epic.org

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

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

April 27, 2026

Representative Michael Marcotte, Chair
Representative Edye Graning, Vice Chair
Vermont House Committee on Commerce and Economic Development

Dear Chair Marcotte, Vice Chair Graning, and Members of the Committee:

EPIC writes in support of S.71 v.2.3, An act relating to consumer data privacy and online surveillance. For more than two decades, powerful tech companies have been allowed to set the terms of our online interactions. Without any meaningful restrictions on their business practices, they have built systems that invade our private lives, spy on our families, and gather the most intimate details about us for profit. These practices harm Vermont's consumers, as well as the small businesses that power Vermont's economy. But it does not have to be this way – we can have a strong technology sector while protecting personal privacy. EPIC believes that S.71 v2.3 accomplishes that goal.

The Electronic Privacy Information Center (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 level.[2]

S.71 v2.3 builds on the Legislature's work last session when it passed a strong, comprehensive privacy law. It mirrors many of the provisions in state privacy laws already enacted in 21 states, provides predictability and clarity for Vermont businesses, and incorporates important provisions to provide Vermonters with the protections they need to stay safe online.[3] Key provisions of S.71 v2.3 include:

- **Data minimization:** S.71 v2.3 establishes limits on the unfettered processing of personal data by setting a baseline requirement that entities only collect, use, and transfer data that is reasonably necessary and proportionate to provide or maintain a product or service requested by the individual. The Maryland Online Data Privacy Act, enacted last year, includes data minimization rules, and Massachusetts is considering similar legislation this session.

- **Strong protections for sensitive data:** S.71 v2.3 sets heightened protections for sensitive data (i.e., biometrics, location, health data) such that its collection and use must be strictly

[1] EPIC, *About EPIC*, https://epic.org/about/.
[2] *See* e.g. EPIC, *The State Data Privacy Act: A Proposed Model State Privacy Bill,* https://epic.org/the-state-data-privacy-act-a-proposed-model-state-privacy-bill/.
[3] *See* EPIC and U.S. PIRG Education Fund, *The State of Privacy 2025: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better* (Jan. 2025), https://epic.org/wp-content/uploads/2025/01/EPIC-PIRG-State-of-Privacy-2025.pdf.

necessary for the product or service the consumer is asking for. Sensitive data may not be sold, a protection included in the recently enacted Maryland Online Data Privacy Act.

- **Protections for children and teens:** S.71 v2.3 prohibits targeted advertising to minors under age 18 and bans the sale of minors' data, which is also included in Maryland's law.

I do want to note that though EPIC supports v2.3, this is a compromise bill. The removal of the private right of action is a massive concession to those who were opposed to the bill last session. The Attorney General has said themselves that they do not have the resources to adequately enforce this law. A law without strong enforcement is merely a suggestion. We recognize that the decision to remove the private right of action was done in the hopes of advancing the bill this session, but we do hope that it is something the Legislature will revisit down the line once the bill is in effect.

In my testimony I will discuss why it is so critical that Vermont pass a strong privacy law, the current state of state privacy laws, and go into detail on a couple of key concepts that are crucial to keep Vermonters safe online.

A. Data Abuse Harms Consumers, and Current State Privacy Laws Don't Do Enough

Companies should not have a limitless ability to decide how much personal data to collect. Unfortunately, this is what all state laws — other than California's and Maryland's — allow. Most existing state privacy laws only limit collection to what is reasonably necessary for "the purposes for which such data is processed, *as disclosed to the consumer*," meaning businesses can collect data for whatever purposes they want, as long as they state that purpose in their privacy policies.[4] This reinforces the failed status quo of "notice and choice" — businesses can list any purpose they choose in their privacy policies, knowing that very few consumers will read them.

The focus on notice has led to longer and more complicated privacy policies that users do not read and could not change even if they did. Technology's prevalence in our work, social, and family lives leaves us with no "choice" but to accept. And online tracking is too complex and opaque for the vast majority of internet users to understand or control.

