

SB541-EPIC-Maryland-Feb2024.pdf

Uploaded by: Caitriona Fitzgerald

Position: FAV

February 13, 2024

The Honorable Pamela Beidle
Senate Finance Committee
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

Dear Chair Beidle and Members of the Committee:

EPIC writes in support of SB 541, the Maryland Online Data Privacy Act of 2024. We commend the sponsors for crafting a bill that provides meaningful privacy protections for Marylanders. 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. But it does not have to be this way – Maryland can have a strong technology sector while protecting personal privacy.

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

In my testimony I will discuss why it is so critical that Maryland pass a privacy law, the current state of state privacy laws, and how SB 541 rightfully includes stronger protections than existing state laws.

A. A Data Privacy Crisis: Surveillance Capitalism Run Wild

The notice-and-choice approach to privacy regulation that has dominated the United States' response to uncontrolled data collection over the last three decades simply does not work. 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. Technologies' prevalence in our work, social, and family lives leaves us with no "choice" but to accept. And modern surveillance systems, including the schemes used to

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.

track our digital and physical activities across the web and across devices, are too complex and opaque for the vast majority of internet users to understand or control.

In 2022, BuzzFeed reported that religious social networking service and app Pray.com was collecting detailed information about its users, including the texts of their posts, and linking it with information obtained from third-parties and data brokers.³ Pray.com was also releasing detailed data about its users with third-parties, including Facebook, meaning “users could be targeted with ads on Facebook based on the content they engage with on Pray.com — including content modules with titles like ‘Better Marriage,’ ‘Abundant Finance,’ and ‘Releasing Anger.’”⁴

In 2020, the investigative journalists at The Markup found that one-third of websites surveyed contained Facebook’s tracking pixel, which allows Facebook to identify users (regardless of whether they are logged into Facebook) and connect those website visits to their Facebook profiles.⁵ They scanned hundreds of websites, discovering alarming instances of tracking, including:

- WebMD and Everyday Health sending visitor data to dozens of marketing companies;
- The Mayo Clinic using key logging to capture health information individuals typed into web forms for appointments and clinical trials, regardless of whether the individual submitted the form or not—and saving it to a folder titled “web forms for marketers/tracking.”⁶

These trackers collect millions of data points each day that are sold to data brokers, who then combine them with other data sources to build invasive profiles. Often these profiles are used to target people with ads that stalk them across the web. In other cases, they are fed into algorithms used to determine the interest rates on mortgages and credit cards, to raise consumers’ interest rates, or to deny people jobs, depriving people of opportunities and perpetuating structural inequalities.⁷

These are just a few of the myriad ways our privacy is invaded every minute of every day. The harms from these privacy violations are real,⁸ and it is past time to correct the course.

³ Emily Baker-White, *Nothing Sacred: These Apps Reserve The Right To Sell Your Prayers*, BuzzFeed (Jan. 25, 2022), <https://www.buzzfeednews.com/article/emilybakerwhite/apps-selling-your-prayers>.

⁴ *Id.*

⁵ Julia Angwin, *What They Know... Now*, The Markup (Sept. 22, 2020), <https://themarkup.org/blacklight/2020/09/22/what-they-know-now>.

⁶ Aaron Sankin & Surya Mattu, *The High Privacy Cost of a “Free” Website*, The Markup (Sept. 22, 2020), <https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites>.

⁷ See *Protecting Consumer Privacy in the Age of Big Data*, 116th Cong. (2019), H. Comm. on the Energy & Comm., Subcomm. on Consumer Protection and Comm. (Feb. 26, 2019) (testimony of Brandi Collins-Dexter, Color of Change), <https://tinyurl.com/53kr6at6>.

⁸ Danielle Citron & Daniel Solove, *Privacy Harms*, 102 B.U.L. Rev. Online 793 (2021), <https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf>.

B. The State of State Privacy Law

Because there is not a federal comprehensive privacy law in the U.S., states have been passing laws to fill this void. Since 2018, 14 states have passed comprehensive privacy laws. EPIC, in partnership with U.S. PIRG, released a report this month grading these state laws.⁹ Of the 14 laws, nearly half received an F on our scorecard, and none received an A. Most provide few meaningful privacy rights for consumers and do little to limit mass data collection and abuse.

With the exception of California, all of these state laws closely follow a model initially drafted by tech giants.¹⁰ This draft legislation was based on a privacy bill from Washington state that was modified at the behest of Amazon, Comcast, and Microsoft.¹¹ An Amazon lobbyist encouraged a Virginia lawmaker to introduce a similar bill, which became law in 2021. Virginia's law received an F on our scorecard. Unfortunately, this Virginia law became the model that industry lobbyists pushed other states to adopt. In 2022, Connecticut passed a version of the Virginia law with some additional protections, which has now become the version pushed by industry lobbyists in select states. Privacy laws, which are meant to protect individuals' privacy from being abused by Big Tech, should not be written by the very industry they are meant to regulate.

Laws based on the Virginia and Connecticut models provide very few protections for consumers. These models do not meaningfully limit what data companies can collect or what they can do with that data — they merely require that companies disclose these details in their privacy policies, which consumers rarely read or understand. 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 the Connecticut Data Privacy Act allow companies to do just that. The CTDPA reads:

A controller shall [...] Limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer.

⁹ Caitriona Fitzgerald, Kara Williams & R.J. Cross, *The State of Privacy: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better*, EPIC and U.S. PIRG (February 2024), <https://epic.org/wp-content/uploads/2024/01/EPIC-USPIRG-State-of-Privacy.pdf>.

¹⁰ Jeffrey Dastin, Chris Kirkham & Aditya Kalra, *Amazon Wages Secret War on Americans' Privacy, Documents Show*, Reuters (Nov. 19, 2021), <https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/>.

¹¹ Emily Birnbaum, *From Washington to Florida, Here Are Big Tech's Biggest Threats from States*, Protocol (Feb. 19, 2021), <https://www.protocol.com/policy/virginia-maryland-washington-big-tech>; Mark Scott, *How Lobbyists Rewrote Washington State's Privacy Law* (Apr. 2019), <https://www.politico.eu/article/how-lobbyists-rewrote-washington-state-privacy-law-microsoft-amazon-regulation/>.

This simply requires that businesses only collect what is reasonably necessary for the purposes they disclose to consumers in their privacy policy. 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. And even on the off-chance that consumers do read a privacy policy, they have no power to change the terms of these agreements, so their only “choice” is not to use the service. The clearer limits on data collection and use in SB 541 are critical because they require companies to better align their data practices with what consumers expect.

C. SB 541 Provides Stronger Privacy Protections by Limiting Data Collection and Establishing Strong Civil Rights Protections

Data Minimization

The excessive data collection and processing that fuel commercial surveillance systems are inconsistent with the expectations of consumers, who reasonably believe that the companies they interact with will safeguard their personal information. These exploitative practices don’t have to continue. SB 541 rightfully integrates a concept that has long been a pillar of privacy protection: data minimization.

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.

SB 541 sets a baseline requirement that entities only collect data that is “*reasonably necessary and proportionate*” to provide or maintain a product or service requested by the individual. For sensitive data, the collection and processing of such data must be “*strictly necessary*.” 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. And 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 Federal Trade Commission has recognized that the overcollection and misuse of personal information is a widespread problem that harms millions of consumers every day and has identified that data minimization is the key to addressing these unfair business practices. As it stated in a recent report:

Data minimization measures should be inherent in any business plan—this makes sense not only from a consumer privacy perspective, but also from a business perspective because it reduces the risk of liability due to potential data exposure. Businesses should collect the data necessary to provide the service the consumer requested, and nothing more.¹²

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

Data minimization is not a new concept. Privacy laws dating back to the 1970s have recognized and applied this concept. The Privacy Act of 1974, a landmark privacy law regulating the personal data practices of federal agencies, requires data minimization. Each agency that collects personal data shall “maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President.”¹³

The recently passed update to the California Consumer Privacy Act also includes provisions requiring a form of data minimization.¹⁴ California regulations establish restrictions on the collection and use of personal information. 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.”¹⁵

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.”¹⁶ 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 Maryland should consider adopting a more concrete set of regulations now that difficulties with interpreting and enforcing

¹² FTC, *Bringing Dark Patterns to Light* 17–18 (2022), <https://www.ftc.gov/reports/bringing-dark-patterns-light>.

¹³ 5 U.S.C. § 552a (e)(1).

¹⁴ Cal. Civ. Code § 1798.100(c).

¹⁵ Cal. Priv. Protection Agency, *Frequently Asked Questions*, Question 1, <https://cppa.ca.gov/faq.html>.

¹⁶ Regulation (EU) 2016/679 (General Data Protection Regulation) Art. 5 § 1(c).

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 included in SB 541.

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 the case in the Connecticut Data Privacy Act). This stricter framework better aligns with consumers expectations when they use a website or app. SB 541 accomplishes this goal.

EPIC does advocate that the rule in § 14-4607(B)(1)(I) be broadened to limit both the collection *and processing* of personal data to purposes that are reasonably necessary to provide or maintain a specific product or service requested by the consumer to whom the data pertains. The biggest impact of adding processing to the rule is that the entities that use our personal information in out-of-context ways, such as data brokers, will be unable to profile consumers in ways unrelated to why a consumer used an online service. The rule will limit the harmful practice of brokering, selling, or sharing personal information unrelated to the primary collection purpose and accordingly limit harmful surveillance advertising. We recommend that the Committee consider broadening that rule, but even a limitation on collection is a step in the right direction.

Civil Rights Protections

Importantly, SB 541 also extends civil rights to online spaces by prohibiting entities from processing data in a way that discriminates or otherwise makes unavailable the equal enjoyment of goods and services on the basis of race, color, religion, national origin, sex, sexual orientation, gender identity, or disability. Most state privacy laws attempt to prevent discrimination online by prohibiting the processing of personal data in ways that violate state and federal anti-discrimination laws. However, existing civil rights laws contain significant gaps in coverage and do not apply to disparate impact.¹⁷ These issues make existing laws insufficient to ensure all people are protected from discrimination online. The language in § 14-4607(A)(7) better protects individuals from discrimination online.

D. Enforcement is Critical

Robust enforcement is critical to effective privacy protection. Strong enforcement by state government via Attorney General authority or the creation of a state privacy agency is a very important piece to include in a strong privacy law.

¹⁷ 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>.

But while government enforcement is essential, the scope of data collection online is simply too vast for one entity to regulate. Individuals and groups of individuals who use these online services are in the best position to identify privacy issues and bring actions to vindicate their interests. These cases preserve the state's resources, and statutory damages ensure that companies will face real consequences if they violate the law.

The inclusion of a private right of action is the most important tool the Legislature can give to their constituents to protect their privacy. A private right of action would impose enforceable legal obligations on companies. As Northeastern University School of Law Professor Woody Hartzog recently wrote with regard to a private right of action in the Illinois biometric privacy law:

So far, only private causes of action seem capable of meaningfully deterring companies from engaging in practices with biometrics based on business models that inevitably lead to unacceptable abuses. Regulators are more predictable than plaintiffs and are vulnerable to political pressure. Facebook's share price actually rose 2 percent after the FTC announced its historic \$5 billion fine for the social media company's privacy lapses in the Cambridge Analytica debacle. Meanwhile, Clearview AI specifically cited BIPA as the reason it is no longer pursuing non-government contracts. On top of that, Clearview AI is being sued by the ACLU for violating BIPA by creating faceprints of people without their consent. [...] In general, businesses have opposed private causes of action more than other proposed privacy rules, short of an outright ban.¹⁸

The ACLU's suit against facial recognition company Clearview AI settled, with Clearview agreeing not to sell its face surveillance system to any private company in the United States.¹⁹ Private rights of action are extremely effective in ensuring that the rights in privacy laws are meaningful.

The statutory damages set in privacy laws are not large in an individual case, but they can provide a powerful incentive in large cases and are necessary to ensure that privacy rights will be taken seriously, and violations not tolerated. In the absence of a private right of action, there is a very real risk that companies will not comply with the law because they think it is unlikely that they would get caught or fined. Private enforcement ensures that data collectors have strong financial incentives to meet their data protection obligations. We would encourage the Committee to strike the text in § 14-4613(2) that states "except for § 13-408 of this Article," which would allow Marylanders to use their existing right to bring suit under the Unfair, Abusive, or Deceptive Trade Practices Act for violations of this bill.

¹⁸ Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), <https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf>

¹⁹ Ryan Mac & Kashmir Hill, *Clearview AI Settles Suit and Agrees to Limit Sales of Facial Recognition database*, N.Y. Times (May 9, 2022), <https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html>.

E. Additional Proposed Amendments

EPIC agrees with Consumer Reports' recommended amendments to broaden opt-out rights to include all data sharing and ensure that targeted advertising is adequately covered, eliminate the GLBA carveout, narrow the loyalty program exemption, remove ambiguities around universal opt-out requirements, and amend the prohibitions on default opt-outs.

F. Conclusion

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 Maryland General Assembly has an opportunity this session to provide real privacy protections for Marylanders.

Thank you for the opportunity to speak today. EPIC is happy to be a resource to the Committee on these issues.

Sincerely,

/s/ Caitriona Fitzgerald

Caitriona Fitzgerald
EPIC Deputy Director

/s/ Kara Williams

Kara Williams
EPIC Law Fellow

SB541 Testimony FAVORABLE The Holland Law Firm PDF

Uploaded by: Casey Santora

Position: FAV

The **HOLLAND LAW FIRM**
for Consumer Rights

Emanwel J. Turnbull
Attorney at Law
eturnbull@hollandlawfirm.com

The Holland Law Firm, P.C.
Mailing Address:
914 Bay Ridge Rd, Ste 230
Annapolis, MD 21403

Testimony to the Senate Finance Committee
SB541 – Maryland Online Data Privacy Act
Position: Favorable

February 9, 2024

Hon. Chair, Senator Beidle, Senate Finance Committee
3 East
Miller Senate Office Building
Annapolis, MD 21401
cc: Members, Senate Finance Committee

Honorable Chair Beidle and Members of the Committee:

Chair and Members of the Committee,

The Holland Law Firm, P.C. is a consumer rights law firm, serving ordinary Marylanders impacted by bad business practices.

I am writing to express my strong support for SB541. Maryland needs a data privacy law. At present a patchwork of state and federal laws protect limited fragments of consumer data. But the bulk of consumer data can be freely exploited by businesses, with little transparency and not even a right of access that data businesses hold on them.

I believe it is particularly important that consumers have a right to access their data about them. I routinely represent consumers who are victims of identity theft. Identity theft often leaves businesses with false, frequently negative, information about victims. Without a right of access to data, consumers cannot know or correct the full extent of the damage an identity thief has done.

SB541 provides this important right to Maryland consumers, and therefore I urge a favorable report on SB541.

By:

/s/ Emanwel J. Turnbull
Emanwel J. Turnbull
THE HOLLAND LAW FIRM, P.C.
914 Bay Ridge Rd, Ste 230
Annapolis, MD 21403
Telephone: (410) 280-6133
Facsimile: (410) 280-8650
eturnbull@hollandlawfirm.com

von Lehmen__Staff_Maryland Cybersecurity Council__

Uploaded by: Greg Lehmen

Position: FAV

TESTIMONY PRESENTED TO THE
SENATE FINANCE COMMITTEE

SB 541(MARYLAND ONLINE DATA PRIVACY ACT OF 2024)

DR. GREG VON LEHMEN
STAFF, MARYLAND CYBERSECURITY COUNCIL

POSITION: SUPPORT
February 14, 2024

Madam Chair, Vice Chair, and members of the committee, thank you for the opportunity to testify. I am Dr. Greg von Lehmen, staff to the Maryland Cybersecurity Council, a statutory body chaired by Attorney General Brown. I am here to support SB 541 as consistent with Council recommendations.

I urge favorable consideration for three reasons.

The bill provides much needed risk-management tools for consumers. When it comes to their sensitive data, consumers are very vulnerable. As this committee knows, data about every aspect of our lives is collected at scale, attached to our personal identities, bought, sold, and diffused across many companies. Much of this activity is without our informed consent or knowledge. A report published by the Maryland Attorney General’s Office indicates that in FY 2022 alone there were almost a million reported Maryland residents whose personal identifying data was impacted by more than 1,300 breaches.¹ The consumer rights in this bill to know, to delete, to opt-out of the sale of personal data are tools that can enable consumers to shrink this exposure. We are talking about the prospect of less ID theft, fewer financial account takeovers, reduced extortion, and on and on.

Second, this bill benefits from national experience. There are now 13 states that have comprehensive consumer privacy rights legislation.² This is a bipartisan effort.

¹ Office of the Attorney General Identity Theft Program. (2023). *Data Breaches FY 2022 Snapshot*. <https://www.umgc.edu/content/dam/umgc/documents/md-cybersecurity-council/data-breaches-fy-2020-snapshot-pdf.pdf> Note: The number of affected residents stated may overstate the number of unique residents impacted. This is because breaches are reported independently by each entity, making it possible that some residents were affected by more than one breach. This is particularly true when viewed longitudinally. The cumulative number of separately reported Maryland residents affected for the four snapshot reports to date comes to more than 6.2 million. The four reports are for 2016, 2018, 2020, and 2022.

² *US State Privacy Legislation Tracker*. (2024, February 2). IAPP. <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>

California was the first. But in the mix is Texas, Tennessee, Virginia, Delaware, and a number of other red and blue states. There is some variation among their statutes reflecting different equilibria of interests. An example is whether to include the right of private action. But at their core, these statutes are very similar. Senate Bill 541 is informed by this experience. It is a good bill for Maryland.

Finally, the question is: if not now, when? The 13 states that I mentioned represent 35% of the American population. In my count, this is the fourth session of the General Assembly that a comprehensive consumer privacy bill has been proposed.³ Given the risks, Maryland residents deserve to be allowed a greater role in controlling their exposure to breaches and the consequences. Senate Bill 541 would do this. The time is now.

I urge favorable consideration of the bill.

Thank you.

³ The others are HB 807/SB 698 (2023), SB 11 (2022), and SB 930 (2021).

SB0541_Common Sense Media_Grosshans_FAV.pdf

Uploaded by: Holly Grosshans

Position: FAV



Written Testimony of Holly Grosshans

Senior Counsel, Tech Policy; Common Sense Media

Before the Maryland Senate Finance Committee

regarding

“Maryland Online Data Privacy Act of 2024”

Bill No: SB0541

Position: Favorable

February 14, 2024

My name is Holly Grosshans. I am the Senior Counsel for tech policy at Common Sense Media, the nation’s largest organization dedicated to ensuring that children and families thrive—and remain safe—in the rapidly-changing digital age. In Maryland alone, more than 2,000 teachers have registered to teach Common Sense Media’s digital citizenship and literacy materials to their students in nearly 800 Common Sense recognized schools. But perhaps most importantly, I am the mother of two elementary school-age children and I care deeply about the privacy and well-being of my kids, and the millions of children like them, who are depending on this committee and this legislature to establish desperately-needed protections for their online safety, privacy, and overall well-being.

My testimony will focus on the consumer risks associated with unregulated online data privacy, the potential harms of personal data processing and targeted advertising to kids and teens, and how the Maryland Online Data Privacy Act will be an effective tool to protect Marylanders’ online privacy.

I. Introduction: Internet privacy is a pressing issue; states are beginning to regulate

Common Sense Media strongly supports the proposed Maryland Online Data Privacy Act of 2024 (SB0541). Recent research makes it clear that concerns about internet privacy are growing—as many as 71% of Americans are worried about how companies are using their personal data, while 89% are somewhat or very concerned about social media companies collecting data about kids.¹ As of this writing, 13 states² have passed comprehensive data privacy bills while at least 20 more³ have proposed bills that would particularly strengthen kids’

¹ Colleen McClain et al., *How Americans View Data Privacy*, Pew Research (Oct. 18, 2023).

² F. Paul Pittman, *US Data Privacy Guide*, White & Case (Feb. 5, 2024).

³ Kirk J. Nahra, *State Child Privacy Law Update*, WilmerHale (Feb. 28, 2023).

data privacy protections. Common Sense believes that Maryland’s kids and families also deserve strong data privacy protections and so supports the Maryland Online Data Privacy Act.

Among the provisions of this bill that we particularly support, this bill offers strong protections against the sale of user data and targeted advertising, will prevent companies from pretending they don’t have kids on their sites, and will protect teenagers’ privacy and create additional benefits for safety. While we recommend that the bill could be further strengthened by clarifying the ban on targeted advertising to children under 13 by changing 14-4607(A)(5) to remove “at least 13 years old and” so that it applies to all consumers under 18, Common Sense Media offers our unambiguous support for your bill.

II. Background: Marylanders, and especially kids, suffer from a lack of data privacy

There is no comprehensive federal data privacy law, and the only federal children’s data privacy law is 25 years old. Maryland does not have its own online data privacy law for adults or for minors. This leaves Marylanders in significant need of this legislation.

The vast majority of Americans believe that they have little or no control over their personal data.⁴ Many report that companies are too opaque about what they do with user data for individuals to even have a say, and the majority of surveyed Americans who report taking their data privacy seriously think that even their making good privacy decisions would have little or no impact on whether companies actually collect their data. Recent consumer research suggests Americans are troubled by this state of affairs—74% of whom rate their data privacy as highly important to them.⁵ But there are also practical concerns: lack of robust data privacy increases the risk of abuse, fraud, and identity theft, and may dissuade users from visiting certain sites or taking advantage of certain internet resources.

Data privacy concerns are particularly acute for kids. Recent research suggests that kids’ internet usage is at an all-time high.⁶ Teens are spending an average of 4.5 hours per day on their phones, with about a quarter of them spending as much as 5 to 8 hours in front of their screens every day. Nearly half of teens report that they feel addicted to their phones.⁷ Teens connect with each other through these platforms at higher rates than any other group, report that these platforms form a larger part of their social life than any other group, and have outsized levels of difficulty stopping technology use once they’ve started.⁸ And kids and teens must use technology for educational purposes, meaning that K–12 students in Maryland and elsewhere don’t have the option to avoid tech and the data privacy concerns it raises. As a result, teens and kids are being surveilled by platforms and having their behavior tracked, packaged, and sold to third-parties at an alarming rate.

⁴ McClain et al., *supra*.

⁵ *What Is Data Privacy & Why Is It Important?*, Dashlane (Apr. 18, 2023).

⁶ Jenny S. Radesky et al., *Constant Companion: A Week in the Life of a Young Person’s Smartphone Use*, Common Sense (2023).

⁷ Kim Chronister, *Teen Phone Addiction*, Key Healthcare (May 4, 2022).

⁸ *Id.*

Worse still, teens are more susceptible than older users to targeted ads and to data mining. Teens are far more likely to overshare information about themselves online thanks in part to their unique social relationship with media platforms, and in part to the underdevelopment of the parts of their brain responsible for dealing with judgment and long-term consequences.⁹ Research suggests teens are less able to identify targeted advertising and, in many cases, don't fully understand that features like algorithmic personalization both require large amounts of their data to function properly and make it harder for teens to stop or decrease screen time.¹⁰

Data privacy regulation is sorely needed. As Americans seek greater protection for their online data and wish for greater control over how their data is used, trust in online companies and their ability to self-regulate is at an all-time low. Decisive regulatory action is the only option and Common Sense supports the Online Data Privacy Act as exactly this kind of action.

III. Common Sense Media Supports the Maryland Online Data Privacy Act of 2024

The Online Data Privacy Act is essential legislation to protect online privacy for kids and their families. We point to three provisions that, as we understand the legislation, provide robust protections.

Strong Protections Against Sale of User Data and Targeted Advertising — Section 14-4607(A) broadly prohibits and limits the collection of personal data “for the sole purpose of content personalization or marketing” without consent from the user. It further bans outright the sale of “sensitive data” which includes data of children under 13. Common Sense believes that these provisions are essential to protecting privacy online. They protect children, teens, and everyone from having their behavior tracked, processed, and monetized. The provisions enable adult users to have control over how their data is used by requiring their consent to process their data. And they allow consumers autonomy in what they choose to reveal to companies; permitting users to make case-by-case judgment calls about the value of the personalization service relative to their data privacy.

The bill also safeguards teens. It only permits sale of teen data with user consent, and creates a blanket ban on the processing for purposes of targeted advertising of teens' (aged 13-18) user data. That there is no consent provision for teens to opt-in to processing and sale of their data is an important safeguard for teens. Otherwise, teens who are primed to engage in risky behavior for short-term rewards may be tempted to give up privacy in order to maximize the personalization of their user experience but, as mentioned, may not fully be able to grasp the consequences of doing so.

As noted above, while we support this section of the bill we believe it could be strengthened. The bill could be clarified with respect to targeted advertising and children under 13; it is not clear that targeted advertising is outright prohibited with respect to such users as it is with

⁹ Devorah Heitner, *Here's why your teen overshares online, and why that could be good*, Washington Post (Sept. 15, 2023).

¹⁰ Samuel Levine, *Protecting Kids from Stealth Advertising in Digital Media*, FTC (Sept. 2023).

teenagers. Specifically, we recommend changing 14-4607(A)(5) to remove “at least 13 years old and” so that it applies to all consumers under 18. This would maximize the Bills’ protection of the most vulnerable users.

Prevent Companies From Pretending They Don’t Have Kids On their Sites — Throughout the bill, heightened protections apply when platforms “know or should have known” that a user was either a child (under 13) or a teen (13-18). Common Sense emphasizes its support for this ‘knew or should have known’ language throughout the bill. The ‘should have known’ portion powerfully holds companies to account by preventing them from pleading ignorance of violations. Without such language, platforms are incentivized to purposefully turn a blind-eye to user age so as to claim they ‘didn’t know’ that their data collection activity swept in children or teens. The ‘should have known’ language creates a statutory safeguard against that ignorance defense by holding companies to what they could reasonably know, not just what they choose to note in their records.

Protect Teenagers’ Privacy and Create Knock-on Benefits for Safety — The bill gives heightened protections not just to children 12 and under, but also to teenagers. This fills an important gap in the federal Children’s Online Privacy Protection Act (COPPA), which currently applies only to children under 13 years of age. In particular, several aspects of the Online Data Privacy Act balance the interests of protecting teens’ data privacy while also encouraging them to develop autonomy concerning their own user data.

As referenced above, teens in particular are spending more and more time on their phones and report skyrocketing rates of digital addiction. This state of affairs is no idle coincidence; social media companies’ business model—based on targeted advertising and data collection—encourages the production of addictive design features such as endless scrolling pages and notification nudging. Common Sense additionally supports this bill to help change those incentives. A general prohibition on the use and sale of consumer data, and children’s data in particular, would curtail the incentive to create features that encourage users to spend more time on their phones.

IV. Conclusion

Marylanders’ online data privacy is currently underprotected and susceptible to use or abuse by companies and others. This presents a particular threat for Maryland’s kids and teens, who are the most vulnerable with respect to data breaches and targeted advertising. The Maryland Online Data Privacy Act creates a stalwart framework for protecting adults’ and childrens’ data privacy, while balancing consumers’ interests in personalized user experiences and parents’ interests in their kids’ online development. Common Sense applauds the bill sponsors for bringing forward this important legislation at a critical time for children and teens online and we urge the committee and the Senate to approve this important measure.

SB 541_MNADV_FAV.pdf

Uploaded by: Melanie Shapiro

Position: FAV



BILL NO: Senate Bill 541
TITLE: Maryland Online Data Privacy Act of 2024
COMMITTEE: Finance
HEARING DATE: February 14, 2024
POSITION: **SUPPORT**

The Maryland Network Against Domestic Violence (MNADV) is the state domestic violence coalition that brings together victim service providers, allied professionals, and concerned individuals for the common purpose of reducing intimate partner and family violence and its harmful effects on our citizens. **MNADV urges the Senate Finance Committee to issue a favorable report on SB 541.**

Senate Bill 541 is an important example of policy and laws that are needed to keep up with rapidly evolving technology. This bill provides protections to consumer information collected online. Most people do not understand the laws governing information shared online and may think that information is in fact protected when it is not protected. For victims of domestic violence, privacy is of the utmost importance and can be critical for their safety.

MNADV supports this legislation because it would allow Maryland to protect the privacy of consumer information. Online vendors would be restricted, except in limited circumstances, from sharing or redisclosing sensitive consumer data without the express consent of the consumer. The legislation also provides additional protection for consumers seeking reproductive and behavioral health services by prohibiting the use of geofencing data to track those consumers.

For the above stated reasons, the **Maryland Network Against Domestic Violence urges a favorable report on SB 541.**

NCADD-MD - 2024 SB 541 FAV - MD Online Data Privac

Uploaded by: Nancy Rosen-Cohen

Position: FAV



**Senate Finance Committee
February 14, 2024**

**Senate Bill 541
Maryland Online Data Privacy Act of 2024
Support**

NCADD-Maryland supports Senate Bill 541 which provides privacy protections for consumer information collected online. The bill generally prohibits the disclosure of consumer information collected by online vendors, unless the disclosure is essential to provide the service offered by the vendor.

There has been a proliferation of online platforms, including downloadable apps, that collect personal information, including sensitive health information. Many of these platforms are not subject to Health Insurance Portability and Accountability Act (HIPAA), as it only protects the electronic health records of health care providers and related business entities, such as health insurers. While these companies establish their own privacy policies, they can be challenging for consumers to navigate and realize a full understand their implications.

There has been an increase in the popularity and use of health and wellbeing apps. There are dozens of apps related to supporting mental health and alcohol and drug use concerns. Unlike prescribed digital therapeutics which we have discussed in this committee in previous years, these apps are not subject to HIPAA, leaving consumers' data at the mercy of the privacy policies set by the vendors. While there has been some attention paid to this issue by the Federal Trade Commission, an individual state has no authority to protect its own residents unless the state adopts specific statutory protections.

NCADD-Maryland supports this legislation because it would allow Maryland to protect the privacy of consumer information. Online vendors would be restricted, except in limited circumstances, from sharing or redisclosing sensitive consumer data without the express consent of the consumer. The legislation also provides additional protection for consumers seeking behavioral health services by prohibiting the use of geofencing data to track those consumers.

We urge a favorable report on Senate Bill 541.

SB541 Testimony - FAVORABLE Peter Holland.pdf

Uploaded by: Peter Holland

Position: FAV

The **HOLLAND LAW FIRM**
for Consumer Rights

Peter A. Holland
Attorney at Law
peter@hollandlawfirm.com

The Holland Law Firm, P.C.
Mailing Address:
914 Bay Ridge Rd, Ste 230
Annapolis, MD 21403

February 13, 2024

Hon. Chair, Senator Beidle, Senate Finance Committee
cc: Members, Senate Finance Committee

**RE: Testimony to the Senate Finance Committee
SB541 – Maryland Online Data Privacy Act**

Position: Favorable

Dear Chair and Members of the Committee,

Our law firm focusses on consumer protection and consumer privacy, including representing many victims of identity theft.

Maryland needs a data privacy law, and I am writing to express my strong support for SB541 because it will give individuals the right to access the information held by businesses about them. This is important because of the degree of false and inaccurate information which exists about many consumers, and because presently no such right to access exists.

At present a patchwork of state and federal laws protect limited fragments of consumer data. However, the bulk of consumer data can be freely exploited by businesses, with little transparency and not even a right of access that data businesses hold on them. SB 541 is a major step toward giving consumers greater access to their own personal data.

Respectfully,

/s/ Peter A. Holland
Peter A. Holland
THE HOLLAND LAW FIRM, P.C.
914 Bay Ridge Rd, Ste 230
Annapolis, MD 21403
Telephone: (410) 280-6133
Facsimile: (410) 280-8650
peter@hollandlawfirm.com

Maryland PIRG SB0539 Testimony + Report.pdf

Uploaded by: RJ Cross

Position: FAV

SB0539: Maryland Online Data Privacy Act of 2024
February 13, 2024
R.J. Cross, Maryland PIRG
Favorable

Maryland PIRG is a state based, small donor funded public interest advocacy organization with grassroots members across the state. We work to find common ground around common sense solutions that will help ensure a healthier, safer, more secure future.

When we use our favorite apps, websites and smart devices, the companies on the other side are often gathering information about us. Sometimes it's data that makes sense; Amazon needs your shipping address to send you a package. Often, however, the data companies collect [far exceeds](#) what's necessary for delivering the service consumer's are expecting to get, and they often use it for irrelevant purposes. These practices are incredibly common - and dangerous for consumers' personal security.

The more data that companies collect about you, and the more companies they sell it to or share it with, the more likely it is your information will be exposed in a breach or a hack. This makes it more likely your information will end up in the wrong hands like with identity thieves or scammers.

The Online Data Privacy Act of 2024, as currently drafted, will protect Maryland residents against threats to their personal security. It is imperative that this legislation does not get watered down.

The heart of the Online Data Privacy Act that will most benefit consumers is its data minimization provisions. These are common sense protections that will make sense to everyone. Namely:

- Limiting the collection of personal data to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer. This would solve the problem of, for example, the fast food chain Tim Hortons allegedly using its [mobile ordering app](#) to harvest the location data of users 24/7, even when the app was closed. Tim Hortons doesn't need to collect my location every day in order for me to place an order at the nearest restaurant once.
- Prohibiting companies from processing, sharing or selling sensitive data - such as health, religious beliefs, or geolocation - in ways that have nothing to do with delivering the service a consumer is expecting to get. This would stop educational apps used by schools, for example, from [selling schoolchildren's data](#) to data brokers and advertising companies. This protection is crucial for minors, but it makes sense for everyone.

The Maryland Online Data Privacy Act of 2024 should strengthen this latter provision to prohibit the secondary uses of **all** consumer data, not just sensitive information. This would be a clear cut solution that is intuitive to people: only gather my data when it's necessary, and use it for what I'm expecting. It makes sense, and it's the single best thing we can do to protect people's personal security.

