April 12, 2024

Chair Kesha Ram Hinsdale
Vice Chair Alison Clarkson
Committee on Economic Development, Housing and General Affairs
Vermont Senate
115 State St.
Montpelier, VT 05633-5301

Re: Feedback on H. 121 Vermont Consumer Privacy Legislation - Version 1.1 (SED Amendment)

Dear Chair Ram Hinsdale and Vice Chair Clarkson,

Consumer Reports[1] sincerely thanks you for your work to advance consumer privacy in Vermont. As passed unanimously by the House, H. 121 would extend to Vermont consumers critical new privacy protections, including among many others, default limits on business' collection and use of information through a data minimization standard, a universal opt-out provision relating to data brokers, strong civil rights protections, and the right for individuals to seek redress in courts when businesses violate the law.

We write to provide feedback on the committee's recently proposed amendments and to address concerns raised by industry in testimony.

Harms

As an initial matter, it is important to clarify why data privacy is such an important issue for groups like Consumer Reports and why we think it is vital the committee take a strong position with H. 121. Consumers currently possess very limited power to protect their personal information in the digital economy, while businesses operate with virtually no limitations as to how they collect and use that information (so long as they note their behavior somewhere in their privacy policy). This, with frightening regularity, results in concrete harms to consumers and

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

is leading to the erosion of our basic expectation of privacy. Reproductive health apps[2] and hospital websites[3] have been caught sharing users' sensitive health information with large social media platforms –- risking the potential for embarrassment, stigmatization, or even criminalization. Retail stores,[4] websites, and apps track our every move in order to segment us into hyper-granularized marketing categories, using data to make inferences about us or our lifestyles (like that we are "economically anxious elders", "heavy purchasers of pregnancy tests," or "frequently depressed")[5] that are ultimately used to target us with advertisements. Several car manufacturers were recently alleged to be surreptitiously sharing driver information with data brokers who then sold the information to insurance companies that, in some cases, used the information to raise consumers' premiums.[6] Facial recognition companies like Clearview AI have exploited lax privacy standards to amass databases of billions of images that allow any person to instantaneously identify any other person and associate them with other personal details, all with just a single image.[7]

Privacy legislation should be strong enough to disrupt these business practices, as well as the surveillance advertising business model that incentivizes companies (especially large social media companies) to keep users on their services for as long as possible. As the committee is aware from their work on Age Appropriate Design Code legislation, this business model has led to many regrettable outcomes, including the marked increase in sensationalistic or divisive content (which reportedly keeps users more engaged on platforms than other types of content),[8] filter bubbles that limit exposure to alternative perspectives,[9] and the rise of addictive platform design that has proven especially damaging to the well-being of children.[10]

---

[2] Catherine Roberts, These Period Tracker Apps Say They Put Privacy First. Here's What We Found, Consumer Reports, (August 30, 2022), https://www.consumerreports.org/health/health-privacy/period-tracker-apps-privacy-a2278134145/

[3] Todd Feathers, Simon Fondrie-Teitler, Angie Waller, and Surya Mattu, Facebook Is Receiving Sensitive Medical Information from Hospital Websites, The Markup (July 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

[4] Jon Keegan, Forget Milk and Eggs: Supermarkets Are Having a Fire Sale on Data About You, The Markup, (February 16, 2023), https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you

[5] Jon Keegan and Joel Eastwood, From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You, The Markup, (June 8, 2023), https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you

[6] Kashmir Hill, Automakers Are Sharing Consumers' Driving Behavior With Insurance Companies, New York Times, (March 13, 2024), https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html

[7] Kashmir Hill, The Secretive Company That Might End Privacy as We Know It, New York Times, (November 2, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[8] See, e.g., Keach Hagey and Jeff Horwitz, Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead, Wall Street Journal (September 15, 2021), https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215?mod=article_inline

[9] Eliot Pariser, *The filter bubble: What the Internet is hiding from you,* London: Penguin UK, (2011)

[10] Georgia Wells, Jeff Horwitz, and Deepa Seetharaman, Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show, Wall Street Journal, (September 14, 2021),

Strong privacy legislation is about much more than just sticking it to the tech companies or reducing data breaches – it is about our right to an autonomous existence and to take back control over the type of society we want to live in.

Data Minimization

Given these stakes, it was unsurprising to hear during the committee's consideration of H. 121 on April 10 industry stakeholders urge the committee to weaken the existing data minimization framework present in H. 121 (itself already a compromise based on language from CCPA rather than the more restrictive standards present in ADPPA). In its current iteration, H. 121's data minimization standard allows companies to use personal data to provide the services requested by the consumer, for other disclosed purposes so long as they are compatible with the reasonable expectations of the consumer, or for any other purpose so long as the business obtains the consumer's consent.[11] While this would prevent unanticipated uses of data without consent, such as cross-website tracking and profiling, it would preserve the ability of businesses to do traditional first-party marketing practices.