Advertisers and data brokers track our every click, and our data is used against us in ways that harm our wallets, opportunities, and rights. At a time when policymakers are concerned about cost-of-living issues for their constituents, the impact of mass data collection and abuse on those costs cannot be ignored. A few examples of these harms include:

1. **Increased insurance premiums.** Last year, Texas Attorney General Ken Paxton sued insurance giant Allstate and its subsidiary Arity for unlawfully collecting, using, and selling data about the location and movement of Texans' cell phones through secretly embedded

[4] *See id.*

software in mobile apps, such as Life360. Paxton alleged that Allstate and other insurers then used the covertly obtained data to justify raising Texans' insurance rates.[5]

2. **Increased pricing on consumer goods**. The Federal Trade Commission recently released initial findings from a study on surveillance pricing, a practice that uses data about consumers' characteristics and behavior to alter prices. "Initial staff findings show that retailers frequently use people's personal information to set targeted, tailored prices for goods and services—from a person's location and demographics, down to their mouse movements on a webpage," said then-FTC Chair Lina M. Khan.[6]

3. **Targeted advertisements can be predatory and harmful.** Targeted ads can be predatory and harmful, using people's online behavioral data to reach vulnerable consumers who meet specific parameters. People searching terms like "need money help" on Google have been served ads for predatory loans with staggering interest rates of over 1,700%.[7] An online casino targeted ads to problem gamblers, offering them free spins on its site.[8] A precious metals scheme used Facebook users' ages and political affiliations to target ads to get users to spend their retirement savings on grossly overpriced gold and silver coins.[9]

4. **Personal data collected for advertising purposes is being used by the Trump Administration to carry out its agenda.** It was recently reported that ICE is exploring how it can use the "bidstream" type data broadcast in ad auctions for investigations.[10] An advertising executive recently wrote an article in an ad trade publication titled "*The Privacy 'Zealots' Were Right: Ad Tech's Infrastructure Was Always A Risk*," noting that the advertising industry should have seen the government's abuse of digital ad data coming.[11]

---

[5] Press Release, Att'y Gen. of Texas, *Att'y Gen. Ken Paxton Sues All-state and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Cos.* (Jan 13, 2025), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-allstate-and-arity-unlawfully-collecting-using-and-selling-over-45.

[6] Press Release, Fed. Trade Comm'n, *FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices* (Jan. 17, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.

[7] Shanti Das, *Google Profiting from 'Predatory' Loan Adverts Promising Instant Cash*, The Guardian (Mar. 13, 2022), https://www.theguardian.com/technology/2022/mar/13/google-profiting-from-predatory-loan-adverts-promising-instant-cash.

[8] Rob Davies, *Online Casino Advert Banned for Targeting Problem Gamblers*, The Guardian (Oct. 9, 2019), https://www.theguardian.com/society/2019/oct/09/casumo-ad-banned-for-targeting-people-trying-to-stop-gambling.

[9] Jeremy B. Merrill, *How Facebook Fueled a Precious-Metal Scheme Targeting Older Conservatives,* Quartz (Nov. 19, 2019), https://www.yahoo.com/video/facebook-fueled-precious-metal-scheme-110044886.html.

[10] Wendy Davis, *ICE Issues RFI For 'Ad Tech Compliant' Data* (Jan. 2026), https://www.mediapost.com/publications/article/412314/ice-issues-rfi-for-ad-tech-compliant-data.html.

[11] David Nyurenberg, *The Privacy 'Zealots' Were Right: Ad Tech's Infrastructure Was Always A Risk*, AdExchanger (Mar. 9, 2026), https://www.adexchanger.com/data-driven-thinking/the-privacy-zealots-were-right-ad-techs-infrastructure-was-always-a-risk/.

Small businesses are harmed by these systems as well. For years, they've been told that success hinges on pouring money into online behavioral advertising, controlled by a handful of tech giants. They enter bidding wars against corporate behemoths. This isn't a level playing field. It's a digital black hole—swallowing resources and crushing entrepreneurial spirit, all to facilitate targeted advertising that is of dubious efficacy.

B. Data Minimization and Strong Enforcement: Two Keys to a Strong Privacy Law

a. Data Minimization

S.71 v2.3 relies on a concept that has long been a pillar of privacy protection: data minimization.

When consumers interact with a business online, they 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 sold to third parties and combined with other data to profile them. And indeed, providing this service does not require selling the customer's location data. Yet these business practices are widespread. Nearly every online interaction can be tracked and cataloged to build and enhance detailed profiles and retarget consumers. Even offline, credit card purchases, physical movements, and "smart" devices in homes create countless data points that are logged and tracked without consumer awareness or control.