There are a few additional provisions we believe should be further added to strengthen the bill. This includes:

- Narrow the Gramm-Leach-Bliley carveout, 14-4603 (3). As drafted, this provision exempts financial institutions or their affiliates (a broad term) from having to follow any of the provisions in this bill. This would better serve consumers if it were limited to just a data-level exemption, like what this bill has done for HIPAA-covered data.
- Narrow the loyalty program exemption, 14-4607(c)(2). As drafted, this provision leaves open the possibility of businesses requiring consumers consent to having their data sold or shared as a part of receiving discounts. Loyalty programs are often [a vehicle](#) for excessive data harvesting. This provision should be clarified.
- Add in a private right of action. Allowing consumers to sue for violating their rights is a [regular target](#) of industry lobbyists. But the best way to deter companies from breaking the law is knowing there will be repercussions. With so many companies to police, it is a very big job for just the AG alone. Allowing consumers to hold companies accountable in court for violating their rights is a much greater deterrence.

A word of warning: Across the country, states are trying to pass data privacy laws that protect people. However, many of them end up facing [significant efforts](#) by [corporate trade](#) groups and [tech lobbyists](#), playing states [off one another](#) and [weakening protections](#) for [consumers](#). Many of the bills have become so industry-friendly, they do virtually nothing for the people they're supposed to protect.

Maryland has the opportunity to take a different path.

This bill is not perfect. We and the Electronic Privacy Information Center recently [released a report](#) grading state privacy bills for how well they actually protect consumers. As drafted, the Maryland Online Data Privacy Act of 2024 receives a B- .

Even so, this bill would put real, meaningful protections in place for any Marylander who uses the Internet.

We respectfully request a favorable report.

Find attached the full text of our joint report with EPIC, including a summary of Maryland's grade.

The State of Privacy

**How state “privacy” laws fail to
protect privacy and what they can
do better**

**Maryland PIRG Foundation
Electronic Privacy Information Center (EPIC)
February 2024**

The State of Privacy:

**How state “privacy” laws fail to protect
privacy and what they can do better**

Written by:

Emily Scarr

R.J. Cross

Maryland PIRG Foundation

Caitriona Fitzgerald

Kara Williams

Electronic Privacy Information Center (EPIC)

February 2024

Maryland PIRG
Foundation

epic.org

ELECTRONIC
PRIVACY
INFORMATION
CENTER

Acknowledgements

EPIC wishes to thank Reset Tech Action, who provided funding that supported the work on this report. We also wish to thank our generous donors, who make it possible for us to stand up to Big Tech as an independently funded organization.

Maryland PIRG Foundation wishes to thank Edmund Coby and Ellen Hengesbach for their substantial research and editorial contributions to this report. We also wish to thank the Rose Foundation for Communities and the Environment for their generous support of our education work and our citizen donors for enabling us to stand up for their rights and the public interest in the long-term.

EPIC and Maryland PIRG Foundation would both like to acknowledge state legislators and their staffs nationwide: You work tirelessly and diligently, often on tight deadlines and with tight resources, in service of your constituents. You have our respect and our thanks.

The authors bear responsibility for any factual errors. Policy recommendations are those of Maryland PIRG Foundation and EPIC. The views expressed in this report are those of the authors and do not necessarily reflect the views of our funders or those who provided review.

The Electronic Privacy Information Center (EPIC) is a 501(c)(3) non-profit public interest research and advocacy center in Washington, D.C. EPIC was established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. Our mission is to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. For more information about EPIC, please visit www.epic.org.

With public debate around important issues, often dominated by special interests pursuing their own narrow agendas, Maryland PIRG Foundation, a 501(c)3 organization, offers an independent voice that works on behalf of the public interest. We investigate problems, craft solutions, educate the public, and offer meaningful opportunities for civic participation, all to better protect the public interest. For more information about Maryland PIRG Foundation, please visit <https://pirg.org/maryland/foundation/>.

Table of contents

- Executive summary..... 3**
- Introduction..... 5**
- The problem: Without rules, data abuse runs rampant..... 7**
 - Many companies collect and use data in surprising — and risky — ways.....7
 - Unchecked data collection puts consumers’ security at risk, turbocharges targeted scams, and increases the odds of identity theft..... 9
 - Data used to profile consumers often leads to discriminatory outcomes.....10
 - Current data practices can inundate consumers with annoying — and even harmful — targeted ads.....11
- Why this is happening: Big Tech is writing the rules..... 13**
- The solution: What a strong privacy law looks like.....16**
 - Features of strong state-level regulations..... 16
 - Data minimization..... 16
 - Strong enforcement..... 18
 - Rulemaking authority..... 19
 - Civil rights protections..... 19
 - Transparency and assessing high-risk data practices..... 19
 - Meaningful individual rights..... 20
 - Banning manipulative design and unfair marketing..... 21
 - Importance of strong definitions..... 22
- Grading on a curve: How state laws fail to protect consumers’ privacy and security..... 24**
 - California: an advancing “B” state..... 25
 - The middling “C” states Colorado..... 26
 - Colorado..... 26
 - New Jersey..... 27
 - Oregon..... 28
 - Delaware..... 29
 - Lagging “D” states..... 30
 - Connecticut..... 30
 - New Hampshire..... 31
 - Montana..... 32
 - The failing “F” states..... 33
 - Texas..... 33
 - Virginia..... 33
 - Indiana..... 33
 - Tennessee..... 33
 - Utah..... 33
 - Iowa..... 33
- Maryland’s opportunity to buck the trend..... 35**
- Appendix A: Methodology..... 36**
- Appendix B: Grading criteria..... 38**

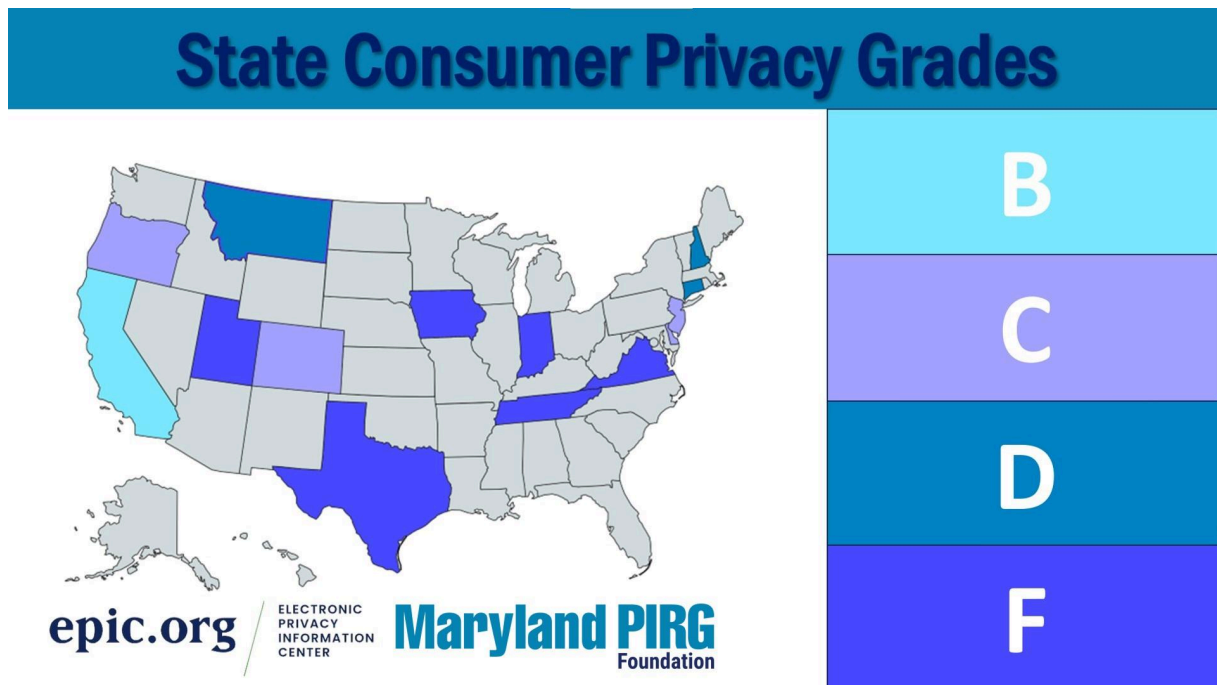
Executive summary

Today, much of our lives are lived online. How we work, learn, and play is often mediated by screens with companies on the other side gathering data about us. Often, these practices are out of line with what consumers expect, and they put consumer security and privacy at risk.

The more data companies collect about us, the more our data is at risk. When companies hold your data, the greater the odds it will be exposed in a breach or a hack and end up in the hands of identity thieves, scammers, or shadowy companies known as data brokers that buy and sell a huge amount of data about Americans. The unregulated online advertising and data broker market can result in turbocharged scams, discrimination, and invasive targeted ads. Yet there are very few rules that prevent all this from happening.

In our evaluation of the 14 states that have passed consumer privacy legislation, nearly half received failing grades, and none received an A.

Despite data collection and sales being a multi-billion-dollar industry propagated by some of the most powerful companies in the world, the U.S. has no federal privacy law. Therefore, an increasing number of states are passing laws that purportedly aim to give people more control over their information. However, these laws largely fail to adequately protect consumers. In our evaluation of the 14 states that have passed consumer privacy legislation, nearly half received failing grades, and none received an A.



Weak, industry-friendly laws allow companies to continue collecting data about consumers without meaningful limits. Consumers are granted rights that are difficult to exercise, and they cannot hold companies that violate their rights accountable in court.

Big Tech has played a big role in the passage of weak state privacy bills. Of the 14 laws states have passed so far, all but California's closely follow a model that was initially drafted by industry giants such as Amazon. In an analysis of lobbying records in the 31 states that heard privacy bills in 2021 and 2022, the Markup identified 445 active lobbyists and firms representing Amazon, Meta, Microsoft, Google, Apple, and industry front groups. This number is likely an undercount.

No laws should be written by the companies they are meant to regulate. Allowing Big Tech to heavily shape our privacy rules allows them to consolidate their already outsized power in the economy and in our lives. Privacy rules should balance the scale in favor of the billions of people who rely on the internet in their day-to-day lives.

State	Grade	Score
California	B+	69
Colorado	C+	41
New Jersey	C	37
Oregon	C-	31
Delaware	C-	30
Connecticut	D	24
New Hampshire	D	22
Montana	D	20
Texas	F	16
Indiana	F	11
Virginia	F	11
Utah	F	6
Tennessee	F	6
Iowa	F	4

A strong comprehensive consumer privacy law would:

- impose data minimization obligations on companies that collect and use personal information – taking the burden off of individuals to manage their privacy online and instead requiring entities to limit their data collection to better match consumer expectations;
- strictly regulate all uses of sensitive data, including health data, biometrics, and location data;
- establish strong civil rights safeguards online and rein in harmful profiling of consumers;
- provide strong enforcement and regulatory powers to ensure the rules are followed; and
- enable consumers to hold companies accountable for violations in court.

A better future is possible. As of this writing, states including Maryland, Illinois, Maine, and Massachusetts are considering strong legislation that would force changes to the abusive data practices driving commercial surveillance and online discrimination, while allowing businesses to continue to innovate. We can have a strong technology sector while also protecting personal privacy. And states can lead the way.

Introduction

In today's world, our lives are increasingly lived online. Nearly everything we do is mediated through personal devices, turning every click, search, and purchase we make on our favorite apps and sites into data points that are collected by companies on the other side of our screens.

These companies — many of whom you've never heard of and don't know you're interacting with — have turned your information into a lucrative business model, threatening your data security and privacy along the way.

In the last two decades, an entire invisible economy has materialized made up of thousands of secretive data companies trafficking in the information of nearly every American. Even companies that are household names are increasingly opening new revenue streams by gathering a lot more data from consumers than is necessary and using it for secondary purposes that have nothing to do with delivering the service consumers are expecting to get.¹

Consumers are increasingly aware of the extent of this near-constant data collection, even though in most cases they don't have a way to stop it. Over 80% of Americans are concerned about how companies collect and use their data.² Many are worried that the growth of artificial intelligence will lead companies to use even more personal data in ways people are not expecting and would not be comfortable with.³

Over 80% of Americans are concerned about how companies collect and use their data.

Despite the public's growing unease, meaningful protections for consumers are largely nonexistent. The U.S. still lacks a comprehensive federal privacy law. The few sector-specific laws that do exist — such as the Electronic Communications Privacy Act and the Health Insurance Portability and Accountability Act — were passed in the '80s and '90s, meaning they fail to address 30 years of significant technological changes and increasingly invasive data practices.⁴

For example, HIPAA essentially only covers personal health information in the hands of traditional doctors' offices and insurance companies. Today's healthcare, however, takes place across a

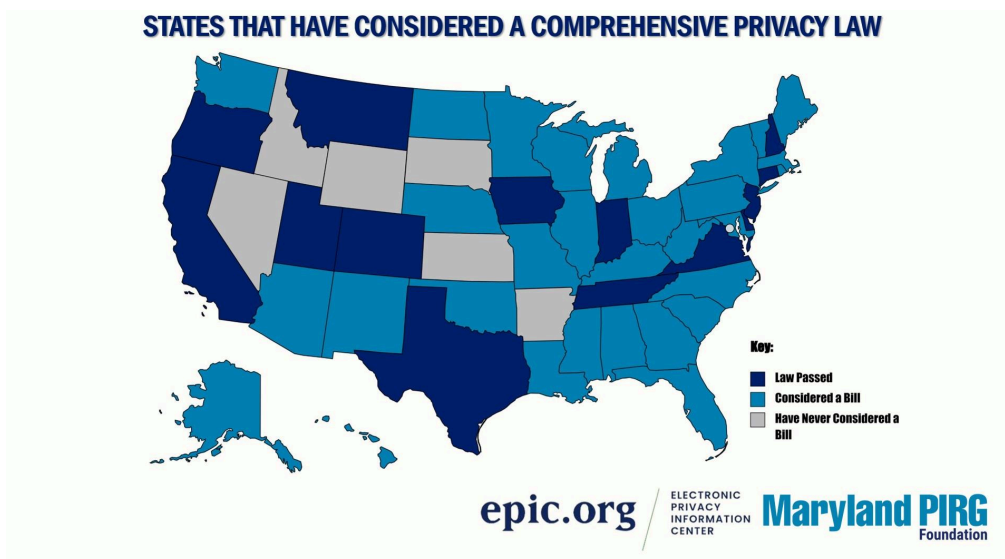
¹ R.J. Cross, *The New Data Brokers: Retailers, Rewards Apps & Streaming Services Are Selling Your Data*, PIRG (June 16, 2023), <https://pirg.org/articles/the-new-data-brokers-retailers-rewards-apps-streaming-services-are-selling-your-data/>.

² Pew Research Center, *How Americans View Data Privacy* (Oct. 18, 2023), <https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-data-and-digital-privacy-laws/>.

³ *Id.*

⁴ EPIC, *Grading on a Curve: Privacy Legislation in the 116th Congress* (April 2020), <https://epic.org/wp-content/uploads/2022/01/EPIC-GradingOnACurve-Apr2020.pdf>.

fragmented array of websites, smartphone apps, and wearable devices like Fitbits that generate and collect data most Americans would consider sensitive health information on a near-constant basis. Because of HIPAA's narrow scope and its passage before these technologies were in common practice, none of this data is protected, and it can all be mined, bought, and sold for commercial use. This runs understandably counter to the expectations of consumers. A 2023 study found that over 80% of Americans assume that the health data collected by apps is covered by HIPAA, even though it isn't.⁵



This lack of regulation has allowed companies to embed commercial surveillance into every aspect of the web. In the absence of strong federal privacy laws, states have begun to take action. Since 2018, 44 states have considered legislation to protect people’s privacy and security. As of February 1, 2024, 14 of those states have passed such laws.⁶

Unfortunately, the vast majority of these statutes fail to give consumers real and meaningful protections and can even end up putting consumers in harm’s way. Many of these laws have been heavily influenced by the very industry they seek to regulate. Consumers are told they have “privacy rights,” but due to the way the laws are written, those rights are nearly impossible for the average American to exercise. Meanwhile, the laws allow Big Tech to continue amassing and abusing our personal data for its own benefit.

In this report, EPIC and Maryland PIRG Foundation have come together to shed light on the alarming trend of poor state privacy laws, why these issues affect us all, and what we can do to change course.

⁵ *Many Americans Don’t Realize Digital Health Apps Could Be Selling Their Personal Data*, ClearData (July 13, 2023), <https://www.cleardata.com/many-americans-dont-realize-digital-health-apps-could-be-selling-their-personal-data/>.

⁶ Andrew Folks, *US State Privacy Legislation Tracker*, IAPP (Jan. 19, 2024), <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>.

The problem: Without rules, data abuse runs rampant

Without meaningful limits on the collection and use of personal data, many companies are incentivized to collect as much data about consumers as possible and to retain it indefinitely. This out of control data collection puts consumers' security and privacy at risk.

Many companies collect and use data in surprising — and risky — ways.

Almost every interaction we have online generates data about us. Sometimes this data collection matches our expectations — Amazon needs your shipping address to send you a package, and Uber needs your location to pick you up. But often, the collection and use of your data is far outside of what you'd expect.

For example, the fast-food chain Tim Hortons was accused by Canadian authorities in 2022 of using its mobile app to harvest users' location data 24/7, even when the app was closed.⁷ And, according to a Mozilla Foundation investigation last year, all 25 major car brands may collect surprisingly intimate data from customers, including in some cases geolocation, health diagnoses, and genetic information using your car's onboard computers and companion apps.⁸

The reality is that tracking systems are embedded in nearly every website you visit and app you download, and they begin to collect information as soon as you connect, tracking your every click, search, and movement across the web.

Companies are incentivized to use our data for purposes that have nothing to do with what we're expecting to get. For example, a 2022 BuzzFeed investigation found the Christian site Pray.com was releasing detailed data about its users with third parties, including Facebook, meaning "users could be targeted with ads on Facebook based on the content they engage with on Pray.com — including content modules with titles like 'Better Marriage,' 'Abundant Finance,' and 'Releasing Anger.'"⁹ A 2022 study by Human Rights Watch found that educational apps and websites used

⁷ Ian Austen, 'A Mass Invasion of Privacy' but No Penalties for Tim Hortons, N.Y. Times (June 11 2022), <https://www.nytimes.com/2022/06/11/world/canada/tim-hortons-privacy-data.html>.

⁸ Jen Caltrider, Misha Rykov & Zoe MacDonald, *It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy*, The Mozilla Foundation (Sept. 6 2023), <https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/>.

⁹ Emily Baker-White, *Nothing Sacred: These Apps Reserve The Right To Sell Your Prayers*, BuzzFeed (Jan. 25, 2022), <https://www.buzzfeednews.com/article/emilybakerwhite/apps-selling-your-prayers>.

by schools were harvesting the data of millions of schoolchildren, sending children’s information to data brokers and advertising technology companies while they learned.¹⁰

The reality is that tracking systems are embedded in nearly every website you visit and app you download, and they begin to collect information as soon as you connect, tracking your every click, search, and movement across the web. And with the increasing proliferation of “smart” devices in homes, offices, and other locations, oftentimes your personal data is being collected even when you aren’t intending to interact with an online service at all. Other activities like credit card purchases¹¹ and even physical movements¹² can be logged and tracked without your awareness.

A recent study from the Irish Council for Civil Liberties found that the Real-Time Bidding market, which is where companies exchange user browsing, location, and other data to drive targeted advertising, alone exposes the average American’s data 747 times per day.¹³ This means U.S. internet users’ online activity and location are being tracked and disclosed 107 trillion times per year.¹⁴

These trackers collect millions of data points each day that are sold or transferred to data brokers, who then combine them with other personal data sources to build invasive profiles. Data brokers are shadowy companies that buy, aggregate, disclose, and sell billions of data elements on Americans, all with virtually no oversight.¹⁵ The profiles they build on us are often used to target us with “personalized” advertisements that stalk us across the web. In other cases, these profiles are fed into secret algorithms used to determine the interest rates on mortgages and credit cards, to raise consumers’ interest rates, or to deny people jobs, depriving them of opportunities.

This ubiquitous tracking of everything we do online, and the entities that aggregate and monetize it, poses threats to consumers’ privacy, autonomy, and security. And it shouldn’t be allowed to continue unregulated. The rules we suggest in this report would limit data collection and use to what is *reasonably necessary* for the product or service you’re requesting, better lining up companies’ data practices with your expectations. This would limit cross-site tracking and stop the flow of endless amounts of personal data to data brokers.

¹⁰ Drew Harwell, *Remote Learning Apps Shared Children’s Data at ‘Dizzying Scale’*, Wash. Post (May 24, 2022), <https://www.washingtonpost.com/technology/2022/05/24/remote-school-app-tracking-privacy/>.

¹¹ R.J. Cross, *How Mastercard Sells its ‘Gold Mine’ of Transaction Data* (Sept. 2023), <https://pirg.org/edfund/resources/how-mastercard-sells-data/>.

¹² Michael Kwet, *In Stores, Secret Surveillance Tracks Your Every Move*, N.Y. Times (June 2019), <https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html>

¹³ Irish Council for Civil Liberties, *The Biggest Data Breach ICCL Report on Scale of Real-Time Bidding Data Broadcasts in the U.S. and Europe* (May 2022), <https://www.iccl.ie/wp-content/uploads/2022/05/Mass-data-breach-of-Europe-and-US-data-1.pdf>.

¹⁴ *Id.* at 2.

¹⁵ EPIC, *Data Brokers*, <https://epic.org/issues/consumer-privacy/data-brokers/>.

Unchecked data collection puts consumers' security at risk, turbocharges targeted scams, and increases the odds of identity theft.

The more data companies collect about us, the more our data is at risk. When companies store our information for longer than necessary, or sell it to other entities, it greatly increases the odds that our personal information will be exposed in a breach or a hack. Once exposed, hackers and other bad actors sell information like consumers' names, contact information, bank account information, personal relationship data, and buying habits on underground markets online. Your information can end up on robocall lists or with identity thieves and scammers. The security of our financial accounts can be compromised when hackers have access to the vast tracking data that online companies generate.

In 2022, the FTC received more complaints about identity theft — over 1.1 million complaints from consumers — than any other category.

These problems affect millions of Americans every year. In 2022, the FTC received more complaints about identity theft — over 1.1 million complaints from consumers — than any other category.¹⁶ The second most common complaint was about imposter scams — schemes where fraudsters falsely claim to be a relative in distress,

a business a consumer has shopped at previously, or an authority figure requesting money or personal information. In 2022, consumers lost nearly \$2.7 billion to imposter scams.¹⁷ The more personal information scammers have about a consumer's life, the more convincing these scams become.

Data brokers may even work directly with scammers. Brokers may compile “suckers lists” of ideal victims most likely to fall for certain types of scams. In 2020 and 2021, the U.S. Department of Justice charged three major data brokers for knowingly supplying lists of millions of vulnerable Americans to scammers, including elderly Americans and people with Alzheimer's.¹⁸

The best way to protect consumer data is to not collect, or not store, personal data beyond what is reasonably necessary. Data that is never collected in the first place, or that is quickly deleted, cannot be breached. The most important step states can take to strengthen data security is to enact a comprehensive privacy law that includes a strong data minimization rule.

¹⁶ FTC, *Consumer Sentinel Network Databook 2022* (Feb. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf.

¹⁷ *Id.*

¹⁸ Alistair Simmons & Justin Sherman, *Data Brokers, Elder Fraud, and Justice Department Investigations*, LawFare (July 25, 2022), <https://www.lawfaremedia.org/article/data-brokers-elder-fraud-and-justice-department-investigations>.

Data used to profile consumers often leads to discriminatory outcomes.

In many cases, the massive collection of data in the hands of data brokers means that consumers are sorted and scored in discriminatory ways.¹⁹ Data brokers build detailed profiles about individuals with information ranging from basic contact information to purchasing habits to sensitive information like race, income, sexuality, and religion. Using raw data, brokers often summarize people with tags such as “working-class mom,” “frequent alcohol drinker,” “financially challenged,” or “depression sufferer.”

Virtually no American is untouched by data brokers. One firm studied by the FTC reported having 3,000 data segments on nearly every U.S. consumer.²⁰ Despite never directly interacting with you, they hold massive amounts of your personal data, which they then use to create your profile.

One firm studied by the FTC reported having 3,000 data segments on nearly every U.S. consumer.

These ever-growing profiles are used to shape customers’ experience of the websites they visit in ways that are entirely opaque to them. These profiles can alter what we see, what prices we pay, and whether we are able to find the information that we seek online (including information about job opportunities, health services, and relationships).

This profiling reinforces discrimination by allowing advertisers to decide who should see a specific product. Advertisers can use characteristics like race, gender, or income (or ZIP code as a proxy for income) to filter their audience and target individuals most likely to buy their product or service. If a company is hiring a CEO, advertisers can choose to show that job opening to only men. If a home is for sale, advertisers can choose to show that listing to only white individuals.

In fact, Facebook was sued by the Department of Housing and Urban Development in 2019 for allowing advertisers to conduct this type of discrimination.²¹ HUD charged Facebook with engaging in housing discrimination by allowing advertisers to control which users saw ads based on characteristics like race, religion, and national origin.²²

¹⁹ See EPIC, Comments to FTC Proposed Trade Regulation Rule on Commercial Surveillance & Data Security (Nov. 2022), <https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf>.

²⁰ FTC, *Data Brokers: A Call for Transparency and Accountability* (May 2014), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-feral-trade-commission-may-2014/140527databrokerreport.pdf>.

²¹ Charge of Discrimination, HUD, et al v. Facebook, Inc., FHEO No. 01-18-0323-8 (Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.

²² *Id.*

Many state laws give consumers the right to opt-out of profiling, which is a step in the right direction. States should also include strong anti-discrimination provisions that prohibit companies from using data in discriminatory ways.

Current data practices can inundate consumers with annoying — and even harmful — targeted advertising.

Massive troves of consumer data flow into the targeted advertising industry. Ads designed to follow users across the Internet can be exhausting and annoying; Americans are inundated with an estimated 5,000 ads daily, up from 500 a day in the 1970s.²³ While consumers can protect their mailboxes from junk mail and phones from spam calls, there's no real recourse for Americans to protect their screens from annoying, distracting, and invasive ads.

Some targeted ads aren't just annoying — they can be predatory and harmful, using people's online behavioral data to reach vulnerable consumers that meet specific parameters. People searching terms like “need money help” on Google have been served ads for predatory loans with staggering interest rates over 1,700%.²⁴ An online casino targeted ads to problem gamblers offering free spins on its site.²⁵ In another example, 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.²⁶

Advertising can still serve businesses' objectives without relying on the collection and sale of personal data that put consumers unnecessarily in harm's way. Many companies rely instead on contextual advertising, serving ads on podcasts based on the topics discussed and likely audiences they intend to reach based on their interests. For example, a company that sells running shoes would likely find their intended audience by advertising on a health and fitness podcast. This type of rich contextual advertising is the evolution of techniques that were traditionally used in print and broadcast media for decades, and this method doesn't require monitoring of users' browsing history or the creation of individual consumer profiles. And some research shows that consumers prefer contextual ads over specifically targeted ones. A study by Seedtag and Nielsen found that contextual advertising actually increases consumer interest by

²³ USCDornsife, *Thinking vs. Feeling: The Psychology of Advertising* (Nov. 17, 2023), <https://appliedpsychologydegree.usc.edu/blog/thinking-vs-feeling-the-psychology-of-advertising>.

²⁴ 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>.

²⁵ 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>.

²⁶ 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>.

32% and that 85% of consumers who saw contextual ads instead of targeted ads were more open to seeing future ads.²⁷

Much of the pervasive tracking that drives targeted ads is not necessary. Online advertising and other business data uses would look different without it, but businesses would still be able to offer goods and services, and advertising could work fine without it. But Big Tech doesn't want to fix the problem they have created. They built systems that invade our private lives, spy on our families, and gather the most intimate details about us for profit, so they oppose legislation that meaningfully protects your privacy. And because of their outsized influence on state policy, we are left with weak privacy laws that do little to protect consumers. The rules we propose in this report allow companies to continue advertising to their intended customers but in a way that doesn't involve ubiquitous tracking of our every movement online.

²⁷ Press Release, Seedtag, *Seedtag and Nielsen Research Finds Contextual Targeting Boosts Consumer Interest in Advertising by 32%* (May 11, 2022), <https://press.seedtag.com/seedtag-and-nielsen-research-finds-contextual-targeting-boosts-consumer-interest-in-advertising-by-32>.

Why this is happening: Big Tech is writing the rules

How can all this be happening? Many consumers would likely be shocked to learn just how little their data is protected and that policymakers have largely failed to take meaningful action.

The U.S. still lacks a comprehensive federal privacy law. The few-sector specific laws that do exist were passed in the '80s and '90s, failing to capture how smartphones and constant internet access have given companies entirely new and unprecedented access to individuals' personal information.²⁸ These outdated laws also fail to cover the relatively new phenomenon of online data brokers — arguably the worst actors in this ecosystem — that have only materialized in the last 20 years.

Because Congress has failed to pass a comprehensive privacy law to regulate the technologies that dominate our lives today, state legislatures have tried to fill the void in order to protect their constituents' privacy. Unfortunately for consumers, in states across the country, legislators introducing consumer privacy bills have faced a torrent of industry lobbying vying to weaken protections. Nearly everywhere, they have succeeded. Of the 14 laws states have passed so far, all but California's closely follow a model that was initially drafted by industry giants such as Amazon.²⁹

Of the 14 laws states have passed so far, all but California's closely follow a model that was initially drafted by industry giants such as Amazon.

In 2021, Virginia became the second state in the nation to pass a comprehensive consumer data privacy law. Where California's law — which was passed in 2018 — established some real protections, Virginia's was almost entirely void of meaningful provisions. A notable difference: While California's rules became law in response to a proposed ballot question, Virginia's legislation had been handed to the bill sponsor by an Amazon lobbyist, and it was based on an earlier bill from Washington state that had been modified at the behest of Amazon, Comcast, and Microsoft.³⁰

The Virginia law was weak: Companies could continue collecting whatever data they wanted as long as it was disclosed somewhere in a privacy policy. While consumers could, in theory, request

²⁸ *Grading on a Curve*, *supra* note 4.

²⁹ Jeffrey Datin, Chris Kirkham & Aditya Kalra, *Amazon Wages Secret War on Americans' Privacy, Documents Show*, Reuters (Nov. 19, 2021), <https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/>.

³⁰ Emily Birnbaum, *From Washington to Florida, Here Are Big Tech's Biggest Threats from States*, Protocol (Feb. 19, 2021), <https://www.protocol.com/policy/virginia-maryland-washington-big-tech>; Mark Scott, *How Lobbyists Rewrote Washington State's Privacy Law* (Apr. 2019), <https://www.politico.eu/article/how-lobbyists-rewrote-washington-state-privacy-law-microsoft-amazon-regulation/>.

companies delete their data, they would have to submit requests one at a time to the hundreds — if not thousands — of entities holding their information. Consumers also had no ability to hold companies accountable in court for violating the privacy law meant to protect them. Virginia, in this scorecard, receives an F.

“Virginia is what the lobbyists were asking for,” Walke said. “Making the bill weaker, I understood. Compromise is always necessary. But making it as weak as Virginia is something I have never understood.”

Unfortunately, Virginia became the model lobbyists have pushed many state legislators to match, particularly in red states such as Kentucky and Montana.³¹ In Oklahoma, former state legislator Collin Walke was asked to water down his 2021 Oklahoma Computer Data Privacy Act.

“It was a bipartisan bill,” Walke said in an interview for this report. “People liked it. Before it even hit the House floor it had some 40 co-authors. It passed out of the House 85-11.” When Walke’s bill stalled in the Senate, he knew he was going to have to negotiate some changes. What he didn’t expect, however, was the lobbyist push for a noticeably weaker, Virginia-style bill.

“Virginia is what the lobbyists were asking for,” Walke said. “Making the bill weaker, I understood. Compromise is always necessary. But making it as weak as Virginia is something I have never understood.”

More recently, and particularly in blue states, lobbyists have pivoted to pushing the “Connecticut model” — a bill similar to Virginia with a couple of concessions to consumers.³² Most notably, Connecticut allows consumers to use a browser tool to automatically opt-out of websites collecting data. The law, however, included no ability for a regulator like the Attorney General to specify what exactly the tool should look like, leaving open questions about how well the provision would serve its purpose. In a pattern seen across the country, the law that passed in Connecticut in 2022 ended up weaker than what co-sponsor Sen. Bob Duff had introduced

³¹ Alfred Ng, *How Montana Passed the Strongest Privacy Law Among Red States*, Politico (June 17, 2023), <https://www.politico.com/news/2023/06/17/montana-tech-privacy-law-00101511>; Anna Edgerton, *Tech Lobbyists Don’t Want States to Let You Sue Over Privacy Violations*, Bloomberg (Mar. 20, 2023), <https://www.bloomberg.com/news/articles/2023-03-20/big-tech-lobbyists-are-fighting-strict-data-privacy-laws-state-by-state>.

³² See, e.g., Letter from Tyler Diers, Technet, to Minnesota State Representative Steve Elkins (Jan. 19, 2024), <https://www.lcc.mn.gov/lcdp/meetings/01222024/TechNet-MN-HF2309.pdf> (“TechNet urges you to consider interoperability with existing models as the default position. As you know, it is important that privacy bills across the country provide for interoperability and we appreciate your efforts with other legislators in other states to do so. To date, 12 states have enacted privacy laws that borrow from the Virginia/Connecticut framework. Each new concept or definitional change could result in consumer confusion and significantly increase compliance costs for businesses.”)

previously — notably from his 2020 privacy bill, which included the ability for consumers to sue.³³ Connecticut, in this scorecard, receives a D.

