. Its mission is to advance consumers' interests through research, advocacy and education.
[2] For a good analysis of the FTC's limitations, *see* Harold Feld, Public Knowledge, *Principles for Privacy Legislation*, December 8, 2017, available at https://www.publicknowledge.org/documents/principles-for-privacy-legislation.

be charged, or make other kinds of judgements about us. The same is true for our online communications.

CFA and other consumer and privacy organizations strongly supported the Federal Communications Commission's (FCC) 2016 Privacy Order,[3] which set commonsense rules to protect the privacy of broadband customers and strengthened the rules concerning telephone privacy. We refuted industry arguments against the broadband privacy rules;[4] many of the same arguments have been made since in opposition to state broadband privacy legislation, and are no more valid now than they were then.

The public outcry around the country and across the political spectrum when the Congress repealed the FCC broadband privacy rules demonstrated that Americans feel strongly about their privacy and want to have real control over their personal information. Current federal law does not adequately protect them. There are no FTC privacy rules, nor does that agency have any rulemaking authority in that regard. Furthermore, Congress' action precludes the FCC from ever adopting substantially similar rules for broadband privacy again.

After the repeal of the FCC broadband privacy rules there was a flurry of activity on the state and local level to fill the gap. Using its authority over cable operators, the City of Seattle enacted broadband privacy rules,[5] and the District of Columbia is considering a similar measure.[6] According to the National Conference of State Legislatures, two states, Nevada and Minnesota, have enacted laws requiring internet service providers to get customers' permission before disclosing certain types of personal information, and many more bills have been proposed.[7]

The most prominent of these was California AB 375, which CFA and other consumer and privacy organizations strongly endorsed. The bill was first introduced on February 9, 2017[8] and amended over the summer, with continued support from consumer and privacy organizations through the September 12, 2017 version, and vehement opposition from ISPs and others.[9] The legislative session ended with the bill just short of passage, and it was taken up again this year. Unfortunately, a set of unusual circumstances derailed it. In an effort to deflect a possible November ballot measure on privacy, California legislators, suddenly and behind closed doors, gutted the bill and replaced it, under the same

---

[3] FCC WC Docket o. 16-106, FCC 16-148, adopted October 27, 2017, https://www.fcc.gov/document/fcc-releases-rules-protect-broadband-consumer-privacy; *see* comments, May 27, 2016, https://consumerfed.org/wp-content/uploads/2016/05/5-26-16-Broadband-Privacy_Letter.pdf.

[4] *See* letter to FCC Chairman Wheeler, September 7, 2016, https://consumerfed.org/wp-content/uploads/2016/09/9-7-16-Broadband-Privacy-Coalition_Letter.pdf, letter to the FCC Chairman and Commissioners, September 28, 2016, https://consumerfed.org/wp-content/uploads/2016/09/9-28-16-Broadband-Privacy_Letter.pdf, and ex parte comments on October 20, https://consumerfed.org/wp-content/uploads/2016/10/10-20-16_FCC-Privacy-Ex-Parte_Comments.pdf.

[5] *See* http://www.seattle.gov/Documents/Departments/SeattleIT/SeattleRule_ITD-2017-01.pdf.

[6] Notice of Proposed Rulemaking available at https://dcregs.dc.gov/Common/NoticeDetail.aspx?NoticeId=N0071499.

[7] *See* list as of 2017, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers.aspx.

[8] Go to https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375, at Version select Introduced from the drop-down menu, and click on Go. All versions can be viewed at this link.

[9] A blog by Ernesto Falcon at the Electronic Frontier Foundation recounts this battle, *see* https://www.eff.org/deeplinks/2017/10/how-silicon-valleys-dirty-tricks-helped-stall-broadband-privacy-california.

number, with completely different and broader online privacy legislation. The new law, enacted on June 28, 2018, contains some good provisions but it also has many provisions that are very concerning to privacy advocates. It is *not* a model for Vermont to follow.[10]

Last fall, New America's Open Technology Institute (OTI) released model state legislation on broadband privacy.[11] This model bill was crafted to take into account the challenges to their authority that states might encounter in legislating in this area.

Vermont Should Consider Regulating Businesses That Handle the Data of Consumers with Whom They Have a Direct Relationship

We supported Vermont legislation to regulate data brokers[12] and salute the state for being first in the nation to take that step. Since data brokers do not have direct relationships with the consumers whose personal information they collect and sell, they are largely invisible. It is important for Vermonters to know what data brokers collect data of individuals in the state, what control they give to those individuals over their data, and how they secure the data.