S.71 v2.3 sets a baseline requirement that entities only collect, use, and transfer data that is "*reasonably necessary and proportionate*" to provide or maintain a product or service requested by the consumer. This standard better aligns business practices with what consumers expect.

Data minimization is essential for both consumers and businesses. Data minimization principles provide much-needed standards for data security, access, and accountability, assign responsibilities with respect to user data, and restrict data collection and use. Indeed, a data minimization rule can provide clear guidance to businesses when designing and implementing systems for data collection, storage, use, and transfer. Data security will be improved because personal data that is not collected in the first place cannot be at risk of a data breach.

The Maryland Online Data Privacy Act, which was enacted last year, and the California Consumer Privacy Act also include provisions requiring a form of data minimization. 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 its privacy policy.

Data minimization offers a practical solution to a broken internet ecosystem by providing clear limits on how companies can collect and use data.

b. How Does Advertising Work Under a Strong Data Minimization Rule?

There were concerns expressed last session about how the data minimization rules would impact small Vermont businesses' ability to advertise. The sponsors of S.71 v2.3 responded to these concerns by setting clear definitions and rules for online advertising. The bill defines three core forms of advertising and provides different rules for each type based on the risks each presents to Vermonters' privacy.

1. Contextual advertising

Businesses engage in contextual advertising when they select advertisements to show consumers based on the topic or content of the media surrounding the advertisement. For example, if the someone in New England searches for soccer scores, Vermont Green FC could place an ad for tickets on that page – that's contextual advertising. Contextual advertising relies on generalizable inferences that people might be interested in products or services related to the content on the website, app, publication, or search result they are viewing. Contextual advertising may also include using a consumer's general location to show ads for local businesses, events, and services. For example, if a local restaurant opens a new location on the other side of town, that restaurant can advertise to consumers within a 10-mile radius of the new location. Contextual advertising is the most privacy-protective of the three advertising types because the ads consumers see do not vary based on their identities. **There are no restrictions on contextual advertising in S.71 v2.3.**

2. First-party advertising

Businesses engage in first-party advertising when they advertise in their own store, on their own website or app, or communicate directly with consumers through mail, email, or text messaging using data they collect. For example, suppose a retailer collects order information or website views as permitted under the data minimization rules. As long as that data does not include sensitive data, the first party may use that data to advertise. This type of advertising aligns with what consumers expect. Most consumers expect that when they browse a company's website and make a purchase, that company is collecting data about what consumers did on the site. **First-party advertising is permitted under S.71 v2.3.**

3. Targeted advertising

There are varying forms of targeted advertising, all with different levels of risk to privacy and data security. S. 71 v2.3 distinguishes between the primary methods of targeted advertising and sets different levels of data protection for each.

Behavioral advertising requires tracking consumers everywhere they go online (often without their knowledge) and building invasive profiles based on that data to target them with ads. An example is the Meta Pixel, which is embedded on many websites and automatically sends

consumers' browsing history to Meta. For example, if I look up a condition on WebMD's site, the information about the page I was reading is sent to Meta automatically, without my knowledge or consent. **By including data collected over time and across websites as a category of sensitive data, S.71 v2.3 bans this incredibly invasive and harmful practice.**

Retargeting is what most people think of when they think of targeted ads. Retargeting involves targeting consumers who visited a website with ads elsewhere online. If a consumer views sneakers on a retailer's website and that retailer then targets that consumer with ads for those same sneakers on other websites, that type of advertising is retargeting. **Retargeting is permitted under the S.71 v2.3, though consumers can opt out of this type of targeted advertising, including (for those with a generalized preference not to receive retargeted ads) through universal opt-out signals.**

The data minimization rules in S.71 v2.3 ensure that Vermont businesses have plenty of methods of marketing themselves to potential consumers while protecting Vermonters from the abuse of their personal data in the most unexpected and harmful ways.

* * *

Privacy is a fundamental right, and it is time for business practices to reflect that reality. Self-regulation is clearly not working, and since Congress has still been unable to enact comprehensive privacy protections despite years of discussion on the topic, state legislatures must act. The Vermont State Legislature has an opportunity this session to provide real privacy protections for Vermonters while allowing Vermont businesses to thrive.

Thank you for the opportunity to speak today. I am happy to be a resource to the Committee as it navigates this complex topic and can be reached at fitzgerald@epic.org.

Sincerely,

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