ConsumersUnion®

THE ADVOCACY DIVISION OF CONSUMER REPORTS

August 6, 2018

Office of the Vermont Attorney General T.J. Donovan
Attn: My-Lanh Graves
109 State Street
Montpelier, VT 05609

***Re: First Hearing on Protecting the Privacy of Vermonters***

Consumers Union (CU), the advocacy division of Consumer Reports,[1] writes to respond to the Vermont Attorney General's request for comment in advance of the August 6, 2018 hearing on protecting the privacy of Vermonters.

**Adoption of regulations concerning telecommunications privacy and whether to model such rules after the FCC's 2016 Privacy Order, WC Docket No. 16-106, FCC 16-148, adopted Oct. 27, 2016. The request for this recommendation was made in Act 66 of 2017.**

First, Consumers Union strongly encourages the adoption of privacy and security rules governing broadband internet service providers (ISPs). Because of their unique relationship with consumers and the comprehensive—and currently unavoidable—nature of their data collection, ISPs merit dedicated rules to limit their collection and use of customer internet behavioral data for advertising and related purposes.

More broadly however, Consumers Union supports the creation of baseline privacy and security protections that would govern how consumer data is collected and used, no matter the point of collection. Edge providers,[2] connected device manufacturers, and telecommunications service providers like ISPs all have duties to respect consumer privacy and data security rights. As we note below, consumers deserve the right to make easy and informed decisions about the

[1] Consumer Reports is the world's largest independent product-testing organization. It conducts its policy and mobilization work in the areas of telecommunications reform, as well as financial services reform, food and product safety, health care reform, and other areas. Using its dozens of labs, auto test center, and survey research department, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

[2] "Edge provider" is a term used to describe "any individual or entity that provides any content, application, or service over the Internet, and any individual or entity that provides a device used for accessing any content, application, or service over the Internet." David Post, *Does the FCC Really Not Get It About the Internet?*, WASH. POST (Oct. 31, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/10/31/does-the-fcc-really-not-get-it-about-the-internet/?utm_term=.6da16a410bca.

collection, use, and retention of their data.[3] In addition, companies that collect and maintain personal information should put in place basic protections that ensure that attackers cannot access it.[4] Consumers should be able to know what data companies maintain about them: access rights are a fundamental part of privacy laws in Europe and elsewhere, and should be in the US as well. US consumers also need a strong enforcement agency to ensure accountability.[5] While we acknowledge that it is more difficult for states to regulate edge providers, like Facebook and Google, than it is for states to regulate ISPs given uncertainty around where individuals reside, states can still lead in this space. For instance, the California Consumer Privacy Act[6] recently became law and provides extensive new protections for consumers.

For more guidance on legislation, see below:

(A) Whether any proposed rules should be modeled after the Federal Communications Commission's 2016 Privacy Order, WC Docket No. 16-106, FCC 16-148, adopted October 27, 2016 and released November 2, 2016.

Because of the repeal of the Federal Communications Commission's (FCC) broadband privacy rules, consumers' online communications are afforded less privacy protection than traditional telephonic or paper communications. Therefore, it is vital that states pass broadband privacy legislation to protect their residents.

Broadband privacy protections are necessary because individuals depend on the internet, ISPs have a unique and all-encompassing view of consumer data through their online gatekeeper role, and consumers greatly value their privacy,[7] yet lack agency to effectuate their preferences due to a non-competitive ISP marketplace.[8] Since the federal government is not acting on the issue of broadband privacy (and there is no issue of preemption of state action), we encourage state and

[3] Consumers Union, *Where We Stand: Congress Should Pass a Strong Privacy Law, Now*, CONSUMER REPORTS (Apr. 9, 2018), https://www.consumerreports.org/privacy/its-time-for-congress-to-pass-a-strong-privacy-law/.
[4] *Id*.
[5] *Id*.
[6] *AB-375*, CALIF. STATE LEGISLATURE, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (last visited July 30, 2018).
[7] A recent survey from Consumer Reports found that 92 percent of Americans think companies should have to get permission before sharing or selling users' online data.# *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.
[8] Most consumers only have a choice of one or two high-speed broadband providers. Forty percent of all Americans are limited to one ISP. (Liza Gonzalez, *Net Neutrality Repeal Fact Sheets*, INST. FOR LOCAL SELF-RELIANCE (Dec. 21, 2017), https://ilsr.org/net-neutrality-repeal-fact-sheets-by-the-numbers-maps-and-data/.) The majority of the US broadband market is controlled by two providers: Comcast and Charter. (John Bergamayer, *We Need Title II Protections in the Uncompetitive Broadband Market*, PUBLIC KNOWLEDGE (Apr. 26, 2017), https://www.publicknowledge.org/news-blog/blogs/we-need-title-ii-protections-in-the-uncompetitive-broadband-market.) The market for wireless internet service, which is already not very competitive particularly in rural areas, may even shrink from four to three available providers. (*Id*.) This lack of competition means that consumers cannot necessarily avoid one ISP's data policies simply by switching service providers.

local action on broadband privacy to protect their residents. Finally, we include our specific recommendations for a state broadband privacy law.

