

230307-SB698-online-biomtrc-data-prvcy.pdf

Uploaded by: Christine Hunt

Position: FAV

Christine Hunt and Jay Crouthers
1014 Dockser Drive
Crownsville, MD 21032

March 7, 2023

Maryland General Assembly
Members of the Finance Committee
Annapolis, MD

RE: SB 698 – Consumer Protection – Online Biometric Data Privacy

Dear Senators,

We support SB 698 and respectfully request that you vote for it.

Based on the Fiscal and Policy Note, the bill appears to be supportive of consumers' right to privacy of their online, personal and biometric data.

Having ads and other information related to recent online activity and searches is just creepy and creates a discomfort of where the information about us is being used and/or abused.

I understand that Delegate Mark Fisher has proposed that the bill should regulate the use of our data not only by private entities, but also by state and local governments. We wholeheartedly support this amendment to the bill and feel that it needs to be included to ensure privacy on all levels.

Please vote for this bill with the amendment.

Sincerely,

Christine Hunt and Jay Crouthers

von Lehmen__Staff_Maryland Cybersecurity Council__

Uploaded by: Greg Lehmen

Position: FAV

TESTIMONY PRESENTED TO THE
SENATE FINANCE COMMITTEE

SB 698
CONSUMER PROTECTION – ONLINE AND BIOMETRIC DATA PRIVACY

DR. GREG VON LEHMEN
STAFF, MARYLAND CYBERSECURITY COUNCIL

POSITION: SUPPORT
MARCH 8, 2023

Madam Chair, Madam Vice Chair, and members of the committee, thank you for the opportunity to testify. I am Greg von Lehmen, staff to the Maryland Cybersecurity Council, a statutory body chaired by Attorney General Brown. Last summer, the Council formed an ad hoc subcommittee on consumer and child privacy. I staffed the subcommittee and produced the final subcommittee report. I have been approved by OAG in my staff role to urge favorable consideration of the bill due to the research I conducted for that report.

Let me say by way of additional background that the subcommittee convened five times between July and December of last year. It received comments from more than ten interested parties, including public policy advocacy groups, an industry representative, privacy law attorneys, and the Attorney General of California, among others. The subcommittee adopted the report in December to help inform privacy legislation for Maryland.

I would make three broad points in connection with the bill.

First, the problem the bill addresses is the enhanced exposure to harm that consumers face as a result of the expansive, commercial collection of sensitive personal information. There is a vast data ecology that is focused on developing as detailed a profile of each consumer as possible. These profiles include where we go on the internet and in our cars, who we co-locate with, where we live, where we have lived, what we buy, our health conditions, our gender orientation, musical and TV

viewership tastes, political leanings, and hundreds of other data points. These data are not pinned to a device; they are pinned to a known person.

There are various types of risk that such detailed profiles pose. A significant risk is the exposure to data breaches. Data from PrivacyRights.org indicates that 10 billion US consumer records have been compromised between 2004 and 2019. Data published for Maryland suggests that in recent years the average number of separately reported residents impacted per year by a breach is about 600,000.¹ With data breaches can come a variety of harms: identity theft, extortion, sextortion, and reputational damage, among others. The US Department of Justice reported that losses in 2018 due to identity theft, including personal account take-overs, exceeded \$15 billion.

The consumer's exposure is becoming more severe as commercial interest grows in using biometric data for a variety of purposes, such as authentication of credit cards at checkout. The problem is that once biometric data held by a company is breached and spilled into the criminal market, countermeasures become very difficult. Biometric data cannot be changed like a password.

Second, considering these risks, the question becomes what tools can be given to consumers to help them manage their exposure. The bill answers this question by incorporating widely accepted privacy principles. These principles include:

- *Transparency.* Consumers have a right to easily understandable information about data collection, use, and sharing practices.
- *Respect for context.* Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- *Data minimization.* Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- *Access, accuracy, and control.* Consumers have a right to access and correct personal data in usable formats as well as to delete personal information entirely.
- *Security.* Consumers have a right to secure and responsible handling of personal data

¹ Note that the total does not likely consist of unique cases, since separately reported breaches may affect some of the same residents. Consequently, the number of unique residents affected is some number lower than the total. See Office of the Maryland Attorney General, data breach snapshots for 2020, 2018, and 2016, respectively, at <https://www.umgc.edu/content/dam/umgc/documents/upload/data-breaches-fy-2020-snapshot-pdf.pdf>, <https://www.umgc.edu/content/dam/umgc/documents/upload/data-breaches-fy-2018-snapshot.pdf>, and <https://www.umgc.edu/content/dam/umgc/documents/upload/data-breaches-fy-2016-snapshot.pdf>

- *Accountability.* There should be mechanisms to enforce these principles.

