Testimony of VPIRG Communications & Technology Director Zachary Tomanelli on Draft Data Privacy Bill

Testimony before the Senate Committee on Economic Development, Housing and General Affairs
February 14, 2019

Introduction

Good morning. My name is Zachary Tomanelli and I am the Communications & Technology Director of VPIRG, the Vermont Public Interest Research Group. For over 45 years, VPIRG has advocated for the public interest in policy debates concerning the environment, health care, consumer protection, and democracy, and so I thank you for this opportunity to share our thoughts on the draft data privacy bill.

VPIRG was very supportive of the data broker law enacted last year which this committee was instrumental in shaping – and we're happy to see that law already providing useful information to consumers.

As this committee knows, the enacted data broker law also required the Attorney General's office to further study the issue of data privacy and make further recommendations on policies the state could adopt to better protect consumers. VPIRG participated in that process – we delivered prepared comments and attended all three hearings on the issue. Several of our members also attended the hearings and hundreds more submitted comments to the AG's office online. Ultimately, we were pleased to see many of our proposals incorporated into the AG's final report, which has served as the basis for the draft legislation you're currently considering.

Let me start by saying that VPIRG supports all aspects of the draft legislation being considered today and believes that every component will advance the cause of better protecting Vermonters' personal information, provide more transparency around what actors (including the state) are collecting and selling Vermonters' data and give Vermonters more information and recourse when their information falls into the wrong hands.

I'd like to briefly touch on the various aspects of the proposed legislation and give a little more rationale on our support for the specific sections of this bill, while also highlighting some of the areas where we see room for improvement.

Chief Privacy Officer/State Privacy Audit

During the discussion around the data broker bill last year there seemed to be widespread agreement that the state should be doing all that it can to "get its own house in order" as it pertains to safeguarding Vermonters' personal information. We certainly agree with that sentiment, however, it seems clear that the first step in "getting our house in order" would be to determine how messy the house is.

A privacy audit, overseen by a Chief Privacy Order, would do just that. Heading into the hearings last year, VPIRG was prepared to make recommendations on changes the state could make with regards to

the data it is currently collecting and selling. However, when we set out to research that we found it extremely difficult to determine what data the state actually collects and sells. This opaqueness has led to confusion and, in some cases, the proliferation of unverified anecdotes of the state selling Vermonters' data to all kinds of third parties.

A privacy audit – as prescribed in this legislation – would give consumers, advocacy organizations and policymakers more information and determine what, if any, steps the state should take to rein in the proliferation of Vermonters' data.

Such an effort would be extensive, and this is partially why we would support the creation of a state Chief Privacy Officer. This individual would be ideally suited to oversee such an audit and be a repository of that information moving forward.

At least 8 other states have established Chief Privacy Officers (Arkansas, Indiana, Kentucky, Ohio, South Carolina, Utah, Washington and West Virginia). In these states the CPOs have a variety of functions (we would recommend talking to some of them to understand what they do and what recommendations they would have). In Washington state – the CPO is "rolling out a privacy checklist app for state and local governments with dozens of topics employees can search, such as how to assess the impact of a program on privacy or protect location-tracking data on mobile devices."[1] Their CPO has also taken on a more consumer-facing role, providing a privacy guide for Washingtonians.

As to the question of whether there's a need for a Chief Privacy Officer in Vermont – just this past week we saw that over 200 Vermont municipalities and the Vermont Tax Department has been using outdated software containing flaws that exposed sensitive information including Social Security numbers of Vermonters. Now while it's no guarantee that a Chief Privacy Officer would have caught this, having an individual tasked with ensuring all state agencies are adhering to best privacy practices should increase the likelihood that similar issues are surfaced and rectified.

All that said – we do believe that if this position is created, it should be provided adequate resources to carry out the full breadth of its mission.

Student Online Privacy Protection

VPIRG is very supportive of the student online privacy protections contained in this bill. Since California enacted its SOPIPA law, several other states have followed suit. It's time Vermont bring our laws up to date and extend these commonsense protections to our students.

