H.208: VERMONT DATA PRIVACY & ONLINE SURVEILLANCE ACT OVERVIEW

SUMMARY

The Vermont Data Privacy & Online Surveillance Act (H.208) establishes comprehensive data privacy rights for Vermonters and requires businesses to limit their collection and use of personal data. The Act grants Vermonters the right to access, correct, delete, and obtain a copy of their personal data, as well as the right to opt out of targeted advertising, the sale of personal data, and certain types of profiling – rights Americans in 19 states already enjoy. The Act also gives heightened protection for sensitive data, minors' data, and consumer health data, and bans the sale of sensitive data outright. The Attorney General is authorized to enforce the Act, and Vermonters may vindicate their rights via a limited private right of action if they are harmed by certain violations by a data broker or large data holders (small businesses are not covered by the private right of action). H.208 remains grounded in the framework of Connecticut SB 6 (2022), as well as subsequent amendments from Connecticut SB 3 (2023). This year's bill also contains a number of revisions in response to thousands of hours of stakeholder feedback (described below). H.208 centers on consumer protection while providing clear direction for businesses - ensuring they can not only comply with the law but also continue to engage with existing customers and attract new ones.

BACKGROUND

The digital age has brought unprecedented opportunities for innovation and connection but has also created significant privacy challenges. Companies collect vast amounts of personal data from consumers, often without their full knowledge or meaningful consent. Ad giants, data brokers, insurance companies, and others use this data for targeted advertising, profiling, and other purposes that consumers don't even realize are happening. According to a Pew Research Center survey, 79% of Americans report being concerned about the way their data is being used by companies. Existing federal laws, such as the Children's Online Privacy Protection Act (COPPA) and the Health Insurance Portability and Accountability Act (HIPAA), provide some data privacy protections in specific contexts, but they do not establish a comprehensive framework for consumer data privacy. This patchwork approach leaves many gaps in protection and creates a complex regulatory landscape. The lack of comprehensive data privacy legislation has led to growing public concern about the collection, use, and sharing of personal data. A survey by the Internet Society found that 75% of users globally feel they have lost control over how their personal information is collected and used online.

PROBLEM

The current data privacy landscape poses several problems for Vermonters:

- **Disadvantaging Small Businesses:** Large tech companies' extensive collection and use of personal data, often without clear consent, creates an unfair advantage. They leverage this data for targeted advertising and potentially exploitative practices, disadvantaging small businesses. These smaller businesses face higher risks from data breaches and are often forced into dependence on the very platforms that undermine their competitiveness, all while consumer trust erodes due to opaque data practices.
- **Increased Cost-of-Living Expenses:** Data abuse is driving up the cost of insurance, groceries, rent, and more. The Texas AG just sued Allstate for using location data from mobile apps to drive

up insurance rates. The FTC recently found that retailers frequently use people's personal information to set targeted, tailored prices for goods and services. Over a dozen state AGs recently sued RealPage for using data-driven algorithms to drive up rents. Data privacy is key to tackling cost-of-living issues for our constituents.

- **Vulnerability to Fraud & Scams:** Fraudsters and other bad actors can use sensitive data to target vulnerable individuals for scams, or otherwise use personal information to cause harm. For example, scammers can use commercially available location data to increase the specificity of their phishing or social engineering scams, such as by including location-specific details, like mentioning a nearby business or the individual's recent activity. Some data brokers sell lists of consumers sorted by characteristics like "Rural and Barely Making It" and "Credit Crunched: City Families," which can be used to target individuals most likely to be susceptible to scams or other predatory products. Location data brokers are also commonly used by abusive individuals to locate people, hunt them down, and stalk, harass, intimidate, assault, or even murder them.
- **Lack of Transparency:** Consumers often lack clear information about how their data is collected, used, and shared. A study by the Annenberg School for Communication found that 91% of adults aged 18-34 in the US agreed to legal terms and conditions without reading them, and that many privacy policies require at least a college-level reading ability, while the average American reads at a 7th-8th grade level. This lack of transparency makes it difficult for consumers to make informed decisions about their data.
- **Data Breaches:** Data breaches are becoming increasingly common and can have serious consequences for consumers. In 2023, 3,205 publicly reported data breaches occurred, compromising an estimated 353,023,789 individuals.
- **Targeted Advertising, Profiling & Discrimination:** The use of personal data for targeted advertising and profiling can lead to manipulation, discrimination, and other harms. There is potential for sensitive data, especially about minorities, to be used to discriminate against these groups. A study by Upturn found that a social media advertising platform allowed housing advertisers to exclude users based on race, gender, and other protected characteristics, in potential violation of fair housing laws.
- **Sale of Personal Data:** The sale of personal data is a lucrative industry, and consumers often have little control over how their data is bought and sold, exposing them to the risk of identity theft. National Public Data, a data broker, was recently breached, exposing the personal data, including SSNs, of nearly 3 billion individuals.
- **Sensitive Data Risks:** The collection and use of sensitive data, such as health information, financial data, and biometric data, pose dangerous risks to consumers. For example, the unauthorized disclosure of health information can lead to loss of job opportunities or life insurance.

