Comments by VPIRG regarding data security and internet privacy

August 6, 2018

Good morning. My name is Christina Fornaciari – and I am the Communications and Engagement Manager for the Vermont Public Interest Research Group, VPIRG, the state's largest environmental and consumer advocacy organization. Before I begin, I'll note that our chief advocate around digital consumer issues, Zach Tomanelli, could not join us today to offer these comments. I would ask that if you have specific questions regarding our recommendations, that you direct them to him.

I'm here today to offer these comments on behalf of VPIRG and our organization's 50,000+ members and supporters across Vermont.

VPIRG were strong advocates of the data broker legislation that was enacted into law earlier this year and we appreciate this group's continued efforts to determine what steps our state should take to better protect Vermonters in the digital space.

Everyday more and more of our lives are playing out online. We as individuals transmit untold amounts of data daily -- often without even realizing it. And while we understand and appreciate that the proliferation of data has become essential to a 21st century economy and can, in many ways, be greatly beneficial – that proliferation poses a tremendous risk to consumers. Too often our sensitive personal information, often through no fault of our own, falls into the hands of nefarious actors. And too often, large companies and corporations buy, sell and transmit our information with much too little regard for the safety and security of individual consumers – consumers who often lack the tools or information to protect themselves.

We believe it's incumbent upon our elected officials to pursue policies that give consumers better security in the digital space, more information about who has their data and what they are using it for, and recourse when that data is misused.

To that end we'd like offer recommendations on policies in three different areas we believe this group and, subsequently the legislature, should explore. These include:

- Improvements to the data broker legislation passed this year
- An expansion of data security protections beyond the data broker industry; including the enactment of broadband privacy rules
- An inward look at how the Vermont state government itself deals with Vermonters' data

Improvements to data broker law (Act 171)

VPIRG believes the data broker law enacted last year was an important and useful step in bringing some transparency to an industry that is very opaque. Much of that law has not been implemented, and we do believe it should be given time to work, and consumers and advocates alike should look at the new information this law will yield before moving forward with any major overhauls or additions. That said, we do believe there are three discrete items that policymakers should consider in the short term:

1. We support the requirement that data brokers adhere to a credentialing program to ensure that when Vermonters information is sold, data brokers have worked to confirm the trustworthiness of the buyers. Upon passage of the data broker law, many of our supporters asked us, will this

prevent data brokers from selling information to nefarious actors – and the unfortunate answer is no. While the law that was enacted does many positive things – the lack of a credentialing requirement is, we believe, an oversight. Many industry representatives testified that credentialing is already a best practice in the industry. By making it a requirement, the state can actually offer safe harbor for these good actors, while actually gaining a tool to go after those who would sell Vermonters' information to anyone, no questions asked.

2. We would recommend requiring direct consumer notification of data broker security breaches. The compromise that was reached in last year's legislation removed the notification requirement. We believe this to be a disservice to consumers who will need to consult the data broker registry annually to learn of possible security breaches – in some cases months after they occurred. And under current law, consumers will have no way of knowing if they were specifically impacted by the breach. Because consumers do not have a direct relationship with data brokers – we believe direct notice from these companies is of paramount importance.
3. Finally, we believe that legislators should move forward with requiring credit report agencies to provide so-called "one-stop" credit security freezes. As we've testified before, security freezes represent the best tool consumers have to protect themselves from identity theft when a breach (like the one that occurred at Equifax in 2017) occurs. Vermont took a big step forward this year by eliminating the fees for these freezes. But the process for freezing and thawing one's credit still remains arduous and likely contributes to the low number of individuals we see taking this option. The major credit reporting agencies already have a system in place to notify one another when a consumer places a fraud alert on their credit. We see no reason why they could not extend this system to cover security freezes as well.

Expansion beyond data broker industry:

VPIRG supports Vermont moving forward with any number of measures beyond regulations specific to the data broker industry that would give consumers more information and more control over their personal data. Specifically, we would support:

Expanding the so-called "Massachusetts" security standard contained in the data broker law to cover a wider range of actors. We recognize and agreed with the argument that requiring data brokers to adhere to a minimum data security standard was sensible – they do, after all, make their business trading in data and do so without any direct connection to consumers. Asking that they adhere to reasonable data security practices is sensible. However, it's not incorrect to point out that any business or organization that collects data should be doing their best to protect that data. This is especially true of entities that deal with "Personally Identifiable Information" – which is what the Massachusetts standard deals with. We recognize that if the state were to expand this standard to a wider range of actors it could and would sweep up entities that have less resources and know-how when it comes to data security. That's why we believe any expansion of the standard should be coupled with the state offering resources and trainings to businesses and organizations that would be subject to the standard. The fact is neither Vermont consumers nor our local businesses *want* to suffer a data breach. But many smaller businesses lack the information and resources to ensure they're doing what they can to protect sensitive information – leaving them particularly vulnerable to attacks. We believe the state should be more pro-active in being that resource.

We also support the adoption of broadband privacy regulations in line with the rules issued by the FCC in October 2016. Those rules would have required internet service providers to obtain an opt-in from consumers before having permission to sell their data to third parties. Those rules never went into effect, however, as Congress and President Trump used the Congressional Review Act to stop them in their tracks. That means it's up to states to move forward with commonsense measures to put consumers back in control over who can and cannot sell their data.

There seems to be an open question as whether states have the authority to act on this. This is a critical question to be sure – and while VPIRG has not conducted specific legal research into this matter, we support and second the arguments advanced by other privacy advocacy organizations – including some testifying today. There can be no federal pre-emption in this case, because the federal government has not actually moved to act in this area. Internet service providers are able to pinpoint their customers, meaning they should have no problem offering state level protections. And finally, this would clearly fall in the realm of consumer protection where states have historically had broad authority to take action.

Getting Vermont's Own House in Order:

Finally we would support several proposed initiatives that would help the state of Vermont get its own house in order as it pertains to Vermonters' data.

We believe that there should be minimal circumstances under which the state would be justified in selling Vermonters' data. We recognize that there may be some legitimate economic rationale or public safety reasons for doing so – but right now there appears to be very limited requirements that the state safeguard or at least get opt-ins from Vermonters before selling their data.

In preparing these comments, we found it difficult to understand exactly what information the state does and does not sell – thus making it difficult to recommend specific policy prescriptions in this area.

Because of this we would recommend, as a start, that the state provide a full and publicly accessible accounting of the data it currently sells, its justification for doing so, and what other data is potentially available even if it isn't currently being sold. Doing so would give consumers, advocacy organizations and policymakers more information and inform what, if any, steps the state should take to rein in the proliferation of Vermonters' data.

A Chief Privacy Officer (something that has been suggested) could lead such an effort. As such, we would support the creation of that office – provided it was given adequate resources.

Finally, one other recommendation we would make internal to Vermont government that falls more on the enforcement side would be the creation of a privacy division within the Attorney General's office. While we would be inclined to leave the structure of such a division up to the AG – it would be our general recommendation that as Vermont rightfully expands protections for Vermonters in the realm of digital privacy it would only make sense that we expand our chief law enforcement agency's capacity to enforce those protections.

Conclusion

In conclusion, we hope that this group take these comments, along with those of all other stakeholders and experts, to craft recommendations for potential legislative action in 2019. Vermont made important strides in this area in 2018 – but the issue of digital privacy and security as a consumer protection

priority cannot be overstated. We cannot afford to be complacent. This may be a broad and complex issue – and there is no “silver bullet” when it comes to protecting consumers’ data. But there are measurable steps we can and should take in the short term to give Vermonters the security they deserve. Thank you for the opportunity to comment.