In 2023, the pressure and the strategy remained the same. In Oregon, for example, the State Privacy and Security Coalition — an industry group representing Amazon and Meta, among others — testified at one point that a stronger draft of the Oregon Consumer Privacy Act “still deviate[d] from other state privacy laws” as to “need significant work.”³⁴ In Delaware, the Computer Communications Industry Association — an industry group representing Google and Apple, among others — encouraged in testimony that the state’s bill should “more consistently align with definitions and principles in other existing comprehensive state privacy laws,” pointing to Virginia and Connecticut in particular.³⁵

Industry lobbying has profoundly shaped how states approach consumer privacy, and their efforts have been significant; an investigation by the Markup identified 445 active lobbyists and firms representing Amazon, Meta, Microsoft, Google, Apple, and industry front groups in the 31 states that heard privacy bills in 2021 and 2022. Because of the opacity of state lobbying records, that number is likely an undercount.³⁶

The accelerating passage of industry-preferred bills not only poses a threat for the residents of the states passing ineffectual laws. The more states that coalesce around regulations heavily influenced by the very industries that need to be regulated, the greater the risk of lowering the bar for the effectiveness of a future federal law, which is exactly what industry is hoping for.

³³ Todd Feathers, *Big Tech Is Pushing States to Pass Privacy Laws, and Yes, You Should Be Suspicious*, The Markup (Apr. 15, 2022), <https://themarkup.org/privacy/2021/04/15/big-tech-is-pushing-states-to-pass-privacy-laws-and-yes-you-should-be-suspicious>.

³⁴ *RE: SB 619 (Comprehensive Privacy)*, written testimony submitted by the State Privacy & Security Coalition (Mar. 6, 2023), <https://olis.oregonlegislature.gov/liz/2023R1/Downloads/PublicTestimonyDocument/61538>.

³⁵ *RE: HB 154 – “the Delaware Data Privacy Act” (Oppose unless Amended)*, written testimony by the Consumer & Communications Industry Association submitted to the Delaware state Senate Banking, Business, Insurance & Technology Committee (June 26, 2023), <https://ccianet.org/library/ccia-comments-on-delaware-hb-154/>.

³⁶ Todd Feathers & Alfred Ng, *Tech Industry Groups Are Watering Down Attempts at Privacy Regulation, One State at a Time*, The Markup (May 26, 2022), <https://themarkup.org/privacy/2022/05/26/tech-industry-groups-are-watering-down-attempts-at-privacy-regulation-one-state-at-a-time>.

The solution: What a strong privacy law looks like

Privacy is a fundamental right, and our laws should reflect that. In this section, we lay out the provisions that states should include in their comprehensive privacy laws to adequately protect consumers online.

Features of strong state-level regulations

Existing state privacy laws simply do not do enough to change business as usual – the collection of endless amounts of personal data that is then used in ways that defy consumers’ expectations. These laws only generally allow individuals to access, correct, and delete personal data about them, or opt-out of certain uses of data – if they have the time and expertise to do so, which is often not the case. On their own, these aren’t real privacy protections.

States should instead impose data minimization obligations on companies that collect and use personal information – taking the burden off individuals to manage their privacy online and instead requiring entities to limit their data collection to better match consumer expectations. They should strictly regulate all uses of sensitive data, including health data, biometrics, and location data. They should establish strong civil rights safeguards online and rein in harmful profiling of consumers. And there needs to be strong enforcement and regulatory powers to ensure the rules are followed.

Data minimization

The excessive data collection and processing that fuels commercial surveillance systems is inconsistent with the expectations of consumers, who reasonably expect that their data will be collected and used for the limited purpose to provide the goods or services that they requested.

Companies should not have a limitless ability to decide how much personal data to collect. Unfortunately, this is what most state laws, including the Virginia and Connecticut “model” laws, allow. By limiting collection to what is reasonably necessary for “the purposes for which such data is processed, *as disclosed to the consumer*,” businesses can collect data for whatever purposes they want, as long as they state that purpose in their privacy policies. 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.

These exploitative practices don’t have to continue. Instead, states can integrate a concept that has long been a pillar of privacy protection: the idea that data collection and use should be limited to what’s necessary in context, known as “data minimization.” To implement this concept, states should integrate the following protections into their privacy laws:

- Data collection, processing, and transfer should be limited to what is reasonably necessary for the product or service an individual requests or for a clearly defined, enumerated permissible purpose. Knowledge or consent should only be relied on in limited circumstances where appropriate.
- Controllers should be required to delete personal data after the data is no longer necessary.
- Very strict limits should be placed on the collection and processing of highly sensitive data, such as biometric, genetic, and precise geolocation data (a “strictly necessary” standard is best).
- Most secondary processing and transfers should be prohibited by default with only narrow exceptions.
- Transfers of sensitive data to third parties (other than to processors) should be prohibited, unless the transfer is strictly necessary and done with affirmative opt-in consent.
- Processors should be explicitly prohibited from engaging in secondary uses and combining data from multiple controllers, and they must adhere to their required contracts with controllers.

Data minimization is essential for both consumers and businesses. Data minimization principles give consumer confidence in using technology, knowing there are rules in place that limit the use of their personal data. And a data minimization rule can provide clear guidance to businesses when designing and implementing their data policies.

Data minimization provisions also increase data security. A data minimization framework means that businesses are collecting less personal data about consumers and promptly deleting data they no longer needed. Ultimately, this means businesses have less data overall, making it less likely that consumer data will be exposed in a data breach.

DATA MINIMIZATION	CA	CO	CT	DE	IN	IA	MT	NH	NJ	OR	TN	TX	UT	VA
Strong data minimization	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Sensitive data collection restriction	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Sensitive data transfer restriction	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Prompt data deletion	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Secondary uses/transfers prohibited	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Universal opt-out signals	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✗	✓	✗	✗

Strong enforcement

Robust enforcement is critical to effective privacy protection. Strong enforcement by state governments via Attorney General authority or the creation of a state privacy agency is a vital piece to include in a strong privacy law.

But while government enforcement is essential, the scope of data collection online is simply too vast for one entity to regulate, particularly state Attorneys General with limited resources. Individuals who use these online services are in the best position to identify privacy issues and bring actions to vindicate their privacy interests. These cases preserve the state's resources, and statutory damages ensure that companies will face real consequences if they violate the law.

A private right of action is the most important tool legislatures can give to their constituents to protect their privacy. Many federal privacy laws include a private right of action, and these provisions have historically made it possible to hold companies accountable for their privacy violations. A private right of action ensures that controllers have strong financial incentives to comply with state privacy laws. We have seen evidence of this in Illinois,³⁷ where a biometric privacy law passed in 2008 includes a private right of action. Lawsuits under that law have led to changes to harmful business practices, such as forcing facial recognition company Clearview AI to stop selling its face surveillance system to private companies.³⁸

ENFORCEMENT	CA	CO	CT	DE	IN	IA	MT	NH	NJ	OR	TN	TX	UT	VA
AG rulemaking	✓	✓	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
AG enforcement authority	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Right to cure *	DISC	SUN	SUN	SUN	MAND	MAND	SUN	SUN	SUN	SUN	MAND	MAND	MAND	MAND
Private right of action	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Injunctive relief	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Statutory damages	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Privacy agency	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

* DISC = Discretionary

SUN = Sunsets

MAND = Mandatory

³⁷ Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), <https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf>.

³⁸ Ryan Mac & Kashmir Hill, *Clearview AI Settles Suit and Agrees to Limit Sales of Facial Recognition Database*, N.Y. Times (May 9, 2022), <https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html>.

Rulemaking authority

California, Colorado, New Jersey, and, to a limited extent, New Hampshire have all included rulemaking authority in their state privacy laws. Rulemaking authority is critical in providing guidance to businesses on compliance with the law and ensuring the law can keep pace with technology.

Civil rights protections

Most state privacy laws attempt to prevent discrimination online by prohibiting the processing of personal data in ways that violate state and federal anti-discrimination laws. However, existing civil rights laws contain significant gaps in coverage and do not apply to disparate impact.³⁹ These issues make existing laws insufficient to ensure all people are protected from discrimination online. Therefore, states 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.”

Transparency and assessing high-risk data practices

Companies collecting and using personal data should be required to assess their systems that present risks of harm to consumers. Many states have included requirements to conduct data protection impact assessments or other similar risk assessments, which can help with meaningful oversight, if done right.

To be meaningful, these assessments should include documentation of what personal data is being collected, why that personal data is being collected, whether and how that personal data is being used and transferred/sold, what risks there are to consumers from use of their personal data, potential benefits to the consumer from the collection and use of their personal data, an explanation of why these benefits outweigh the risks, how these risks are being mitigated, and identification of alternatives to profiling and why these alternatives were rejected.

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.

³⁹ 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>.

Critically, a version of this risk assessment (or, at minimum, a summary of the risk assessment) must be accessible to the public. Without this requirement, these assessments can simply become internal box-checking exercises.⁴⁰

TRANSPARENCY AND DATA SECURITY	CA	CO	CT	DE	IN	IA	MT	NH	NJ	OR	TN	TX	UT	VA
Data security requirement	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Privacy policy standards	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Notice of policy changes	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
Accessible privacy policies	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Impact assessments	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓
Reasonable time	✗	✓	✗	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗
Regularly reviewed	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Publicly available	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

Meaningful individual rights

Every state privacy law reviewed in this report contains some form of individual rights. These rights typically include the right to access and correct inaccuracies in your personal data and to request its deletion. These rights alone are not enough to protect privacy, but they are an important component of any comprehensive privacy bill.

There are four key protections within individual rights that states should integrate to make those rights meaningful:

- Require companies to honor universal opt-out signals. Many states have included this requirement in their privacy laws.
- Deletion rights should apply to any data connected to a consumer, not solely data collected from the consumer. The language from Connecticut’s law can be used (“delete personal data provided by, or obtained about, the consumer”).
- Oregon and Delaware have added the right to obtain information about third parties to whom a company has disclosed your personal data.
- 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

⁴⁰ See generally Ari Ezra Waldman, *Industry Unbound* (2021) (demonstrating that many privacy impact assessments conducted under GDPR have become little more than checkbox forms).

Consumer Reports have found that it helps make consumers' individual rights more meaningful.⁴¹

CONSUMER RIGHTS	CA	CO	CT	DE	IN	IA	MT	NH	NJ	OR	TN	TX	UT	VA
Right to access	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Right to correct	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓
Right to delete	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓
Authorized agent can exercise	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Profiling opt-out	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓
Bans discrimination for using rights	✓	✗	✓	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗
Protection for minors' data	✓	✗	✓	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗

Banning manipulative design and unfair marketing

Individuals should not be forced to trade basic privacy rights to obtain services. Such provisions undermine the purpose of privacy law: to ensure baseline protections for consumers.

There are a few key protections states should include in their privacy laws to prevent unfair business practices. First, the use of data collected for loyalty programs should be limited to what is functionally necessary to operate the loyalty program. Companies should not be able to collect consumers' personal data with the promise of a discount or loyalty program perk and then turn around and sell that data to other companies to make a profit. Companies do not need to sell personal data to scores of third parties in order to operate a loyalty program. The use of personal data collected for such programs for cross-site targeted advertising and sale to third parties should be prohibited.

Second, states should prohibit discrimination against consumers who exercise their privacy rights. Consumers should not be charged a higher price for goods if they have opted out of targeted advertising.

⁴¹ 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/>.

Third, “dark patterns,” or manipulative design meant to subvert consumer choice, should be prohibited in both the definition of consent and in the provisions granting consumer rights. Design choices that purposely deter consumers from exercising their privacy rights undermine the very purpose of a privacy law – to empower consumers.

UNFAIR BUSINESS PRACTICES	CA	CO	CT	DE	IN	IA	MT	NH	NJ	OR	TN	TX	UT	VA
Civil rights protections	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Loyalty program data limits	✓	X	X	X	X	X	X	X	X	X	X	X	X	X
Prohibits dark patterns	✓	✓	✓	✓	X	X	✓	✓	✓	✓	X	✓	X	X

Importance of strong definitions

Definitions can make or break a privacy law. Some key definitions EPIC and U.S. PIRG analyzed in our review are:

Personal data: Personal data should be defined as information that is linked to or could be linked to a person, household, or device and should include inferences/derived data. Most states fail to include inferences or derived data. Sensitive inferences about us are often derived from publicly available data, and those should be covered in the definition of personal data. Pseudonymous data should not be exempted from the definition (or any portion of a privacy bill), as it includes identifiers such as IP addresses and device IDs that can be easily reassociated with an individual.

Controllers/covered entities: Ideally, state privacy laws should include all entities that handle personal data. Any threshold for coverage should be based on the amount of data a company collects or processes, not on revenue – many startups might have no revenue but do have the ability to collect mass amounts of sensitive personal data. Any carveouts for entities covered by existing privacy laws should be limited to the specific information protected by existing privacy laws, not the entity (or their affiliates) as a whole. For example, many states exempt entities covered by the Gramm-Leach-Bliley Act (GLBA). GLBA is weak legislation that primarily requires financial institutions to offer an opt out of disclosure to third parties and does not provide even basic access or deletion rights. It is inappropriate to exempt entire entities from coverage of a comprehensive privacy law simply because some of the data they collect is covered by a federal law with limited privacy protections.

Sale/share/transfer: Most privacy laws modeled on Virginia or Connecticut define “sale of personal data” so narrowly that it fails to cover many harmful data uses that consumers should be protected from. The definition should be broadened to include making data available for any commercial purpose, not only for monetary or other valuable consideration. Many unexpected

secondary uses of consumers’ personal data happen when access to their personal data is sold for the purposes for targeting or profiling, but because the personal data itself is not exchanged in these instances, these uses fall outside of many definitions. This was one of the primary reasons that California’s privacy law was updated via ballot question in 2020.

Profiling: Any definition of profiling or automated decision-making system should focus on the function of the system (aiding or replacing human decision-making) and cover both sophisticated AI models and simpler algorithms and automated processes. The definition in the Connecticut law is a good model definition.

Targeted advertising: The definition of targeted advertising should match consumer expectations of what that term means. States should be careful not to incorporate loopholes into this definition that would fail to cover companies with massive troves of consumer data, such as Google and Meta, using that data to serve targeted ads – to do so would defeat the entire purpose of a targeted advertising opt-out.

Biometric data: Most state laws define biometric data too narrowly, requiring that the biometric data “is used” to identify an individual. Biometric data should include information that could be used to confirm the unique identification of a consumer rather than limited to data that is affirmatively used to do so. A fingerprint or faceprint is very sensitive data, whether it has been used to identify the individual yet or not.

STRONG KEY DEFINITIONS	CA	CO	CT	DE	IN	IA	MT	NH	NJ	OR	TN	TX	UT	VA
Personal/covered data	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗
No pseudonymous exemption	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✗	✗	✓	✗
Biometric data	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗
Covered entity/controller	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓
Narrow carveouts	✓	✓	✗	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗
Sell/share	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗
Profiling	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓
Targeted advertising	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Grading on a curve: How state laws fail to protect consumers' privacy and security

We evaluated each of the 14 state comprehensive consumer privacy laws that have been passed as of February 1, 2024.

We graded the state laws based on the provisions explained above — elements that would be found in a privacy law that provides meaningful protections for consumers. The most important aspects of a protective privacy law — data minimization requirements, strong Attorney General enforcement and rulemaking, and a private right of action — earned the most points. Our full scorecard, including a breakdown of how points were allocated, can be found in Appendix B.

Of the 14 laws, nearly half received a failing grade. None received an A.

California: an advancing “B” state

California

California Consumer Privacy Act
Date law took effect: January 1, 2020
Score: 69/100

B+

In 2018, California passed the nation's first comprehensive privacy law, the California Consumer Privacy Act. This law was amended in 2020 when voters passed a ballot initiative known as the California Privacy Rights Act, which strengthened the 2018 law. As it stands today, California's privacy law is the strongest in the nation, though it does lack many critical consumer protections.

California recently passed the DELETE Act,⁴² which would allow California residents to make one deletion request that all data brokers in the state must comply with. Under the text of the CCPA and corresponding regulations, the right to delete applies only to personal information provided by the consumer (rather than personal data obtained about the consumer). However, the recently enacted DELETE Act, which will be enforced by the California Privacy Protection Agency, covers the deletion of all personal data about a consumer who submits a request. Based on these protections, we awarded California the point for the right to delete.

Privacy-protective provisions:

- Established an independent privacy agency with rulemaking authority
- Prohibits the use of financial incentive practices (such as loyalty programs) that are unjust, unreasonable, coercive, or usurious in nature
- Limited carveouts only for data regulated by other privacy laws (rather than entity-level)
- No exemption for pseudonymous data
- Privacy protections cannot be weakened by the Legislature

Missing provisions:

- Heightened protections for sensitive data by default
- Clear limits on cross-site browser tracking
- Detailed restrictions in statute's data minimization framework
- Private right of action for violations of the law outside of those that result in data breaches

Possible amendments/rulemaking:

- Strengthen the definition of biometric data.
- Strengthen anti-discrimination provision to provide meaningful civil rights protections.
- Continue using rulemaking authority to protect consumers' data and privacy rights.

⁴² Cal. Civ. Code § 1798.99.86 (West 2023).

The middling “C” states

Colorado

Colorado Privacy Act

Date law took effect: July 1, 2023

Score: 41/100



When Colorado enacted the Colorado Privacy Act in 2021, the state included strong rulemaking authority for the Attorney General for purposes of implementing the law. This has allowed the Attorney General to provide guidance to both businesses and consumers on the more technical aspects of the bill, such as what constitutes a dark pattern and how to implement a global opt-out mechanism. In July 2024, Colorado residents will be able to download and use the Global Privacy Control tool to automatically broadcast to websites that they don't want their data collected. (You can download that [here](#), and see CoPIRG's consumer guide [here](#).)

Privacy-protective provisions:

- Attorney general has rulemaking authority
- Requires controllers to honor global opt-out signals
- Limited carveouts only for data regulated by other privacy laws rather than broad, entity-level exemptions
- Robust prohibitions on dark patterns/deceptive design

Missing provisions:

- No private right of action
- Limited data minimization requirements

Possible amendments/rulemaking:

- Strengthen the definition of sell/share.
- Strengthen anti-discrimination provision to provide meaningful civil rights protections.
- Require companies to make impact assessments (or a summary) available to the public.
- Prohibit price discrimination against consumers who exercise their privacy rights.
- Continue using rulemaking authority to protect consumers' personal data and privacy rights.

New Jersey



Senate Bill 332 (name pending)

Date law will take effect: January 16, 2025

Score: 37/100

New Jersey is one of the most recent states to pass a privacy law. The governor signed it into law on Jan. 16, 2024.

Privacy-protective provisions:

- Attorney general has rulemaking authority
- No exemption for pseudonymous data

Missing provisions:

- No data minimization requirements
- No private right of action

Possible amendments/rulemaking:

- Strengthen anti-discrimination provision to provide meaningful civil rights protections.
- Require companies to make impact assessments (or a summary) available to the public.
- Strengthen definitions of personal data and biometric data.
- Change carveout for GLBA from all financial institutions covered by the law to only the data that is regulated by the law.
- Use rulemaking authority to its fullest extent to protect consumers' personal data and privacy rights.

Oregon



Oregon Consumer Privacy Act

Date law will take effect: July 1, 2024

Score: 31/100

Passed in June 2023, the Oregon Consumer Privacy Act was the result of a working group led by the Oregon Attorney General's office. Despite this, it still followed the Connecticut model, though Oregon did add some important protections – including minimizing the number of entities who were exempt from the law.

Privacy-protective provisions:

- No exemption for pseudonymous data
- Limited carveouts only for data regulated by other privacy laws rather than broad, entity-level exemptions
- Broad definition of sensitive data that includes “status as transgender or nonbinary” and “status as a victim of a crime”
- Adds a consumer right to obtain a specific list of third parties to which the controller has disclosed either that consumer's personal data or personal data generally

Missing provisions:

- No Attorney General rulemaking authority
- No private right of action
- No data minimization requirements

Possible amendments:

- Strengthen the definition of sell/share.
- Strengthen anti-discrimination provision to provide meaningful civil rights protections.
- Require companies to make impact assessments (or a summary) available to the public.

Delaware

Delaware Personal Data Privacy Act

Date law will take effect: January 1, 2025

Score: 30/100



The Delaware governor signed the Personal Data Privacy Act into law on Sept. 11, 2023. State lawmakers heard the same message from Big Tech that industry has repeated since passage of the Virginia "model": Delaware's bill should "more consistently align with definitions and principles in other existing comprehensive state privacy laws," pointing to Virginia and Connecticut.⁴³

Privacy-protective provisions:

- Bans targeted advertising to minors under 18 years old
- Broad definition of sensitive data that includes "status as pregnant" and "status as transgender or nonbinary"
- Gives consumer the right to obtain a list of the categories of third parties with whom the controller has shared the consumer's own personal data

Missing provisions:

- No Attorney General rulemaking authority
- No private right of action
- No data minimization requirements

Possible amendments:

- Strengthen definitions of personal data, sell/share, and biometric data.
- Change carveout for GLBA from all financial institutions covered by the law to only the data that is regulated by the law.
- Strengthen anti-discrimination provision to provide meaningful civil rights protections.
- Require companies to make impact assessments (or a summary) available to the public.

⁴³ The Computer Communications Industry Association (CCIA) — an industry group representing Google and Apple, among others — testified at hearings about the Delaware law. *RE: HB 154 – "the Delaware Data Privacy Act" (Oppose unless Amended)*, written testimony by the Consumer & Communications Industry Association submitted to the Delaware state Senate Banking, Business, Insurance & Technology Committee (June 26, 2023) <https://ccianet.org/library/ccia-comments-on-delaware-hb-154/>.

Lagging “D” states

Connecticut



Connecticut Data Privacy Act

Date law took effect: July 1, 2023

Score 24/100

Connecticut’s Data Privacy Act was first introduced in 2019 and originally included strong provisions such as a private right of action. The bill, however, was whittled down over time, making it more similar to Virginia’s failing law. In 2022, Connecticut’s bill was passed with a few additional provisions — such as requirements to honor global opt-out signals — making it a little stronger than Virginia. This bill has now become a favored piece of template legislation for lobbyists, particularly in bluer states.

A year after its original passage, Connecticut passed legislation amending the law to include heightened protections for kids and teens online and adding a category of sensitive data for “consumer health data.” The “Connecticut model” pushed by industry in other states does not include these updates.

Privacy-protective provisions:

- Requires controllers to honor global opt-out signals (though requirement that controllers “accurately determine” residency should be revised)
- Enhanced protections for minors under 18, including a ban on targeted advertising (Note: these additional protections are part of the 2023 amendments, not the original “Connecticut model” being pushed by industry.)

Missing provisions:

- No data minimization requirements
- No private right of action
- No Attorney General rulemaking authority

Possible amendments:

- Strengthen definitions of personal data, sell/share, and biometric data.
- Strengthen anti-discrimination provision to provide meaningful civil rights protections.
- Change carveouts for existing privacy laws to be data-level exemptions rather than entity-level exemptions.
- Require companies to make impact assessments (or a summary) available to the public.

New Hampshire



Senate Bill 255 (*name pending*)

Date law will take effect: January 1, 2025

Score: 22/100

New Hampshire is the most recent comprehensive consumer privacy law to pass. The bill passed out of the Legislature on Jan. 18, 2024 and is awaiting the governor's signature.

Privacy-protective provisions:

- Some Attorney General rulemaking authority (though limited)

Missing provisions:

- No data minimization requirements
- No private right of action

Possible amendments:

- Strengthen definitions of personal data, sell/share, and biometric data.
- Strengthen anti-discrimination provision to provide meaningful civil rights protections.
- Require companies to make impact assessments (or a summary) available to the public.
- Change carveouts for existing privacy laws to be data-level exemptions rather than entity-level exemptions.
- Expand Attorney General rulemaking authority to better protect consumers' personal data and privacy rights.

Montana



Consumer Data Privacy Act

Date law will take effect: October 1, 2024

Score: 20/100

Before Republican Sen. Daniel Zolnikov introduced the Consumer Data Privacy Act, a tech lobbyist told him the Connecticut model was too difficult for industry to comply with and that it would be better to introduce something closer to the weaker Virginia model. According to Politico, after Zolnikov heard the same lobbyist testify in Maryland — a blue state — that industry would be happy with a Connecticut model, he strengthened his bill.

Zolnikov has expressed frustration with being pushed to pass a weaker bill in Montana than in blue state counterparts. “I’m not an idiot,” Zolnikov said in an interview with Politico after the passage of his bill, directing his comments at the lobbyist. “And you treating us in Montana like a bunch of rural backwoods folks is quite an insult.”⁴⁴

Privacy-protective provisions:

- Requires controllers to honor global opt-out signals (though requirement that controllers “accurately determine” residency should be revised)
- Though it includes a right to cure for Attorney General enforcement, that requirement sunsets 18 months after enactment.

Missing provisions:

- No data minimization requirements
- No private right of action
- No Attorney General rulemaking authority

Possible amendments:

- Strengthen definitions of personal data, sell/share, and biometric data.
- Change carveouts for existing privacy laws to be data-level exemptions rather than entity-level exemptions.
- Strengthen anti-discrimination provision to provide meaningful civil rights protections.
- Require companies to make impact assessments (or a summary) available to the public.

⁴⁴ Ng, *supra* note 31.

The failing “F” states

Below are the 6 states that received an F: Texas, Virginia, Indiana, Tennessee, Utah, and Iowa. These laws all scored less than 20%.

The first of these states to pass a privacy law was Virginia. Amazon targeted business-friendly Virginia Sen. David Marsden and handed him ready-to-go legislation that would allow Big Tech’s business model to continue uninterrupted.⁴⁵ That bill became Virginia law in 2021 and quickly became the model pushed by the tech industry across the country.



Utah took the Virginia model and made it even more business-friendly, changing the law so that it only covered businesses making more than \$25 million. The state ultimately passed its failing law in March 2022.

Iowa, Indiana, Tennessee, and Texas all passed versions of this “Virginia model” throughout the spring and summer of 2023.

These laws’ dismal — and strikingly similar — scores reflect their weak, business-friendly language and lack of meaningful consumer protections. These state laws represent the first industry success stories, where the law written by Amazon, passed by Virginia, and copied by these states was enacted.

Texas

Texas Data Privacy and Security Act
Date law will take effect: July 1, 2024
Score: 16/100

Tennessee

Tennessee Information Protection Act
Date law will take effect: July 1, 2025
Score: 6/100

Virginia

Consumer Data Protection Act
Date law took effect: January 1, 2023
Score: 11/100

Utah

Utah Consumer Privacy Act
Date law took effect: December 31, 2023
Score: 6/100

Indiana

Consumer Data Protection
Date law will take effect: January 1, 2026
Score: 11/100

Iowa

Iowa Data Privacy Act
Date law will take effect: January 1, 2025
Score: 4/100

⁴⁵ Datin, Kirkham & Kalra, *supra* note 29.

None of these laws provides meaningful privacy protections to consumers.

Without a data minimization framework, these laws allow companies to continue their business as usual — collecting as much personal data as they can so that they can target individual consumers with incessant targeted advertisements, sell it to massive data brokers to aggregate and create profiles of consumers, and make enormous profits off of the thriving advertising ecosystem.

Without a requirement that businesses honor universal opt-out signals, consumers are forced to play whack-a-mole with companies, telling businesses one by one not to sell their data or target them with ads.

Without a private right of action, consumers have no way to protect the minimal privacy rights these laws do provide.

At best, these laws enshrine the status quo. At worst, they allow Big Tech to say they care about privacy while at the same time lobbying in states all across the country to strip away consumer protections and weaken privacy laws.

Maryland's opportunity to buck the trend

Maryland gets an “incomplete,” as it has yet to pass a comprehensive consumer privacy law. However, it currently has the opportunity to pass one of the strongest laws in the nation and disrupt the Big Tech and industry narrative.

Maryland Online Data Privacy Act (HB567/SB541)

B-

If the Maryland Online Data Privacy Act passed as currently written, it would be the second-strongest comprehensive privacy law in the country, trailing only California. The bill does not incorporate every recommendation we gave in this report, but it would provide real protections for Maryland residents that are not present in most other state laws.

The Maryland Online Data Privacy Act strictly limits the collection and use of sensitive data, limits data collection to what is reasonably necessary to provide a product or service, bans targeted advertising and sale of data of children and teens under 18, requires businesses to honor universal opt-out mechanisms, and includes strong civil rights protections.

While these provisions would provide Maryland residents with better privacy protections than residents of most other states, there is still more the Maryland Online Data Privacy Act could do. Adding provisions requiring data minimization for all data use instead of only collection, giving consumers a private right of action to protect their privacy rights in court, and granting the Attorney General rulemaking authority, would make this bill closer to an A grade.

Appendix A: Methodology

Which laws were evaluated?

We evaluated only state privacy laws that are comprehensive in scope and excluded more narrow laws focusing on one specific area of privacy. For example, laws such as Washington’s My Health, My Data⁴⁶ or Illinois’s Biometric Information Privacy Act⁴⁷ were not included in this report because they cover only a narrow slice of consumer data. While sectoral privacy laws like these do protect some types of information, this report focuses on state laws that claim to provide broad privacy protections for consumers across all types of personal data.

The states with comprehensive privacy laws that we evaluated are: California, Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah, and Virginia. We did not include the Florida Digital Bill of Rights as a comprehensive privacy law because of its limited applicability to only businesses with more than \$1 billion in revenue.⁴⁸

Funding

Even the most well-written comprehensive privacy law can only be effective if it allocates adequate funding for the Attorney General’s office to conduct rulemaking and enforce the law. Without funding to enforce the law, even laws that meet the above criteria are meaningless. Because of how vital adequate funding is, we included it on the scorecard as a key provision of a strong privacy law.

However, because states have different mechanisms for allocating funding (in separate appropriations bills, for example), we did not evaluate or assign any points to any state for this criteria. Funding is included in the scorecard to emphasize its importance, but it did not play a role in the grade any state received due to the difficulty in assessing this factor.

States with rulemaking authority

The laws in California, Colorado, and New Jersey all granted rulemaking authority to the state’s Attorney General. In scoring these laws, we awarded full points if the actual statutory text of the California and Colorado laws met our rubric criteria. We awarded partial points if those states’ regulations fulfilled our rubric criteria.

Because the New Jersey bill was only signed into law a few weeks before this report’s publication, the state does not yet have any regulations. Thus, New Jersey’s score was based only on the text of its statute.

⁴⁶ Wash. Rev. Code Ann. § 19.373.005 (West, Westlaw Edge through 2023 Reg. and First Special Sessions).

⁴⁷ 740 ILCS 14/1 (West 2008).

⁴⁸ § 501.701 Fla. Stat. (2023).

New Hampshire also granted extremely limited rulemaking authority to the Secretary of State. Based on this, New Hampshire received partial points in the rulemaking category, and given that the law was only signed into law a few weeks before this report's publication, there are no regulations yet to score.

Interactions with other state laws

There may be other state laws that could be relevant to some of the criteria we identified. For example, states may have anti-discrimination laws or data security laws that are separate from the comprehensive privacy laws we evaluated.

For the grading, we only generally considered the text of the specific statute we were evaluating as well as any corresponding regulations, when applicable. Because we did not have the ability to look at every law within each state that we graded, the grades are based solely on the text of the state's privacy law.

Appendix B: Grading criteria

STRONG KEY DEFINITIONS (6)

- **Personal data** definition should cover information that is linked or could be linked to a person, household, or device and should include inferences/derived data. (1)
 - *Exemption for pseudonymous data (-3 if present)*
 - *Or, if exemption for pseudonymous data applies only to consumers' rights to access, correct, delete (-1 if present)*
- **Controllers/covered entities** definition should include all entities that handle personal data, and requirements should be defined based on how much data entities process rather than their revenue. (1)
 - *Broad, entity-level carveouts for entities covered by existing privacy laws rather than narrow, data-level carveouts (-5 if present)*
 - *Or, if only some carveouts are entity-level while others are data-level (-3/-2 if present, depending on scope)*
- **Sell/share** definition should include disclosing, making available, transferring, or otherwise communicating personal data to a third party for monetary or other valuable consideration or otherwise for a commercial purpose. (1)
- **Profiling** definition should be defined as the use of an automated processing or decision-making system to process personal data to evaluate, infer, or predict information about an individual. (1)
- **Targeted advertising** definition should cover the targeting of advertisements to a consumer based on the consumer's interactions with one or more businesses, distinctly branded websites, applications, or services other than the business, distinctly branded website, application, or service with which the consumer intentionally interacts. (1)
- **Biometric data** definition should include information that can be used to confirm the unique identification of a consumer rather than information that is affirmatively used to do so. (1)

ENFORCEMENT AND REGULATORY BODIES (22)

- Strong rulemaking authority (8)
- Strong enforcement authority in the Attorney General or independent privacy agency (8)
 - No mandatory right to cure (6)
 - Right to cure at the discretion of the Attorney General (4)
 - Right to cure that sunsets (3)
 - Mandatory right to cure with no sunset (0)
- Establishes an independent privacy agency (+10)
- Appropriates adequate funding for rulemaking and enforcement*

ENFORCEMENT VIA PRIVATE RIGHT OF ACTION (14)

- Private right of action (7)
 - Injunctive relief available (4)
 - Statutory damages available (3)

DATA CONTROLLER/PROCESSOR OBLIGATIONS

Data Minimization (14)

- Data collection, processing, and transfer is limited to what is reasonably necessary for the product or service the consumer requested or a clearly defined, enumerated purpose (7)
- Data must be deleted when no longer necessary for original purpose (3)
- Collection and processing of sensitive data must be strictly necessary (4)
*Knowledge and consent did not receive any points.