These principles are not arbitrary but have developed over time out of a sense of concern about data accumulation and its impacts. The federal government first formulated and implemented most of the principles just mentioned starting in the 1970s because of the troves of personal data that it holds. These are known as the Fair Information Principles Practices (FIPPS).² With the growth in commercial data collection, the Obama Administration in 2012 called for the application of those principles in an expanded form to the commercial sector. This was the Administration's Consumer Bill of Rights.³ Similar concerns prompted the EU's General Data Protection Regulation (GDPR) in 2014.⁴ Today five US states have implemented the foregoing principles in some measure for millions of Americans: California, Colorado, Connecticut, Virginia, and Utah. These statutes have created a track record. The risk of unintended consequences can be known and minimized. There is no reason that I can see for not implementing the foregoing principles in Maryland law as the bill would do.

Finally, parents need help in managing the risk to their children. The federal Children's Online Privacy Protection Act (COPPA) has not kept pace with the explosion of mobile devices that allow children to access apps not just at home but wherever they are.

- Children misrepresent their age in violation of terms of use and participate on general audience platforms: Facebook, TikTok, Snapchat, among others—at scale.
- The risks that children face on these platforms are well documented—grooming is one—but it also includes targeted advertising. Repeated reports of the American Psychological Association, the Journal of Pediatrics, and others have shown that targeted advertising affects children's self-image, how they compare themselves to others, and results in harmful behaviors.
- Hundreds of thousands of child-directed applications—children's games—do collect what COPPA defines as personal information on children, including information on their device and browsing that is then linked to them. Moreover, they do it without any meaningful mechanism for first obtaining verifiable parental consent as COPPA requires. Here, too, the data is used to shape advertising that is targeted at them.

² See Fair Information Principles Practices (FIPPS) at <https://www.fpc.gov/resources/fipps/>

³ The White House (2012). Consumer Privacy in a Networked World. <https://nsarchive.gwu.edu/document/16084-white-house-consumer-data-privacy>

⁴ General Data Protection Regulation at <https://gdpr-info.eu/>

The bill takes some remedial steps in connection with these problems. The ad hoc subcommittee report goes further, including recommendations such as a different knowledge standard for companies operating general audience platforms.

Consequently, I support the language at the end of the bill that would establish a Task Force to examine COPPA-related issues and consider appropriate recommendations.

To conclude, I urge a favorable consideration of the bill. Thank you for the opportunity to testify.

OAG-CPD Testimony SB 698 SUPPORT.pdf

Uploaded by: Hanna Abrams

Position: FAV

ANTHONY G. BROWN
Attorney General

CANDACE MCLAREN LANHAM
Chief of Staff

CAROLYN QUATTROCKI
Deputy Attorney General



WILLIAM D. GRUHN
Chief
Consumer Protection Division

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION

March 8, 2023

TO: The Honorable Melony Griffith, Chair
Finance Committee

FROM: Hanna Abrams, Assistant Attorney General

RE: Senate Bill 698 – Consumer Protection – Online and Biometric Data
Privacy (SUPPORT)

The Consumer Protection Division of the Office of the Attorney General supports Senate Bill 698 (“SB 698”), sponsored by Senator Augustine. Senate Bill 698 provides Marylanders with control over who can collect, share, and use their personal information and information collected based on their online activities and behaviors.

The issues surrounding the use of personal data reach well beyond traditional notions of privacy – to issues like discrimination, algorithmic fairness, and accountability.¹ Right now, companies are collecting and selling increasing amounts of sensitive information about our lives without our knowledge or consent. Unlike consumers in California, Colorado, Connecticut, or even Europe, Maryland consumers have no way of knowing when this occurs and no ability to protect themselves. Businesses have previously raised concerns about interoperability and implementation challenges. Senate Bill 698 ensures that Maryland consumers have privacy rights while simultaneously ensuring interoperability with the privacy laws that have been enacted in Connecticut, Colorado and other states.

Companies are collecting information that gives strangers personal information about us including mental health, gender, religious beliefs, sexual preferences, and even our precise locations. The adtech industry regularly collects, shares, sells, and processes consumer data. At least 70% of mobile apps share data with third parties, and 15% of the apps reviewed were connected to *five or more* trackers.² For example, digital health companies and mobile apps

¹ See *Algorithmic Bias Detection and Mitigation* (Brookings, May 2019), <https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/>

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>.

share user health data with third parties for advertising purposes.³ The extraction of personal information, particularly because it is done frequently without consumer knowledge, poses a significant threat to both our privacy and our safety.