*The Unique Role of ISPs.*

An ISP has an intimate, all-encompassing window into its customers' behavior because they provide internet service that gives them access to a vast amount of data from and about their consumers. While it may be possible for some consumers to take action to reduce their privacy risks once they are online, they have no choice but to use an ISP to access the internet and thus to subject all of their online data to unfettered access by the ISP. And consumers often have no choice over which ISP to use. All of an individual's traffic flows over that internet connection, traffic which can convey very personal information such as personal banking details, presence at home, sexual preference, physical ailments, physical location, race or nationality, and religion.[9] Even when traffic is encrypted, ISPs still know the sites and services their customers use.

With such comprehensive data, ISPs can create intricately detailed profiles of their customers to sell for a variety of purposes, including targeted digital advertisements for products like payday loans or expensive and unnecessary medications. Consumers should have control over whether their ISP monetizes the data it collects to provide internet service. In addition, consumers desire the protections the FCC rules would have provided.[10] For these reasons, we encourage state and local governments to reinstate broadband privacy rules for their residents in order to protect their privacy and security.

*Repeal of the FCC's Broadband Privacy Rules.*

In October 2016, the FCC passed rules to protect consumers' broadband privacy. These rules required ISPs to obtain their customers' affirmative consent before using and disclosing their web browsing history, application usage data, and other sensitive information for marketing purposes and with third parties. In addition, under the rules, ISPs were required to be transparent about their privacy practices in a simple and comprehensible way. The rules also created a breach notification regime that would have required ISPs to inform their customers when their information has been accessed by unauthorized parties and could cause harm.[11]

---

[9] *See What ISPs Can See*, UPTURN (Mar. 2016), https://www.teamupturn.com/reports/2016/what-isps-can-see.

[10] Recent research from Forrester shows that consumers in the US and Europe are increasingly concerned about how their data is being used online. (Greg Sterling, *Survey: Chasm Exists Between Brands and Consumers on Data Privacy*, MARTECH (Apr. 6, 2018), https://martechtoday.com/survey-chasm-exists-between-brands-and-consumers-on-data-privacy-213646.) This concern has resulted in individuals trusting fewer brands. (*Id.*) Additionally, 61 percent of US adults expressed concern about the sharing of their data or online behaviors between companies. (*Id.*) And an increasing number of consumers (33 percent) block ads when online and use browser do-not-track settings (25 percent). (*Id.*) Despite these tools, the majority of consumers (61 percent) would like to do more to protect their privacy. (Lee Raine, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RESEARCH CTR. (Mar. 27, 2018), http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.)

[11] Historically, ISPs had not used subscriber data for advertising purposes, but in recent years many of the large ISPs began to build the capacity to monetize personal user data. Matt Keiser, *For Telecoms, The Adtech Opportunity is*

Despite consumers' desire for these protections,[12] in March 2017, the US Congress voted to repeal the rules with a resolution of disapproval under the Congressional Review Act (CRA)—thereby preventing the FCC from ever passing a rule in "substantially the same form" in the future.[13]

*No Federal Preemption of State Action on Broadband Privacy.*

The federal government can only preempt[14] a state law or regulation when there is a federal law or regulation on the issue. Due to the repeal of the FCC's broadband privacy rules, there is no federal authority that is acting, or can act, to enact rules to limit ISP surveillance of customer communications for marketing or other commercial purposes. Nor is there a rule at the federal level regulating broadband privacy. In the wake of this repeal, 24 states and the District of Columbia have introduced legislation concerning residents' online privacy.[15] In addition, at least 19 states and the District of Columbia have introduced or are considering legislation reinstating some or all of the protections contained within the FCC rules.[16] Two states have passed legislation that requires ISPs to protect some private information about consumers and one state, Minnesota, also requires ISPs to get permission from customers before disclosing browsing information.[17]

Modern courts have generally applied a presumption against preemption, especially in regulatory areas ordinarily left to the states. Courts have declined to find state law preempted unless a federal statute provides a "clear statement" that state law is to be preempted.[18] In this case there is no federal rules regulating consumer broadband privacy, let alone clear statements providing express preemptive language, so there is no threat of federal preemption on state consumer

---

*Massive*, eMARKETER (Jan. 18, 2017), https://www.emarketer.com/Article/Telecoms-Ad-Tech-Opportunity-Massive/1015052; *see*, Anthony Ha, *Verizon Reportedly Closes in on a Yahoo Acquisition with a $250M Discount*, TECHCRUNCH (Feb. 15 2017), https://beta.techcrunch.com/2017/02/15/verizon-yahoo-250-million/.

[12] Consumers' privacy concerns have translated into a desire for stronger laws to help them protect their privacy while online: two-thirds of Americans say that current laws are not good enough in protecting their privacy and the majority of consumers (64 percent) support more regulation of advertisers. *Americans' Complicated Feelings*, *supra* note 10.

[13] 5 U.S.C. § 801(b)(2).

[14] By way of background, legal preemption occurs when, by legislative or regulatory action, a "higher" level of government (in this case, federal) eliminates or reduces the authority of a "lower" level (e.g., state) over a given issue.