There are also concerns, however, when companies with which consumers have direct relationships disclose or sell their personal data to third parties, or use the data themselves, for secondary purposes – that is, for purposes unrelated to fulfilling customers' requests or that are not necessary for operational purposes such as fraud detection. The Facebook/Cambridge Analytica controversy serves as a good example of how consumers' data can be used for secondary purposes that they may not expect or desire.[13]

One of the arguments that ISPs make is that broadband privacy rules are not needed because they do not sell or share customers' personal information.[14] Perhaps they don't,[15] but there are other ways to monetize customers' personal information. For example, the infographics from the Center for Digital Democracy at https://www.democraticmedia.org/content/big-cable-companies-track-target-you-tv-mobile-pc illustrate how cable companies can track customers' activities across multiple platforms, profile them based on that information, and serve them targeted ads on behalf of other companies – a

[10] *See* blog by Allie Bohm at Public Knowledge analyzing the new California statute, https://www.publicknowledge.org/news-blog/blogs/is-californias-new-privacy-law-right-for-the-united-states/.
[11] *See* blog by Eric Null at OTI with link to the model bill, https://www.newamerica.org/oti/blog/oti-publishes-model-state-legislation-help-states-protect-broadband-privacy/.
[12] Letter to Vermont Senator Peter Sirotkin in support of H. 764, April 12, 2018, from CFA, Consumer Action, Consumer Watchdog, National Consumers League, and Privacy Rights Clearinghouse, available at https://consumerfed.org/wp-content/uploads/2018/05/consumer-groups-support-vermont-bill-H764.pdf.
[13] *See* Kevin Granville, "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens," New York Times, March 19, 2018, available at https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.
[14] *See* Jacob Kastrenakes, The Verge, "Comcast, AT&T, and Verizon say you shouldn't worry about gutting of internet privacy rules," March 31, 2017, available at https://www.theverge.com/2017/3/31/15138094/comcast-att-fcc-internet-privacy-rules-response.
[15] Some of these same companies were recently accused of selling wireless customers' real-time location data, see Gary Guthrie, ConsumerAffairs, "Verizon and AT&T to stop selling customers' location information to data brokers," June 20, 2018, available at https://www.consumeraffairs.com/news/verizon-and-att-to-stop-selling-customers-location-to-data-brokers-062018.html.

service for which the advertisers pay. ISPs and other companies are doing this as well, and this is Google's business model.

No matter whether consumers' personal information is being kept in-house by a company with which they have a relationship or provided to third parties, we believe that it should not be used for secondary purposes without those consumers' express, affirmative consent (opt-in) based on clear information about who will be using it and for what (it might be appropriate to allow the first party to use customers' data to promote its own products or services to them, with the ability of customers to opt-out of such marketing). For broadband privacy, that is essentially what the FCC rules and the California bill would have required (with some reasonable exceptions, such as sharing consumers' locations in emergency situations). Crucially, the California bill would have barred ISPs from requiring consumers to consent in order to use the service and from charging a higher price or providing them with a lower level of service if they refused.

We urge you to consider whether Vermonters should have opt-in control of secondary uses of their personal information by businesses with which they have direct relationships.

Vermont Should Designate a Chief Privacy Officer

According to sources at the National Association of State Chief Information Officers, West Virginia, South Carolina, Ohio, Kentucky, Arkansas, Indiana, Utah, and the State of Washington have created the position of Chief Privacy Officer (CPO). New York City, the City of Seattle, and Santa Clara County, California, have done so as well.[16] This trend is welcome. State agencies collect enormous amounts of personal information from individuals, some of it very sensitive, for a variety of legitimate reasons. As more government services are provided online and as data collected by states are increasingly stored electronically, securing that data from unintentional exposure or intentional acts such as hacking is obviously very important and requires oversight by qualified personnel.

There are many other issues that states must address beyond data security, however, such what kinds of personal information are necessary to collect for government functions, how long should the data be retained, and under what circumstances should state agencies share the data with each other, with municipalities, with the federal government, and with the private sector.

A CPO can help the state develop comprehensive and consistent policies for issues such as these and coordinate and oversee their implementation. In our view, however, the duties of a CPO should be even broader. The CPO should undertake public education initiatives, not only about Vermonters' privacy rights and agencies' responsibilities related to government collection and use of personal information, but about individuals' rights and businesses' responsibilities with respect to personal information collected and used in the private sector. The CPO should also be called upon to provide input to the appropriate state officials about new laws or regulations (or changes to existing ones) that may be needed to better protect Vermonters – for example, in regard to broadband privacy and data breach notification. In addition, the CPO should help to route privacy-related complaints to the appropriate authorities and convene stakeholders to discuss emerging privacy issues and concerns.

[16] Benjamin Freed, Statescoop.com, "New York City appoints its first chief privacy officer," April 5, 2018, available at https://statescoop.com/new-york-city-appoints-laura-negr%C3%B3n-as-its-first-chief-privacy-officer.

Conclusion

Privacy legislation does not hamper innovation; businesses will continue to innovate, as they always have, within the parameters that public policy sets. States have always led the way on privacy, enacting laws on data breach notification,[17] online privacy policies,[18] biometric data,[19] data security,[20] and many other areas. We support states' action to protect the privacy of their residents and believe that any federal legislation should create a "floor," not a "ceiling," enabling states to provide stronger protections as they see fit.

Thank you for considering these comments. We hope that they are helpful as you consider moving forward to strengthen the privacy protections of Vermonters.

Sincerely,

Susan Grant
Director of Consumer Protection and Privacy
Consumer Federation of America

[17] *See* list of data breach notification laws from National Conference of State Legislatures at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[18] *See* California law requiring commercial websites to provide privacy policies, http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=8.&title=&part=&chapter=22.&article=.

[19] *See* Illinois Biometric Privacy at, http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

[20] *See* Massachusetts standards for protecting personal information, https://www.mass.gov/regulations/201-CMR-17-standards-for-the-protection-of-personal-information-of-residents-of-the.