Use and Disclosure Limitations (12)

- Prohibits most secondary processing and transfers by default (8)
 - Or, covered entities are required to honor universal opt-out signals (3)
 - Or, if covered entities are required to honor universal opt-out signals, but there are unnecessary authentication requirements (2)
- Transferring sensitive data to third parties is prohibited (unless strictly necessary and done with opt-in consent) (4)
- *Targeted advertising is banned (+5)*

Data Security Requirements (2)

- Controllers have a duty of care to protect data (2)

Transparency about Business Practices (-4 if not present)

- Controllers and processors must have privacy policies that meet certain minimum standards (-2 if not present)
- Consumers must be notified of material changes and given the opportunity to withdraw consent (-1 if not present)
- Privacy policies must be easily accessible to all consumers (-1 if not present)

Enhanced Protections for Children and Teens (+3)

- *Targeted advertising to minors is banned (+3)*
 - *Or, required opt-in consent for targeted advertising to teens (already required for children under 13 by COPPA) (+1)*

PROHIBITS DISCRIMINATORY USES OF DATA (5)

- Bans processing of data in a manner that discriminates, in treatment or effect, or otherwise makes unavailable the equal enjoyment of goods or services on the basis of a protected class (5)

**Provisions that only prohibit discrimination that violates state or federal law did not receive points.*

PROFILING AND IMPACT ASSESSMENTS (12)

- Requires controllers to conduct impact assessments that meet a minimum standard on use of personal data for profiling or other uses that present a risk of harm (4)
 - Impact assessments should be done within a reasonable time (1)
 - Impact assessments should be updated regularly (1)
 - Impact assessments (or a summary) should be made publicly available (4)
- Consumers have the right to opt-out of profiling (2)
- *Especially harmful uses of AI are prohibited (+5)*

INDIVIDUAL RIGHTS (6)

- Access (2)
- Accuracy and correction (2)
- Deletion (must include data obtained about a consumer, not just collected from the consumer) (2)

**One point was awarded for the existence of each right, and one point was awarded if authorized agents are allowed to exercise that right on behalf of a consumer.*

BANS MANIPULATIVE DESIGN AND UNFAIR MARKETING PRACTICES (7)

- Bans price discrimination against consumers who exercise individual rights, including the right to opt-out of targeted advertising (2)
- Limits use of loyalty program data to what is necessary to operate program (3)
- Bans dark patterns/deceptive design (2)
 - Or, if only dark patterns in obtaining consent were banned (1)

02.13 - SB 541 - Maryland Online Data Privacy Act

Uploaded by: Robin McKinney

Position: FAV



SB 541 - Maryland Online Data Privacy Act of 2024

Finance Committee

February 14, 2024

SUPPORT

Chair Beidle, Vice-Chair Klausmeier and members of the committee, thank you for the opportunity to submit testimony in support of Senate Bill 541. This bill will increase data rights protections for Marylanders.

The CASH Campaign of Maryland promotes economic advancement for low-to-moderate income individuals and families in Baltimore and across Maryland. CASH accomplishes its mission through operating a portfolio of direct service programs, building organizational and field capacity, and leading policy and advocacy initiatives to strengthen family economic stability. CASH and its partners across the state achieve this by providing free tax preparation services through the IRS program 'VITA', offering free financial education and coaching, and engaging in policy research and advocacy. **Almost 4,000 of CASH's tax preparation clients earn less than \$10,000 annually. More than half earn less than \$20,000.**

The ability for consumers to regulate how businesses collect and store their personal data and use their personal data is a right that all Marylanders should have. Consumer data is not only an issue of privacy but also an issue of security. Data breaches are disturbingly common incidents that impact consumers across Maryland. **In 2023, Maryland had over 500 instances of data breaches.**¹ There are already several large data brokers who collect volumes of information on consumers and sell the information for a fee.

SB 541 includes provisions on protecting an individual's private data, including biometric data. Biometric data consists of a person's unique physical characteristics like fingerprints, palmprints, voiceprints, facial, or retinal measurements. It is increasingly becoming more popular to use biometrics in law enforcement, healthcare, and commercial industries. As the use of this data becomes more popular, the risk to consumers of having their personal biometric data breached is also increased. Unfortunately, this can result in consumers becoming victims of identity fraud.

Low-income consumers are at even greater risk of harmful data breaches, as they are more likely to use older devices that aren't equipped for newer security updates.² SB 541 would establish greater data privacy protections for all Marylanders, which would be especially beneficial to low-income residents. Consumers must be very careful about who has access to their personal information. CASH supports legislation that will ensure Maryland remains a national leader in consumer protection policy.

Thus, we encourage you to return a favorable report for SB 541.

¹ <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/breachnotices.aspx>

² <https://carnegieendowment.org/2023/03/13/cyber-resilience-must-focus-on-marginalized-individuals-not-just-institutions-pub-89254#>

2024 ACNM SB 541 Senate Side.pdf

Uploaded by: Robyn Elliott

Position: FAV



Committee: Senate Finance Committee

Bill Number: SB 541 – Maryland Online Data Privacy Act of 2024

Hearing Date: February 14, 2024

Position: Support

The Maryland Affiliate of the American College of Nurse Midwives (ACNM) strongly supports *Senate Bill 541 – Maryland Online Data Privacy Act of 2024*. The bill would safeguard personal information collected online and provide consumers more control over the use and redisclosure of the data.

ACNM supports this legislation because not all health data is protected by the Health Insurance Portability and Accountability Act (HIPAA). HIPAA only protects the information collected by providers in electronic health records. State confidentiality laws extend similar protections to any paper health records. However, HIPAA and state laws do *not* protect health data that consumers provide to entities who are not connected to health care providers. For example, there are a proliferation of apps that help consumers track their menstrual cycles, health indicators such as heart rate, and sleep patterns.

This legislation is essential to providing safeguards, so that consumers may determine how their personal data is used and shared. It also provides essential protections to consumers seeking reproductive or behavioral health, as it prohibits the use of geofencing data that could later be used to penalize or intimidate consumers.

We urge a favorable report. If we can provide any further information, please contact Robyn Elliott at relliott@policypartners.net.

2024 LCPCM SB 541 Senate Side.pdf

Uploaded by: Robyn Elliott

Position: FAV



Committee: Senate Finance Committee

Bill Number: SB 541 – Maryland Online Data Privacy Act of 2024

Hearing Date: February 14, 2024

Position: Support

The Licensed Clinical Professional Counselors of Maryland supports *Senate Bill 541 – Maryland Online Data Privacy Act of 2024*. The bill provides protection of consumer information collected online. LCPCM supports this bill because there are a growing number of online vendors, including apps, that collect mental health information that is not protected by the Health Insurance Portability and Accountability Act (HIPAA). HIPAA only protects the information in health provider records. When there is a platform offered by entity not affiliated with a health care provider, there are few, if any, privacy protections in state or federal law. There are a growing number of platforms that advertise being able to help consumers improve their mental health and wellbeing. Consumers may be providing sensitive person information without understanding that there are virtually no legal barriers to the platform selling or redisclosing that data. The sharing of this data may be detrimental to consumers' health. Therefore, LCPCM supports this legislation which will begin to provide some safeguards to this data. We ask for a favorable report. If we can provide any further information, please contact Robyn Elliott at relliott@policypartners.net.

HIPAA only protections the information collected by providers in electronic health records. State confidentiality laws extend similar protections to any paper health records. However, HIPAA and state laws do *not* protect health data that consumers provide to entities who are not connected to health care providers. For example, there are a proliferation of apps that help consumers track their menstrual cycles, health indicators such as heart rate, and sleep patterns.

This legislation is essential to providing safeguards, so that consumers may disclose how their personal data is used and shared. It also provides essential protections to consumers seeking reproductive or behavioral health, as it prohibits the use of geofencing data that could later be used to penalize or intimidate consumers.

We urge a favorable report. If we can provide any further information, please contact Robyn Elliott at relliott@policypartners.net.

2024 WLCM SB 541 Senate Side.pdf

Uploaded by: Robyn Elliott

Position: FAV

Committee:	Senate Finance Committee
Bill Number:	SB 541 – Maryland Online Data Privacy Act of 2024
Hearing Date:	February 14, 2024
Position:	Support

The Women’s Law Center of Maryland (WLC) strongly supports *Senate Bill 541 – Maryland Online Data Privacy Act of 2024*. The bill provides privacy protections for consumer information collected online. The bill generally prohibits the disclosure of consumer information collected by online vendors, unless the disclosure is essential to provide the service offered by the vendor.

In recent years, there has been a proliferation of online platforms, including apps, that collect health and other sensitive personal information. Consumers may have an expectation of privacy, as the public generally thinks that health information is protected by the Health Insurance Portability and Accountability Act (HIPAA). However, many online platforms are not subject to HIPAA, as HIPAA only protects the electronic health records of health care providers and related business entities, such as health insurers.

Online platforms generally may set their own privacy policies. These policies, even when disclosed, may be challenging for consumers to navigate and fully understand their implications. WLC believes that the lack of privacy standards may compromise consumers’ safety and wellbeing; and in some cases, redisclosure of information may create legal peril for consumers.

There has been an increase in the popularity and use of health and wellbeing apps. Consumers can use apps to track their menstrual periods, sleep cycles, and mental health. However, most of these apps are not subject to HIPAA, leaving consumers at the mercy of the privacy policies set by the vendors. This problem has gained more attention in the wake of the *Dobbs* decision, as information from period tracking apps and geofencing data could be used by prosecute people leaving states that ban abortion to seek care elsewhere. The Federal Trade Commission has fined some period tracking apps for redisclosure of health information.^{i ii} However, an individual state has no authority to protect its own residents unless the state adopts specific statutory protections.

WLC supports this legislation because it would allow Maryland to protect the privacy of consumer information. Online vendors would be restricted, except in limited circumstances, from sharing or redisclosing sensitive consumer data without the express consent of the consumer. The legislation also provides additional protection for consumers seeking reproductive and behavioral health services by prohibiting the use of geofencing data to track those consumers.

We ask for a favorable report. If there is additional information that we can provide, please contact Robyn Elliott at relliott@policypartners.net.

The Women’s Law Center of Maryland is a private, non-profit, legal services organization that serves as a leading voice for justice and fairness for women. It advocates for the rights of women through legal assistance to individuals and strategic initiatives to achieve systemic change, working to ensure physical safety, economic security, and bodily autonomy for women in Maryland.

ⁱ <https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc>

ⁱⁱ <https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc>

DG Written Testimony_SB0541.pdf

Uploaded by: Senator Gile

Position: FAV

DAWN D. GILE
Legislative District 33
Anne Arundel County

Finance Committee

Chair

Anne Arundel County
Senate Delegation



Miller Senate Office Building
11 Bladen Street, Suite 3 East
Annapolis, Maryland 21401
410-841-3568 · 301-858-3568
800-492-7122 Ext. 3568
Dawn.Gile@senate.state.md.us

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

Testimony in Support of SB0541 - Maryland Online Data Privacy Act of 2024

Madame Chair, Madame Vice Chair, and Fellow Members of the Senate Finance Committee:

Currently, Maryland lacks a comprehensive online privacy law, presenting a significant issue. Companies operate unchecked, gathering and monetizing personal and sensitive information from our lives without our awareness or consent. When we download seemingly “free” applications, they come at the cost of our personal data, surreptitiously collected by these apps. We unwittingly become both consumers and commodities. Shockingly, over 70% of mobile apps share user data with third parties, and research reveals that 15% of these apps are linked to five or more tracking mechanisms. This data encompasses a wide range of personal information, from mental health and reproductive data to location data, all gathered, aggregated, and traded without our explicit consent or knowledge.

For example, imagine a scenario where someone downloads a fitness tracking app to monitor their daily exercise routine. Unbeknownst to them, the app not only records their workout sessions but also collects data on their sleep patterns, heart rate, and even their location throughout the day. This information, seemingly innocuous on its own, becomes part of a vast network of data points that are bought and sold by third-party companies. Eventually, this individual’s personal habits and whereabouts are commodified without their consent, raising serious concerns about privacy infringement and potential misuse of sensitive data.

Consider another recent example wherein it was revealed that Pray.com, a popular religious app, had been sharing comprehensive user data with third-party entities. Users were shocked to learn that their personal information, including intimate details such as mental health struggles, had been shared without their explicit consent. For instance, they found themselves targeted with ads on platforms like Facebook, promoting services like “Better Marriage,” “Abundant Finance,” and “Releasing Anger.” This breach of trust raised profound ethical concerns regarding the handling of sensitive user data by technology firms and underscored the critical need for robust privacy regulations and increased transparency from app developers concerning data collection and sharing practices.

In Europe, comprehensive data privacy laws, exemplified by the General Data Protection Regulation (GDPR), afford extensive safeguards for individuals' personal data, prioritizing transparency and user consent. Conversely, the United States federal government has not yet implemented legislation comparable to the GDPR. In response to this federal inaction, numerous states across the nation have taken proactive measures to protect consumer privacy. Presently, fourteen (14) states have enacted data privacy laws, while several others have similar legislation pending. These laws encompass a range of provisions, including mandatory disclosure of data breaches and granting individuals greater control over the usage of their personal data. This collective endeavor by individual states underscores a dedication to bolstering consumer privacy and fostering trust in digital interactions.

Solution

SB0541 establishes a number of consumer protections, including:

- Data minimization – making sure companies are only collecting and processing the data needed for the transaction at hand;
- Data protection – ensuring companies keep the data they do collect safe;
- Consumer control over personal data – giving consumers the right to know what is collected and who it is shared with, along with the right to correct the data, delete the data, and opt out of targeted ads, sale of data and profiling;
- Extra layers of protection for sensitive data. Sensitive data includes:
 - Biometrics
 - Geolocation
 - Reproductive, mental health, and gender affirming care.
 - Racial or ethnic origin, religious beliefs, sexual orientation, citizenship, or immigration status
 - Personal data that a controller knows or has reason to know is that of a child.

Because this is a lengthy bill, I am submitting with this testimony an overview of the bill for the Committee's convenience.

I respectfully request a favorable report on SB0541.

SB0541- MD OPA 2024 Overview.pdf

Uploaded by: Senator Gile

Position: FAV

SB0541 Overview

Application

Bill covers personal data, defined as “data that can be reasonably linked to an identified or identifiable consumer.”

- It also addresses sensitive data (biometrics, child data, consumer health data, data revealing race, gender identity, etc.)

The bill applies to a person that:

- Conducts business in the state; or
- Produces services or products that are targeted to residents of the state; and
 - Controlled or processed the personal data of at least 35,000 consumers (excluding solely for a payment transaction); or
 - Controlled or processed the persona data of at least 10,000 consumers and derived 20% of gross revenue from the sale of personal data.

Bill exempts several entities, as well as a number of specific types of data.

Consumer Rights

Bill grants consumers certain rights:

1. Right to confirm a controller is processing their personal data.
2. Access that data.
3. Correct the data.
4. Require the controller to delete the data.
5. Obtain a copy of the data.
6. Obtain a list of categories of third parties to whom the controller has disclosed the personal data.
7. Opt-out of the processing for:
 - a. Targeted advertising.
 - b. The sale of personal data.
 - c. Profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.
8. Designate an authorized agent to opt-out of the processing in right #7.

Exercising those rights

A controller:

1. Must establish a secure way for consumers to exercise their rights.
2. Shall respond to the request within 45 days. Controllers can extend this period.
3. Must notify the consumer within 15 days that they complied.
4. May decline. If they do, they shall inform the consumer and provide an appeal process.

Controllers

Controllers are the one who “determines the purpose and means of processing personal data.” The bill puts guardrails on controllers’ activities: data minimization, restrictions on collection and use of sensitive data, protecting data confidentiality, and limits on the use of personal data.

Details:

A. If a controller processes data

- They shall protect the confidentiality and security of the data.
- Reduce risks of harm to the consumers relating to the collection, use, or retention of the data.
- Process the data to the extent it is reasonably necessary and proportionate to the purposes in the bill and is adequate, relevant, and limited to what is necessary.

B. Responsibilities

A controller may not:

1. Collect personal data for the sole purpose of content personalization or marketing, unless they have the consumer’s consent.
2. Collect, process, or share sensitive data concerning a consumer (except where strictly necessary to provide or maintain a specific product or service requested by the consumer, and only with the consumer’s consent).
3. Sell sensitive data.
4. Process personal data in violation of anti-discrimination laws.
5. Process personal data for purposes of targeted advertising or sell the consumer’s personal data, if controller knows or has reason to know the consumer is between 13-18.
6. Discriminate against a consumer for exercising their rights under this title.
7. Collect, process, or transfer personal data in a way that discriminates or makes unavailable the equal enjoyment of goods (Civil Rights language from bi-partisan federal bill).
8. Process personal data for a purpose that is not reasonably necessary to or compatible with the disclosed purposes for which the data is processed (unless consumer consents).

A controller shall:

1. Limit the collection of personal data to what is reasonably necessary and proportionate to provide or maintain a service requested by a consumer.
2. Establish reasonable security practices to protect the data.
3. Provide a reasonable mechanism for a consumer to revoke consent.
4. Stop processing data within 15 days of a consent revocation.
5. Provide a clear privacy notice that includes:
 - a. Categories of personal data processed, including sensitive data.
 - b. Purpose for processing the data.
 - c. How a consumer may exercise their rights.
 - d. Categories of third parties with which the controller shares data, with sufficient detail so the consumer understands what they are and how they may process the data.
 - e. Categories of data shared with third parties.

- f. Active email address to contact the controller.

C. Other

Nothing in this bill:

1. Requires a controller to provide a product or service that requires data they don't collect.
2. Prohibits a controller from offering different levels of service if the offering is in connection with a loyalty program.

Processors

A processor is "a person that processes personal data on behalf of a controller."

Processors and controllers must enter a contract that includes:

- Instructions for processing the data.
- Nature and purpose of processing.
- Type of data subject to processing.
- Duration of processing.
- Duty of confidentiality.
- Issues of retention/return/deletion of data.

Processors:

1. Help controllers comply with the Act.
2. May engage subcontractors with controller's consent.

Controller v. processor? A processor:

- Is limited in processing of specific data per controller's instruction.
- Can be deemed a controller if they
 - Fail to adhere to instructions.
 - Determine purposes and means of processing data.

"Processing Activities that Present a Heightened Risk of Harm" and Data Assessments

This section sets out requirements for processing activities that 'present a heightened risk of harm.' Those are defined as:

1. The processing of personal data for targeted advertising.
2. The sale of personal data.
3. The processing of sensitive data.
4. Processing of personal data for the purposes of profiling, which risks:
 - a. Unfair, abusive, or deceptive treatment.
 - b. Having an unlawful disparate impact.
 - c. Financial, physical, or reputational injury.
 - d. Physical or other intrusion into private affairs.
 - e. Other substantial injury.

For each activity in #4, a controller must conduct a data protection assessment. This assessment shall:

1. Identify and weigh the benefits to the controller, the consumer, and the public against the risks to the consumer (as mitigated by any safeguards the controller employs) and the necessity of processing in relation to the stated purpose of the processing.
2. Include various factors, such as
 - a. The use of de-identified data.
 - b. Consumer expectations.
 - c. Context.
 - d. Relationship between controller and consumer.
3. Be made available to the OAG Div. of Consumer Protection where relevant to an investigation.

Misc.

These pages lay out a series of things the tech industry negotiated for in other states' bills. For example, they do not have to:

- Maintain data in an identifiable form.
- Collect any data to authenticate a consumer request.
- Comply with a request if they can't associate the request with the data

The bill doesn't restrict controllers or processors from a litany of actions, including complying with laws, subpoenas, cooperate with law enforcement, establish a defense to a claim, provide a product specifically requested, perform under a contract, protect life or physical safety, prevent/detect fraud, assist another with obligations under this bill, effectuate a recall, identify, and repair technical errors, perform internal operations.

Enforcement

- By the Office of the Attorney General.
- No Private Right of Action.
- Violation is an unfair, abusive, or deceptive trade practice.
- Other remedies in law that are available to consumers.

SB541 Testimony 2024.pdf

Uploaded by: Zoe Gallagher

Position: FAV



SB541 Maryland Online Data Privacy Act of 2024

Position: Favorable

2/14/2024

The Honorable Senator Pamela Beidle, Chair
Finance Committee
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

CC: Members of the Senate Finance Committee

Economic Action Maryland (formerly the Maryland Consumer Rights Coalition) is a people-centered movement to expand economic rights, housing justice, and community reinvestment for working families, low-income communities, and communities of color. Economic Action Maryland provides direct assistance today while passing legislation and regulations to create systemic change in the future.

As an organization with a long history of advocating for consumer protection, I am writing today to urge your favorable report on SB541, the Maryland Online Data Privacy Act of 2024. This bill would limit the consumer data that companies collect online to only what is necessary for business operations.

Every day, companies are collecting and selling consumer data for an enormous profit, while many consumers remain unaware that their personal information is being traded and sold. In 2019, an estimated \$33 billion of revenue was collected from data sales alone just in the United States.¹ The unclear relationship between data collection and company profit has led to a significant amount of distrust from consumers. According to our published [report on digital equity](#), reluctance to use and distrust of the internet is one of the most significant factors challenging digital equity in Maryland. Reforms that seek to mitigate distrust from users is key to closing digital equity gaps.

The harmful effects of nonconsensual data collection can manifest in a myriad of ways. For example, tenant screening agencies scrape the internet for information on previous evictions and court cases and then sell their services to landlords so they can make “more informed decisions” on approving housing applicants without that prospective tenant even knowing the landlord had access to that data.² Data collection is also increasingly being utilized in the job market, where hiring agencies use data to determine characteristics of the “ideal applicant³.” This can create the major risk of discrimination against vulnerable populations, and prevent skilled applicants from finding employment.

This bill empowers consumers by providing them with new rights, including the ability to view, correct, delete, and opt out of data collection. Allowing consumers to choose what data is collected is beneficial in

¹ https://econaction.org/wp-content/uploads/2023/11/rhinesmith_2023_digital_equity_justice_maryland.pdf

² *ibid.*

³ *ibid.*



many contexts, from This increased control over their personal information gives consumers a say in how their data is used, promoting digital equity.

Additionally, requiring large companies to limit the collection of consumer data to what is necessary for legitimate business needs promotes data minimization practices. This helps prevent the unnecessary collection of sensitive information, reducing the potential for misuse or data breaches, further protecting consumers from harm.⁴

Maryland lacks a comprehensive data privacy law and this bill seeks to close this regulatory gap by introducing measures that address the challenges posed by rapid technological advancements, demonstrating a commitment to keeping consumer protections up to date and responding to emerging technologies. Our state has a long history of standing up for consumers, and we should continue to lead the nation in innovative policy that puts consumer protection and privacy at the forefront.

For these reasons we urge a favorable report on SB541.

Sincerely,
Zoe Gallagher, Policy Associate

⁴<https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/?sh=1fffbab51da4>

OAG-CPD Privacy Unit Amendments.pdf

Uploaded by: Anthony Brown

Position: FWA

OAG AMENDMENTS TO HOUSE BILL 567

On page 2, after line 10, insert:

ARTICLE – STATE GOVERNMENT

Section(s) 6–201 through 6–203 and the subtitle “Subtitle 2. Electronic Transactions Protection Act” of Article – State Government of the Annotated Code of Maryland are repealed.

On page 2, after line 11, insert:

13-204.1.

- (A) THERE IS A PRIVACY PROTECTION AND ENFORCEMENT UNIT IN THE DIVISION.
- (B) THE PURPOSE OF THE UNIT IS TO PROTECT THE PRIVACY OF INDIVIDUALS’ PERSONAL INFORMATION AND TO PROTECT THE PUBLIC FROM UNFAIR, ABUSIVE OR DECEPTIVE PRACTICES ONLINE.
- (C) THE UNIT SHALL:
 - (1) ENFORCE THE MARYLAND ONLINE DATA PRIVACY ACT, TITLE 14, SUBTITLE 46 OF THIS ARTICLE, AND RELATED STATE AND FEDERAL PRIVACY LAWS;
 - (2) EMPOWER AND EDUCATE MARYLAND CONSUMERS WITH INFORMATION ON THEIR RIGHTS AND STRATEGIES FOR PROTECTING THEIR PRIVACY AND ONLINE SAFETY;
AND
 - (3) ASSIST, ADVISE, AND COOPERATE WITH LOCAL, STATE, AND FEDERAL AGENCIES AND OFFICIALS TO PROTECT AND PROMOTE THE INTERESTS OF CONSUMERS IN THE STATE REGARDING PRIVACY RELATED ISSUES AND UNLAWFUL ONLINE CONDUCT OR PRACTICES.

LOC -- SB0541.pdf

Uploaded by: Craig Behm

Position: FWA



February 12, 2024
The Honorable Pamela Beidle
Chair, Finance Committee
3 East
Miller Senate Office Building
Annapolis, MD 21401

Dear Chair Beidle –

On behalf of the Chesapeake Regional Information System for our Patients (CRISP), the designated health information exchange (HIE) and health data utility (HDU) for Maryland, I am writing to express our concern for SB541 – *The Maryland Online Data Privacy Act of 2024*. Although we are advocates of data privacy, we believe that the bill language should be modified to exempt certain entities rather than just the information they might collect.

Specifically, §14-4603(B) exempts “protected health information under [the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)],” but, unlike the exceptions in subsection (A) of the same section, does not exempt entities that are HIPAA-covered or their respective business associates, as defined by HIPAA. Without this change, covered entities and their business associates, like CRISP, would have to segment “health information” coming from covered entities and “health information” coming from non-covered entities like community-based organizations. This segmentation often results in incomplete data and a lack of coordinated care between health care providers and social services, further exacerbating disparities.

Therefore, we request that the Committee amend the bill to add the following section (4) to §14-4603(A):

(4) A covered entity or business associate of a covered entity as defined by HIPAA.

As a strong proponent of patient consent and privacy, CRISP supports the overall intent of this bill; however, since covered entities and their business associates are already highly regulated by HIPAA, we believe that, similar to the carve-outs for financial institutions subject to privacy regulations in section (A)(3) of the bill, the privacy concerns are addressed in HIPAA without the resulting issues of care coordination presented by the current draft of this bill.

Thank you for your consideration and the opportunity to express our concerns regarding the current language in SB541.

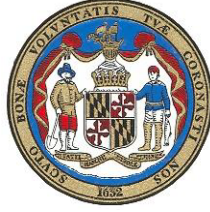
Best,

Nichole Ellis Sweeney, JD
CRISP General Counsel and Chief Privacy Office

SB 541 - STO Testimony.pdf

Uploaded by: Dereck Davis

Position: FWA



MARYLAND STATE TREASURER
Dereck E. Davis

Testimony of the Maryland State Treasurer’s Office

Senate Bill 541: Maryland Online Data Privacy Act of 2024

Position: Favorable with Amendments

Senate Finance Committee

February 14, 2024

Since assuming responsibility of the Maryland 529 Program on June 1, 2023, the State Treasurer’s Office (STO) has become more familiar with privacy-related issues that arise in the savings program space. Proper data privacy protections are especially important when individuals’ personal savings are involved.

Senate Bill 541 specifies that the new requirements do not apply to “a regulatory, administrative, advisory, executive, appointive, legislative, or judicial body of the State, including a board, bureau, commission, or unit of the State or a political subdivision of the State.”¹ While this language clearly demonstrates an intent to exempt State entities, scenarios could arise where the program managers who administer the Maryland College Investment Plan, the Maryland Prepaid College Trust, and the Maryland Achieving A Better Life Experience (ABLE) Program would not be covered by the exemption. For this reason, STO respectfully requests an amendment to clarify that the new subtitle does not apply to instrumentalities of the State.

With the addition of the clarifying amendment, STO requests that the Committee give Senate Bill 541 a favorable with amendments report. Please contact Laura Atas, Deputy Treasurer for Public Policy (latas@treasurer.state.md.us), with any questions.

¹ Commercial Law, § 14-4603(a)(1).

SB 541_NICB_De Campos_FWA.pdf

Uploaded by: Eric De Campos

Position: FWA



February 12, 2024

The Honorable Pamela Beidle and Members of the Committee
Senate Finance Committee
Maryland General Assembly

RE: Senate Bill 541- Maryland Online Data Privacy of 2024

Dear Chair Beidle and Members of the Committee:

I am writing on behalf of the National Insurance Crime Bureau (“NICB”) to address concerns with Senate Bill 541 regarding consumer data privacy. As written, the bill would pose serious hardships on the ability of NICB – along with that of the Maryland Insurance Administration, our Maryland state and local law enforcement partners, and our member insurance companies – to combat insurance fraud.

Organization and Purpose

Headquartered in Des Plaines, Illinois, and with a 110-year history, the National Insurance Crime Bureau is the nation’s premier not-for-profit organization exclusively dedicated to leading a united effort to prevent insurance fraud through intelligence-driven operations.

NICB sits at the intersection between the insurance industry and law enforcement, helping to identify, prevent, and deter fraudulent insurance claims. NICB’s approximately 400 employees work with law enforcement entities, government agencies, prosecutors, and international crime-fighting organizations in pursuit of its mission. NICB is primarily funded by assessments on our nearly 1,200-member property-casualty insurance companies, car rental companies, and other strategic partners. While NICB provides value to our member companies, we also serve a significant public benefit by helping to stem the estimated billions of dollars in economic harm that insurance crime causes to individual policy holders across the country every year.

NICB maintains operations in every state around the country, including in Maryland where NICB works together with law enforcement, state agencies, and prosecutors in a joint effort to protect Maryland consumers. NICB is an unmatched and trusted partner in the fight against insurance fraud.

Maryland’s Fraud Mandate and Specific References to NICB in Statute

The Maryland General Assembly acknowledged the public policy benefits of enabling the flow of insurance fraud reporting by enacting a requirement that insurers report suspected fraud to the Insurance Fraud Division. Md. Insurance Code § 27-802; *see also* COMAR 31.04.15.05. The Insurance Fraud Division receives this information from most insurers through NICB’s Fraud Bureau Reporting System (FBRP). That same statute provides NICB immunity from civil liability by facilitating insurance fraud reporting information through the FBRP. *Id.* § 27-802(c)(1)(iii).

The General Assembly also recognized the importance of NICB’s mission by specifically naming NICB in statute as a mandatory member of the Maryland Vehicle Theft Prevention Council within the Department of State Police. Md. Public Safety Code § 2-702.

Applicability of Senate Bill 541 and News Sections of Articles 13 and 14 of the Annotated Code of Maryland

Senate Bill 541 establishes various consumer rights relating to their personal data. The bill applies to any “person” conducting business in Maryland. Unlike laws enacted in California, Utah, Virginia, and Connecticut, the bill does not provide any exemption for non-profit organizations.

Section (A) of 14-4612 of the bill does provide certain limitations on the reach of the statute in order for entities to cooperate with law enforcement agencies concerning conduct or activity that may violate federal, state or local laws and regulations. Although our Charter aligns with this provision, and NICB would benefit from this section, our understanding is that the language of Section 14-4612 (A) is not meant to provide a wholesale exemption for such activities – meaning that, notwithstanding our ability to continue fighting fraud and other insurance crimes consistent with our Charter, NICB would still be subject to consumer requests to, for example, delete their data. Even for non-viable requests under this bill, NICB would nevertheless bear the burden of proving to each consumer directly, or in litigation, that NICB’s activities fall within the exception. The obligation to do so would strain our organization’s resources to such a degree that our operations, and ability to protect Maryland policyholders, would be drastically encumbered and diminished.

Although all entities within the scope of S.B. 541 would incur some level of compliance costs, the policy reasons for excluding NICB from these burdens are several-fold. First, NICB provides significant benefits to the general public and to the millions of consumers who are victims of insurance fraud. Second, as a non-profit organization that serves a public interest, NICB is not equally situated with private entities that typically establish more complex compliance infrastructure for private-sector-related obligations. For a public-service non-profit operating on an extremely lean budget, the potential cost of complying with S.B. 541 would drastically reduce the benefits NICB provides to the overall public good – without any associated benefit to consumers. Third, NICB’s required responses to individual consumer requests, or involvement in civil litigation, would likely expose otherwise covert criminal investigations. For example, if an illicit actor who is involved in multiple criminal conspiracies demands that NICB confirm that we are processing that individual’s data and requests access to that data, a mere response from NICB tying that information to a fraud-related purpose would provide a clear signal to that individual, thereby exposing any criminal investigation. Lastly, imposing what is essentially a “compliance, response, reporting and litigation” obligation – without any benefit to consumers – is wholly inconsistent with current insurance fraud reporting statutes and civil immunity provisions referenced above, which were enacted to facilitate the mandatory flow of insurance fraud information to Maryland state authorities. *See* Md. Insurance Code § 27-802; COMAR 31.04.15.05.

In addition to the constraints that the fraud limitation would provide as set forth above, that section would not provide NICB any protection for our operations relating to catastrophic events. For example, NICB provides invaluable assistance to federal, state, and local emergency response agencies and law enforcement entities in response to hurricanes, tornados, floods and other natural disasters. NICB partners with these entities in the lead up to and immediate aftermath of these events. NICB often deploys agents to assist with emergency responders and law enforcement in many different ways. The Geospatial Insurance Consortium (GIC), which is an initiative developed by NICB, has become an integral part of public agencies’ overall response plans to significant catastrophic events. GIC is an information sharing partnership designed to provide aerial maps and other information to help response agencies efficiently allocate their resources to the most heavily impacted areas. NICB provides sensitive information for purposes of taking aerial images and facilitating the flow of imagery information to emergency responders and law enforcement. This service is available as a result of partnerships with several public and private organizations and is provided at no cost to the public.

If the bill were enacted as is, the GIC program would be substantially impacted and could ultimately be shut down because not all critical information obtained and provided through the program would neatly apply within the limitation of Section 14-4612 (A). As a consequence, the service would be unavailable to public agencies and their overall response management plan. Without access to that information, the ability for first responders and law enforcement to successfully deploy resources in the most efficient way possible would be severely reduced. Moreover, information that NICB provides on an as-needed basis could be eliminated, further reducing the effectiveness of the public response to catastrophic events.

Proposed Changes and Policy Rationale

Consistent with longstanding public policy determinations already enshrined in Maryland law referenced above, NICB respectfully requests a narrow exemption to S.B. 541 by amending the following language into Section 14-4603 (A):

(4) a not-for-profit entity that collects, processes, uses, or shares data solely in relation to identifying, investigating, or assisting:

(I) Law enforcement agencies in connection with suspected insurance-related criminal or fraudulent acts; or

(II) First responders in connection with catastrophic events

The policy reasons for such an exclusion are several-fold. First, NICB provides significant benefits to the general public, and to the millions of consumers who are victims of insurance fraud, in particular. Our law enforcement partners will bear testament to the enormous value NICB delivers. Second, NICB's mission is to lead a united effort to combat and prevent insurance crime. Subjecting NICB to data subject demands and potential litigation costs would be inconsistent with the plain language, intent, and spirit of the insurance fraud immunity statutes and the wholesale immunity provisions outlined above that are specifically designed to protect the sharing of information for insurance fraud reporting purposes. Even with the limitations described above, the bill would be at odds with that grant of immunity. Finally, the bill would not only impose significant compliance costs but could also substantially impact or eliminate NICB's catastrophic event response programs, thereby potentially diminishing and drastically reducing the benefits that NICB provides to the overall public good.

