epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

March 5, 2024

Hon. Michael Marcotte and Members of the Committee
Committee on Commerce and Economic Development
Vermont House of Representatives

RE: H. 121 – Vermont Data Privacy Act

Dear Chair Marcotte and Members of the Committee:

EPIC writes in regard to H. 121, draft 7.1, the Vermont Data Privacy Act. We urge the Committee to strengthen the duties of controllers in the bill to provide more meaningful protections for Vermonters. EPIC is an independent nonprofit research organization in Washington, DC, established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.[1] EPIC has long advocated for comprehensive privacy laws at both the state and federal levels.[2]

Vermont Should Integrate Meaningful Data Minimization Rules

When consumers interact with a business online, they reasonably expect that their data will be collected and used for the limited purpose and duration necessary to provide the goods or services that they requested. For example, a consumer using a map application to obtain directions would not reasonably expect that their precise location data would be disclosed to third parties and combined with other data to profile them. And indeed, providing this service does not require selling, sharing, processing, or storing consumer data for an unrelated secondary purpose. Yet these business practices are widespread. Nearly every online interaction can be tracked and cataloged to build and enhance detailed profiles and retarget consumers.

Companies should not be allowed to determine for themselves what are the permissible purposes of collecting and using consumers' personal information. Without meaningful limitations, companies can, and do, claim that they need nearly unlimited data collection, transfer, and retention periods in order to operate their businesses. Unfortunately, the limitations on data collection in H. 121, draft 7.1 allow companies to do just that. Section 2419(a)(1)-(2) reads:

[1] EPIC, *About EPIC*, https://epic.org/about/.
[2] *See, e.g.,* Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security: Hearing before the Subcomm. on Consumer Protection & Comm. of the H. Comm. on Energy & Comm., 117th Cong. (2022) (testimony of Caitriona Fitzgerald, Deputy Director, EPIC), https://epic.org/wp-content/uploads/2022/06/Testimony_Fitzgerald_CPC_2022.06.14.pdf.

(a) A controller shall:

(1) specify in the privacy notice described in subsection (d) of this section the express purposes for which the controller is collecting and processing personal data;

(2) limit the controller's collection of personal data to only the personal data that is adequate, relevant, and reasonably necessary to serve the purposes the controller specified in subdivision (1) of this subsection;

Subsection (b)(1) then specifies that processing of personal data must also be reasonably necessary for those initially disclosed purposes.

Unfortunately, these provisions give a green light to businesses to collect data for whatever purposes they choose. This does little to change the status quo, as businesses can list any purpose they choose in their privacy policies, knowing that very few consumers will read them. The Vermont Legislature should enact a stronger data minimization standard.

Last session, bipartisan leaders in Congress proposed the American Data Privacy and Protection Act ("ADPPA"). The bill went through extensive negotiations between members of Congress, industry, civil rights groups, and consumer and privacy groups. The ADPPA received overwhelming bipartisan support in the House Energy & Commerce Committee, where it was favorably approved on a 53-2 vote. Congress failed to enact ADPPA, but Vermont legislators can now take advantage of the bipartisan consensus language in ADPPA, as state legislators in Maine, Maryland, and Massachusetts are currently doing.

The ADPPA set a baseline requirement that entities only collect and process data that is "*reasonably necessary and proportionate*" to provide or maintain a product or service requested by the individual (or pursuant to certain enumerated purposes).[3] For sensitive data, it must be "*strictly necessary*," and may not be used for targeted advertising. This standard better aligns business practices with what consumers expect.

The key with a data minimization provision is to ensure it is tied to the specific product or service requested by the individual, not simply to whatever purpose the collecting entity decides it wants to collect data for and discloses in their privacy policy. EPIC suggests the following redlines to Section 2419(a)(1)-(2) to integrate this approach:

(a) A controller shall:

(2) limit the controller's collection and processing of personal data to only the personal data that is ~~adequate, relevant, and~~ reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains~~to serve the purposes the controller specified in subdivision (1) of this subsection~~;

[3] H.R. 8152 at §101 (2022), *available at* https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

Additional redlines would be necessary to allow for some purposes that don't fall neatly under this rule, as was the case in the American Data Privacy and Protection Act, but the above redline demonstrates what the overarching rule would look like.