However, industry representatives instead argued that H. 121's data minimization standard would prevent companies from carrying out even the most uncontroversial activities, such as a hotel advertising its restaurant when a consumer reserves a room. But this type of contextual advertising would clearly be aligned with the reasonable expectations of consumers and is explicitly exempted from the definition of targeted advertising (Section 2415 50(B)(II)), which would otherwise require the business to give the consumer an opportunity to opt-out of such advertising. We've also reviewed similar claims from the Retailers and Grocers Association, as well as the same industry representative, who argue that the minimization standard would prevent businesses from advertising to existing customers based on their purchase history (for example, a seasonal bowtie being advertised to a consumer that had previously purchased similar seasonal attire). First-party targeted advertising of this nature would also likely meet the reasonable expectations standard and would also qualify for a *different* exemption from the definition of targeted advertising (Section 2415 50(B)(I)), meaning that businesses would not even be required to honor an opt-out for such uses of data. It is clear that the intent of the bill is not to disrupt these types of business practices.

Private Right of Action

The committee's amendment proposes a number of changes to Section 2427, which provides for the private right of action. The amendment would delay the effective date of the private right of action by one year, would allow businesses 120 days to cure violations (instead of 60), and would bar class action suits. Additionally, the amendment would limit the applicability of the private right of action remedy to only apply to businesses that derive more than half of their

---

https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739?mod=article_inline

[11]H. 121, Section 2419(2).

revenue from the sale of personal data. This last change would essentially limit the private right of action to data brokers or companies that depend on targeted advertising for the majority of their revenue – while ignoring other tech companies, like Amazon, whose primary source of revenue resides elsewhere but nevertheless also operates a massive data collection empire that exposes consumers to a great deal of risk.[12]

If the committee is intent on limiting the private right of action, it should at least tether such limitations to a revenue threshold that ensures the largest, riskiest companies are still liable. The committee could borrow from the recently announced, bipartisan federal American Privacy Rights Act, which defines the term "large data holder", which include entities that had an annual gross revenue of not less than $250,000,000 in the previous calendar year, in addition to several other factors.[13] Furthermore, given such limitations, class actions should be reinstated, as they have proven one of the most effective ways to put a stop to harmful data practices when present in other privacy laws. For example, a landmark settlement under Illinois' BIPA class action remedy prevented further harm from Facebook's illegal collection of consumers' facial templates.[14]

Data Broker Deletion Requests

The committee's amendment proposes a change in Section 2448(a)(2)(A) to mirror language from Section 2418(c)(5)(A) that would allow a data broker to respond to a consumer's deletion request by either "retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's data remains deleted" or "opting the consumer out of the processing of the consumer's data".

This language (pulled from several other state privacy laws) contains a common loophole we've warned other lawmakers about. As written, it is not sufficiently clear that the controller or data broker must actually delete the information in response to the request, even though that seems to be the intent. In both instances where this language appears, Subsection A should begin by clarifying that the controller must actually delete the information first, and *then* simply retain a record of the deletion request so that the information stays deleted.

Subsection B should be deleted outright – controllers that have obtained personal data about a consumer from a source other than the consumer should not have the option to ignore a deletion request and instead process it as an opt-out. Opt-out and deletion rights are not

---

[12] Will Evans, Amazon's Dark Secret: It Has Failed to Protect Your Data, Wired, (November 18, 2021), https://www.wired.com/story/amazon-failed-to-protect-your-data-investigation/

[13] APRA, Sec. 2(25), (noting that the additional data-level criteria are based on national standards that likely wouldn't make sense for Vermont), https://d1dth6e84htgma.cloudfront.net/American_Privacy_Rights_Act_of_2024_Discussion_Draft_0ec8168a66.pdf

[14] Kim Lyons, Judge approves $650 million Facebook privacy settlement over facial recognition feature, The Verge, (February 27, 2021), https://www.theverge.com/2021/2/27/22304618/judge-approves-facebook-privacy-settlement-illinois-facial-recognition

synonymous, especially in the data broker context where consumers might have good reason to want to delete a historical data trove about them that they never consented to being collected by the broker. It's not clear why these entities should receive special leeway to treat requests in their preferred manner. Notably, the recently enacted privacy laws Delaware and New Jersey do not include this provision.

Suggested redline for both instances where this language appears:

> *A controller that has obtained personal data about a consumer from a source other than the consumer may comply with a consumer's request to delete such data pursuant to [section reference] by either:*
>
> *(1) deleting the consumer's personal data, and retaining a record of the deletion request, retaining the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the business's records, and not using the retained data for any other purpose; or*
>
> ~~*(2) opting the consumer out of the processing of such personal data for any purpose except for those exempted pursuant to the provisions of [section reference]r.*~~

Thank you again for your consideration, and for your work on this legislation. We look forward to working with you to ensure that Vermont residents have the strongest possible privacy protections.

Sincerely,
Matt Schwartz
Policy Analyst