Conclusion

We appreciate your consideration of our concerns. I welcome the opportunity to follow up directly with your staff to discuss these issues in more detail. In the meantime, if you have any questions or need additional information, please contact me at edecampos@nicb.org or 847.989.7104.

Respectfully,



Eric M. De Campos
Senior Director
Strategy, Policy and Government Affairs
National Insurance Crime Bureau

CPD Written Testimony SB541.pdf

Uploaded by: Hanna Abrams

Position: FWA

CANDACE MCLAREN LANHAM
Chief Deputy Attorney General

CAROLYN A. QUATTROCKI
Deputy Attorney General

LEONARD J. HOWIE III
Deputy Attorney General

CHRISTIAN E. BARRERA
Chief Operating Officer

ZENITA WICKHAM HURLEY
Chief, Equity, Policy, and Engagement

PETER V. BERNS
General Counsel



ANTHONY G. BROWN
Attorney General

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION

WILLIAM D. GRUHN
Chief
Consumer Protection Division

Writer's Direct Dial No.
(410) 576-7296

February 14, 2024

TO: The Honorable Pamela Beidle, Chair
Finance Committee

FROM: Hanna Abrams, Assistant Attorney General

RE: Senate Bill 541 – Consumer Protection – Maryland Online Data Privacy
Act of 2024 (SUPPORT WITH AMENDMENT)

The Consumer Protection Division of the Office of the Attorney General supports Senate Bill 541 (“SB 541”), sponsored by Senators Gile, Hester, Augustine, Feldman, and Ellis and Chair Beidle. Senate Bill 541 provides Marylanders with much needed control over who can collect, share, use, and sell their personal information.

Today, companies collect vast amounts of consumer data without consumer knowledge or consent. This data is sometimes used to serve consumer needs, but it can also be used to target, exploit, and expose consumers in harmful and sometimes dangerous ways.¹ Consumer data is often combined to provide detailed insights into very personal issues including mental health, gender, racial identity, religious beliefs, sexual preferences, and even our precise locations.² Indeed, data brokers compile data into lists of specific individuals with highly personal characteristics³ and sell it to third parties to be used to deliver everything from targeted

¹ See Technology Safety, Data Privacy Day 2019: Location Data & Survivor Safety (Jan. 28, 2019), <https://www.techsafety.org/blog/2019/1/30/data-privacy-day-2019-location-data-amp-survivor-safety>.

² Lee Matthews, *70% Of Mobile Apps Share Your Data with Third Parties*, Forbes, (June 13, 2017), <https://www.forbes.com/sites/leemathews/2017/06/13/70-percent-of-mobile-apps-share-your-data-with-third-parties/#562270ce1569> (finding that at least 70% of mobile apps share data with third parties, and 15% of the apps reviewed were connected to five or more trackers).

³ Drew Harwell, *Now For Sale: Data on Your Mental Health*, Washington Post (Feb.14, 2023), <https://www.washingtonpost.com/technology/2023/02/13/mental-health-data-brokers/> (citing a Duke University study that found that based on data amassed online data brokers marketed lists of individuals suffering from anxiety and a spreadsheet entitled “Consumers with Clinical Depression in the United States”).

advertising,⁴ to differential pricing, to enable algorithmic scoring⁵ which can have discriminatory outcomes.⁶ Unlike consumers in thirteen other states, Maryland consumers have no knowledge or control over what is collected about them or what is done with that personal information.

Senate Bill 541 provides individuals with some transparency into and control over how their data is used. This transparency, coupled with giving users the right to access, correct, or delete their data, empowers individuals to protect themselves. They can reduce their data footprint, or remove their data from insecure third parties, minimizing the risk of fraud, identify theft, and exploitation.

Consumer Rights Provided by Senate Bill 541

Senate Bill 541 will provide Marylanders with important rights over their personal information, and impose specific obligations on businesses who handle consumers' personal data, including:

- *Right to Know:* consumers will have the right to know whether controllers are processing their data, as well as the categories of data being processed and the third parties the data has been disclosed to. Consumers will also have a right to obtain a copy of the consumer's personal data that a controller has or is processing;
- *Right to Correct:* Consumers will have the right to correct inaccuracies in their data;
- *Right to Delete:* Consumers will have the right to require a controller to delete their personal data;
- *Right to Opt-out of Sale:* Consumers will have the right to opt out of processing of the personal data for targeted advertising, sale, or profiling of the consumer in a way that produces legal effects.

In addition, SB 541 provides heightened protections for “sensitive data” – including, genetic, biometric, and geolocation data – which by its nature is especially revealing. Senate Bill 541 provides specific limitations on data that “presents a heightened risk of harm to a consumer” by limiting entities' ability to sell, monetize, or exploit this data.

⁴ *FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising* (Feb. 1, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising>.

⁵ A Berkeley study found that biases in “algorithmic strategic pricing” have resulted in Black and Latino borrowers paying higher interest rates on home purchase and refinance loans as compared to White and Asian borrowers. This difference costs them \$250 million to \$500 million every year. Laura Counts, *Minority homebuyers face widespread statistical lending discrimination, study finds*, Haas School of Business at the University of California, Berkeley, (Nov. 13, 2018), <http://newsroom.haas.berkeley.edu/minority-homebuyers-face-widespread-statistical-lending-discrimination-study-finds/>; Upturn, *Led Astray: Online Lead Generation and Payday Loans*, (Oct. 2015), <https://www.upturn.org/reports/2015/led-astray/>. See also Yeshimabeit Millner and Amy Traub, *Data Capitalism and Algorithmic Racism, Data for Black Lives and Demos* (2021), https://www.demos.org/sites/default/files/2021-05/Demos_%20D4BL_Data_Capitalism_Algorithmic_Racism.pdf

⁶ Julia Angwin et al., *Facebook (Still) Letting Housing Advertisers Exclude Users By Race*, ProPublica (Nov. 21, 2017), <https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin>.

Importantly, SB 541 sets an important baseline requirement that entities only collect data that “is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains.” This limits the misuse and accidental leakage of data by restricting what is collected at the outset.

Proposed Amendments

We do, however, have some recommendations in connection with SB 541:

Definitions:

Affiliate: In SB 541, “affiliate” is defined as a person that “shares common branding with another person” (page 2, lines 20-23) with no other limitations. We have concerns that this definition is overly broad and captures more than what would be traditionally considered an “affiliate.” We recommend amending the definition of affiliate to:

a person that, directly or indirectly through one or more intermediaries, controls, is controlled by or is under common control with another person such that: (a) The person owns or has the power to vote more than 50 percent of the outstanding shares of any voting class of the other person’s securities; (b) The person has the power to elect or influence the election of a majority of the directors, members or managers of the other person; (c) The person has the power to direct the management of another person; or (d) The person is subject to another person’s exercise of the powers described in paragraph (a), (b) or (c) of this subsection.⁷

Deidentified Data: Page 6, line 5, replace the word “if” with “and” to conform to the definition found in the Maryland Genetic Information Privacy Act.

Personal Data: On page 7, we recommend adding to the end of line 20 “consumer *or to a device identified by a unique identifier*” in order to be consistent with the definition of targeted advertising.

Exemptions:

We have concerns about the breadth of the exemptions in SB 541 that could serve to dilute the effect of the law, which we have shared with the sponsor. For example, page 12 lines 28-30, exempts *all* financial institutions and *all* affiliates of financial institutions subject to the federal Gramm-Leach-Bliley Act (GLBA) regardless of whether the personal data is governed by the GLBA. Advocates for financial institutions will claim that the industry is highly regulated and therefore they do not need additional privacy regulations, but financial institutions and their affiliates regularly collect information that is not governed by the GLBA. For example, when a financial institution collects information from non-customers or obtains information from a third-party or an affiliate outside of the context of providing a joint product or service, that personal information is not governed by federal privacy regulations.⁸ Given the breadth of the affiliate

⁷ Oregon Consumer Privacy Act, definition of “affiliate.”

⁸ 16 CFR § 313.1(b).

relationship, the Division recommends that page 12, lines 28-30 be replaced with the following language:

- (3)(i) A financial institution, as defined by Md. Code, Fin. Inst. § 1-101, or a financial institution’s affiliate or subsidiary that is only and directly engaged in financial activities, as described in 12 U.S.C. 1843(k);*
- (ii) An insurer, as defined by Md. Code, Ins. §§ 1-101(v), other than a person that, alone or in combination with another person, establishes and maintains a self-insurance program and that does not otherwise engage in the business of entering into policies of insurance;*
- (iii) An insurance producer, as defined by Md. Code, Ins. § 1-101(u); and*
- (iv) A person that holds a license issued under Md. Code, Ins. § 10-103.*

Similarly, we recommend clarifying that the exemption found on page 13, line 3, applies to protected health information that is regulated by the Health Insurance Portability and Accountability Act of 1996 by replacing it with the following language:

Protected health information that a covered entity or business associate processes in accordance with, or documents that a covered entity or business associate creates for the purpose of complying with, the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, and regulations promulgated under the Act, as in effect on the effective date of this 2023 Act.

Controller Obligations:

We recommend clarifying, on page 22, line 21, that the disclosure applies to “sale” as well as processing (conspicuously disclose the *sale or processing...*”). This resolves an internal inconsistency because according to lines 17-18, the paragraph applies if a controller “sells personal data . . . or processes personal data,” but the term sale is absent from the controller disclosure obligations on line 21.

Finally, we note that SB 541 does not include a private right of action. Without a private right of action, as the lone entity able to take action against violators, the Consumer Protection Division will need significantly more resources to enforce this bill. To that end, the Office of the Attorney General believes that a Privacy Protection and Enforcement Unit with sufficient resources should be established within the Consumer Protection Division.

We urge the Finance Committee to issue a favorable report on SB 541 with the amendments discussed.

cc: Members, Finance Committee
The Honorable Dawn Gile
The Honorable Malcolm Augustine
The Honorable Brian J. Feldman
The Honorable Pamela Beidle
The Honorable Arthur Ellis

SB 541 - SUPP - FIN - Online Data Privacy - Feb 14

Uploaded by: Henry Bogdan

Position: FWA

February 14, 2024

Statement on Senate Bill 541
Maryland Online Data Privacy Act of 2024
Senate Finance Committee

Position: Amend

Maryland Nonprofits is a statewide association of more than 1800 nonprofit organizations and institutions. We respectfully ask that Senate Bill 541 be amended to exempt nonprofit organizations that are exempt from taxation under Section 501(C)(3) of the Internal Revenue Code.

We recognize that the bill, or amendments being discussed, may or may not exempt some groups of charitable organizations, however, for those that fall within the ambit of its provisions, it would impose significant compliance burdens, such as providing an extensive process for consumers to find out what personal data the organization has collected on them, as well as rights to correct the data, delete it, etc., along with various notification and appeal procedures.

The relationship between charities and donors is not the same as most commercial transactions between businesses and customers, and charities already have strong motivations to respect donor wishes and preferences. Honoring donor privacy is an element of prominent 'best practice' standards in the nonprofit community, as in Maryland Nonprofits nationally recognized *Standards of Excellence* code: "D. DONOR RELATIONSHIPS AND PRIVACY - (1) Nonprofits should respect the donor's right to determine how their name and contact information is used, including providing opportunities to remain anonymous, request that the organization curtail repeated mailings or telephone solicitations from in-house lists, and have their names removed from any mailing lists which are sold, rented, or exchanged."

We would point out that the majority (10) of the states that have enacted similar legislation have excluded 501(C)(3) exempt organizations, recognizing the burden this could place on charitable operations.

We urge the adoption of an amendment to exempt nonprofits exempt under that provision of the Internal Revenue Code from Senate Bill 541.

SB541_Online.Data.Privacy_FWA[47522].pdf

Uploaded by: Jamie Gregory

Position: FWA

SB541: Maryland Online Data Privacy Act of 2024

Finance Committee – February 14, 2024

Sponsors: Senators Gile, Hester, Augustine, Feldman, Beidle, and Ellis

Position: FAVORABLE with AMENDMENT

Testimony on behalf of Airbnb, Inc. by Jamie Gregory, Calfee Strategic Solutions

Chairman Beidle, Vice Chairman Klausmeier, and members of the Finance Committee, thank you for the opportunity to testify today.

I am here on behalf of Airbnb, which was founded in 2008 in San Francisco, CA and now operates worldwide. Specifically in Maryland, in 2022 approximately 800,000 visitors stayed with an Airbnb Host. This totaled over 240,000 separate visits of about 3 persons per group with most guests staying 4-5 nights. However, this still only amounted to seven tenths of 1% of homes in MD. The typical MD host self-reports as being 60% female and earning about \$13,000 in additional income from sharing their home. Over 20% of hosts in MD are over 60 years old.

Background:

Airbnb takes its responsibility seriously to protect the personal identifying data of its hosts and users. The proposed amendments are consistent with federal guardrails around how such sensitive information can and should be disclosed. Codifying this standard in the Maryland Code will both provide clear guidance to local governments and help safeguard user information.

Recommended Amendments:

On Page 31, line 2 a new (A):

A local governing body shall not require a controller or processor to disclose personal data of consumers, unless pursuant to a subpoena or court order,

Existing (A) to become (B) along with subsequent paragraph identifications.

Under (2) on current lines 6-8:

Comply with a civil OR criminal, [or regulatory inquiry, investigation,] subpoena, or summons by a federal, state, local, or other JUDICIAL BODY [governmental authority];

Airbnb respectfully asks for your consideration of these proposed changes. Please let us know if there are questions or additional information that can be provided.

FavWAmEd AHA Data Privacy SB 541.pdf

Uploaded by: Laura Hale

Position: FWA



February 9, 2024

Testimony of Laura Hale
American Heart Association

Favorable W/ Amendment SB 541 Maryland Online Data Privacy Act of 2024

Dear Chair Beidle, Vice Chair Klausmeier and Honorable Members of the Finance Committee,

Thank you for the opportunity to speak before the committee today. My name is Laura Hale, and I am the Director of Government Relations for the American Heart Association. The American Heart Association expresses its support for SB 541 with one amendment.

We appreciate your leadership on the important issue of consumer data privacy and support the Legislature's desire to establish important consumer protections. The AHA shares this goal and, as such, uses industry standard security protocols to protect our donors' and volunteers' information, and readily make our privacy policy available to the public. We do, however, have some concerns that the current version of Senate Bill 541 will create unintended consequences for non-profit organizations.

The cost of proving our compliance with the policy is high and is burdensome for nonprofit organizations. Every dollar that a public charity must devote to data privacy compliance is a dollar that we cannot use to further our missions. For AHA, this means less going toward funding cardiovascular research, setting clinical guidelines for cardiac and stroke care, and providing CPR training materials and courses that are used throughout the US. Moreover, when a public charity like AHA does not commercialize that data (i.e., sell it), the costs are even more painful. Donors expect their funds to support the mission, not for handling consumer data questions and portability support requests, and they can easily read the privacy policies and charity watchdog ratings to see how their data is used.

With that in mind, we recommend connecting 501(c)3 nonprofit compliance with this legislation to the Better Business Bureau Standards for Charity Accountability¹. By being registered and in compliance with these standards, we are following the spirit and intent of the Data Privacy Law. By being able to demonstrate that we are registered and in compliance (by the rating provided by the BBB Standards for Charity Accountability) nonprofits would both demonstrate that we are complying with data privacy, but also remove the more burdensome process of demonstrating this compliance. Below I have copied the standards outlined by the BBB Standards for Charity Accountability:

"Address privacy concerns of donors by

¹ [Implementation Guide to the BBB Standards for Charity Accountability \(give.org\)](https://www.give.org/standards)

- a. providing in written appeals, at least annually, a means (e.g., such as a check off box) for both new and continuing donors to inform the charity if they do not want their name and address shared outside the organization, and
- b. providing a clear, prominent and easily accessible privacy policy on any of its websites that tells visitors (i) what information, if any, is being collected about them by the charity and how this information will be used, (ii) how to contact the charity to review personal information collected and request corrections, (iii) how to inform the charity (e.g., a check off box) that the visitor does not wish his/her personal information to be shared outside the organization, and (iv) what security measures the charity has in place to protect personal information. “

Bearing this in mind, we ask for a tailored amendment that substantively reflects what is outlined below. We are very open to conversations on how best to work towards this amendment (or similar language) and look forward to continued discussion with the sponsors.

Amendment Language:

14-4603

A. THIS SUBTITLE DOES NOT APPLY TO:

.....

(4) A 501(c)3 NONPROFIT CHARITY THAT IS REGISTERED WITH THIS STATE AND COMPLIANT WITH THE BETTER BUSINESS BUREAU WISE GIVING ALLIANCE STANDARDS FOR CHARITY ACCOUNTABILITY

The American Heart Association urges amending this legislation to lessen the burden on nonprofits for compliance with this legislation.

BIO Letter with amendment request SB 541 2-12-24.p

Uploaded by: Laura Srebnik

Position: FWA



Biotechnology Innovation Organization
1201 New York Ave., NW
Suite 1300
Washington, DC, 20005
202-962-9200

February 13, 2024

The Honorable Pamela Beidle, Chair
Senate Committee on Finance
Miller Senate Office Building, 3 East Wing 11 Bladen St., Annapolis, MD 21401 – 1991

Re: SWA SB 0541, *Maryland Online Data Privacy Act of 2024*

Dear Chair Beidle and Members of the Committee:

On behalf of the Biotechnology Innovation Organization (BIO) and our members, we thank you for the opportunity to submit written testimony for SB 541, the Maryland Online Data Privacy Act of 2024 establishing the manner in which consumer’s personal data may be processed and authorizing a consumer to exercise certain rights in regard to their data.

About BIO

BIO is the world's largest trade association representing biotechnology companies, academic institutions, state biotechnology centers and related organizations across the United States and in more than 30 other nations.

BIO members are involved in the research and development of innovative healthcare, agricultural, industrial and environmental biotechnology products. BIO also produces the [BIO International Convention](#), the world’s largest gathering of the biotechnology industry, along with industry-leading investor and partnering meetings held around the world.

SB 541

After reviewing the bill, we were pleased to see provisions included that balance patient rights to privacy while maintaining the important public policy goal of promoting biomedical innovation and research in the state of Maryland.

However, in order to facilitate and maintain biomedical research efforts, we encourage you to consider including in the definition of “de-identified data” data that is de-identified pursuant to HIPAA standards.

The existing framework under HIPAA minimizes unnecessary data gathering, allows patients to exercise appropriate levels of autonomy over their PHI, and facilitates healthcare research and innovation. Bill SB 541 captures and preserves a number of elements of the HIPAA legislation, with the exception of the de-identification standard, which our members rely on to harmonize data collection practices for research purposes.

Maintaining current HIPAA and research requirements that BIO members are already adhering to is critical. HIPAA creates clear guidelines for the appropriate use and disclosure of PHI, while also recognizing the critical role PHI plays in research and healthcare innovation. HIPAA recognizes the careful balance between protecting patient privacy and facilitating research.

The HIPAA de-identification standard establishes rules and mechanisms such that the individual to whom protected health information applies cannot be identified nor can the information be re-identified. This allows for safe, secure, and private use of health care data for research purposes.

Failure to include this standard would result in significant operational challenges for companies conducting or looking to initiate biomedical research in Maryland. Many other states in the country with privacy legislation include the HIPAA deidentification standard (see e.g. Virginia H2037(2021) and Colorado Sb190 (2021)).

To address this concern, please consider the amendment below, which makes no substantive changes to the original de-identification data definition, and only adds an additional provision by which one would be able to classify their de-identification practices to be consistent with the Maryland legislation:

14-4601

(P) “DE-IDENTIFIED DATA” MEANS DATA THAT CANNOT REASONABLY BE USED TO INFER INFORMATION ABOUT OR OTHERWISE BE LINKED TO AN IDENTIFIED OR IDENTIFIABLE CONSUMER, OR A DEVICE THAT MAY BE LINKED TO AN IDENTIFIED OR IDENTIFIABLE CONSUMER,

(1) IF THE CONTROLLER THAT POSSESSES THAT INFORMATION:

(i) TAKES REASONABLE MEASURES TO ENSURE THAT THE INFORMATION CANNOT BE LINKED WITH A CONSUMER;

(ii) COMMITS IN PUBLICLY AVAILABLE TERMS AND CONDITIONS OR IN A PUBLICLY AVAILABLE PRIVACY POLICY TO MAINTAIN AND USE THE INFORMATION IN DE-IDENTIFIED FORM; AND

(iii) CONTRACTUALLY OBLIGES ANY RECIPIENTS OF THE INFORMATION TO COMPLY WITH ALL PROVISIONS OF THIS SUBSECTION;

OR

(2) the requirements for de-identification set forth in 45 CFR 164.514 that is derived from individually identifiable health information as described in the Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191) or personal information consistent with the human subject protection requirements of the United States Food and Drug Administration are met.

Thank you for your consideration of this change. If you have any questions, please do not hesitate to contact me.

Sincerely,

/s/

Laura Srebnik

Director, State Government Affairs – Eastern Region

The Biotechnology Innovation Organization (BIO)

1201 New York Ave., NW

Suite 1300

Washington, DC 20005

206.293.1195 (mobile)

Marriott MD DataPrivacy Amends.pdf

Uploaded by: Marta Harting

Position: FWA

MARRIOTT INTERNATIONAL
PROPOSED AMENDMENTS TO HB567/SB541 (ONLINE DATA PRIVACY ACT)

Amendment #1: On page 14, strike lines 28-30.

The access limitation outlined here is unworkable as to employees because we do not have contracts with our employees. They must maintain confidentiality by company policy but there is no contract under which to establish a duty of confidentiality.

Amendment #2: On page 19, strike lines 27-29.

As currently drafted, this provision effectively establishes an “opt-in” requirement for marketing and personalization. The other protections in this section will apply to the collection of data for these purposes, and striking this language would better align this legislation with other state laws that have been enacted across the country.

Amendment #3: On page 17, strike lines 15-17.

It is duplicative and unnecessary to require the controller to notify the consumer that the controller has complied with the request since the law will require the controller to comply with and respond to a consumer’s request within 45 days unless the controller affirmatively communicates to the consumer that an extension is necessary under subsection (e)(2)(i) and (ii) of this section. We are unaware of any other state laws that require this additional step. If it is not removed, this additional step would be difficult for us to operationalize given the diversity of our systems.

2024 NAMIC letter SB541 Consumer data privacy.pdf

Uploaded by: Matt Overturf

Position: FWA

Senate Finance Committee

MARYLAND SB 541: Consumer Data Privacy

Favorable w/Amendment | February 14, 2024

Chair Beidle and Members of the Senate Finance Committee:

On behalf of the National Association of Mutual Insurance Companies¹ (NAMIC) thank you for the opportunity to submit this statement of Favorable with Amendment (FWA) to Senate Bill 541.

NAMIC consists of nearly 1,500 member companies, including seven of the top 10 property/casualty insurers in the United States. The association supports local and regional mutual insurance companies on main streets across America as well as many of the country's largest national insurers.

The insurance industry takes consumer privacy very seriously and have been subject to numerous laws and regulations for years for the protection of consumer data. Our industry's commitment to appropriate use and safeguarding of consumer information has helped establish what has become a comprehensive federal and state regulatory framework governing the use and disclosure of personal information for the insurance industry.

Exceptions for GLBA-Subject Financial Institutions

NAMIC is very appreciative of the inclusion of GLBA exemption language in House Bill 567 and would respectfully request the exemption be amended slightly to include 'data' as well as citing the implementing regulations of Title V of the Gramm-Leach Bliley Act of 199 in the Maryland Insurance Code Sec. 2-109.

When considering the broad privacy landscape, NAMIC encourages legislators to fully understand all the existing frameworks of laws and regulations currently in place, which can vary significantly from industry to industry. New provisions would not be enacted in a vacuum. This is especially true for insurance -- each state and the federal government already has robust laws/regulations to address data privacy, security, and other requirements. By recognizing that this is not a blank slate and to forestall confusion and conflicts, NAMIC advocates that new provisions are not a disconnected additional layer of obligations. To avoid unintended consequences, NAMIC encourages policy makers to recognize existing laws and regulations.

Given the vital business purposes for data in the insurance transaction, historically policy makers have recognized the important role information plays in insurance and, with certain protections in place, they have allowed collection, use, and disclose for operational and other reasons.

Title V of the Gramm-Leach-Bliley Act (GLBA)² provides a landmark privacy framework for financial services, including insurance. It sets forth notice requirements and standards for the disclosure of nonpublic personal

¹ NAMIC member companies write \$357 billion in annual premiums and represent 69 percent of homeowners, 56 percent of automobile, and 31 percent of the business insurance markets. Through its advocacy programs NAMIC promotes public policy solutions that benefit member companies and the policyholders they serve and fosters greater understanding and recognition of the unique alignment of interests between management and policyholders of mutual companies.

² See 15 U.S.C. Sec. 6801 et. seq.



financial information – it specifically requires giving customers the opportunity to opt-out of certain disclosures. Under GLBA, functional financial institution regulators implemented the privacy standards. Given concerns with consistency, the National Association of Insurance Commissioners (NAIC) has adopted multiple model laws with regard to data privacy and cybersecurity³. And states have moved forward with adopting those models. For insurers, the Maryland Insurance Administration (MIA) regulates privacy matters (including consistent with Md. Code regs. 31.16.08.01 to 31.16.08.24) and provides robust oversight.

When it comes to retaining information, insurers are already subject to specific record retention requirements. This information is important for several reasons. Insurers need to have information available for claims and litigation and insurance regulators rely on data for market conduct purposes. Again, insurance-related data is subject to numerous existing laws and regulations.

While NAMIC is pleased to see the inclusion of a GLBA exemption in SB 541, the exception should apply to both the data and entity subject to the GLBA as follows:

(3) A Financial Institution or affiliate of a financial institute or *data* that is subject to Title V of the Federal Gramm-Leach-Bliley Act and regulations adopted under the act and the rules and implementing regulations promulgated thereunder or to Maryland Insurance Code Ann. Sec. 2-109 and the rules and implementing regulations promulgated thereunder.

Thank you for taking the time to consider our position on Senate Bill 541.

Sincerely,

Matt Overturf
Regional Vice President
Ohio Valley/Mid-Atlantic Region

³See NAIC Model Laws [668](#), [670](#), [672](#), [673](#)

SB 541 Support with Amendments.pdf

Uploaded by: Matt Power

Position: FWA



140 South Street,
Annapolis, MD 21401
410-269-0306
www.micua.org



Support with Amendments

Senate Finance Committee

Senate Bill 541 (Gile) Maryland Online Data Privacy Act of 2024



Matt Power, President

mpower@micua.org

February 14, 2024



On behalf of the member institutions of the Maryland Independent College and University Association (MICUA) and the nearly 55,000 students we serve, I thank you for the opportunity to provide this written testimony support with amendments [SB 541 \(Gile\) Maryland Online Data Privacy Act of 2024](#). This bill establishes a new standard for data privacy in Maryland both for consumers as well as controllers of data.



The bill is similar to legislation passed in other states across the country to provide consumers a greater say in the use and sale of their data. MICUA members take data privacy extremely seriously and spend a tremendous amount of time and resources to keep student data protected. Unfortunately, the bill seems to inadvertently single out non-profit institutions of higher education for inclusion while exempting public institutions of higher education. Similar bills in other states like Utah, Colorado and Connecticut have exempted both public and non-profit institutions of higher education.



MICUA requests that the sponsors consider a friendly amendment to Sec. 14-4603(3) that would include an exemption for non-profit institutions of higher education.



If you have any questions or would like additional information, please contact Irnande Altema, Associate Vice President for Government and Business Affairs, ialtema@micua.org.



For all of these reasons, MICUA requests a favorable Committee report, with amendments, for Senate Bill 541.



Consumer Reports - Re_ S.B. 541 Maryland Online Da

Uploaded by: Matt Schwartz

Position: FWA



February 13, 2024

Chair Pamela Beidle
Vice Chair Katherine Klausmeier
Finance Committee
Maryland Senate
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

Re: S.B. 541 Maryland Online Data Privacy Act - SUPPORT WITH AMENDMENTS

Dear Chair Beidle, Vice Chair Klausmeier, and Members of the Finance Committee,

Consumer Reports¹ sincerely thanks you for your work to advance consumer privacy in Maryland. S.B. 541 would extend to Maryland consumers important new protections, including meaningful data minimization restrictions, heightened standards for the processing of sensitive data, and strong civil rights protections. The bill also creates baseline consumer privacy rights, including the right to know the information companies have collected about them, the right to access, correct, and delete that information, as well as the ability to require businesses to honor universal opt-out signals and authorized agent requests to opt out of sales, targeted advertising, and profiling.

Consumers currently possess very limited power to protect their personal information in the digital economy, while online businesses operate with virtually no limitations as to how they process that information (so long as they note their behavior somewhere in their privacy policy). As a result, consumers are constantly tracked online and their behaviors are often combined with offline activities to provide detailed insights into their most personal characteristics, including health conditions, political affiliations, and sexual preferences. This information is sold as a matter of course, is used to deliver targeted advertising, facilitates differential pricing, and enables opaque algorithmic scoring—all of which erode individuals' basic expectation of privacy and can lead to disparate outcomes along racial and ethnic lines.

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.

This bill's data minimization provision (Section 14-4607 (B)(1)(I)) surpasses many other states' and would go a long way toward mitigating many of these types of harms. While we prefer privacy legislation that limits companies' collection, use, *and* disclosure of data to what is reasonably necessary to provide the service requested by the consumer (the bill only currently applies this standard to data collection, while allowing a much looser standard for processing activities)², simply reigning in systemic over-collection of consumers' personal information alone would help eliminate common practices that have contributed to, among other things, the persistent drip of massive data breaches.

Suitably, S.B. 541 also seeks to reduce unwanted secondary processing of data by creating a framework for universal opt-out through universal controls. Privacy legislation with universal opt-outs empowers consumers by making it easier to set their preferences relating to secondary processing, like sales or targeted advertising, eliminating the need for them to manage the otherwise untenably complicated ecosystem of privacy notices, opt-out requests, and verification.³ The goal of universal opt-out is to create an environment where consumers can set their preference once and feel confident that businesses will honor their choices as if they contacted each business individually.

Aside from this bill's thoughtful approach to minimization and opt-outs, we also appreciate that it includes the following elements:

- *Special Protections for Sensitive Data.* The bill builds on the underlying data minimization standard by requiring that the collection, processing, or sharing of any *sensitive* information be "strictly necessary" to provide the service requested by the consumer and that the controller obtain consent prior to undertaking any of these activities. These restrictions would effectively ban third-party targeted advertising and data sales based on our most personal characteristics, including data about our race, religious beliefs, health data, and data about children (targeted advertising to teens is also separately banned), which would represent a major change to the digital ecosystem, appropriately shifting the burden of privacy protection away from consumers themselves to companies that otherwise have every incentive to exploit consumer data for their own benefit. While we have concerns that this section's opt-in consent provisions may introduce unnecessary consent fatigue (if data processing is truly limited to providing what the consumer asked for, why should they need to consent on top of that), we support the intent of this provision wholeheartedly.

² Section 14-4607(9) of the bill ostensibly includes data minimization language restricting processing activities; however, because data processing is limited to any purpose listed by a company in its privacy policy — instead of to what is reasonably necessary to fulfill a transaction — that language will in practice have little effect for secondary purposes after data is collected.

³ Aleecia M. McDonanld and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society*, vol. 4, no. 3 (2008), 543-568.
https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf?sequence=1&isAllowed=y

We also note that Section 14-4604 (4) should be eliminated, since consumer health data is included as a category of sensitive data, and sales of sensitive data would never be “strictly necessary” to provide or maintain a service.

- *Strong civil rights protections.* This bill appropriately addresses a key harm observed in the digital marketplace today: the disparate impact that can occur through processing of personal data for the purpose of creating granularized profiles of individuals based off of data both collected and inferred about them. The bill ensures that a business’ processing of personal data cannot lead to discrimination against individuals or otherwise make opportunity or public accommodation unavailable on the basis of protected classes. A number of privacy bills introduced federally in recent years have included similar civil rights protections, including the American Data Privacy and Protection Act which overwhelmingly passed the House Energy and Commerce Committee on a 53-2 bipartisan vote.⁴ Consumer Reports’ Model State Privacy Legislation also contains similar language prohibiting the use of personal information to discriminate against consumers.⁵

At the same time, the legislation still contains several loopholes that would hinder its overall effectiveness. We offer several suggestions to strengthen the bill to provide the level of protection that Maryland consumers deserve:

- *Broaden opt-out rights to include all data sharing and ensure targeted advertising is adequately covered.* S.B. 541’s opt-out should cover all data transfers to a third party for a commercial purpose (with narrowly tailored exceptions). In California, many companies have sought to avoid the CCPA’s opt-out requirements by claiming that much online data sharing is not technically a “sale” (appropriately, CPRA expands the scope of California’s opt-out to include all data sharing and clarifies that targeted ads are clearly covered by this opt out).⁶ We recommend including “sharing” in S.B. 541’s opt-out right and using the following definition:

“Share” [or sell] means 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.