[15] *Privacy Legislation Related to Internet Service Providers*, NAT'L CONF. OF STATE LEGISLATURES (May 8 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers-2018.aspx.

[16] *Id.*; James K. Wilcox, *States Push Their Own Internet Privacy Rules*, CONSUMER REPORTS (Apr. 20, 2017), https://www.consumerreports.org/privacy/states-push-their-own-internet-privacy-rules/.

[17] "Nevada and Minnesota require internet service providers (ISPs) to keep private certain information concerning their customers, unless the customer gives permission to disclose the information. Both states prohibit disclosure of personally identifying information…" *Privacy Legislation*, *supra* note 15.

[18] *See*, *e.g.*, *Rice v, Santa Fe Elevator Corp.*, 331 U.S. 218, 230 (1947); *Tennessee, v. Federal Communications Com'n*, 832 F.3d 597 (6th Cir. 2016); *Nixon v. Missouri Municipal League,* 541 U.S. 125 (2004).

privacy laws.

In addition, states have a lot of authority over the ISPs that operate within their borders.[19] In addition, ISPs are already equipped to implement state-specific privacy protections given that they know the precise location of all their customers. The cost to implement this change would also be very small, and thus will not burden interstate commerce, because it should only require modest coding changes. Due to the fact that most, if not all, ISPs provide opt-outs allowing users to effectuate their data privacy preferences, all a privacy rule would require is that the company sets the default for residents of a state to be the more privacy protective one (i.e., essentially changing their opt-outs to opt-ins).[20] And for critical protections not already covered by their opt-outs the it is not unreasonable for these companies to bear a small cost for added software changes to ensure the protection of Vermont residents.

*Specific Elements of a State Broadband Privacy Proposal.*

State legislators have started drafting proposals for reinstating the broadband privacy protections contained in the now-repealed FCC broadband privacy rules in order to adequately protect and secure their residents' online privacy. Many of the state proposals are strong and closely align to the FCC's rule and the recently-published model state legislation[21] authored by New America's Open Technology Institute and supported by a coalition of consumer and public interest organizations, including Consumers Union. This model legislation does, and any other approach to state broadband privacy law should, at a minimum, include:

- **Data practice transparency.** In order for consumers to make decisions about their data, they need to be informed of ISPs' data practices. Each provider should be required to disclose the types of personal information it collects about its users, how that information is used, and how long the company retains the data. In addition, the ISP should reveal the circumstances under which it discloses, sells, or permits access to personal customer information. The consumer should also know what categories of entities the company discloses, shares, or permits access to this information and the purposes for which each category of entity will use that information. Consumers must also have a clear statement from the company regarding the consumer's right to consent with regard to the use of, disclosure of, sale of, or access to their personal information and how that right may be exercised.

---

[19] Since ISPs are companies that operate in and seek business with a state, states have broad purview over these companies. For instance, in Vermont, the Public Service Board has jurisdiction over ISPs.

[20] Libby Watson, *Want to Stop Your Internet Service Provider from Selling Your Browsing Data? It Ain't Easy*, GIZMODO (Apr. 7, 2017), https://gizmodo.com/want-to-stop-your-internet-provider-from-selling-your-b-1793902371.

[21] *Open Technology Institute Publishes Model State Legislation for Broadband Privacy*, OPEN TECH. INST. (Oct. 30, 2017), https://www.newamerica.org/oti/press-releases/open-technology-institute-publishes-model-state-legislation-broadband-privacy/.

- **Comprehensive definition of personal data.** The scope of personal information that should be protected as private and subject to opt-in consent for use, disclosure, sale, or access should include such identifiers as name and billing information and government-issued identifiers, but also any information that the ISP has access to by virtue of their role as a gatekeeper to the internet such as unique device identifiers, internet addresses, browsing information, and app usage. Although it is permissible to exclude aggregated data from "personal information," we caution against excluding de-identified browsing data from this definition since it is hard to render such data unidentifiable.[22] The definition of personal information should be broad enough to include any information concerning a customer that is collected or made available and is maintained in a way that the information is linked or reasonably linkable to a customer or device.
- **Separate, opt-in consent for most secondary usage or transfer of data.** Consumers are less aware and less able to control what secondary usage is made of their data that the company has collected about the consumer by providing internet access. Consumers should have a dedicated prompt requiring opt-in approval for secondary use or transfer of their data, including for advertising, marketing, and research purposes. Some bills have only sought to limit the sale or transfer of data, but protections should apply even if the data never leaves the ISP—consumers still do not expect their service provider to surveil their online traffic to target ads or for vague research purposes.
- **ISPs cannot discriminate against users who opt out.** Americans depend on home and mobile internet service for daily tasks. Privacy should not be a luxury good, and any service plan that charges users more for making privacy-conscious choices will disproportionately affect lower income households. Pay-for-privacy schemes are especially pernicious in the broadband industry because (1) the marketplace is uncompetitive, (2) ISPs have an all-encompassing and unique view of all of a user's activities online, and (3) consumers depend on and need broadband internet access to perform daily tasks. Accordingly, broadband providers should be prohibited from denying or providing worse service to customers or applicants who do not opt-in to the use of their data, including charging them higher prices or offering inferior products or service.
- **Reasonable exceptions for operational use.** The general prohibition on secondary usage without consent should include thoughtful exceptions allowing collection and use of consumer data for reasonable operational purposes. Thus, a provider should be able to use or disclose consumer personal information without consumer approval for the purpose of delivering its services, to comply with legal processes or other legal orders, and to initiate, render, bill for, and collect payment for the service. A legislative proposal should also allow the use of customer information for security and fraud prevention, and to improve network performance, but such collection and use should be limited and