SOLUTION

The Vermont Data Privacy & Online Surveillance Act addresses these problems by:

- **Strengthening Small Businesses:** The Act levels the playing field by requiring transparency and consent for personal data use. This limits large tech companies' data advantage, reduces data breach risks, and fosters consumer trust. The Act empowers small businesses to compete fairly, build direct customer relationships, and reduce reliance on dominant platforms, promoting a more equitable and sustainable digital economy.
- **Limiting the Amount of Data Collected About Us:** Businesses must limit data collection to what is reasonably necessary to provide the product or service the consumer is asking for.

- **Promoting data security:** Requires businesses to implement reasonable data security practices and provide clear privacy notices.
- **Giving Consumers Rights to Control Their Data:** The Act grants consumers the right to access, correct, delete, and obtain a copy of their personal data. Consumers can also opt out of targeted advertising, the sale of personal data, and certain types of profiling.
- **Requiring Review of High-Risk Activities:** Businesses must conduct assessments for high-risk activities, such as the sale of personal data and the processing of sensitive data. Assessments done to comply with other states' laws satisfy compliance with Vermont's law.
- **Protecting Sensitive Data:** The Act includes specific provisions related to the use of sensitive data, including a ban on the sale of sensitive data.
- **Protecting Minors' Data:** To protect our kids and teens, companies may not sell minors' data or target them with ads.
- **Protecting Health Data:** The Act includes provisions to protect the confidentiality of consumer health data, including restrictions on the use of geofencing near healthcare facilities.
- **Enforcement:** The AG is authorized to enforce the Act. A private right of action is (1) limited in scope (anchored to violations of specific parts of the bill) and (2) limited in applicability - to data brokers (entities that sell personal data) as well as large data holders (businesses that collect the data of 100,000 Vermonters or more per year). Consumers cannot bring a private right of action against any company earning less than $25 million in annual revenue.

RESPONDING TO STAKEHOLDER FEEDBACK

H.208 contains a number of adjustments that address concerns from stakeholders, including members of the business community, while maintaining the core consumer protections expected by Vermonters. H.208 remains grounded in the framework of Connecticut SB 6 (2022), as well as subsequent amendments on consumer health and minor protections from Connecticut SB 3 (2023). Changes from previous legislation include:

- Clearer distinctions between first-and third-party **marketing**, as well as contextual and targeted advertising. Businesses can continue to use data they gather from their customers and website visitors to communicate and send ads.
- Significant revision to the **enforcement** section. In H.208:
    - Consumers must first engage in intermediary steps with the Attorney General before pursuing a private right of action to address violations;
    - Consumers cannot bring a private right of action against any company earning less than $25 million in annual revenue;
    - The private right of action continues to be limited in scope (anchored to violations of specific parts of the bill) and limited in applicability - to data brokers (entities that sell personal data) and large data holders (businesses that collect the data of 100,000 Vermonters or more per year).
- **Exceptions have been added allowing controllers and processors to use data for critical purposes,** including product recalls, performing research projects, carrying out necessary internal operations, and identifying and repairing technical errors.
- Under the 2024 version, businesses that have already created a data protection assessment to comply with another state's requirements would not need to craft a separate, Vermont-specific assessment. **This interoperability provision now also extends to privacy policies.**