We also recommend refining the definition of “targeted advertising” to better match consumer expectations of the term. The drafted definition opens a loophole for data

⁴ See Section 2076, Amendment in the Nature of a Substitute to the American Data Privacy and Protection Act,

<https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-117-8152-P000034-Amdt-1.pdf>

⁵ See Sections 125 and 126, Consumer Reports, Model State Privacy Act, (Feb. 2021)

https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf

⁶ Id.

collected on a single site; it only includes ads based on a “consumer’s activities over time and across nonaffiliated **websites**” (plural, emphasis ours). This would exempt “retargeted” ads from the scope of the bill’s protections — ads based on one particular product you may have considered purchasing on another site. Such advertising — such as a pair of shoes that follows you all over the internet after you had left a merchant’s site — are the stereotypical example of targeted advertising; the law’s opt-out provisions should certainly apply to it. We suggest a shift toward the following definition:

“Targeted advertising” means the targeting of advertisements to a consumer based on the consumer’s activities with one or more businesses, distinctly-branded websites, applications or services, other than the business, distinctly branded website, application, or service with which the consumer intentionally interacts. It does not include advertising: (a) Based on activities within a controller’s own commonly-branded websites or online applications; (b) based on the context of a consumer’s current search query or visit to a website or online application; or (c) to a consumer in response to the consumer’s request for information or feedback.

- *Add a private right of action.* Given the AG’s limited resources, a private right of action is key to incentivizing companies to comply. Under an AG-only enforcement framework, businesses that recognize that the AG is only capable of bringing a handful of enforcement actions each year might simply ignore the law and take their chances in evading detection. Further, it’s appropriate that consumers are able to hold companies accountable in some way for violating their rights. We strongly encourage legislators to include a private right of action in future drafts of the legislation.
- *Eliminate the GLBA carveout.* The bill currently exempts from coverage any financial institution or an affiliate of a financial institution, as defined in the Gramm-Leach-Bliley Act. This carveout makes it so that large tech companies (Apple, Amazon, Google, Facebook, and Microsoft) would be exempted from the entire bill if one arm of their business crosses the threshold into providing traditional financial services, a line many of them are already skirting, if not already well past.⁷ The bill should instead simply provide an exemption for *information* that is collected pursuant to GLBA, as was done with HIPAA covered data.
- *Narrow the loyalty program exemption.* We are concerned that the exception to the anti-discrimination provision when a consumer voluntarily participates in a “bona fide loyalty, rewards, premium features, discounts, or club card program” (Section 14-4607(c)(2)) is too vague and could offer companies wide loopholes to deny or discourage consumer rights by simply labeling any data sale or targeted advertising practice as part of the “bona fide loyalty program.” We urge the sponsors to adopt a more precise definition and provide clearer examples of prohibited discrimination that

⁷ See e.g., The Economist, “Big Tech Pushes Further into Finance,” (Dec. 15, 2022), <https://www.economist.com/business/2022/12/15/big-tech-pushes-further-into-finance>; Richard Waters,

does not fall under this exception. For example, it's reasonable that consumers may be denied participation in a loyalty program if they have chosen to delete information or deny consent for processing that is functionally necessary to operate that loyalty program. That is, if you erase a record of having purchased nine cups of coffee from a vendor, you cannot expect to get the tenth cup for free. However, generally controllers do not need to sell data to others or to engage in cross-context behavior advertising in order to operate a bona fide loyalty program – such behaviors have nothing to do with the tracking of purchases to offer discounts or first-party advertising.

Loyalty programs take advantage of the exact type of informational asymmetry that privacy laws should strive to eliminate. While consumers typically view loyalty programs as a way to save money or get rewards based on their repeated patronage of a business, they rarely understand the amount of data tracking that can occur through such programs.⁸ For example, many grocery store loyalty programs collect information that go far beyond mere purchasing habits, sometimes going as far as tracking consumer's precise movements within a physical store.⁹ This information is used to create detailed user profiles and is regularly sold to other retailers, social media companies, and data brokers, among others. Data sales are extremely profitable for such entities — Kroger estimates that its “alternative profit” business streams, including data sales, could earn it \$1 billion annually.¹⁰ At a minimum, businesses should be required to give consumers control over how their information is collected and processed pursuant to loyalty programs, including the ability to participate in the program without allowing the business to sell their personal information to third-parties.¹¹

- *Remove ambiguities around requirements that the universal opt out mechanism not “unfairly disadvantage” other controllers.* The bill requires controllers to allow consumers to opt out of sales and targeted advertising through an opt-out preference signal (OOPS). However, the bill would also confusingly prohibit OOPSs from “unfairly disadvantage[ing]” other controllers in exercising consumers’ opt-out rights. It is unclear what “unfairly disadvantage” might mean in this context, as by their definition mechanisms that facilitate global opt-outs “disadvantage” some segment of controllers by limiting their ability to monetize data. Consumers should be free to utilize OOPSs to opt out from whatever controllers they want. For example, a consumer may want to use a certain OOPS that specifically opts them out from data brokers (or may configure a general purpose mechanism to only target data brokers); in that case, a consumer (and the OOPS) should be empowered to only send opt-out requests to data brokers. The

⁸ Joe 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>

⁹ *ibid.*

¹⁰ *ibid.*

¹¹ See Consumer Reports’ model State Privacy Act, Section 125(a)(5) for an example of a concise, narrowly-scoped exemption for loyalty programs. <https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/>

term “unfairly” introduces unnecessary ambiguity and the subsection should be eliminated.

- *Amend prohibitions on default opt-outs.* Currently, the bill states that OOPSs cannot send opt-out requests or signals by default. The bill should be amended to clarify that the selection of a privacy-focused user agent or control should be sufficient to overcome the prohibition on defaults; an OOPS should not be required to specifically invoke Maryland law when exercising opt-out rights. OOPSs are generally not jurisdiction-specific — they are designed to operate (and exercise relevant legal rights) in hundreds of different jurisdictions. If a consumer selects a privacy-focused browser such as Duck Duck Go or Brave — or a tracker blocker such as Privacy Badger or Disconnect.me — it should be assumed that they do not want to be tracked across the web, and they should not have to take additional steps to enable the agent to send a Maryland-specific opt-out signal. Such a clarification would make the Maryland law consistent with other jurisdictions such as California and Colorado that allow privacy-focused agents to exercise opt-out rights without presenting to users a boilerplate list of all possible legal rights that could be implicated around the world.

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

Sincerely,
Matt Schwartz
Policy Analyst

SB 541 Privacy SWA APCIA 021424 .pdf

Uploaded by: Nancy Egan

Position: FWA



Testimony of
American Property Casualty Insurance Association (APCIA)
Senate Finance Committee
SB 541- Maryland Online Data Privacy Act of 2024
February 14,2024

Support with Amendments

The American Property Casualty Insurance Association (APCIA) is the primary national trade organization representing nearly 60 percent of the U.S. property casualty insurance market. Our members write approximately 67.1 percent of total property and casualty insurance sold in Maryland. APCIA appreciates the opportunity to provide written comments regarding SB 541.

It is important to avoid creating duplicative and potentially inconsistent obligations nationally and within the state of Maryland. Our insurance regulators understand the unique business needs of the insurance industry and how privacy laws interact with those needs and the need for effective consumer protection. Building on another layer of prescriptive laws and an additional regulatory enforcement body can create unnecessary confusion and have unintended consequences, such as interfering with existing compliance requirements. As such, a comprehensive privacy bill must recognize existing frameworks and exempt entities that are already subject to proven, effective existing requirements and regulatory regimes.

Insurance licensees operating in Maryland are already governed by a comprehensive framework for the protection of personal information. Specifically, Maryland’s regulations, (31.16.08 et. seq.) “Privacy of Consumer Financial and Health Information” already regulate the collection, use and disclosure of nonpublic personal information gathered about individuals by all insurance licensees. This rule:

1. Requires a licensee to provide notice to individuals about its privacy policies and practices;
2. Describes the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal financial information about individuals to affiliates and nonaffiliated third parties; and
3. Provides methods for individuals to prevent a licensee from disclosing nonpublic personal financial information and nonpublic personal health information.

In addition, insurers are subject to the federal *Gramm-Leach-Bliley Act* (GLBA), which requires that financial institutions (including insurers) maintain consumer privacy protections. The GLBA also regulates how such institutions may disclose certain consumer information to non-affiliated third parties. GLBA is an established and comprehensive law that provides robust protections for consumers. Entities and the data they collect that are subject to GLBA should be completely exempt from the requirements imposed by this legislation.

The inclusion of this exemption is necessary to ensure the proper functioning of existing privacy laws for Maryland public and private entities that rely on this data. Due to the comprehensiveness of this existing, effective federal oversight scheme, many state privacy laws already exempt financial institutions subject to the GLBA and the data that they collect. We appreciate that the bill **does include a GLBA exemption for financial**

institutions or an affiliate of a financial institution, but it currently fails to include data subject to GLBA, which we believe is also necessary to exempt.

Therefore, we respectfully request the following language be added: (page 12-Lines 28-29)

(3) A FINANCIAL INSTITUTION, OR AN AFFILIATE OF A FINANCIAL INSTIUTION, **OR DATA** THAT IS SUBJECT TO

Once again, thank you for the opportunity to provide comments and request this simple amendment to Senate Bill 541.

Nancy J. Egan,

State Government Relations Counsel, DC, DE, MD, VA, WV

Nancy.egan@APCIA.org Cell: 443-841-4174

AdvaMed Written Testimony_MD SB 541_Finance.pdf

Uploaded by: Roxy Kozyckyj

Position: FWA



February 14, 2024

Senator Pamela Beidle, Chair
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

Senator Katherine Klausmeier, Vice-Chair
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

RE: Maryland Online Data Privacy Act of 2024 – MedTech Health Privacy Concerns Support with Amendments

Chair Wilson, Vice-Chair Crosby, and Members of the Committee,

AdvaMed appreciates your willingness to support the overall effort to provide confidence to your constituents that their data privacy is secured. SB 541 would provide the residents of Maryland with transparency and control over their personal data and provide new privacy protections. AdvaMed appreciates the opportunity to provide comments regarding SB 541 before the committee to offer support for the bill with two requested amendments that address med tech health privacy concerns.

AdvaMed member companies produce the medical devices, diagnostic products, and digital health technologies (collectively, “Medical Technologies”) that are transforming health care through the potential for earlier disease detection, less invasive procedures, and more effective treatments. AdvaMed members range from the largest to the smallest medical technology innovators and companies. We are committed to ensuring patient access to lifesaving and life-enhancing devices and other advanced medical technologies in the most appropriate settings.

AdvaMed champions a **patient-centered framework** for the use and disclosure of health information. AdvaMed believes this can be accomplished by (i) ensuring transparency around the collection, use, and sharing of health information, (ii) ensuring that obtaining consent does not unduly delay or diminish the quality of patient care, and (iii) harmonizing health privacy and security laws and regulations.

AdvaMed Recommendations

AdvaMed recommends the addition of two clarifying provisions that are consistent with the consumer privacy laws adopted in all states to date to avoid negatively impacting patient care and research and development.



Information treated like PHI under HIPAA.

As discussed below, some Health Care Provider (HCP) use of medtech data in patient care is not technically PHI under HIPAA (e.g., the concierge medicine example above). Data from such devices are not exempted under any of the current exemptions of HB 567. Thus, for example, patient data from ultrasounds used by HCPs who are covered recipients under HIPAA is excluded under HIPAA, while patient data from ultrasounds used by concierge physicians is regulated as personal data under the HB 567 even though the manufacturer treats data from both devices in the same way. However, various consumer rights and controller duties that are inconsistent with patient care and regulatory obligations would apply to the data from the concierge physician's ultrasound. Other health care providers that do not conduct HIPAA covered transactions also include free clinics, direct primary care/subscription-based care, cosmetic surgeons, and free-standing cosmetic surgery centers. Data from medical devices used by these other providers that do not accept insurance would similarly fall under the HB 567 regulatory framework instead of HIPAA.

This conflict can be addressed through an exclusion for information treated like PHI collected, used, or disclosed by a covered entity or business associate under HIPAA when the information is disclosed in accordance with HIPAA and afforded all the privacy protections and security safeguards of HIPAA and its implementing regulations. Such a provision could be inserted in § 14-4603 just after § 14-4603(B)(1) exempting PHI under HIPAA as shown below.

§ 14-4603.

...

(B) The following information and data are exempt from this subtitle:

(1) Protected health information under HIPAA.

(2) [Information treated like protected health information collected, used, or disclosed by a covered entity or business associate under HIPAA when the information is used or disclosed in accordance with HIPAA and the information is afforded all the privacy protections and security safeguards of the federal laws and implementing regulations under HIPAA.](#)

...

Unify De-identified Data Definition with HIPAA.

Data de-identified under HIPAA may not be considered "de-identified data" under this bill. Some patient data controlled or processed by medtech companies is de-identified under the HIPAA and transmitted for analysis, research, development, or some other essential health care purpose. AdvaMed recommends adding a clarifying provision so that data de-identified under HIPAA can continue to be used for analysis, private research, and development that can advance scientific understanding and lead to improvements in care and innovative solutions. This can be



accomplished by supplementing the definition of “de-identified data” with an additional sentence, as shown by the blue underlined text below.

§14-4601.

(A) In this subtitle the following words have the meanings indicated.

...

(P) “De-identified data” means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data does all of the following:

- (1) Takes reasonable measures to ensure that such data cannot be associated with an individual.
- (2) Commits in publicly available terms and conditions or in a publicly available privacy policy to maintain and use the information in de-identified form; and
- (3) Contractually obliges any recipients of the information to comply with all provisions of this subsection.

“De-identified data” also includes data de-identified in accordance with the requirements in 45 CFR 164 (HIPAA), where any recipients of such data are contractually prohibited from attempting to reidentify such data.

MedTech Privacy Concerns

The medical technology industry is committed, and continues to be highly incentivized, to implement privacy and data security practices that enhance the protection of patients and the quality and reliability of products and services. Unlike companies in other sectors that may focus on collecting and monetizing personal information as their primary commercial objectives, medtech companies use data about patient and health care professional users’ experiences to evaluate the safety and effectiveness of potential products, and — if and when cleared or approved for marketing — to support the ongoing legal compliance of products. AdvaMed member companies take seriously the level of trust placed in them by patients and have consistently taken action to self-identify best practices to balance innovation with patient protections.

While transparency is a crucial element of patient-centered health care, requiring specific and potentially repetitive affirmative consent for certain health-related uses is incompatible with our health care ecosystem. It is critical for patient care, device oversight, and the interests of public health that essential uses of patient and health information are not unduly impeded and that legislation be harmonized with existing laws and regulations that permit or require retention of



health-related data for specific purposes (e.g., for treatment, payment, health care operations, research, and FDA-regulatory purposes).

We believe that essential health care- and Medical Technology-related purposes (for which the public interest supports broad data use by Medical Technology companies without repeated affirmative consent for each separate element) ("**Essential Purposes**") include:

- Patient treatment and related activities, including efforts to address equitable access;
- Product monitoring (including safety activities and research to improve safety profiles);
- Research and development;¹
- Personalized medical device manufacturing/customization (e.g., 3D printed implant or other bespoke device tailored to individualized specifications that requires scans, images, and patient data to be sent to the manufacturer/service provider for customization);
- Product development and improvement (e.g., data is needed by artificial intelligence technologies to train and develop algorithms, and it is unrealistic to back out data from a working algorithm in a cleared product after the fact. It is becoming increasingly clear that reducing bias and developing equitable algorithms will require access to expanded and diverse datasets);
- Regulatory and payer compliance (including evidentiary requirements for coding, coverage, and reimbursement);
- Participation in value-based health care arrangements;
- Ongoing operations (including customer support); and
- Other activities in the interest of the public good, such as contributing to the response to a public health emergency.

Unique MedTech Data Privacy Issues in Patient Care

No Direct Interface with the Patient. In many instances, medtech companies do not directly interface with patients--often, a physician is the individual who selects the device and chooses to use it with certain patients based on their clinical judgment. In certain scenarios, patient data collected by medical devices is not Protected Health Information under HIPAA, as exemplified in the concierge physician example above. Furthermore, some health care providers purchase medtech through third-party distributors. In some of those instances, the medtech company will not have a means of interacting with clinicians to ascertain whether or not they are covered entities under HIPAA. These dynamics pose tension with certain provisions of SB 541.

An affirmative express consent framework is inappropriate for many medical devices used in patient care. While obtaining patient consent may be appropriate for some of these other use cases, requiring specific and potentially repetitive affirmative consent for certain uses related to health care threatens to prove unworkable. This is particularly true given that a

¹ R&D is distinguishable from product development and can lead to advancing medical science and innovative procedures or solutions.

patient may interact with many different Medical Technologies in an instance of acute healthcare need. The burden of obtaining and recording consent would fall on already time-pressed health care professionals to collect individual consent for each device utilized. Requiring specific and potentially repetitive consent for the permutations of data uses that support essential health care purposes is an unworkable approach.

A patient may interact with many different technologies during a single episode of care—vitals, pulse oximetry, *in vitro* diagnostic tests, EKG, echocardiogram, fluoroscopy or other diagnostic imaging, heart monitor, and electronic medical records. Requiring consents specific to each device during an urgent care situation would waste valuable time. In less urgent scenarios, repeated consent could more detrimentally burden the very sick or elderly. That is why Congress adopted a notice framework for HIPAA rather than a consent framework that requires consent for all health- and medtech-related uses of information, which is ill-suited for our health care system. However, some medtech data in patient care is not technically protected health information under HIPAA, since certain providers are not covered entities because they do not engage in HIPAA covered transactions.

Certain Consumer Personal Data Rights Conflict with Other Regulatory Obligations for MedTech

For example, the right to delete personal data obtained about the consumer is inconsistent with data retention requirements for medical records and FDA regulatory requirements.

MedTech Company application of HIPAA protections to data that is not Protected Health Information (PHI) under HIPAA.

The HIPAA regulations apply to “covered entities,” including payers and certain health care providers, as well as their “business associates.” HIPAA requires covered entities to use risk-based administrative, technical, and physical safeguards to keep protected health information private and secure and outlines specific criteria for when such data may be shared. HIPAA business associates carry out various functions for covered entities and must enter into a HIPAA Business Associate Agreement requiring them to comply with the same HIPAA restrictions that apply to the covered entity.

Some medtech companies treat all patient data in the manner that HIPAA-Covered Entity/Business Associate must treat Protected Health Information.

Medtech companies can be a Covered Entity/Business Associate under HIPAA with regard to certain patients but technically not a HIPAA-regulated entity in relation to other patients. Such companies may choose to handle all patient data from devices in both scenarios as a HIPAA-covered entity should for operational consistency or because they do not have insight into which scenario the patient falls under.

- **Patient Data from MedTech Devices Outside of HIPAA—Concierge Medicine Example.** HIPAA only regulates a Health Care Provider (HCP) when it conducts certain transactions² related to health insurance coverage electronically. A concierge physician

² 45 C.F.R. 160.103 (Covered entity means . . . (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

who does not accept insurance will not engage in HIPAA-covered transactions (electronic transmissions of patient information related to insurance coverage) and, accordingly, will not be a covered entity under HIPAA. Thus, technically, information from medical devices utilized by such concierge physicians is not protected under HIPAA. However, medtech companies navigating the unique complexity of whether or not HIPAA applies to certain patient data will likely choose to treat all data from such devices as protected under HIPAA out of an abundance of caution and maintain the data in the manner required of covered entities/business associates.

Conclusion

AdvaMed appreciates this opportunity to offer comments. To date, fourteen states have passed their data privacy reform laws that include amendments similar to those requested above. Most recently, New Hampshire passed legislation inclusive of all key healthcare exemptions that allow healthcare delivery, research, and patient privacy to interact and proceed unimpeded. We encourage the committee to follow suit and ensure that there continues to be alignment across the country with respect to data privacy.

Thank you, Chair Beidle and Vice-Chair Klausmeier, for your consideration, and we look forward to working with you and the committee on these amendments. We welcome any opportunity to serve as a resource, especially as it relates to medtech data privacy and security. If you have any questions or need additional information, please contact rkozyckyj@advamed.org.

Respectfully submitted,



Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions: (1) Health care claims or equivalent encounter information. (2) Health care payment and remittance advice. (3) Coordination of benefits. (4) Health care claim status. (5) Enrollment and disenrollment in a health plan. (6) Eligibility for a health plan. (7) Health plan premium payments. (8) Referral certification and authorization. (9) First report of injury. (10) Health claims attachments. (11) Health care electronic funds transfers (EFT) and remittance advice. (12) Other transactions that the Secretary may prescribe by regulation.)



SB 541_Maryland Online Data Privacy Act of 2024_MD

Uploaded by: Andrew Griffin

Position: UNF



LEGISLATIVE POSITION:

Unfavorable

Senate Bill 541

Maryland Online Data Privacy Act of 2024

Senate Finance Committee

Wednesday, February 14, 2024

Dear Chairwoman Beidle and members of the committee:

Founded in 1968, the Maryland Chamber of Commerce is the leading voice for business in Maryland. We are a statewide coalition of more than 6,800 members and federated partners working to develop and promote strong public policy that ensures sustained economic health and growth for Maryland businesses, employees, and families.

Senate Bill 541 would establish a framework for regulating how consumer's personal data is controlled and processed. The bill would also grant certain rights to consumers regarding their personal data and establish methods for consumers to exercise those rights. The Maryland Chamber of Commerce and its members place a high priority on consumer privacy and believe that privacy laws should provide strong safeguards for consumers but also balance the need for industry to innovate.

The Chamber recognizes the work and collaboration that have gone into writing SB 541 compared to iterations of past years. To that end, it is imperative from the Chamber perspective, that members of the General Assembly and stakeholders continue working toward a data privacy law that mirrors the budding regional approach, providing a clear set of rules for businesses and consumers, no matter their location. Areas of outstanding concern with HB 564 include:

- 1. Aligning definitions and requirements with those in other states.**
 - a. The definition of biometric information, consumer health data, and sensitive data is of most concern.
- 2. Ensuring the Attorney General retains sole responsibility of enforcement.**
- 3. Remove the requirement for permission to use personalized marketing techniques.**
- 4. Extending the effective date to October 2026 to provide adequate time for compliance.**

The Maryland Chamber of Commerce represents businesses of all sizes and industries, many of which would be impacted in some way by SB 541. We look forward to continuing the conversation on behalf of our diverse membership to produce legislation that is effective, consistent, and avoids unnecessary burdens.

SPSC - MD SB 541 (Omnibus) - Unfavorable Testimony

Uploaded by: Andrew Kingman

Position: UNF

STATE PRIVACY & SECURITY COALITION

February 9, 2024

Chair Pamela G. Beidle
Vice Chair Katherine A. Klausmeier
Senate Committee on Finance
Miller Senate Office Building
3 East Wing, 11 Bladen St.
Annapolis, MD 21401-1991

Re: Comprehensive Privacy (SB 541) - Unfavorable

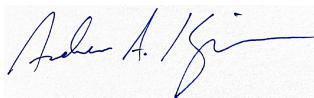
Dear Chair Beidle and Vice Chair Klausmeier,

The State Privacy and Security Coalition (SPSC), a coalition of over 30 companies and six trade associations the retail, telecom, tech, automotive, and payment card sectors respectfully opposes SB 541 in its current form, but writes with general recommendations to Senate Bill 541 and the hope that this bill can be improved and in a place to be enacted in 2024. We appreciate that Maryland is taking a comprehensive approach to privacy legislation and respectfully request amendments that effectively balance consumer protections in Maryland with implementation and compliance by the business community in a way that aligns with the protections provided and obligations imposed by other states that have adopted similar frameworks.

We appreciate the diligence from and consideration by the sponsors regarding the concerns that we have communicated to them, and look forward to continuing our conversations. Our primary concerns stem around provisions that are either unique to this bill (they do not appear in any other US privacy law) or provisions that are in all other laws which do not currently appear in SB 541.

We believe that working from a comprehensive, interoperable framework that provides strong privacy protections for consumers, clear and robust obligations for businesses, while still maintaining interoperability with other states, will provide the most seamless and modern approach to privacy for Maryland consumers. After a number of years of consideration by this legislature, we are hopeful that SB 541 represents a path forward that will put Maryland with the growing number of states with a comprehensive privacy framework.

Respectfully submitted,



Andrew A. Kingman
Counsel, State Privacy & Security Coalition

Maryland Online Data Privacy Act of 2024 SENATE BI

Uploaded by: cailey locklair

Position: UNF



Maryland Online Data Privacy Act of 2024

February 14, 2024

Position: Unfavorable as introduced, neutral with amendments

Background: SB541 Establishes generally the manner in which a controller or a processor may process a consumer's personal data; authorizing a consumer to exercise certain rights in regards to the consumer's personal data; requiring a controller of personal data to establish a method for a consumer to exercise certain rights in regards to the consumer's personal data; etc.

Comments:

1. Page 4, line 23: STRIKE "status" and INSERT in its place: "condition or diagnosis."
 - a. This change further clarifies the meaning of the term and mirrors CT law.
2. Page 5, line 13: INSERT "intentionally" before "designed or manipulated."
 - a. Dark pattern violations are like fraud and should be considered an intentional act of deceit.
3. Page 6, line 1: STRIKE OR DEFINE "(8) access to essential goods or services".
 - a. This is problematic without a precise definition of "essential goods and services". Further, this category is not traditionally included in the list.
4. Page 10, line 20: STRIKE "(1) Data revealing" and ADJUST remaining numbering.
 - a. This edit clarifies the definition of "Sensitive Data" by removing an ambiguous qualifier that could unintentionally broaden the term to include non-sensitive data as explained below. It maintains the same list of data elements that defines "Sensitive Data" without the unnecessary and problematic qualifier.
 - b. This inclusion of the qualifier "data revealing" should be struck as it broadens the defined term of "sensitive data" to potentially include "non-personal data". This non-personal data may imply inaccurate information about consumer (e.g., buying a cross might "reveal" one is Christian; buying cosmetics might "reveal" race). A law based on possible inferences drawn from retail purchases would be problematic.

MARYLAND RETAILERS ALLIANCE

The Voice of Retailing in Maryland



5. Page 11, line 17: STRIKE “controller’s” and INSERT “unaffiliated” before “websites or online applications”.
 - a. The current definition of “target advertising” could include providing ads based on a consumer’s activities on a business’s first-party website or mobile app, which has no precedence of being considered targeted advertising in state privacy laws.
 - b. This issue could also be addressed by adding “advertisements based on a consumer’s activity displayed by a controller on any first-party website or mobile app owned or operated by that control” to the list of exemptions of “targeted advertising” beginning on page 10, line 20.

6. Page 12, line 8: REPLACE “produces” with “provides”.
 - a. “Provides” is a more standard term used for this policy in other states. “Produces” could have unclear meaning and unintended consequences.

7. Page 12, line 12: REPLACE “35,000 consumers” with “100,000 consumers”.
 - a. Setting the threshold at 35,000 is far too low to protect small businesses. Most states use 100K.

8. Page 12, line 9: REPLACE “35,000 consumers” with “100,000 consumers” AND on page 12, line 16, REPLACE “20%” with “50%”.
 - a. This should say at least 100,000 consumers and derived more than 50% of revenue from the sale to remain consistent with almost every other state.
 - b. These edits ensure that Main Street businesses, including 98% of retailers that are single-location stores with less than 100 employees, are properly exempted from regulations as they are in most other states.

9. Page 15, line 27: ADD “, unless retention of the personal data is required by law” after “consumer”.
 - a. Create an exception that allows a controller to dismiss a consumer’s request to delete and retain information if it is required by another area of law.

10. Page 19, lines 27 through page 20 lines 5: STRIKE lines in their entirety, from “(1) collect personal data...” through “share sensitive data concerning a consumer;” ADJUST remaining numbering.
 - a. Section 14-4607(A)(1) and (2) are highly problematic. Like other consumer-facing businesses, retailers typically grow by attracting new customers. For example, retailers opening new store locations traditionally obtain lists of local households to send mailers announcing the new store opening. The law must preserve the same ability to collect data in the online environment for the purpose of marketing to prospective customers.



Personalized marketing does not create a harm for a consumer and should not be treated like sensitive information.

- b. Further, the law should not limit collection or processing to that “strictly necessary” to provide or maintain a “specific product or service requested by the consumer”. Retailers have always marketed products to inform the public of what is available for purchase. The inclusion of “strictly necessary” would limit the ability to provide this information to consumers.
11. Page 21, line 5: ADD “and processor” after “controller”.
 - a. Data minimization provisions should apply equally to both processors and controllers alike, and not to controllers alone. There is no legitimate public policy justification for limiting this requirement to controllers only; processors oppose data minimization requirements for their own benefit. The policy should establish an equal playing field.
 12. Page 21, line 21: REPLACE “15” with “45”
 - a. Extend the amount of time controllers have to respond to consumer requests to be in line with response requirements on Page 17, lines 5 and 8 and consistent with requirements in other states’ consumer privacy laws.
 13. Page 27, line 16: INSERT “designed” before “to ensure”.
 - a. Controllers cannot guarantee that a processor will adhere to instructions. Including “designed” protects controllers when processors do not follow instructions that are intended to limit consumer data processing.
 14. Page 28, line 15: STRIKE “(V) Other substantial injury to a customer”.
 - a. “Other substantial injury” is not defined, so this potential risk is unclear and should be removed.
 15. Page 32, line 29 through p. 33, line 2, inclusive – STRIKE AND REPLACE WITH:
“A controller or processor that discloses personal data to a processor or third party in accordance with this subtitle shall not be deemed to have violated this subtitle if the processor or third party that receives and processes such personal data violates this subtitle, provided, at the time the disclosing controller or processor disclosed such personal data, the disclosing controller or processor did not have actual knowledge that the receiving processor or third party would violate this subtitle. A third party or processor receiving personal data from a controller or processor in compliance with this subtitle is likewise not in violation of this subtitle for the transgressions of the controller or processor from which such third party or processor receives such personal data, provided, at the time the receiving processor or third party did not have actual knowledge that the disclosing controller or processor would violate this subtitle.”



- a. The protection provided to third party controllers or processors in 14-4611(D) needs to run both ways to protect controllers from the independent misconduct of third-party processors and controllers, as it does in most state privacy laws. Controllers must similarly be protected from the violations of the law by processors and third parties and held harmless unless they have actual knowledge the processor or third party intends to violate the law with the consumer data they receive from the controller.
16. Page 33, lines 10-12: ADD “or processor” after “If a controller” and ADD “or processor” before “shall demonstrate that the processing:”
- a. This obligation should apply equally to both controllers and processors.
17. Page 34, lines 11-12: STRIKE lines 11-12 in entirety, from “(B) This section” to “other remedy provided by law”.
- a. We would ask that private right of action be prohibited AND making clear that AG enforcement is an exclusive remedy by INSERTING the following language:
“THE ATTORNEY GENERAL SHALL HAVE EXCLUSIVE ENFORCEMENT AUTHORITY TO ENFORCE VIOLATIONS OF THIS ACT. (D) NOTHING IN THIS ACT SHALL BE CONSTRUED AS PROVIDING THE BASIS FOR, OR BE SUBJECT TO, A PRIVATE RIGHT OF ACTION FOR VIOLATIONS OF THIS OR ANY OTHER LAW.”
18. Page 34, line 18: REPLACE “2024” with “2025”.
- a. Controllers need adequate time to prepare for compliance with these requirements, especially the tens of thousands of retailers who are single-location stores that have not had to comply with other states’ privacy laws to date and must contract with service providers to help them implement these new obligations. Note that when California did a study on the cost of implementing their state’s requirements (which are approximately the same as those in this bill) for even the smallest of controllers (less than 50 employees), it was approximately \$100,000 to implement for first time.
19. Page 34 – In Section 14-4613: INSERT a notice-and-cure provision permitting the AG to notify businesses of potential infractions and permitting up to 30 or 60 days for the businesses to come into compliance with the law.
- a. This is a standard provision in all state privacy laws and should be included in this bill. A notice-and-cure period is especially important when a state first adopts a privacy law and many businesses have not yet had an opportunity to comply with these regulations. It permits them to have a direct dialogue with the AG to ensure they are implementing the law correctly, especially with the subjective determinations required throughout a bill like this.
 - b. Importantly, the California AG reported in their first year of compliance that approximately 75% of all businesses notified had resolved the alleged violation and come into full compliance with the provisions within 30 days.

MARYLAND RETAILERS ALLIANCE

The Voice of Retailing in Maryland



- c. A notice-and-cure provision helps increase compliance with the new law and keep state budgets in check by avoiding costly enforcement actions and it is therefore a mechanism welcomed by most state AGs and businesses alike.

With specific regard to loyalty rewards programs and suggested amendment 16, the bill clearly states that:

(E) IF A CONTROLLER SELLS PERSONAL DATA TO THIRD PARTIES OR PROCESSES PERSONAL DATA FOR TARGETED ADVERTISING OR FOR THE PURPOSES OF PROFILING THE CONSUMER IN FURTHERANCE OF DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT EFFECTS, THE CONTROLLER SHALL CLEARLY AND CONSPICUOUSLY DISCLOSE THE PROCESSING, AS WELL AS THE MANNER IN WHICH A CONSUMER MAY EXERCISE THE RIGHT TO OPT OUT OF THE PROCESSING.

Since the bill already has a disclosure requirement for data sales, and not all retailers engage in data sales with respect to their customer loyalty plan data, it does not make sense to add a duplicative disclosure requirement or-- worse – ban data sales from loyalty plans when their data sales are not banned outright in every other use case.

We suggest adding language clarifying that the disclosure requirements related to data sales also applies to loyalty plans, and in fact, you do not get your exemption for loyalty plans unless you are in compliance with those disclosure obligations in subsection (E) of the same section 14-4607 where the loyalty plan language is located.

Suggested amendment in bold.

14-4607.

* * *

(C) NOTHING IN SUBSECTION (A) OR (B) OF THIS SECTION MAY BE CONSTRUED TO:

* * *

(2) PROHIBIT A CONTROLLER FROM OFFERING A DIFFERENT PRICE, RATE, LEVEL, QUALITY, OR SELECTION OF GOODS OR SERVICES TO A CONSUMER, INCLUDING OFFERING GOODS OR SERVICES FOR NO FEE, IF THE OFFERING IS IN CONNECTION WITH A CONSUMER'S VOLUNTARY PARTICIPATION IN A BONA FIDE LOYALTY, REWARDS, PREMIUM FEATURES, DISCOUNTS, OR CLUB CARD PROGRAM THAT COMPLIES WITH SUBSECTION (E).