Data minimization offers a practical solution to a broken internet ecosystem by providing clear limits on how companies can collect and use data. The ADPPA set out a model for data minimization that was subject to intense scrutiny by many parties as it moved through Congress. Vermont can now take advantage of that bipartisan consensus language by integrating it into H. 121.

Existing data minimization rules in other jurisdictions

The California Consumer Privacy Act includes provisions requiring a form of data minimization.[4] California regulations establish restrictions on the collection and use of personal information.[5] The California Privacy Protection Agency explained that this "means businesses must limit the collection, use, and retention of your personal information to only those purposes that: (1) a consumer would reasonably expect, or (2) are compatible with the consumer's expectations and disclosed to the consumer, or (3) purposes that the consumer consented to, as long as consent wasn't obtained through dark patterns. For all of these purposes, the business' collection, use, and retention of the consumer's information must be reasonably necessary and proportionate to serve those purposes."[6]

The EU's General Data Protection Regulation (GDPR) requires companies, among other things, to minimize collection of consumer data to what is "[a]dequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed."[7] This is layered on top of restrictions on the legal bases under which companies can process personal data. The GDPR was groundbreaking in establishing broad data protection rights online, but Vermont should consider adopting a more concrete set of regulations now that difficulties with interpreting and enforcing GDPR have been revealed. Luckily a significant amount of the compliance work businesses are already doing to comply with GDPR would be applicable to the data minimization rules proposed above.

The key with a data minimization provision is to ensure it is tied to the specific product or service requested by the individual, not simply to whatever purpose the collecting entity decides it wants to collect data for and discloses in their privacy policy (as is currently the case in many states and in H. 121). This better aligns with consumers expectations when they use a website or app.

[4] Cal. Civ. Code § 1798.100(c).
[5] Cal. Code Regs. tit. 11 § 7000, et seq.
[6] Cal. Priv. Protection Agency, *Frequently Asked Questions*, 1, https://cppa.ca.gov/faq.html.
[7] Regulation (EU) 2016/679 (General Data Protection Regulation) Art. 5 § 1(c).

Additional Proposed Amendments

Civil Rights Protections

Privacy laws should prohibit discriminatory uses of data. H. 121 aims to do that by prohibiting the processing of personal data in violation of existing state and federal laws prohibiting unlawful discrimination. However, existing civil rights laws contain significant gaps in coverage and do not apply to disparate impact.[8] These issues make existing laws insufficient to ensure all people are protected from discrimination online. Therefore, H. 121 should instead include language that prohibits controllers and processors from collecting, processing, or transferring personal data "in a manner that discriminates or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability."

Data Protection Assessments

Companies collecting and using personal data should be required to assess their systems that present risks of harm to consumers. H. 121 includes requirements to conduct data protection impact assessments, which can help with meaningful oversight, if done right.

- Risk assessments should be required within a reasonable time of the law going into effect and should cover processing activity that began before the law's enactment but is ongoing.

- Controllers should be required to do these assessments on a regular basis and update them upon any material changes. Currently, H. 121 only requires this of data protection assessments done for processing involving minors, but not generally. This requirement should be added to §2423 to require regular updates to data protection assessments. The regulations issued by the Colorado Attorney General under the Colorado Privacy Act include this requirement.[9]

- A summary of data protection assessments should be made available to the public to avoid the assessments simply becoming internal box checking exercises.