[22] Kevah Waddell, *Your Browsing History Alone Can Give Away Your Identity*, THE ATLANTIC (Feb. 6, 2017), https://www.theatlantic.com/technology/archive/2017/02/browsing-history-identity/515763/.

proportionate—an ISP should not collect and store all possible data in perpetuity simply because it might theoretically have some value in the future. However, a bill should not allow for broad exceptions for measurement, product improvement, or research. If an ISP wants a customer's data for those purposes, it should ask and receive permission first.

- **Reasonable data security.** ISPs should be required to implement and maintain reasonable measures to protect consumer personal information from unauthorized use, disclosure, sale, access, destruction, or modification. Reasonable security measures means that the measures are informed by the nature and scope of the ISP's activities, the sensitivity of the data it collects, the size of the ISP, and the technical feasibility of the measures.
- **Reasonable data minimization.** The ISP shall not retain consumer personal information for longer than reasonably necessary to accomplish the purposes for which the information was collected. Data minimization also decreases the amount of consumer information that is vulnerable to a future breach, and thus is part of reasonable data security practices.
- **Reasonable data breach notification.** In the case of a breach of consumer personal information, ISPs should notify affected customers, the state body charged with supervision of telecommunications service providers, and law enforcement unless the provider is able to reasonably determine that a data breach is unlikely to pose a risk of harm to the affected customers. The notice should detail what kind of information was breached. The ISP should notify state and local authorities within seven business days of when the provider reasonably determines that a breach has occurred if the breach impacts 5,000 or more customers. ISPs must provide notice to affected customers without unreasonable delay, but within no more than 30 days.
- **Robust enforcement.** Under the applicable state laws and regulations, the provisions in the broadband privacy legislation should be subject to robust enforcement in order to ensure that residents are sufficiently protected and their choices regarding the collection and use of their data are respected. The penalties to the ISP for failing to meet the requirements of the broadband privacy legislation must be clear and meaningful. In addition to enforcement by a state attorney general—and potentially local enforcers as well—we encourage the implementation of a private right of action so ISPs are sufficiently incentivized to protect consumer privacy.

(B) Whether any rules should include: (i) disclosure requirements pertaining to a provider's privacy policies;[23]

Unfortunately, privacy policies are an ineffective method of providing information directly to consumers. Because the law does not clearly mandate specific disclosures, and because most

[23] *Act 66 of 2017*, 9 V.S.A. § 264, *available at* https://legislature.vermont.gov/assets/Documents/2018/Docs/ACTS/ACT066/ACT066%20As%20Enacted.pdf.

Federal Trade Commission (FTC) privacy cases are predicated upon a specific misstatement in a privacy policy or elsewhere, privacy policies tend to be vague and expansive. But even if they were more precise, it would not be efficient for consumers to read them: a study by Aleecia McDonald and Lorrie Cranor estimated that reading every site's privacy policy would take users over 244 hours per year, at a collective societal cost in wasted opportunity of over $600 billion.[24]

However, we do think privacy policies have a role to play. A privacy law should require companies to provide more detailed information about their actual practices within their privacy policies—not for consumers, but for regulators, journalists, civil society, and ratings services such as Consumer Reports. As such, privacy policies would function more like financial filings, which are important accountability documents, and which are not necessarily read by ordinary investors, but which are processed by intermediaries to convey meaningful information to the marketplace.

(ii) opt-in or opt-out procedures for obtaining customer approval to use and share sensitive or nonsensitive customer proprietary information, respectively;[25]

Even with improved transparency, a privacy law should not place all the burden on individuals to manage the collection and sharing of their personal information. As evidenced by the use of coercive "dark patterns"[26] in response to the European Union's General Data Protection Regulation (GDPR) to manipulate users into broadly agreeing to a wide swath of opaque behaviors, even mandating consent can be abused.[27] Consumers Union supports the prohibition of some broadly unacceptable behaviors—or the requirement that companies obtain the user's affirmative direction in order for the company to use an individual's data for some purposes (as opposed to merely clicking "OK" to a consent box). For practices that are conducted on an opt-out basis, users need powerful, industry-wide opt-outs that let them make easy and manageable choices (such as "Do Not Call" or "Do Not Track"). Today's privacy framework in the US puts too much burden on individuals to try to understand and control an increasingly complex and undecipherable array of behaviors.