We welcome working with the sponsor and committee to resolve these issues.

MARYLAND RETAILERS ALLIANCE

The Voice of Retailing in Maryland



SB0541_UNF_MTC_Maryland Online Data Privacy Act of

Uploaded by: Drew Vetter

Position: UNF



MARYLAND TECH COUNCIL

TO: The Honorable Pamela Beidle, Chair
Members, Senate Finance Committee
The Honorable Dawn Gile

FROM: Andrew G. Vetter
Pamela Metz Kasemeyer
J. Steven Wise
Danna L. Kauffman
Christine K. Krone
410-244-7000

DATE: February 14, 2024

RE: **OPPOSE UNLESS AMENDED** – Senate Bill 541 – *Maryland Online Data Privacy Act of 2024*

The Maryland Tech Council (MTC) writes in **opposition unless amended** to *Senate Bill 541: Maryland Online Data Privacy Act of 2024*. We are a community of nearly 800 Maryland member companies that span the full range of the technology sector. Our vision is to propel Maryland to become the number one innovation economy for life sciences and technology in the nation. We bring our members together and build Maryland’s innovation economy through advocacy, networking, and education.

Consumer privacy is of the utmost importance to members of the MTC, so we are supportive of the concept of protecting the private data of Maryland residents. We appreciate the efforts of the bill sponsors to model this bill on laws in other states and the attempt to craft a law that works for Maryland consumers and businesses. The most important issue for the MTC is to have a data privacy law where full compliance is not overly burdensome. In many respects, this bill is based on laws that have been passed in other states such as Connecticut, Delaware, Colorado, Virginia, and others. In fact, there have been 13 states to date that have passed “comprehensive” data privacy laws, such as the one proposed here. In that spirit, the MTC has remaining concerns about portions of the bill that make compliance more difficult or impractical.

First, the MTC encourages the committee to align defined terms and data processing provisions as closely as possible to those in already-enacted laws in other states. There are MTC member companies doing business in other states and have already adapted their business practices in those states to align with these definitions and provisions. Having different rules and misaligned definitions of the same terms from state to state makes compliance impractical. We are aware that trade groups like TechNet and SPSC have been working with the bill sponsors to highlight these differences. The MTC is strongly in support of aligning these definitions and provisions to consensus language in other states.

Second, the MTC strongly advocates for the inclusion of a right to cure provision in the bill. By nature, a comprehensive online data privacy bill is lengthy and complicated. Businesses, especially smaller businesses, will be challenged in digesting these complex new requirements and bringing their business processes and systems into compliance. Our members appreciate the need for a comprehensive

data privacy bill and want to be in compliance. Businesses should be given the opportunity under the bill to correct minor compliance issues or mistakes before they are subject to enforcement actions. An opportunity to correct errors, even for some reasonable period of time, is merited in this circumstance, given the complex nature of the bill and the extent of new requirements.

Third, and also in the vein of compliance, the MTC recommends pushing back the effective date of the bill. The proposed effective date in the bill is October 1, 2024. That leaves businesses only 6 months from the end of Session until the effective date to get into compliance with this new law. Again, the requirements contained within this bill are lengthy and complex. Many of the Maryland-based companies impacted by this bill are small and do not have compliance teams or in-house attorneys to quickly operationalize these new requirements. These companies should be given more time to make the changes necessary to comply with this law by pushing back the effective date.

In conclusion, the MTC's concerns with this legislation can be summarized into two main areas: consistency and compliance. We urge the committee to make this bill as consistent as possible with comprehensive data privacy laws already passed in other states. We also request that the committee amend the bill to make it more feasible for companies to comply, specifically by looking at provisions, such as a right to cure and a different effective date.

The MTC recommends an unfavorable report unless amended consistent with this testimony. Thank you for the consideration.

SB0541(MD) SIA Concerns.pdf

Uploaded by: Jacob Parker

Position: UNF



February , 2023

The Honorable Pamela Beidle
Chair
Senate Finance Committee
Maryland General Assembly
Annapolis, MD

RE: Security Industry Association (SIA) position on Senate Bill 541, Data Privacy

Dear Chair Beidle, Vice-Chair Klausmeier and Members of the Finance Committee:

On behalf of the Security Industry Association (SIA) and our members, I am writing to express our concerns with SB 541 as it currently stands under consideration by the committee.

SIA is a nonprofit trade association located in Silver Spring, MD that represents companies providing a broad range of safety and security-focused products and services in the U.S and throughout Maryland, including more than 40 companies headquartered in our state. Among other sectors, our members also include the leading providers of biometric technologies available in the U.S.

Privacy is important to the delivery and operation of security systems and services, and our members are committed to protecting personal data. Given the lack of congressional action on a nationwide data privacy framework, in 2024, more than a dozen U.S. states have enacted consumer data privacy laws and many more are considering similar measures during legislative sessions this year.

While we are pleased to see that the measure as introduced is similar to the emerging consumer data privacy standard common among the vast majority of states that have enacted such measures, we believe numerous changes are critical to bring it into full alignment that will support uniform and thorough compliance.

Of these, we have submitted several key proposed adjustments to the House and Senate sponsors of the measure, none of which alter its intended effect:

- Ensuring the definition of “biometric data” is consistent with the current standard across existing state data privacy laws.
- Ensuring similar definitional alignment for various security/anti-fraud exceptions.
- Addition of explicit language ensuring exclusive Attorney General enforcement, which is uniform across existing state data privacy laws.

- Addition of a local preemption provision, which is also standard across existing state data privacy laws.

These key changes would address our concerns with SB 541. We urge the committee not to approve the measure unless these changes are made.

Again, we support the overall goal of SB 541 in safeguarding personal data and information, and we stand ready to provide any additional information or expertise needed as you consider these issues.

Respectfully,



Jake Parker
Senior Director, Government Relations
Security Industry Association
Silver Spring, MD
jparker@securityindustry.org
www.securityindustry.org

CTIA Testimony in Opposition to Maryland SB 541 -

Uploaded by: Jake Lestock

Position: UNF



**Testimony of
JAKE LESTOCK
CTIA**

In Opposition to Senate Bill 541

Before the Maryland Senate Finance Committee

February 14, 2024

Chair Beidle, Vice-Chair Klausmeier, and members of the committee, on behalf of CTIA®, the trade association for the wireless communications industry, I submit this testimony in opposition to Senate Bill 541. Our members support strong consumer privacy protections, including empowering consumers with the rights necessary to control their data. While consumer data is best addressed at the federal level, we look forward to working with the sponsor to ensure this legislation aligns with existing state frameworks on consumer protection.

Consumer privacy is an important issue and the stakes involved in consumer privacy legislation are high. State-by-state regulation of consumer privacy is creating an unworkable patchwork that will lead to consumer confusion. That is why CTIA strongly supports ongoing efforts within the federal government to develop a uniform national approach to consumer privacy. Deviating from clearly defined definitions, obligations, and privacy protections could have serious consequences for consumers, innovation, and competition in Maryland. A



patchwork quilt of state regulations would only complicate federal efforts and impose serious compliance challenges on businesses, ultimately confusing consumers.

The Maryland legislature is considering a privacy law that would generally apply to all industries. While a national standard is our preferred approach, we understand the concerns driving state action on these issues in the absence of a federal privacy law. The comprehensive approach in SB 541 is the right approach for state regulation. Importantly, it largely aligns with the comprehensive frameworks enacted in fifteen other states to date. This alignment is critical to ensure consistently strong consumer protections for consumers and to drive interoperable compliance processes for businesses with customers in many states.

We encourage the Maryland legislature to continue with this approach and to make some amendments to ensure the bill is interoperable with the laws that have already passed in other states. For example, we urge the legislature to further conform definitions like “targeted advertising” and “consumer health data” to match other state laws. General data collection and use restrictions also need to be further aligned with existing state laws. Ensuring conformity in definitions will ensure strong consumer privacy rights and protections and impose robust but clear obligations on businesses.

Additionally, SB 541 does not include a provision for a right to cure, which is found in the Virginia, Connecticut, Colorado, and Utah data privacy frameworks. This is a significant tool that allows a state enforcement authority to seek speedy resolution to good faith



compliance issues, and to focus their resources for enforcement actions on those businesses that either will not or cannot come into compliance within the statutory cure period.

In closing, we reiterate our concern about the enactment of state laws that create further fragmentation at the state level and recommend Maryland looks to further conform definitions and data collection restrictions with existing state laws and include a right to cure provision. For these reasons, CTIA respectfully opposes SB 541. We look forward to working with the sponsor to address some ways the bill can be amended to better align with existing state laws.

CHPA Amendment Request MD SB 541.pdf

Uploaded by: John McLuckie

Position: UNF



CONSUMER
HEALTHCARE
PRODUCTS
ASSOCIATION

Taking healthcare personally.

February 13, 2024

Senator Pamela Beidle
Chair, Senate Finance Committee
3E Miller Senate Office Building
11 Bladen Street
Annapolis, MD 21401

Re: S.B. 541 - Maryland Online Data Privacy Act of 2024

Dear Chair Beidle,

On behalf of the Consumer Healthcare Products Association (CHPA), the Washington, D.C. based national trade organization representing the leading manufacturers of over-the-counter (OTC) medicines, dietary supplements, and consumer medical devices, thank you for the opportunity to comment on S.B. 541. Unfortunately, I'm writing to express opposition to this bill as currently drafted. Although we do not object to the overall goal of the bill, which aims to empower consumers to have greater authority over their personal data, we do hold reservations about its compatibility with current federal regulations pertaining to controlled substances. Given the potential clash between these laws, we are against S.B. 541 unless it undergoes amendments to accommodate the existing federal obligations regarding data collection.

Controlled Substances Act

The Controlled Substances Act (CSA), also referred to as the Comprehensive Drug Abuse Prevention and Control Act, was enacted by Congress in 1970 with the aim of regulating the production, distribution, and utilization of controlled substances. As per 21 U.S.C. Section 830 of this Act, individuals or entities involved in transactions concerning listed chemicals (such as pharmacies selling allergy medications containing ephedrine or pseudoephedrine) are obligated to gather and retain identifiable personal records pertaining to these transactions and to share the data with law enforcement as required. Unfortunately, this bill does not provide an exemption for such transactions from its privacy provisions.

Amendment Recommendations

To avoid potential conflict with already existing federal law, CHPA recommends the following amendment to S.B. 541 on page 14, line 22 as item (13):

[\(13\) Personal data collected and used for purposes of the federal policy under the Controlled Substances Act Section on the Regulation of Listed Chemicals under 21 U.S.C. SEC. 830.](#)

Conclusion

CHPA and its members are committed to safeguarding the privacy of our customers' data. We commend the Senate Finance Committee for taking on this important issue, but unfortunately, we cannot support this bill in its current form. We look forward to continued dialogue with the hope we can come to an equitable resolution.

Respectfully submitted,

A handwritten signature in blue ink that reads "Carlos I. Gutiérrez". The signature is written in a cursive style with a large, stylized "G" at the end.

Carlos I. Gutiérrez
Vice President, State & Local Government Affairs
Consumer Healthcare Products Association
Washington, D.C.
cgutierrez@chpa.org | 202-429-3521

Cc: Members of the Senate Finance Committee

2024-2-9_CCIA Comments on MD SB 541.pdf

Uploaded by: Khara Boender

Position: UNF



February 9, 2024

Senate Finance Committee
3 East
Miller Senate Office Building
Annapolis, MD 21401

RE: SB 541 - “Maryland Online Data Privacy Act of 2024” (Unfavorable)

Dear Chair Beidle and Members of the Senate Finance Committee:

On behalf of the Computer & Communications Industry Association (CCIA)¹, I write to respectfully oppose SB 541, unless amended.

CCIA supports the enactment of comprehensive federal privacy legislation to promote a trustworthy information ecosystem characterized by clear and consistent consumer privacy rights and responsibilities for organizations that collect and process data. A uniform federal approach to the protection of consumer privacy throughout the economy is necessary to ensure that businesses have regulatory certainty in meeting their compliance obligations and that consumers are able to exercise their rights. CCIA appreciates, however, that in the absence of baseline federal privacy protections, state lawmakers are attempting to fill in the gaps. To inform these efforts, CCIA produced a set of principles to promote fair and accountable data practices.²

CCIA strongly supports the protection of consumer data and understands that Maryland residents are rightfully concerned about the proper safeguarding of their data. CCIA also appreciates the significant effort that lawmakers have undertaken to strike the appropriate balance for meaningful protections while preserving benefits consumers receive and the ability for innovation to thrive. As you know, in the absence of a comprehensive law at the federal level, there is a growing number of states that have enacted their own laws. The majority of these laws harmonize a key set of definitions and concepts related to privacy. While we appreciate the sponsors’ work on this bill, as written, SB 541 still would diverge from existing frameworks in several key ways.

Definitions and controller obligations should be clear and interoperable.

Existing broad-based privacy laws typically recognize a core set of rights and protections including individual control, transparency of processing activities, and limitations on third-party disclosures. However, even minor statutory divergences between frameworks for key definitions or the scope of privacy obligations can create onerous costs for covered organizations. Therefore, CCIA encourages that any consumer privacy legislation is reasonably aligned with existing definitions and rights in other jurisdictions’ privacy laws so as to avoid unnecessary costs to Maryland businesses. As drafted, key

¹ CCIA is an international, not-for-profit trade association representing small, medium, and large communications and technology firms. For over 50 years, CCIA has promoted open markets, open systems, and open networks. For more information about CCIA please see: <https://www.ccianet.org/about>.

² Computer & Communications Industry Association, *Considerations for State Consumer Privacy Legislation: Principles to Promote Fair and Accountable Data Practices* (January, 2022), <https://www.ccianet.org/wp-content/uploads/2022/02/CCIA-State-Privacy-Principles.pdf>



definitions in SB 541 are likely to prompt significant statutory interpretation and compliance difficulties, even for businesses with existing familiarity with other US state laws. Specifically, CCIA recommends attention to the following terms to align definitions such as: “biometric data”, “consumer health data”, and “targeted advertising”. We also suggest aligning the definition of “geofence” based on existing state laws, such as in Washington and New York. As currently written, the bill’s definition of “geofence” is inconsistent and conflicts with the bill’s definition of “precise geolocation data”.

CCIA also suggests clarifying that the definition of “sensitive data” would encompass the personal data of a *known* child. This would be consistent with the *actual knowledge* standard under COPPA and remove ambiguity.

CCIA suggests slight amendments to the definition of “publicly available information” to align with definitions in Oregon or Virginia. Under the current definition, a Maryland "consumer" (resident) that is not acting in a commercial or employment context would be required to make data publicly available. By extension, this would mean that any public information about a Maryland resident made available by persons other than a “consumer” could be excluded from being considered “publicly available information” and it would be treated as “personal information”. This would be a significant departure from the understanding of what constitutes “personal information” and could create a broadly sweeping “right to be forgotten”, where a person could request for data generally accepted as “publicly available” to be deleted. These provisions could have broad implications for other uses of such data, including search indexing, and training of artificial intelligence models, creating potential quality and bias concerns.

Finally, SB 541 would require a controller to obtain consumer consent prior to collecting personal data for content personalization or marketing. CCIA recommends striking this language as it is a novel provision in the context of other state data privacy laws, hindering the development of new products and services. This provision would also limit businesses' ability to conduct ad measurement, which would limit digital advertising for businesses large and small and have significant impacts on the internet economy.

CCIA requests further clarification regarding the enforcement provisions.

CCIA appreciates Maryland lawmakers’ consideration of appropriate enforcement mechanisms for a comprehensive data privacy framework and requests further clarity that SB 541 would not permit consumers to bring legal action against businesses that have been accused of violating new regulations. Every state that has established a comprehensive consumer data privacy law to date has opted to invest enforcement authority with their respective state attorney general. Private rights of action on other issues in states, such as under the Illinois Biometric Information Privacy Act, have resulted in plaintiffs advancing frivolous claims with little evidence of actual injury. These lawsuits also prove extremely costly and time-intensive for all parties involved, including the state, and it is foreseeable that these costs would be passed on to individual consumers in Maryland, disproportionately impacting smaller businesses and startups across the state.

* * * * *

CCIA and our members are committed to providing consumers with protections and rights concerning their personal data, however, further harmonization with established frameworks is needed. We



appreciate your consideration of these comments and stand ready to provide additional information as the legislature considers proposals related to technology policy.

Sincerely,

Khara Boender
State Policy Director
Computer & Communications Industry Association

UNFAVORABLE.SB541.HB567.MDRTL. LauraBogley.pdf

Uploaded by: Laura Bogley

Position: UNF



Opposition Statement SB541/HB567 – Request for Amendment

Maryland Online Data Privacy Act of 2024

Laura Bogley-Knickman, JD

Director of Legislation, Maryland Right to Life

We Oppose SB541/HB567 as written

On behalf of our 200,000 followers across the state, we respectfully yet strongly object to HB567/SB541 as written. This bill is unconstitutional, as it infringes on the First Amendment right to freedom of speech.

The bill infringes on First Amendment Free Speech

This bill, without due process of law, would deny free speech by prohibiting the use of geofencing within proximity of reproductive health clinics. Geofence marketing or “geofencing” is a commonly used location-based **marketing** and advertising strategy that allows you to send targeted ads to customers within a given geographical area. This marketing technology relies only on locating mobile signals within a triangulated area from a cell tower.

Geofencing technology locates cell phone signals but does not access data from cell phones or computers and therefore does not violate an individual’s right to privacy. This legal marketing method is a relatively less expensive way for a nonprofit or community-based organization to communicate with or educate potential customers. This bill would discriminately impose economic restrictions on the ability of Maryland nonprofits and other businesses to conduct business in the state. This violates the Equal Protection clause of the Constitution.

This bill discriminates on the content of speech by prohibiting geofence marketing only in proximity to “reproductive health” clinics and not other locations or business industries.

The offending section reads as follows and should be removed:

14–4604. A PERSON MAY NOT: (3) USE A GEOFENCE: (I) TO IDENTIFY, TRACK, COLLECT DATA FROM, OR SEND A NOTIFICATION TO A CONSUMER REGARDING THE CONSUMER’S CONSUMER HEALTH DATA; AND (II) WITHIN 1,750 FEET OF A MENTAL HEALTH FACILITY OR REPRODUCTIVE OR SEXUAL HEALTH FACILITY;

The bill denies women and girls Informed Consent

By limiting the use of geofencing in proximity to reproductive health clinics, the state would be denying women who seek reproductive health services, access to additional and/or alternative services related to reproductive health. In enacting this bill, the state would be denying Maryland women the right to informed consent by blocking access to educational and informational resources relevant to reproductive health. By denying women informed consent, the state subjects women to reproductive coercion and other forms of medical abuse.

Federal Precedent Prohibits Targeting Pro-life Speech

In conflict with federal court precedent, this bill attempts to **target and suppress pro-life speech** in Maryland. In [*Greater Baltimore Ctr. for Pregnancy Concerns, Inc. v. Mayor & City Council of Baltimore*, 879 F.3d 101 \(4th Cir. 2018\)](#), the City of Baltimore acting on behalf of abortion advocates, attempted unsuccessfully to put pro-life pregnancy centers out of business by enacting a targeted ordinance against commercial speech as "deceptive advertising".

The federal appeals court for the 4th Circuit affirmed the lower court's decision in favor of the pro-life pregnancy center, noting that ***"the City has considerable latitude in regulating public health and deceptive advertising. But Baltimore's chosen means here are too loose a fit with those ends, and in this case compel a politically and religiously motivated group to convey a message fundamentally at odds with its core beliefs and mission."*** The City also failed to establish that the pro-life pregnancy center was engaged in commercial or professional speech, which required the Court to apply higher scrutiny against the government action. Without proving the inefficacy of less restrictive alternatives, providing concrete evidence of deception, or more precisely targeting its regulation, the City did not prevail.

For these reasons we ask for your amendment to remove the offending provision or urge your unfavorable report.

[MD] SB 541 Privacy_TechNet_written_pdf.pdf

Uploaded by: margaret durkin

Position: UNF



TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Mid-Atlantic | Telephone 717.585.8622
www.technet.org | @TechNetMidAtla1

February 13, 2024

The Honorable Pam Beidle
Chair
Senate Finance Committee
Maryland Senate
3E Miller Senate Office Building
11 Bladen Street
Annapolis, MD 21401

RE: SB 541 (Gile) - Maryland Online Data Privacy Act of 2024.

Dear Chair Beidle and Members of the Committee,

On behalf of TechNet, I'm writing to offer remarks on SB 541 related to omnibus data privacy.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over 4.2 million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance. TechNet has offices in Austin, Boston, Chicago, Denver, Harrisburg, Olympia, Sacramento, Silicon Valley, and Washington, D.C.

We appreciate your leadership and thoughtful approach to consumer data privacy. The technology industry is fully committed to securing privacy and security for consumers and engages in a wide range of practices to provide consumers with notice, choices about how their data is used, as well as control over their data. TechNet believes that any consumer privacy bill should be oriented around building consumers' trust and fostering innovation and competitiveness. New privacy laws should provide strong safeguards to consumers while also allowing the industry to continue to innovate. These new laws should be based upon a uniform set of standards to avoid imposing a patchwork of policies across jurisdictions.

Thank you to Senator Gile for including TechNet in the stakeholder process early on and for incorporating several of our suggested changes. As mentioned during discussions with the sponsors, interoperability among states is key in the absence of a federal privacy standard. As such, TechNet continues to seek changes to SB 541, which are outlined below.

Definitions

TechNet requests that definitions in the bill align with other states' models. Specifically, we request that the definition of "Biometric Data" include the language "are used", as opposed to "can be used", and "identify" instead of "authenticate". For "Consumer Health Data", we request this definition be aligned with Connecticut's definition to avoid a different set of data being covered by each state. We also request that "status" in the definition be struck and replaced with "condition or diagnosis". For "Sale" and "Targeted Advertising", we request those match other states. For "De-identified Data", we request that the requirement of publicly committing not be limited to a privacy policy or terms and conditions. On "Precise Geolocation", we request a comma after "contents of communication". This is a clarifying change, universal among states. For "Sensitive Data", we suggest using the language "known child" and "for the purpose of uniquely identifying an individual" after genetic data or biometric data. No other state uses a "knows or has reason to know" standard.

Enforcement

TechNet requests at least a one-year effective date, right to cure period, and clarifying language around prohibiting private rights of action. Companies, large and small, will need adequate time to come into compliance with this bill by implementing consent mechanisms, renegotiating all existing contracts with vendors, and establishing new teams for Data Protection Assessments, among several others. A right to cure period allows for injunctive relief for the consumer and allows time for businesses to right any perceived wrongs while coming into compliance with this bill. TechNet thanks the sponsor for their intention to not include a private right of action in this legislation; however, to avoid loopholes, TechNet requests the below language to take that intent a step further.

- THE ATTORNEY GENERAL SHALL HAVE EXCLUSIVE ENFORCEMENT AUTHORITY TO ENFORCE VIOLATIONS OF THIS ACT. NOTHING IN THIS ACT SHALL BE CONSTRUED AS PROVIDING THE BASIS FOR, OR BE SUBJECT TO, A PRIVATE RIGHT OF ACTION FOR VIOLATIONS OF THIS OR ANY OTHER LAW.

14-4607 – Controller Responsibilities

On page 19 of the bill, please strike lines 27 through 29 dealing with content personalization. Content personalization is a major outlier and strays from other states' models. Regarding the standard of "knew or should have known", TechNet is requesting that phrase be struck and replaced with "has actual knowledge or willfully disregards...". To our knowledge, no other state has a "knew or should have known" standard, so we have aligned this to the standard in most other states.

Finally, as other state AGs develop their own lists of approved opt-out signals, we believe it makes sense to state that if a controller is working from a list of approved signals by another state AGO, it shall be deemed in compliance with this section.

Additional requests are appended in this document and have been shared with the sponsors ahead of this hearing.

TechNet joins industry partners and strongly encourages Maryland to look to the protections for consumers included in other states' omnibus privacy laws to avoid a patchwork of state laws that are difficult to comply with and confusing for consumers. Our members are committed to being collaborative in Maryland as the process moves forward. Please continue to consider TechNet's members a resource in this effort. Thank you for your time and we look forward to continuing these discussions with you.

Sincerely,

Margaret Durkin

Margaret Durkin
TechNet Executive Director, Pennsylvania & the Mid-Atlantic

**MD COMPREHENSIVE PRIVACY BILL (SB 541 / HB 567)
TOP PRIORITIES**

1. Definitions:

a. Biometric Data

- i. "Are used" vs. "Can be used" (overinclusive)
- ii. "Identify" vs. Authenticate (underinclusive)

b. Consumer Health Data

- i. Match to CT (implementing language as well)
 - 1. Sale w/ consent permitted for all sensitive data

c. Sale

- i. Match exceptions to all other states

d. Targeted Advertising

- i. Match to all other states

e. Deidentified Data

- i. "publicly commits"

f. Precise Geolocation

- i. "Contents of communications, or"

g. Sensitive Data

- i. Biometric/genetic "for the purpose of uniquely identifying..."
- ii. "Known child" instead of "reason to know"

2. Enforcement

a. "Nothing in this act..." and "AG exclusive authority" language

- i. "This act does not prevent a consumer from pursuing any other remedy provided by law."

b. Right to Cure

c. Effective Date

d. Preemption

3. §14-4607

a. Delete Consent for use of marketing/personalization if sole use (not in any of the 13 states, can be deceiving).

b. Align Data minimization with all 13 other states

c. Prohibition on selling sensitive data without the consumer's consent

d. "Actual knowledge or willfully disregards..." instead of "known or should have known" phrasing

4. DPA Requirements

a. "For each algorithm used"

b. "On a regular basis"

c. DPA's not retroactive

5. Exemptions

a. Conduct solely internal research

- b.** No liability for misuse by other party if no actual knowledge
- c.** Exemptions for current MD Medical Records/Information statutes
- d.** GLB – add data
- e.** HIPAA/Healthcare alignment with other states

6. Non-Conforming Provisions that Do Not Advance Privacy/Tweaks

- a.** 14-4608(A)(3)(II) and (III) deletion
- b.** 14-4608(B)(1) deletion
- c.** 14-4607(D)(4) conformance with CT (Privacy Policy) or CO if needed (as outlined in redline)
- d.** 14-4608(D)(4) – Delete third party reference
- e.** 14-4605(E)(2)(III) deletion
- f.** Delete 14-4612(B)(1) exception
- g.** 14-4606(A) – clarify that opt-out mechanism applies only to sale/targeted advertising
- h.** Replace all references to “Person” with “A controller or processor”
- i.** Add consent requirement to (A)(9)

SB541_NFIB_unfav (2024).pdf

Uploaded by: Mike O'Halloran

Position: UNF



NFIB-Maryland – 60 West St., Suite 101 – Annapolis, MD 21401 – www.NFIB.com/Maryland

TO: Senate Finance Committee

FROM: NFIB – Maryland

DATE: February 14, 2024

RE: **OPPOSE SENATE BILL 541** – Maryland Online Data Privacy Act of 2024

Founded in 1943, NFIB is the voice of small business, advocating on behalf of America’s small and independent business owners, both in Washington, D.C., and in all 50 state capitals. With more than 250,000 members nationwide, and nearly 4,000 here in Maryland, we work to protect and promote the ability of our members to grow and operate their business.

On behalf of Maryland’s small businesses, NFIB opposes Senate Bill 541 as currently drafted – legislation setting up a regulatory framework for controlling and processing personal data.

NFIB is thankful to the sponsors for removing the private right of action provision in the bill and recommends the legislature maintain it if it moves forward with the bill. Small business owners should not be held liable for damages if a company a small business utilizes to process personal data fails to comply with established data privacy regulations.

In its current form, SB541 does not contain a right to cure provision. NFIB supports adding this. This law and subsequent regulations will no doubt be lengthy and detailed. Small businesses deserve the chance to address data breaches before the Attorney General begins a proceeding.

Finally, SB541 will subject a small business owner to the requirements of the bill if it has 35,000 total consumers or 10,000 consumers and derives 20% of its gross revenue from the sale of personal data. These are the same thresholds as Delaware’s data privacy law. For perspective, Maryland’s population is more than six times that of Delaware. Virginia, for example, has thresholds of 100,000 total consumers *or* 25,000 consumers if the business derives 50% of its gross revenue from the sale of personal data.

For these reasons, **NFIB opposes SB541** as introduced and requests an unfavorable report.

MDDC UNFAV SB541.pdf

Uploaded by: Rebecca Snyder

Position: UNF



Maryland | Delaware | DC Press Association

P.O. Box 26214 | Baltimore, MD 21210

443-768-3281 | rsnyder@mddcpres.com

www.mddcpres.com

To: Senate Finance Committee

From: Rebecca Snyder, Executive Director, MDDC Press Association

Date: February 14, 2024

Re: **SB541 - OPPOSE**

The Maryland-Delaware-District of Columbia Press Association represents a diverse membership of newspaper publications, from large metro dailies such as the Washington Post and the Baltimore Sun, to hometown newspapers such as the Star Democrat and Maryland Independent, to publications such as The Daily Record, Baltimore Jewish Times, and online-only publications such as the Baltimore Banner, MoCo 360, Maryland Matters and Baltimore Brew.

The Press Association cannot support SB 541 as written. Previous versions of the bill were more strictly tailored to biometric data and the Press Association chose not to weigh in. We have concerns with recent changes to the bill, now called the Maryland Online Data Privacy Act of 2024.

We believe some modifications in this year's version of the bill could impose unintended negative consequences on Maryland's news media entities, which in turn would curtail access to vital journalism resources for the state's residents.

We have been working with the House sponsor on these proposed amendments and look forward to continuing those conversations. Three top concerns are highlighted below, and we welcome the opportunity to provide further feedback and redlines as you consider the legislation.

- 1. Geofencing:** We recognize the Legislature's intent in including restrictions on the use of geofencing in sensitive health-related settings. However, we believe the new language may contain a drafting error that would create a technical violation for common advertising practices completely unrelated to the protected facility.

Connecticut's amended privacy legislation [Public Act No. 23-56](#) reads:

"No person shall:...(C) use a geofence to establish a virtual boundary that is within one thousand seven hundred fifty feet of any mental health facility or reproductive or sexual health facility *for the purpose of* identifying, tracking, collecting data from or sending any notification to a consumer regarding the consumer's consumer health data; or (D) sell, or offer to sell, consumer health data without first obtaining the consumer's consent."

In contrast, HB 0567 reads: "14-4604. A PERSON MAY NOT: (3) USE A GEOFENCE:

(I) TO IDENTIFY, TRACK, COLLECT DATA FROM, OR SEND A NOTIFICATION TO A CONSUMER REGARDING THE CONSUMER'S CONSUMER HEALTH DATA; AND

(II) WITHIN 1,750 FEET OF A MENTAL HEALTH FACILITY OR REPRODUCTIVE OR SEXUAL HEALTH FACILITY; OR



We believe a strong news media is central to a strong and open society.

Read local news from around the region at www.mddcnews.com

(4) SELL OR OFFER TO SELL CONSUMER HEALTH DATA WITHOUT THE CONSENT OF THE CONSUMER WHOSE HEALTH DATA IS TO BE SOLD OR OFFERED TO BE SOLD. “

As drafted, the Maryland Online Data Privacy Act of 2024 could restrict the ability to use a geofence to send notifications to or communicate with consumers, even with their consent. The reordering of the section would also prohibit the use of a geofence within 1,750 of a facility regardless of purpose. Particularly in densely developed urban and suburban areas, there is a high likelihood of colocation of pharmacies and other medical practices with the protected facilities in question. The effect is highly likely to result in unintended technical violations of the bill.

Worse, the language could severely impact the ability of local merchants and businesses who happen to be within 1750 feet of a facility to engage in effective and compliant marketing and advertising practices to draw attention to and benefit businesses. Local news media entities often provide some services on behalf of these businesses. We urge adoption of the Connecticut language.

2. Controller Data Collection Limitations: We have two concerns with new bill language.

First, sections 14-4607. (A) (1), (3), (5) and (6) contain language that mirrors other legislation, most notably Connecticut, but with slight changes in sentence drafting. These changes could have the unintended consequence of banning any marketing, sale of sensitive data, or the processing of data that is consistent with COPPA. We welcome the opportunity to suggest technical redlines to restore the intent of the bill.

Second, the previous version, 2023’s HB 0807, contained controller duties that were largely similar to those with other states, such as Connecticut: “A controller shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary to collect for the purposes for which the data is processed” which is consistent with well-understood principles of data minimization.

The exact section in HB 0567 has been modified as follows:

“14-4607. (B) (1) A CONTROLLER SHALL: (I) LIMIT THE COLLECTION OF PERSONAL DATA TO WHAT IS REASONABLY NECESSARY AND PROPORTIONATE TO PROVIDE OR MAINTAIN A SPECIFIC PRODUCT OR SERVICE REQUESTED BY THE CONSUMER TO WHOM THE DATA PERTAINS;

Advertising is a secondary purpose of all businesses. They sell a specific product and this language is so limiting that it would preclude them from selling or offering by email, advertising or other item, for other items. Small biz & news media have secondary purpose. We believe the language as written will preclude any good faith, beneficial to consumers advertising. We are concerned the amended language would prohibit well-understood, expected data processing tasks done in service of common activities such as research and development, audience analysis, or marketing.

Most critically, as written, the language serves as a *de facto* opt-in for targeted advertising, which directly conflicts with the clearly outlined sections in the bill that outline opt-out requirements for targeted advertising.

3. Enforcement: Consistent with other states’ comprehensive consumer privacy legislation, we appreciate that the Maryland Online Data Privacy Act of 2024 does not include a private right of action. However, we note the addition of the following language:

“14-4613. (B) THIS SECTION DOES NOT PREVENT A CONSUMER FROM PURSUING ANY OTHER REMEDY PROVIDED BY LAW.”

Okay with adding AG piece, doesn’t want to foreclose the possibility of other laws that would allow prosecution. Negotiation with big tech.