Definition of sale

The definition of "sale/sell/sold" includes only the "exchange of personal data for monetary or other valuable consideration." This definition does not include companies sharing or making available personal data to other companies for other commercial purposes, which leaves a major

[8] *See* Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security: Hearing before the Subcomm. on Consumer Protection & Comm. of the H. Comm. on Energy & Comm., 117th Cong. (2022) (testimony of David Brody, Lawyer's Comm. for Civil Rights Under Law), https://docs.house.gov/meetings/IF/IF17/20220614/114880/HHRG-117-IF17-Wstate-BrodyD-20220614.pdf.
[9] 4 Colo. Code Regs §904-3 Rule 8.05 ("

loophole for companies to continue their same harmful data practices. This loophole is so large that it was one of the main reasons California updated its law via ballot initiative only two years after its privacy law originally passed. The practice of companies sharing personal data in exchange for the opportunity to advertise, for example, is common—the California Attorney General just settled with DoorDash over allegations that the company was engaged in this very practice, in violation of the California Consumer Privacy Act.[10] This loophole can be closed by amending the definition of "sale/sell/sold" in H. 121 to read:

> Renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration, or otherwise for a commercial purpose.

Unnecessary verification requirements for universal opt-out

The requirement in §2419(e)(3)(E) that requires that controllers "accurately determine" whether a consumer has made a "legitimate request" to opt-out of targeted advertising or data sales is very restrictive and gives companies leeway to argue that they cannot honor an opt-out because they couldn't "accurately determine" that it was a legitimate request. One option would be to change "accurately" to "reasonably," though this provision could also be simply cut entirely.

Right to Use Authorized agents Should Extend to Consumer Rights

Authorized agents should be permitted to execute all individual rights, not solely opt-out rights. The California Consumer Privacy Act contains this right, and researchers at Consumer Reports have found that it helps make consumers' individual rights more meaningful.[11]

Ban the Use of Dark Patterns in Exercising Consumer Rights

In order to ensure that businesses do not improperly limit access to the consumer rights established in the bill, a provision should be added that prohibits misleading or deceptive practices that have the effect of impairing consumers' ability exercise their rights. The following language should be added to section §2418 as a new subsection (c)(6):

> A controller may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of a right under this section through—

---

[10] Press Release, *Attorney General Bonta Announces Settlement with DoorDash, Investigation Finds Company Violated Multiple Consumer Privacy Laws*, CA DOJ (Feb. 21, 2024), https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-doordash-investigation-finds-company.

[11] Kaveh Waddell, *How 'Authorized Agents' Plan to Make It Easier to Delete Your Online Data,* Consumer Reports (Mar. 21, 2022), https://www.consumerreports.org/electronics/privacy/authorized-agents-plan-to-make-it-easier-to-delete-your-data-a8655835448/.

(A) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or

(B) the design, modification, or manipulation of any user interface with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision making, or choice to exercise such right.

Prohibit Targeted Advertising to Minors

Children and teens should be able to use technology to learn, connect with loved ones, play games, and explore their developing identities without being subject to constant surveillance for the purpose of serving them with targeted ads. President Biden called for a ban on targeted advertising to children in last year's State of the Union Address.[12] States such as Connecticut and Delaware prohibit processing the personal data for the purposes of targeted advertising if they know or willfully disregard that the consumer is a teenager (age 13-16 in Connecticut, ages 13-18 in Delaware).[13] Vermont should provide equivalent protections.

Narrow the Loyalty Program Exemption

We appreciate the changes that were made to the loyalty program provisions in §2419(c)(2) to limit transfers of personal data to third parties but believe more changes are needed. Consumers should not be forced to consent to the sale of their personal data to data brokers and other third parties simply to participate in a loyalty program. Businesses do not need to *sell* personal data to third parties to operate a loyalty program. We support the suggestions that Consumer Reports has made to close the possible loopholes created by loyalty program language.

Conclusion

EPIC appreciates your work on this issue and is happy to continue to be a resource on H. 121. Please let us know if you would like to talk further about these suggested amendments.

Sincerely,

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Deputy Director

/s/ *Kara Williams*
Kara Williams
EPIC Law Fellow

[12] The White House, State of the Union Address (Feb. 7, 2023), https://www.whitehouse.gov/state-of-the-union-2023/ ("And it's time to pass bipartisan legislation to stop Big Tech from collecting personal data on kids and teenagers online, ban targeted advertising to children, and impose stricter limits on the personal data that companies collect on all of us.")
[13] Conn. Gen. Stat. § 42-520; Del. Code. Ann. Tit. 6, § 12D.