(iii) data security and data breach notification requirements.[28]

Consumers Union generally supports reasonable data and cybersecurity requirements. For suggestions on data breach notification requirements please refer to the section below entitled:

---

[24] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, J. OF LAW & POLICY FOR THE INFO. SOCIETY (2008), https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf.
[25] *Act 66 of 2017*, *supra* note 23.
[26] *See*, Dan Schlosser, *LinkedIn Dark Patterns*, MEDIUM (June 5, 2015), https://medium.com/@danrschlosser/linkedin-dark-patterns-3ae726fe1462.
[27] *Deceived by Design*, NORWEGIAN CONSUMER COUNCIL (June 27, 2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf; *and see*, Allen St. John, *CR Researchers Find Facebook Privacy Settings Maximize Data Collection*, CONSUMER REPORTS (June 27, 2018), https://www.consumerreports.org/privacy/cr-researchers-find-facebook-privacy-settings-maximize-data-collection/.
[28] *Act 66 of 2017*, *supra* note 23.

"Changes that should be made to Vermont's Security Breach Notice Act, 9 V.S.A. § 2435."

(C) Proposed courses of action that balance the benefits to society that the telecommunications industry brings with actual and potential harms the industry may pose to consumers.[29]

Unfortunately, the scale is already tipped in favor of the ISPs. The majority of the US broadband market is controlled by two providers: Comcast and Charter.[30] Most consumers only have a choice of one or two high-speed broadband providers and 48 percent of all Americans are limited to one ISP.[31] This is especially true for the rural market: 68 million rural Americans are served by one of two companies (Charter or Comcast).[32] This lack of competition means that consumers cannot necessarily avoid ISP data policies simply by switching service providers. Historically, ISPs did not surveil user behavior for advertising and related purposes; it was to forestall this emerging model that the FCC passed their broadband privacy rules in October of 2016. Consumers already pay hundreds of dollars a month to their ISPs; they do not expect those service providers to monetize the very personal information contained in their internet traffic. Therefore, we support states reinstating broadband privacy protections for consumers in order to help alleviate this unbalanced relationship between consumers and their internet provider.

For connected devices and services, in many (though not all) instances, there are more choices, but consumers lack the ability to evaluate these services and products on the basis of privacy and security. In either case, more protections in this market would benefit consumers by giving them more power in the marketplace and discouraging bad actors from entering the industry.

**Whether Vermont should designate a Chief Privacy Officer, and what the responsibilities of that Officer would be. This request was made in Act 171 of 2018.**

Due to the amount of sensitive personal data that the State of Vermont is tasked with safeguarding, it is in the state's best interest to designate a Chief Privacy Officer. Many US companies now employ a Chief Privacy Officer either to comply with privacy regulations or to ensure that the company's data is sufficiently secured. As the Vermont state government is responsible for securing the personal data of over 600,000 people, we encourage the state to take reasonable steps to ensure that they protect the sensitive data they process and collect. The Chief Privacy Officer should: (1) help educate government employees about responsible data practices; (2) assess the state's data protection measures; and (3) and help prevent data security incidents like data breaches and ransomware attacks through the implementation of routine security

[29] *Id*.
[30] *We Need Title II Protections*, *supra* note 8.
[31] Liza Gonzalez, *Net Neutrality Repeal Fact Sheets*, INST. FOR LOCAL SELF-RELIANCE (Dec. 21, 2017), https://ilsr.org/net-neutrality-repeal-fact-sheets-by-the-numbers-maps-and-data/.
[32] Jon Brodkin, *Comcast, Charter Dominate US; Telcos "Abandoned Rural America," Report Says*, ARSTECHNICA (July 31, 2018), https://arstechnica.com/information-technology/2018/07/comcast-or-charter-is-the-only-25mbps-choice-for-68-million-americans/.

patches, periodic updates to the state's systems, and other reasonable data security practices. We also encourage the Chief Privacy Officer to monitor reports by the Multi-State Information Sharing & Analysis Center, an organization that works to improve cybersecurity for state and local governments.[33]

**Whether to regulate businesses that handle the data of consumers with whom they have a direct relationship, as requested in Act 171.**

As we discuss above, Consumers Union believes there should be stronger privacy rules for all companies that manage consumer data, regardless of their direct or indirect connection to an individual consumer. Different rules may apply depending on the nature of a company's relationship with a consumer, and we are glad to see Vermont require more transparency disclosures from data brokers given the somewhat shadowy role they play. However, although consumers are given more disclosures about data broker activity in Vermont, the law does not enact any substantive limitation on data sharing, or give consumers any way to exercise their data privacy preferences.

First-party companies that handle consumer data should have greater transparency obligations. And consumers should, at the very least, be able to opt out of sharing of their data by companies they interact with. However, consumers also need a way to effectuate their data preferences in a way that is scalable: consumers should not be tasked with the time-intensive process of constantly ensuring that they have opted out of data sharing that they do not approve of. Although companies should make opt-outs easily available to consumers, this is not always the case. Companies commonly bury opt-outs in order to discourage consumers from exercising control of their personal data. If companies were required to be more transparent about their data practices, consumers would have the necessary information to choose to engage with the company that will best protect their data and privacy.