VPIRG supports extending digital privacy protections to all Vermonters – but recognizes the importance and urgency of extending protections to our most vulnerable populations. This certainly includes our students. When our children are using the latest technology to enhance their learning (as they should), neither they nor their parents should be concerned that doing so will lead to their sensitive personal information falling into the hands of bad actors. Likewise, the information they provide in an educational setting should not be used for advertising purposes. This legislation ensures that won't happen.

[1] https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2018/08/21/more-states-appoint-chief-privacy-officers-to-protect-peoples-data

VPIRG is supportive of the "compromise language" suggested in the latest draft version of the bill – as we believe is does provide additional clarity to the law and gives parents more flexibility in safeguarding their children's personal information.

We would suggest a few improvements that the committee may want to consider – recognizing that the tech industry would not likely look favorably on these additions, and thus would not be likely to support a bill that includes these. Those improvements include:

- Extending these protections to every student -- including pre-k, college and post-graduate students
- Including a private right of action against companies that misuse student data
- Removing the exemption for so-called "general Internet audience websites"

Security Breach Notification Changes

VPIRG supports this bill's expansion of the definition of "Personally Identifiable Information" (the class of information that, if exposed, triggers a breach notification to consumers). This bill would expand that universe of information to include things such as biometric data and user names and passwords. With modern computing methods, nefarious actors are able to commit fraudulent activity with disparate data points. If a hacker gains an individual's name, username and password for a single site – that's enough information to do tremendous damage to that individual. It would stand to reason that if that information is breached, a consumer deserves to know about it. This legislation accomplishes that.

We would recommend going even one step further with regards to usernames and passwords. As currently written, a company would only need to notify consumers if usernames and passwords are lost *in combination* with the individual's name. As companies move to deidentify their databases – it's not beyond the realm of possibility that they could suffer a breach where *only* usernames and passwords are lost -- decoupled from an individuals' name. Usernames and passwords on their own are enough for a bad actor to damage an individual – and as such we'd recommend revising the language so that usernames and passwords on their own constitute "personally identifiable information".

ISP Privacy AKA Broadband Privacy

The original draft of this bill included a section that would have required internet service providers to disclose their privacy policies to customers and receive acknowledgement from the customer that they've read the privacy policy prior to the start of service. While this certainly would be a step toward transparency and greater understanding for consumers, concerns raised that this may simply be yet another long agreement that consumers gloss over and ignore are not unfounded. That's certainly not true of all consumers however, and we would support inclusion of this provision in the bill as small step forward. However, VPIRG would much prefer more robust privacy protections for consumers with regards to internet service providers.

That's why we continue to advocate for the adoption of state-level broadband privacy protections – specifically, 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 monetize their data. 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 consumer advocacy organizations who affirm that 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.

The telecoms have repeatedly expressed their opposition to this and have spent millions of dollars defeating similar proposals in other states. The telecoms assert that these protections aren't necessary because the FTC has enforcement authority. However, the FTC can only act if a telecom violates its own terms of service – and even then, action can only be taken after a consumers' data has been misused. It does little to prevent the misuse in the first place and robs the consumer of essential control.

The telecoms have also asserted that these rules unfairly don't deal with so-called edge providers (Google, Facebook etc.) – while true, the relationship of consumers to ISPs is different to that of edge providers. Consumers can elect to use a search engine that has different privacy policies than Google. They can choose not use a particular social media service. However, individuals in 2019 need reliable internet access – and in many cases they may only have one option. In these cases, the consumer's choice is between allowing an ISP to monetize their data or not having internet access at all.

With that said – while we strongly support the enactment of broadband privacy legislation, we recognize the strong opposition it has drawn from industry and would be cautious of including it in larger legislation, such as this, lest it prevent the enactment of these other proposals where there seems to be broader agreement.

Conclusion

In summary, VPIRG appreciates the Committee's time and attention to this matter, and we broadly support the reforms put forth in this draft legislation. Thank you for the opportunity to present this testimony.