As evidenced by discussions over the state’s anti-SLAPP legislation, news media entities are disproportionately vulnerable to baseless, frivolous lawsuits. Given Maryland’s robust ability to enforce unfair, abusive, or deceptive trade practices under Title 13, we recommend striking the language above from the bill, and/or adding the following:

“THE ATTORNEY GENERAL SHALL HAVE EXCLUSIVE AUTHORITY TO ENFORCE VIOLATIONS OF SECTIONS OF THIS ACT.”

We look forward to working with the sponsor on these technical amendments. Until these amendments are made, we urge an unfavorable report.

Joint Ad Trade Letter in Opposition to Maryland SB

Uploaded by: Travis Frazier

Position: UNF



February 12, 2024

Senator Pamela Beidle
Chair of the Maryland Senate
Finance Committee
3 East Miller Senate Office Building
11 Bladen Street
Annapolis, MD 21401

Senator Dawn Gile
3 East Miller Senate Office Building
11 Bladen Street
Annapolis, MD 21401

Delegate C. T. Wilson
Chair of the Maryland House
Economic Matters Committee
231 Taylor House Office Building
6 Bladen Street
Annapolis, MD 21401

Delegate Sara Love
210 Lowe House Office Building
6 Bladen Street
Annapolis, MD 21401

Senator Katherine Klausmeier
Vice Chair of the Maryland Senate
Finance Committee
123 James Senate Office Building
11 Bladen Street
Annapolis, MD 21401

Senator Katie Fry Hester
304 James Senate Office Building
11 Bladen Street
Annapolis, MD 21401

Delegate Brian M. Crosby
Vice Chair of the Maryland House
Economic Matters Committee
231 Taylor House Office Building
6 Bladen Street
Annapolis, MD 21401

Delegate Kriselda Valderrama
362 Lowe House Office Building
6 Bladen Street
Annapolis, MD 21401

RE: SB 541 and HB 567 – Maryland Online Data Privacy Act - Oppose

Dear Chair Beidle, Vice Chair Klausmeier, Senator Gile, Senator Hester, Chair Wilson, Vice Chair Crosby, Delegate Love, and Delegate Valderrama:

On behalf of the advertising industry, we write to **oppose SB 541 and HB 567**,¹ the Maryland Online Data Privacy Act (“MODPA”). We provide this letter to offer our non-exhaustive list of concerns about this legislation. As described in more detail below, the bills contain provisions that are out-of-step with privacy laws in other states and will only add to the increasingly complex privacy landscape for both businesses and consumers across the country. We ask you to harmonize MODPA with other state privacy laws by recognizing the privacy benefits of pseudonymous data, removing onerous consent requirements, and clarifying that the bills do not create a private right of action.

¹ Maryland SB 541 (Gen. Sess. 2024), located [here](#) and Maryland HB 567 (Gen. Sess. 2024), located [here](#) (hereinafter, collectively, “MODPA”).

As the nation’s leading advertising and marketing trade associations, we collectively represent thousands of companies across the country. These companies range from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies that power the commercial Internet, which accounted for 12 percent of total U.S. gross domestic product (“GDP”) in 2020.² By one estimate, over 160,000 jobs in Maryland are related to the ad-subsidized Internet.³ We would welcome the opportunity to engage with you further on the non-exhaustive list of issues with MODPA we outline here.

I. MODPA Should Be Harmonized with Existing State Privacy Laws

A patchwork of differing privacy standards across the states creates significant costs for businesses and consumers alike. Efforts to harmonize state privacy legislation with existing privacy laws are critical to minimizing costs of compliance and fostering similar privacy rights for consumers no matter where they live. One way MODPA significantly diverges from the vast majority of state privacy laws is by proposing a flat ban on all sales of sensitive data.⁴ No other state has imposed such a restrictive requirement; instead, other states permit sensitive data processing subject to an opt out or require consumer consent for such processing. A flat ban on the sale of sensitive data takes control out of the hands of consumers and prevents businesses from engaging in beneficial uses of sensitive data for which they would otherwise be able to obtain consumer consent in most other states.

Another way MODPA is out-of-step with existing state privacy laws is that it lacks a concept of pseudonymous data. Almost all state privacy laws recognize the privacy benefits of “pseudonymous data,” which is typically defined to include personal data that cannot be attributed to a specific natural person without the use of additional information. These other state laws exempt this data from consumer rights to access, delete, correct, and port personal data, provided that the pseudonymous data is maintained separately from information needed to identify a consumer and is subject to effective technical and organizational controls that prevent the business from accessing such identifying information. Absent an explicit exemption for pseudonymous data from consumer rights, companies could be forced to reidentify data or maintain it in identifiable form so that they can, for example, return this information when responding to a consumer access request. Requiring businesses to link pseudonymous data with identifiable information provides less privacy protections for consumers than a framework that permits and encourages companies to maintain data sets separately. We ask you to amend MODPA and harmonize it with the majority of other state privacy laws to exempt pseudonymous data from the consumer rights of access, correction, deletion, and portability.

Compliance costs associated with divergent privacy laws are significant. To make the point: a regulatory impact assessment of the California Consumer Privacy Act of 2018 concluded that the initial compliance costs to California firms would be \$55 billion.⁵ Another recent study found that a consumer data privacy proposal in a different state considering privacy legislation would have

² John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 15 (Oct. 18, 2021), located at https://www.iab.com/wp-content/uploads/2021/10/IAB_Economic_Impact_of_the_Market-Making_Internet_Study_2021-10.pdf.

³ *Id.* at 127.

⁴ MODPA at § 14-4607(A)(3).

⁵ See State of California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations*, 11 (Aug. 2019), located at https://dof.ca.gov/wp-content/uploads/sites/352/Forecasting/Economics/Documents/CCPA_Regulations-SRIA-DOF.pdf.

generated a direct initial compliance cost of \$6.2 billion to \$21 billion and ongoing annual compliance costs of \$4.6 billion to \$12.7 billion for the state.⁶ Other studies confirm the staggering costs associated with varying state privacy standards. One report found that state privacy laws could impose out-of-state costs of between \$98 billion and \$112 billion annually, with costs exceeding \$1 trillion dollars over a 10-year period, and with small businesses shouldering a significant portion of the compliance cost burden.⁷ Harmonization with existing privacy laws is essential to create an environment where consumers in Maryland have privacy protections that are consistent with those in other states, while minimizing unnecessary compliance costs for businesses. Maryland should not add to this compliance bill for businesses and should instead opt for an approach to data privacy that is in harmony with already existing state privacy laws.

II. A Consent Requirement for Content Personalization and Marketing Would Negatively Impact Maryland Residents and Hinder Economic Growth

MODPA would unreasonably require businesses to obtain consent from consumers before collecting data for the purpose of content personalization or marketing.⁸ No other state privacy law imposes an opt-in consent requirement for such marketing uses, and MODPA's restrictions on undefined terms could be read broadly to apply to even the most basic and routine processing activities, such as recommending new content based on a consumer's prior interactions with the business's digital properties or sending existing customers information about upcoming sales or product launches. Rather than providing consumers meaningful new privacy protections, an opt-in consent requirement like the one proposed would hinder Marylanders' ability to seamlessly engage online. If enacted, this requirement would exacerbate notice fatigue for Maryland consumers, who would be inundated with consent requests to collect data for routine, responsible uses as consumers navigate the Internet. Such a shift would virtually ensure Maryland residents have a vastly different online experience than consumers in neighboring or nearby states, such as Virginia, Delaware, and New Jersey, and would not receive the same opportunities to access resources available due to the ad-subsidized Internet as consumers from all other states. Maryland should not proceed with a blanket opt-in approach for marketing that starkly diverges from the approach in all other states that have enacted consumer data privacy legislation.

III. MODPA's Consent Requirements Should Be Amended to Reflect the Realities of the Online Ecosystem

Additionally, a consent approach ignores the realities of the online ecosystem. In general, third parties do not have a direct relationship with consumers, and therefore have no way to effectively obtain consent from consumers to collect personal data for personalization and marketing purposes. Therefore, MODPA's consent requirements could shut off the ability of third parties to participate in

⁶ See Florida Tax Watch, *Who Knows What? An Independent Analysis of the Potential Effects of Consumer Data Privacy Legislation in Florida*, 2 (Oct. 2021), located at <https://floridataxwatch.org/DesktopModules/EasyDNNNews/DocumentDownload.ashx?portalid=210&moduleid=34407&articleid=19090&documentid=986>.

⁷ Daniel Castro, Luke Dascoli, and Gillian Diebold, *The Looming Cost of a Patchwork of State Privacy Laws* (Jan. 24, 2022), located at <https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws> (finding that small businesses would bear approximately \$20-23 billion of the out-of-state cost burden associated with state privacy law compliance annually).

⁸ MODPA at § 14-4607(A)(1).

the data marketing ecosystem, undermining competition in the marketplace and lowering the availability of goods and services to consumers. Even states such as California have recognized other reasonable mechanisms for third parties to meet notice and choice requirements.⁹

Services provided by third parties help to create a more level economic playing field so small, mid-size, and start-up companies, many of which are minority and women-owned, can attract customers and compete in the marketplace with larger players. Third-party data sets are a key data asset that smaller entities utilize to reach and generate new audiences for their offerings. MODPA's consent requirement for content personalization and marketing would virtually ensure that the smallest of companies lose a vital resource for attracting and interacting with a customer base. In addition, MODPA would severely limit Maryland residents' exposure to new products and services from niche and small businesses that may interest them.

To avoid the unintended consequence of stopping third parties from participating in the market and the negative downstream consequences of that result for Maryland consumers, we urge the Committee to remove the consent requirement for content personalization and marketing, or, alternatively, to permit third parties to rely on contractual assurances with their data providers who have direct relationships with consumers to satisfy this requirement. This would involve a business that provides data to a third party representing, and the third party relying on those representations, that the consumer consented to collection for content personalization or marketing purposes at the time of collection. Such a clarification would allow the direct consumer touchpoint to satisfy the bill's consent requirements and allow competition and consumer benefits to continue to flow from third-party data use.

IV. A Private Right of Action Is an Inappropriate Form of Enforcement for Privacy Legislation

As presently drafted, MODPA allows a consumer to seek a remedy under another law and thus could be read to allow for private litigants to bring lawsuits.¹⁰ MODPA should be updated to clarify that it does not create a private right of action under any law. We strongly believe private rights of action should have no place in privacy legislation. Instead, enforcement should be vested with the Attorney General ("AG") alone, because such an enforcement structure would lead to stronger outcomes for Maryland residents while better enabling businesses to allocate resources to developing processes, procedures, and plans to facilitate compliance with new data privacy requirements. AG enforcement, instead of a private right of action, is in the best interests of consumers and businesses alike.

The possibility of a private right of action in MODPA would create a complex and flawed compliance system without tangible privacy benefits for consumers. Allowing private actions will flood Maryland's courts with frivolous lawsuits driven by opportunistic trial lawyers searching for technical violations, rather than focusing on actual consumer harm.¹¹ Private right of action provisions

⁹ Cal. Code Regs. tit. 11, § 7012(i).

¹⁰ MODPA at § 14-4613(B).

¹¹ A select few attorneys benefit disproportionately from private right of action enforcement mechanisms in a way that dwarfs the benefits that accrue to the consumers who are the basis for the claims. For example, a study of 3,121 private actions under the Telephone Consumer Protection Act ("TCPA") showed that approximately 60 percent of TCPA lawsuits were brought by just forty-four law firms. Amounts paid out to consumers under such lawsuits proved to be insignificant,

are completely divorced from any connection to actual consumer harm and provide consumers little by way of protection from detrimental data practices.

Additionally, a private right of action would have a chilling effect on the state's economy by creating the threat of steep penalties for companies that are good actors but inadvertently fail to conform to technical provisions of law. Private litigant enforcement provisions and related potential penalties for violations represent an overly punitive scheme that do not effectively address consumer privacy concerns or deter undesired business conduct. They expose businesses to extraordinary and potentially enterprise-threatening costs for technical violations of law rather than drive systemic and helpful changes to business practices. A private right of action would also encumber businesses' attempts to innovate by threatening companies with expensive litigation costs, especially if those companies are visionaries striving to develop transformative new technologies. The threat of an expensive lawsuit may force smaller companies to agree to settle claims against them, even if they are convinced they are without merit.¹²

Beyond the staggering cost to Maryland businesses, the resulting snarl of litigation could create a chaotic and inconsistent enforcement framework with conflicting requirements based on differing court outcomes. Overall, the possibility of a private right of action would serve as a windfall to the plaintiff's bar without focusing on the business practices that actually harm consumers. We therefore encourage legislators to clarify that MODPA does not create a private right of action under any law and vests enforcement authority with the AG alone.

V. The Data-Driven and Ad-Supported Online Ecosystem Benefits Maryland Residents and Fuels Economic Growth

Over the past several decades, data-driven advertising has created a platform for innovation and significant growth opportunities. One recent study found that the Internet economy's contribution to the United States' GDP grew 22 percent per year since 2016, in a national economy that grows between two to three percent per year.¹³ In 2020 alone, the Internet economy contributed \$2.45 trillion to the U.S.'s \$21.18 trillion GDP, which marks an eightfold growth from the Internet's contribution to GDP in 2008 of \$300 billion.¹⁴ Additionally, more than 17 million jobs in the U.S. were generated by the commercial Internet in 2020, 7 million more than four years prior.¹⁵ More Internet jobs, 38 percent, were created by small firms and self-employed individuals than by the largest Internet companies, which generated 34 percent.¹⁶ The same study found that the ad-supported Internet supported 168,600 full-time jobs across Maryland, more than double the number of Internet-driven

as only 4 to 8 percent of eligible claim members made themselves available for compensation from the settlement funds. U.S. Chamber Institute for Legal Reform, *TCPA Litigation Sprawl* at 2, 4, 11-15 (Aug. 2017), located [here](#).

¹² For instance, in the early 2000s, private actions under California's Unfair Competition Law ("UCL") "launched an unending attack on businesses all over the state." American Tort Reform Foundation, *State Consumer Protection Laws Unhinged: It's Time to Restore Sanity to the Litigation* at 8 (2003), located [here](#). Consumers brought suits against homebuilders for abbreviating "APR" instead of spelling out "Annual Percentage Rate" in advertisements and sued travel agents for not posting their phone numbers on websites, in addition to initiating myriad other frivolous lawsuits. These lawsuits disproportionately impacted small businesses, ultimately resulting in citizens voting to pass Proposition 64 in 2004 to stem the abuse of the state's broad private right of action under the UCL. *Id.*

¹³ Deighton & Kornfeld 2021 at 5.

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Id.* at 6.

jobs from 2016.¹⁷

A. Advertising Fuels Economic Growth

Data-driven advertising supports a competitive online marketplace and contributes to tremendous economic growth. Overly restrictive legislation that significantly hinders certain advertising practices, such as third-party tracking, could yield tens of billions of dollars in losses for the U.S. economy—and, importantly, not just in the advertising sector.¹⁸ One recent study found that “[t]he U.S. open web’s independent publishers and companies reliant on open web tech would lose between \$32 and \$39 billion in annual revenue by 2025” if third-party tracking were to end “without mitigation.”¹⁹ That same study found that the lost revenue would become absorbed by “walled gardens,” or entrenched market players, thereby consolidating power and revenue in a small group of powerful entities.²⁰ Smaller news and information publishers, multi-genre content publishers, and specialized research and user-generated content would lose more than an estimated \$15.5 billion in revenue.²¹ According to one study, “[b]y the numbers, small advertisers dominate digital advertising, precisely because online advertising offers the opportunity for low cost outreach to potential customers.”²² Absent cost-effective avenues for these smaller advertisers to reach the public, businesses focused on digital or online-only strategies would suffer immensely in a world where digital advertising is unnecessarily encumbered by overly-broad regulations.²³ Data-driven advertising has thus helped to stratify economic market power and foster competition, ensuring that smaller online publishers can remain competitive with large global technology companies.

B. Advertising Supports Maryland Residents’ Access to Online Services and Content

In addition to providing economic benefits, data-driven advertising subsidizes the vast and varied free and low-cost content publishers offer consumers through the Internet, including public health announcements, news, and cutting-edge information. Advertising revenue is an important source of funds for digital publishers,²⁴ and decreased advertising spends directly translate into lost profits for those outlets. Revenues from online advertising based on the responsible use of data support the cost of content that publishers provide and consumers value and expect.²⁵ And, consumers tell us that. In fact, consumers valued the benefit they receive from digital advertising-subsidized online content at \$1,404 per year in 2020—a 17% increase from 2016.²⁶ Another study found that the free and low-cost goods and services consumers receive via the ad-supported Internet amount to

¹⁷ Compare *id.* at 127 (Oct. 18, 2021) with John Deighton, Leora Kornfeld, and Marlon Gerra, *Economic Value of the Advertising-Supported Internet Ecosystem*, INTERACTIVE ADVERTISING BUREAU, 106 (2017), located <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf> (finding that Internet employment contributed 61,898 full-time jobs to the Maryland workforce in 2016 and 168,600 jobs in 2020).

¹⁸ See John Deighton, *The Socioeconomic Impact of Internet Tracking* 4 (Feb. 2020), located [here](#).

¹⁹ *Id.* at 34.

²⁰ *Id.* at 15-16.

²¹ *Id.* at 28.

²² J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 9 (2022), located [here](#).

²³ See *id.* at 8.

²⁴ See Howard Beales, *The Value of Behavioral Targeting* 3 (2010), located [here](#).

²⁵ See John Deighton & Peter A. Johnson, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the US Economy* (2015), located [here](#).

²⁶ Digital Advertising Alliance, *Americans Value Free Ad-Supported Online Services at \$1,400/Year; Annual Value Jumps More Than \$200 Since 2016* (Sept. 28, 2020), located [here](#).

approximately \$30,000 of value per year, measured in 2017 dollars.²⁷ Legislative frameworks that inhibit or restrict digital advertising can cripple news sites, blogs, online encyclopedias, and other vital information repositories, and these unintended consequences also translate into a new tax on consumers. The effects of such legislative frameworks ultimately harm consumers by reducing the availability of free or low-cost educational content that is available online.

C. Consumers Prefer Personalized Ads and Ad-Supported Digital Content and Media

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. One study found more than half of consumers (53 percent) desire relevant ads, and a significant majority (86 percent) desire tailored discounts for online products and services.²⁸ Additionally, in a recent Zogby survey conducted by the Digital Advertising Alliance, 90 percent of consumers stated that free content was important to the overall value of the Internet and 85 percent surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers must pay for most content.²⁹

Unreasonable restraints on advertising create costs for consumers and thwart the economic model that supports free services and content online. For example, in the wake of the GDPR, and the opt-in consent requirements under that regime, platforms that have historically provided products and services for free have announced proposals to start charging consumers for access to their offerings.³⁰ MODPA would create a similar environment where many companies could be forced to charge for services and products that were once free to Maryland residents. Indeed, as the Federal Trade Commission noted in one of its submissions to the National Telecommunications and Information Administration, if a subscription-based model replaces the ad-based model of the Internet, many consumers likely will not be able to afford access to, or will be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.³¹ A subscription model will diminish the number of channels available to access information, increase costs to consumers, curtail access to a diversity of online voices, and create an overall Internet environment where consumers with means can afford to access content, while consumers with less expendable income will be forced to go without access to online resources.

Laws that restrict access to information and economic growth can have lasting and damaging effects. The ability of consumers to provide, and companies to responsibly collect and use, consumer data has been an integral part of the dissemination of information and the fabric of our economy for decades. The collection and use of data are vital to our daily lives, as much of the content we consume over the Internet is powered by open flows of information that are supported by advertising. We

²⁷ J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 2 (2022), located [here](#).

²⁸ Mark Sableman, Heather Shoenberger & Esther Thorson, *Consumer Attitudes Toward Relevant Online Behavioral Advertising: Crucial Evidence in the Data Privacy Debates* (2013), located [here](#).

²⁹ Digital Advertising Alliance, *Zogby Analytics Public Opinion Survey on Value of the Ad-Supported Internet Summary Report* (May 2016), located [here](#).

³⁰ See, e.g. Megan Cerullo, *Meta proposes charging monthly fee for ad-free Instagram and Facebook in Europe*, CBS NEWS (Oct. 3, 2023), located [here](#); see also Ismail Shakil, *Google to block news in Canada over law on paying publishers*, REUTERS (Jun. 29, 2023), located [here](#).

³¹ Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located [here](#).

therefore respectfully ask you to carefully consider MODPA's potential impact on advertising, the consumers who reap the benefits of such advertising, and the overall economy before advancing it through the legislative process.

* * *

We and our members strongly support meaningful privacy protections for consumers supported by reasonable and responsible industry practices and support a national standard for data privacy accordingly. We believe, however, that MODPA would impose particularly onerous requirements that would unreasonably restrict the free flow of information that powers the economy and Maryland residents' access to resources. We therefore respectfully ask you to reconsider MODPA and would welcome the opportunity to engage further and work with you to hone a workable privacy framework that benefits Maryland businesses and consumers alike.

Thank you in advance for your consideration of this letter.

Sincerely,

Christopher Oswald
EVP for Law, Ethics & Govt. Relations
Association of National Advertisers
202-296-1883

Alison Pepper
EVP, Government Relations & Sustainability
American Association of Advertising Agencies, 4A's
202-355-4564

Lartase Tiffith
Executive Vice President, Public Policy
Interactive Advertising Bureau
212-380-4700

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
202-898-0089

Lou Mastria, CIPP, CISSP
Executive Director
Digital Advertising Alliance
347-770-0322

CC: Bill Sponsors
Members of the Senate Finance Committee
Members of the House Economic Matters Committee

Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP

BSA Letter on Maryland Online Data Privacy Act Feb

Uploaded by: Matthew Lenz

Position: INFO



February 12, 2024

The Honorable Sara Love
Lowe House Office Building, Room 210
6 Bladen St., Annapolis, MD 21401

The Honorable Dawn Gile
Miller Senate Office Building, 3 East Wing
11 Bladen St., Annapolis, MD 21401

Dear Delegate Love and Senator Gile:

BSA | The Software Alliance¹ supports strong privacy protections for consumers and appreciates your work to improve consumer privacy through House Bill 567 (HB 567) and Senate Bill 541 (SB 541), the Maryland Online Data Privacy Act. In our federal and state advocacy, BSA works to advance legislation that ensures consumers' rights — and the obligations imposed on businesses — function in a world where different types of companies play different roles in handling consumers' personal data. At the state level we have supported strong privacy laws in a range of states, including consumer privacy laws enacted in Colorado, Connecticut, and Virginia.

BSA is the leading advocate for the global software industry. Our members are enterprise software and technology companies that create the business-to-business products and services to help their customers innovate and grow. For example, BSA members provide tools including cloud storage services, customer relationship management software, human resource management programs, identity management services, and collaboration software. Businesses entrust some of their most sensitive information — including personal data — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations.

We appreciate the opportunity to share our feedback on HB 567/ SB 541. Our recommendations below focus on key priorities in the legislation: interoperability with other state privacy laws, creating obligations for processors that reflect their role of handling data on behalf of other companies, and ensuring any universal opt-out mechanisms work in practice.

¹ BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Okta, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

I. **BSA Supports an Interoperable Approach to Privacy Legislation.**

BSA appreciates your efforts to ensure that HB 567/SB 541 create privacy protections that are interoperable with protections created in other state privacy laws. Privacy laws around the world need to be consistent enough that they are interoperable, so that consumers understand how their rights change across jurisdictions and businesses can readily map obligations imposed by a new law against their existing obligations under other laws.

We appreciate the harmonized approach you have taken in aligning many of HB 567/SB 541's provisions with the Colorado Privacy Act and the Connecticut Data Privacy Act, which create a range of new protections for consumers. BSA supported Colorado and Connecticut's privacy laws and has supported strong state privacy laws across the country that build on the same structural model of privacy legislation enacted in both states. In particular, we support HB 567/SB 541's focus on creating new rights for consumers, creating a range of obligations for businesses that require them to handle data responsibly, and focus on consumer-facing data rather than employment data, which can raise distinct and separate privacy concerns.

We highlight four areas in which interoperability of state privacy laws is particularly important:

- *Enforcement.* We encourage you to support consistency with other state privacy laws in HB 567/SB 541's enforcement provisions by giving the state Attorney General exclusive enforcement authority. Effective enforcement is important to protecting consumers' privacy, ensuring that businesses meet their obligations, and deterring potential violations. BSA supports strong and exclusive regulatory enforcement by a state's Attorney General, which promotes a consistent and clear approach to enforcing new privacy obligations. State Attorneys General have a track record of enforcing privacy-related laws in a manner that creates effective enforcement mechanisms while providing consistent expectations for consumers and clear obligations for companies. As currently written, HB 567/SB 541 do not explicitly provide for exclusive Attorney General enforcement.
- *Data Protection Assessments:* Like other state privacy laws, HB 567/ SB 541 would establish an obligation for controllers to conduct data protection assessments for processing activities presenting a heightened risk of harm to consumers. BSA supports requiring data protection assessments for high-risk activities. However, Section 14-4610(B) of HB 567/ SB 541 would require data protection assessments to include "an assessment for each algorithm that is used." No other state privacy law establishes this requirement, which if interpreted broadly, could become impractical to carry out in practice because companies can use a wide range of algorithms within a single product or service. Rather than assess the risks of these algorithms in isolation, data protection assessments should require companies to look at the risk from an overall product, service, or processing activity. Additionally, as multiple states begin to require data protection assessments, promoting consistency in the scope and content of such assessments will help companies invest in strong assessment practices that can be

leveraged in more than one state, instead of fragmenting risk-management and compliance efforts across jurisdictions even when those jurisdictions adopt similar substantive requirements.

- *Role of Third Parties:* We appreciate that HB 567/ SB 541’s definition of “third party” is consistent with the definition in other state privacy laws. However, there are several provisions of the legislation applying to third parties that diverge from other privacy laws and could result in conflating third parties with controllers and processors. For instance, Section 14-4607(D)(4) requires privacy notices to include the categories of third parties with which the controller shares personal data and “to the extent possible, how each third party may process the personal data.” But once a third party receives data from a controller, it becomes the controller of that data – and must address its processing in its own privacy notice. Additionally, Section 14-4612(D) states that “a third-party controller or processor that receives personal data from a controller or processor in compliance with this subtitle is not in violation...for the independent misconduct of the controller or processor.” Section 14-4611(B)(3) also provides that controllers are not required to comply with authenticated consumer rights requests if they do not “sell the personal data to a third party or otherwise voluntarily disclose the personal data to a third party other than a processor.” These sections are inconsistent with HB 567/ SB 541’s definition of “third party,” which specifically provides that term covers “persons other than the relevant consumer, controller, processor, or affiliate of the controller or processor.” Moreover, these sections could raise questions about the classification of controllers, processors, and third parties under the bill. For these reasons, we encourage you to harmonize the sections relating to third parties with those found in other state privacy laws.
- *Controller Obligations:* We are also concerned that some aspects of the obligations HB 567/ SB 541 would place on controllers in Section 14-4607(A) depart from those established under other state privacy laws. Instead, we recommend aligning the bill’s approach to controller obligations with the approach of the Colorado, Connecticut, and Virginia.

II. Distinguishing Between Controllers and Processors Benefits Consumers.

We support HB 567/ SB 541’s clear recognition of the unique role of data processors. Leading global and state privacy laws reflect the fundamental distinction between processors, which handle personal data on behalf of another company, and controllers, which decide when and why to collect a consumer’s personal data. Indeed, all states with comprehensive consumer privacy laws recognize this critical distinction.² In California, the state’s privacy law for several years has distinguished between these different roles, which it terms businesses and service providers, while all other state comprehensive privacy laws use the terms controllers and

² BSA | The Software Alliance, The Global Standard: Distinguishing Between Controllers and Processors in State Privacy Legislation, *available at* <https://www.bsa.org/files/policy-filings/010622ctrlprostatepriv.pdf>.

processors.³ This longstanding distinction is also built into privacy and data protection laws worldwide and is foundational to leading international privacy standards and voluntary frameworks that promote cross-border data transfers.⁴ BSA and its members applaud you for incorporating this globally recognized distinction into HB 567/ SB 541.

While the bill includes this important distinction, as noted above, we are concerned that HB 567/SB 541's provisions on third parties create uncertainty about the bill's treatment of processors. As other state laws recognize, processors are not third parties — and are subject to special rules restricting how they process data on behalf of a controller, unlike a third party. We strongly urge you to revise HB 567/SB 541's provisions on third parties and align them with the third-party provisions of the Colorado, Connecticut, and Virginia laws to avoid potential confusion about the distinct roles of processors and third parties

III. The Bill's Provisions Giving Controllers an Opportunity to Object to Processors' Use of Subcontractors Should be Revised.

As noted previously, BSA appreciates HB 567/ SB 541's clear recognition of the unique role of data processors, which process data on behalf of other companies and pursuant to their directions. While provisions in HB 567/ SB 541 robustly address the obligations of processors — which process personal data on behalf of controllers — including by ensuring they assist controllers in responding to rights requests and in implementing data security measures, Section 14-4608(A)(3)(VI) of the legislation creates significant concerns. This section provides that processors shall engage a subcontractor "after providing the controller an opportunity to object" and "in accordance with a written contract that requires the subcontractor to meet the processor's obligations regarding the personal data."

We recognize the need for a consumer's data to be protected regardless of whether they are held by a processor or a subprocessor. However, we strongly recommend a different approach: requiring processors to notify a controller about the use of a subprocessor and pass on their obligations to that subprocessor — but not requiring controllers have the opportunity to object to subprocessors. This edit is particularly important, because of the

³ See, e.g., Cal. Civil Code 1798.140(d, ag); Colorado CPA Sec. 6-1-1303(7, 19); Connecticut DPA Sec. 1(8, 21); Delaware Personal Data Privacy Act, Sec. 12D-102(9, 24); Florida Digital Bill of Rights Sec. 501.702((9)(a)(4), (24)); Indiana Senate Enrolled Act No. 5 (Chapter 2, Sec. 9, 22); Iowa Senate File 262 (715D.1(8, 21)); Montana Consumer Data Privacy Act Sec. 2(8,18); New Jersey Senate Bill 332/Assembly Bill 1971 (Section 1); Oregon CPA Sec. 1(8, 15); Tennessee Information Protection Act 47-18-3201(8, 20); Texas Data Privacy and Security Act Sec. 541.001(8, 23); Utah CPA Sec. 13-61-101(12, 26); Virginia CDPA Sec. 59.1-575.

⁴ For example, privacy laws in Hong Kong, Malaysia, and Argentina distinguish between "data users" that control the collection or use of data and companies that only process data on behalf of others. In Mexico, the Philippines, and Switzerland, privacy laws adopt the "controller" and "processor" terminology. Likewise, the APEC Cross Border Privacy Rules, which the US Department of Commerce has strongly supported and promoted, apply only to controllers and are complemented by the APEC Privacy Recognition for Processors, which helps companies that process data demonstrate adherence to privacy obligations and helps controllers identify qualified and accountable processors. In addition, the International Standards Organization in 2019 published its first data protection standard, ISO 27701, which recognizes the distinct roles of controllers and processors in handling personal data. For additional information on the longstanding distinction between controllers and processors — sometimes called businesses and service providers — BSA has published a summary available [here](#).

frequency with which processors engage subcontractors to provide services requested by controllers. In many cases, processors will rely on dozens (or more) of subprocessors to provide a single service, and may need to replace a subcontractor quickly if the subcontractor is not able to perform a service due to operational, security, or other issues. Requiring that controllers have an opportunity to object slows down the delivery of services and products to consumers, without clear benefits to privacy. Instead, we believe a processor should be required to notify a controller about subprocessors and pass on obligations to subcontractors via contract, to ensure consumers' personal data remains protected.

IV. Consider Practical Issues Involved in Creating a System for Recognizing Universal Opt-Out Mechanisms.

We believe that consumers should have clear and easy-to-use methods to exercise new rights given to them by any new privacy law. Like the state privacy laws enacted in Colorado and Connecticut, HB 567/SB 541 include a clear requirement for controllers to honor a consumer's use of a universal opt-out mechanism to exercise new rights to opt out of targeted advertising or the sale of their personal data. Under Section 14-4607(F)(3)(II), controllers must honor these mechanisms no later than October 1, 2025.

If the bill retains this requirement, we strongly encourage you to focus on creating a universal opt-out mechanism that functions in practice. It is important to address how companies will understand which universal opt-out mechanism(s) meet HB 567/ SB 541's requirements. One way to address this concern is by creating a clear process for developing a public list of universal opt-out mechanisms and soliciting stakeholder feedback as part of that process, similar to the approach contemplated under the Colorado Privacy Act.⁵ Focusing on the practical aspects of implementing this requirement can help companies develop strong compliance programs that align their engineering and other resources accordingly. We also encourage you to focus on recognizing a universal opt-out mechanism that is interoperable with mechanisms recognized in other states. Interoperability is essential in ensuring that any universal opt-out mechanism is workable and allows consumers to effectuate their rights across state lines.

Finally, as you consider how to ensure any universal opt-out mechanism works in practice, we recommend educating consumers about what universal opt-out mechanisms do in addition to their limitations. For example, if a consumer uses a browser-based mechanism to opt out of the sale or sharing of the consumer's personal information, the browser may be able to effectuate that request for activity that occurs within the browser, but not activity outside of the browser. Consumers should be aware of this and other limitations.

Thank you for your continued leadership in establishing strong consumer privacy protections, and for your consideration of our views. We welcome an opportunity to further engage with you or a member of your staff on these important issues.

Sincerely,

⁵ See Colorado Department of Law, Universal Opt-Out Shortlist, *available at* <https://coag.gov/uoom/>.

The Honorable Sara Love
The Honorable Dawn Gile
February 12, 2024
Page 6

A handwritten signature in black ink that reads "Matthew Lenz". The signature is written in a cursive, flowing style with a horizontal line crossing through the middle of the name.

Matthew Lenz
Senior Director and Head of State Advocacy