**Questions, concerns, and recommendations regarding the implementation of the Data Broker Registry, as authorized in Act 171.**

Though more needs to be done to control data brokers, we hope that the new law requiring them to register with the state will help bring them out of the shadows. Some data brokers, such as Acxiom and Intelius, collect personal details such as consumers' behavior online, income, and addresses, which are used for marketing purposes and potentially for other purposes, including lending decisions.[34] Data brokers also typically evade the accuracy and transparency requirements placed on credit bureaus by the Fair Credit Reporting Act (FCRA). While data

[33] *See*, MULTI-STATE INFO. SHARING & ANALYSIS CTR., https://www.cisecurity.org/ms-isac/ (last visited July 30, 2018).
[34] *Big Data, A Big Disappointment for Scoring Consumer Credit Risk*, NAT'L CONSUMER LAW CTR. (Mar. 2014), 15-16, https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf.

brokers frequently sell information that is used to make employment or other decisions about consumers, many claim not to be credit reporting agencies as defined by the FCRA.[35] Many consumers do not even know which data brokers are collecting information about them, or how to contact them.

We recommend that Vermont take steps to ensure that the law remains focused on regulating data brokers like Acxiom, which collect and sell information about consumers for commercial purposes, and not the news media. The current definition of a data broker could sweep in news-gathering organizations: "a business, or unit or units of business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship."

Vermont may want to look to the newly-passed California Consumer Privacy Act,[36] which avoids this issue by exempting from commercial purposes: "the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism." Without including an exemption, not only could the new law inappropriately hinder the legitimate activities of newspapers and other media, but it could be vulnerable to a First Amendment challenge—leaving consumers with even fewer protections.

**Changes that should be made to Vermont's Security Breach Notice Act, 9 V.S.A. § 2435.**

The dramatic increase in data breaches in recent years highlights the need for a stronger data breach notification law. Every state has passed a data breach notification law, many of which have higher standards than Vermont.[37] Any data breach notification law should adequately cover consumers' sensitive information, and should have strong penalties for failure to comply. To that end, we suggest the following changes to strengthen the Vermont Security Breach Notice Act.

- Expand the definition of PI. It is important that Vermont is able to amend the definition of personal information over time, as technologies and norms evolve. Some states have revised their breach notification rules to include online accounts for email, photo storage, and social media, and Vermont should follow their lead. These types of accounts often include incredibly sensitive information, and consumers should be told if those accounts are compromised. Biometric data, too, should be included in any definition of personal

[35] *Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA*, FED. TRADE COMM'N (June 12, 2012), https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed; *Big Data: A Big Disappointment for Scoring Consumer Credit Risk*, NAT'L CONSUMER LAW CTR. (2014), at 26 *available at* https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf.

[36] *AB-375*, *supra* note 6.

[37] *Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES (Mar. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

information, just as it is included in the new category of personal information created by the data broker bill, "brokered personal information."

- No safe harbor. Vermont law should remain flexible in order to reflect new threats and challenges. As such, we recommend removal of the safe harbor for financial businesses in compliance with the programs issued by the Federal Reserve, the FDIC, the OCC, the Office of Thrift Supervision, and the National Credit Union Administration, as outlined in (f)(1)-(2).
- Enforcement. Strong penalties provide important incentives for companies to maintain strong data security practices. Consumers should have the right to file suit against covered entities who fail to comply with the law, so that they are held accountable in appropriate cases even if state authorities decline to take action.
- Remediation. Businesses that fail to protect consumer data have a responsibility to help consumers cope with the effects of a data breach. We recommend that those required to provide notification in the event of a data breach should also provide a minimum of 12 months of free identity theft protection services to anyone whose personal information was affected to help limit the fallout of any disclosure of information.

**Questions or concerns regarding the State of Vermont's handling of citizen's data.**

As a controller of sensitive data about its residents, the State of Vermont should take steps to prevent against a data breach or a ransomware attack.

Data breaches. When companies, or governments and their agencies, fail to sufficiently protect consumer data, individuals and their data are left vulnerable. Massive data breaches have become commonplace, as companies accumulate vast troves of valuable consumer data but frequently fail to put adequate systems in place to protect it. The Target data breach of 2013 compromised the information of an estimated 110 million people, including the payment card information of about 40 million consumers.[38] Hackers obtained the data of about 80 million people in the Anthem data breach of 2015.[39] And last year, criminals took advantage of well-known vulnerabilities in software used by Equifax to access the Social Security numbers of over 145 million people.[40] Targeted entities often have the opportunity to head off a breach but neglect to take action. For example, the software vulnerabilities that made Equifax a ripe target for

[38] Rachel Abrams, *Target to Pay $18.5 Million to 47 States in Security Breach Settlement*, N.Y. TIMES (May 23, 2017), https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html.
[39] Brendan Pierson, *Anthem to Pay Record $115 Million to Settle U.S. Lawsuits over Data Breach*, REUTERS (Jun. 23, 2017), https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-us-lawsuits-over-data-breach-idUSKBN19E2ML.
[40] *Equifax Announces Cybersecurity Firm Has Concluded Forensic Investigation of Cybersecurity Incident*, EQUIFAX.COM (Oct. 2, 2017), https://www.equifaxsecurity2017.com/2017/10/02/equifax-announces-cybersecurity-firm-concluded-forens ic-investigation-cybersecurity-incident/.

attackers had been public for months, but Equifax failed to address them before the breach.[41]

The failure to protect personal data causes real harm to individuals. Nearly 17 million US consumers fell victim to identity theft in 2017, with total US losses approaching $17 billion.[42] Victims spend precious time and money repairing the damage to their credit and accounts. Medical identity theft, in which thieves use personal information to obtain medical services, exhausts consumers' insurance benefits and leaves them with exorbitant bills. Tax identity theft occurs when thieves use consumers' Social Security numbers to obtain tax refunds. Fraudulent information on credit reports also causes consumers to pay more for a loan or be denied credit. But despite these clear harms, many organizations fail to the requisite measures to protect against these incidents.

