Testimony of VPIRG Consumer Protection Advocate Zachary Tomanelli on H.121 - An Act Relating to Enhancing Consumer Privacy

Testimony before the House Commerce & Economic Development Committee
February 9, 2023

Introduction

Good morning. My name is Zachary Tomanelli and I am the consumer protection advocate for VPIRG, the Vermont Public Interest Research Group. For nearly 50 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 H.121.

Overview

I'll start by noting that VPIRG is broadly supportive of this bill and urges the committee to advance this bill with a favorable recommendation.

Vermont has taken great strides to better protect consumers' sensitive information in recent years through the enactment of our data broker registry law and student online privacy law, among others, but we've stopped short of enacting more comprehensive data privacy legislation that VPIRG thinks is necessary for giving Vermont consumers the broadest protections possible.

Five other states – California, Utah, Colorado, Virginia and Connecticut – have enacted some kind of comprehensive data privacy legislation in recent years. Those laws are not identical, and we think they all have different strengths and weaknesses. Nevertheless, the movement on data privacy reforms in this diverse collection of states demonstrates that this isn't a partisan issue—the idea that consumers should have a reasonable amount of control over their own information transcends party lines.

This legislation is essential for our state to keep up with the rapidly changing data landscape, and provide Vermonters with critical, commonsense data protections.

Why this bill is necessary

VPIRG's support for this legislation is grounded in three essential principles:

- **Consumer privacy is a fundamental right.** We believe that consumers should be able to conduct transactions with businesses under the assumption that any information the consumer provides as a part of that transaction will not be used or shared for purposes inconsistent with the completion of that transaction. This used to be the baseline assumption between consumers and businesses – but the digitization and, importantly, monetization of data has upended this.

- **The proliferation of consumer data can have real tangible harms**. This isn't just about privacy for privacy's sake. The more that data is shared, spread, packaged, sold and analyzed – the greater the risk becomes for that data to be misused or fall into the hands of malicious actors,

exposing consumers to scams, identity theft, unwanted tracking, and discrimination.

- **Our current protections leave significant gaps.** There isn't a comprehensive federal privacy law in the United States. The U.S. takes a sectoral approach to data privacy – which can make it difficult and confusing for consumers to exercise their privacy rights, as they often don't know what information is actually protected or which data collectors are covered by existing data privacy laws. Companies like data brokers, social media platforms, and most websites and apps have no legal requirement to keep consumer data private and secure.

It's VPIRG's position that we should enact policies that treat consumer data privacy as a default and, as much as possible, remove the onus from Vermonters themselves to exercise their privacy rights and place the responsibility on would-be data collectors to respect Vermonters' data privacy. We believe this legislation achieves that in a number of important ways.

Points of emphasis

As I noted – VPIRG is broadly supportive of this bill, so I wanted to highlight a few aspects of the legislation, as drafted, that we think are absolutely essential:

- **Data minimization and limits on secondary sharing**: We're thrilled to see this included in the bill (although do think improvements can be made to the language, more on that below)**.** Nevertheless, a strong data minimization standard is key to moving toward consumer data privacy as a default. Data minimization can limit many of the other problems the bill seeks to solve by removing the incentive and ability of data collectors to collect, store, and share data beyond that which is necessary to provide consumers with the good or service they are seeking.

- **Additional protections regarding data brokers:** VPIRG strongly supported the data broker registry law that was enacted because of the unique nature of the relationship between data brokers and consumers--namely that there isn't one. Consumers do not interact directly with data brokers and therefore already have much less knowledge about and control over the information a data broker may have on them. As such, requiring data brokers to report the breach of brokered personal information, provide an opt-out, and perform adequate credentialing of their potential clients seems reasonable and necessary.

- **Private right of action for biometric data violations:** We support all of the biometric data protections enumerated in the legislation. Unlike other personal identifiers such as usernames, passwords, addresses, account numbers, etc., biometric data is generally immutable. As such, it deserves to be treated with particular care and laws—such as the proposed legislation—that provide consumers with clear notice when their biometric data is being collected and require affirmative consent for the collection and use of that data—provide essential protections for this sensitive information. However, we've seen time and again that privacy laws require robust enforcement to be maximally effective. The inclusion of a private right of action ensures robust enforcement of the law. We know that the resources of the Attorney General's office are not limitless. They may only be able to bring action for a handful of violations over the course of a year. Private rights of action ensure compliance and provide ordinary tech users recourse when their privacy rights have been violated.

Areas for improvement

VPIRG supports this bill and believes that, if enacted, it would put Vermont at the forefront of privacy protections for consumers nationwide. We do offer, for the committee's consideration, these possible improvements to the bill:

1. **Stronger, clearer data minimization language:** The data minimization language contained in this bill mirrors that in the California Privacy Rights Act. While we understand the desire to conform with the existing language of another state statute, we believe this language could be stronger. Take the language as drafted:

   Data minimization. A data collector's collection, use, retention, and sharing of personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed or for another disclosed purpose that is compatible with the context in which the personal information was collected and not further processed in a manner that is incompatible with those purposes.

   The intent of the standard, as we understand it, is to limit data collectors from collecting, using, retaining, and sharing data that is unnecessary or unrelated to the good, service, or purpose that the consumer is seeking. However, the language here is ambiguous regarding *whose* purposes the data usage must serve for it to be permissible. We believe it should be clear that it is the purpose *as the consumer understands it*.

   Further, we worry that the allowance for "another disclosed purpose" incentivizes data collectors to merely enumerate all the "purposes" for which they intend to use the collected data in a long, unwieldly disclosure that they know the consumer won't read.

   We offer, for the committee's consideration, language from Consumer Reports model state privacy legislation[1], which lays out an unambiguous data minimization standard:

   Data minimization and opt out of first party advertising.

   (a) A business that collects a consumer's personal information shall limit its collection and sharing of that information with third parties to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or is reasonably necessary for security or fraud prevention. Monetization of personal information shall not be considered reasonably necessary to provide a service or conduct an activity that a consumer has requested or reasonably necessary for security or fraud prevention.

   (b) A business that collects a consumer's personal information shall limit its use and retention of that information to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or a related operational purpose, provided that

[1] Source: Consumer Reports Model State Privacy Act. https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf

data collected or retained solely for security or fraud prevention may not be used for operational purposes.

(c) A consumer shall have the right, at any time, to direct a business that uses personal information about the consumer to personalize advertising not to use the consumer's personal information to personalize advertising, and the business shall have the duty to comply with the request, promptly and free of charge, pursuant to regulations developed by the Attorney General. A business that uses a consumer's personal information to personalize advertising shall provide notice that consumers have the "right to opt out" of the use of their personal information to personalize advertising.

2. Add a prohibition on dark patterns: Dark pattern user design has become a real issue as companies seek to subvert consumer intent and effectively coerce consumers – through deceptive design – into opting into a variety of agreements. This is commonly used to get consumers to agree to data sharing that might otherwise be prohibited. The aforementioned draft state privacy legislation provides suggested language for such a prohibition:

Prohibition of dark patterns.

(a) It shall be unlawful for any company to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice, as further defined by regulation.

3. Add an explicit private right of action for violations of the data minimization standard. As we previously noted with respect to biometric data protections – privacy protections require strong enforcement. Including a private right of action for data minimization violations will ensure compliance with the standard.

Conclusion

In summary, VPIRG appreciates the Committee's time and attention to this matter, and we broadly support the proposed legislation, noting those areas for further consideration. We urge you to advance this bill. Thank you for the opportunity to present this testimony.