Although companies are often subject to data breaches, states and state agencies are also targets and should take measures to protect against data breaches. For instance, in February of 2018, a data breach at the California Department of Fish and Wildlife exposed the names and Social Security numbers of thousands of state workers.[43] Data entrusted to states and their agencies can be exposed through targeted attacks, technical errors, as well as human error: Recently, state governments have received letters, accompanied by malware-laden CDs, sent from China. Krebs on Security released a warning at the end of July to state governments and local agencies about this latest phishing attack;[44] From August 7, 2017 to January 23, 2018, a technical error permitted users to view private data from about 16,500 business taxpayers controlled by the Massachusetts Department of Revenue;[45] And, in 2017, the personal records of 6,000 people were exposed when a North Carolina Department of Health and Human Services employee emailed a spreadsheet containing names, Social Security numbers, and test results in error to a vendor via an unencrypted email.[46] These incidents demonstrate how important for a state to ensure that it is effectively protecting its residents data through employee education and use of reasonable data security practices. We urge the State of Vermont to adequately invest in data

---

[41] Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sep. 14, 2017), https://www.wired.com/story/equifax-breach-no-excuse/.

[42] *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study*, JAVELIN (Apr. 24, 2018), https://www.google.com/url?hl=en&q=https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin&source=gmail&ust=1533316386215000&usg=AFQjCNHG35NLIAox3Tzr9LoEWQjH58LRcw.

[43] Adam Ashton, *Social Security Numbers from Thousands of California State Workers Exposed in Data Breach*, THE SACRAMENTO BEE (Feb. 16, 2018), https://www.sacbee.com/news/politics-government/the-state-worker/article200628124.html.

[44] Brian Krebs, *State Govts. Warned of Malware-Laden CD Sent Via Snail Mail from China*, KREBSONSECURITY (July 27, 2018), https://krebsonsecurity.com/2018/07/state-govts-warned-of-malware-laden-cd-sent-via-snail-mail-from-china/.

[45] Joshua Miller, *Yikes! Data Breach at Mass. Tax Agency Allowed Companies to Peek in on Competitors' Data*, BOSTON GLOBE (Feb. 13, 2018), https://www.bostonglobe.com/business/2018/02/13/yikes-data-breach-mass-tax-agency-allowed-companies-peek-competitors-data/2yMkzh5EO1Pvv3h4Cn7OYK/story.html.

[46] Dan Way, *Are State Agencies Waiting to Disclose Data Breaches?*, CAROLINA JOURNAL (Dec. 11, 2017), https://www.carolinajournal.com/news-article/are-state-agencies-waiting-to-disclose-data-breaches/.

security in order to protect their residents from the harms posed by a data breach.

Ransomware. Large systems can be compromised by a targeted attack through the use of ransomware, a type of malware that prevents users from accessing their system or computer until a ransom is paid. One recent, large-scale attack was the WannaCry ransomware attack in May of 2017. WannaCry, a type of ransomware, infected more than 230,000 computers by exploiting a vulnerability in Windows.[47] This gigantic attack affected Britain's National Health Service as well as companies like FedEx.[48] The WannaCry incident raised awareness of of the threat ransomware poses and the importance of timely software patches to fix known vulnerabilities since the threat of the WannaCry ransomware could have been neutralized if companies patched their systems when the Windows update was available in April of 2017.[49] However, even a year after the release of the patch, many organizations still had not applied it.[50]

Ransomware attacks can also cripple state agencies, cities, and local medical centers and incur millions of dollars of expenses in the process. Following a February 2018 attack on Colorado's Department of Transportation, the state spent between $1 million and $1.5 million recovering from the incident.[51] And, in March of 2018, the city of Atlanta, Georgia was the target of a ransomware attack that crippled the city's services for days.[52] The Erie County Medical Center in Buffalo, New York spent around $10 million responding to a ransomware attack in July of 2017.[53] However, governments and their agencies can avoid some ransomware threats by practicing good cybersecurity practices such as updating software regularly to ensure vulnerabilities are patched in a timely manner.[54]

**Laws and regulations that can be adopted to encourage the growth of privacy-oriented technology companies in Vermont.**

We support the State of Vermont adopting transparency provisions to help create a market for

[47] Danny Palmer, *WannaCry Ransomware Crisis, One Year On: Are We Ready for the Next Global Cyber Attack?*, XDNET (May 11, 2018), https://www.zdnet.com/article/wannacry-ransomware-crisis-one-year-on-are-we-ready-for-the-next-global-cyber-attack/.
[48] *Id*.
[49] *Id*.
[50] *Id*.
[51] Benjamin Freed, *Colorado Has Spent More Than $1 Million Bailing Out From Ransomware Attack*, STATESCOOP (Apr. 10, 2018), https://statescoop.com/colorado-has-spent-more-than-1-million-bailing-out-from-ransomware-attack.
[52] The City of Atlanta spent almost $5 million just to procure emergency IT services. James Rogers, *City of Atlanta Hit by Ransomware Attack*, FOX NEWS (Mar. 22, 2018), http://www.foxnews.com/tech/2018/03/22/city-atlanta-hit-by-ransomware-attack.html.
[53] Henry L. Davis, *ECMC Spent Nearly $10 Million Recovering From Massive Cyberattack*, THE BUFFALO NEWS (July 26, 2017), https://buffalonews.com/2017/07/26/cost-ecmc-ransomware-incident-near-10-million/.
[54] The appointment of a Chief Privacy Officer for the State of Vermont could also help facilitate good data security practices by monitoring state processes and ensuring that employees are educated about phishing attacks and other risks.

technology companies that wish to lead competitively on their privacy and data practices. Consumers need better information and tools to evaluate and compare privacy choices. Without transparency about what data companies collect and how this data is used, individuals will be unable to evaluate similar services and effectuate their data privacy preferences. To that end, Consumer Reports and its partners have developed The Digital Standard,[55] an open standard for testing products for privacy and security in order to help consumers make informed decisions in the marketplace. The testing includes assessments of a company's stated privacy practices in both the user interfaces and in their privacy policies. This effort depends on the transparency that privacy policies and user interfaces provide consumers. In addition, one of the important criteria under our Digital Standard[56] is that the user can see and control everything the company knows about the individual. In order for a company's data practices to be responsible under the Standard, the company must enable the consumer to be able to know to know what user information the company is collecting, the company only requests and collects information that is needed to make the product or service work correctly, and the company explicitly discloses every way in which it uses the individual's data.[57]

The State of Vermont could require similar disclosure requirements of companies that collect residents' data. One example of a state measure that will require more transparency about data collection is the California Consumer Privacy Act.[58] This legislation will give consumers meaningful control over the data sharing that threatens their privacy, subjects them to harmful and irritating solicitations, exposes them to discrimination, and can even cause them to lose out on a job opportunity or get turned down for credit. The Act would require businesses in California to tell consumers what types of information they are collecting about them—in clear, easy-to-understand terms. It also gives consumers an easy way to opt out of data sharing or sales. Importantly, consumers cannot be charged more for refusing to share their data. And, it would hold companies that fail to implement reasonable security practices and procedures responsible in the event of a data breach. The initiative also ensures strong penalties for failure to comply.

**The necessity of any additional approaches to protecting the data security and privacy of Vermont consumers.**

With the increasing enactment of numerous privacy standards around the globe—including the General Data Protection Regulation in the European Union and the California Consumer Privacy

[55] The Digital Standard (theDigitalStandard.org) was launched on March 6th, 2017 and is the result of a collaboration with our cybersecurity partners, Disconnect, Ranking Digital Rights, and the Cyber Independent Testing Lab. The Standard is designed to hold companies accountable and equip Consumer Reports and other organizations to test and rate products for how responsibly they handle our private data. This is a collaborative and open source effort. The Standard is designed to empower consumers to make informed choices about the connected products, apps, and services consumers use everyday.

[56] *The Standard*, THE DIGITAL STANDARD, https://www.thedigitalstandard.org/the-standard.

[57] *Id*.

[58] *AB-375*, CALIF. STATE LEGISLATURE, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (last visited July 30, 2018).

Act here in the US, it is clear that consumers need comprehensive data protection reforms and baseline privacy protections. Consumers deserve the right to make easy and informed decisions about the collection, use, and retention of their data.[59] In addition, companies that collect and maintain personal information should put in place basic protections that ensure that attackers cannot access it.[60] Consumers should be able to know what data companies maintain about them. Access rights are a fundamental part of privacy laws in Europe and elsewhere, and should be in the US as well. We encourage the State of Vermont to act to protect their residents by strengthening current consumer protections and taking steps to help protect residents' privacy.

Thank you for the opportunity to respond to your request for comment on protecting the privacy of Vermonters. For more information on Consumers Union's data security or privacy legislation recommendations please feel free to contact us directly or refer to and our work[61] on privacy and technology issues.

Sincerely,

Katie McInnis
Policy Counsel

Maureen Mahoney
Policy Analyst

Consumers Union
Suite 500
1101 17th Street, NW
Washington, DC 20036

[59] Consumers Union, *Where We Stand: Congress Should Pass a Strong Privacy Law, Now*, CONSUMER REPORTS (Apr. 9, 2018), https://www.consumerreports.org/privacy/its-time-for-congress-to-pass-a-strong-privacy-law/.
[60] *Id*.
[61] *Our Work: Privacy*, CONSUMERS UNION, https://consumersunion.org/topic/phones-media/privacy-2/ (last visited July 31, 2018).