Once collected, this sensitive information is frequently sold to third parties with whom consumers have no relationship. Recently, a Duke University study found that data brokers were selling everything from a list of individuals suffering from anxiety to a spreadsheet entitled “Consumers with Clinical Depression in the United States.”⁴

There are real consequences to the collection of information. Personal information, collected and shared without consumer knowledge, has caused the loss of jobs⁵ and has led to threats to personal safety.⁶ The personal information collected also feeds into algorithms used for advertising and eligibility decisions that frequently produce discriminatory outcomes and restrict access to housing,⁷ employment,⁸ credit,⁹ and education.¹⁰

Senate Bill 698 provides individuals with some transparency into and control over how their data is used. This transparency, coupled with giving users the ability 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.

We do, however, have concerns about the breadth of the exemptions in SB 698 that could serve to dilute the effect of the law, which we have shared with the sponsor. For example, page 11, lines 12 and 15-16, exempt “covered entities [and] business associates [under HIPAA]” and “an entity, or an affiliate of an entity, subject and in compliance with the federal Gramm-Leach-Bliley Act [GLBA]” respectively. While we acknowledge that there are other statutes that govern certain information, it is critical that sensitive information be governed by some form of privacy regulation. As drafted, SB 698 exempts *entities* that operate under the GLBA and

³ *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>.

⁴ 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/>.

⁵ Molly Omstead, *A Prominent Priest Was Outed for Using Grindr. Experts Say It’s a Warning Sign*, Slate (July 21, 2020), <https://slate.com/technology/2021/07/catholic-priest-grindr-data-privacy.html>.

⁶ 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>.

⁷ 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>.

⁸ Julia Angwin et al., *Facebook Job Ads Raise Concerns About Age Discrimination*, N.Y. Times (Dec. 20, 2017), <https://www.nytimes.com/2017/12/20/business/facebook-job-ads.html>.

⁹ 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/>.

¹⁰ 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

HIPAA entirely, even if the personal information they collect is not governed by those laws. Advocates for financial institutions will claim that the industry is highly regulated and therefore they do not need additional privacy regulations, but financial institutions 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.¹¹ Similarly, entities that provide healthcare services may be governed by HIPAA when providing those services, but may collect personal information that is not personal health information and therefore not regulated by HIPAA. To exempt these entities in their entirety would leave significant gaps in the privacy protections that SB 698 provides consumers. The Division believes it is important that personal information be governed by a privacy regulation, whether state or federal, and recommends that these exemptions be stricken and any carve-outs be limited to the *personal information* collected “pursuant and in accordance with” the applicable federal law.

We also have concerns about the exemptions to the definition of “targeted advertising” on page 10, lines 1-4, because they permit targeted advertising based on consumer activities on specific websites without a consumer request. Moreover, because the definition of “affiliate” includes all entities with common branding (page 3, line 9), the Division is concerned that large businesses with many affiliates will take this as permission to advertise about any of their affiliates without regard to whether the consumer has ever visited any of the affiliates’ websites.

Finally, we think it is important to ensure that definitions be consistent across related statutes. Maryland’s Personal Information Protection Act includes a definition of “personal information” that is similar, but not identical to the definition of “confidential data” in SB 698.

We also would like the Committee to consider whether lower thresholds might be appropriate in Maryland for example, in California, a much larger state, the threshold is lower: it is only 50,000 consumers, households, or devices.

Senate Bill 698 incorporates the separately introduced Biometric Data Privacy bill (SB 169) which ensures that immutable identity traits – biometrics – are not collected without consent and are never sold. Biometrics, because of their unchanging nature, make a person particularly vulnerable to identity theft and when stolen, cannot be altered like financial information. Companies’ unfettered collection of this information is a security threat and it is particularly important for companies to obtain consent and for consumers to be aware of which companies hold their biometrics. The Division previously submitted support for SB 169.

We urge the Finance Committee to issue a favorable report on SB 698.¹²

cc: Members, Finance Committee
The Honorable Malcolm Augustine

¹¹ 16 CFR § 313.1(b).

¹² The Division has been in contact with industry representatives and understands that a workgroup may be in the works to address the concerns of both consumers and industry. We have also been in contact with law enforcement agencies and have proposed language to avoid impacting their work pursuant to Title 17 of the Criminal Proc. Code.

Common Sense Media, Irene Ly - MD SB 698 Privacy B

Uploaded by: Irene Ly

Position: FAV



Written Testimony of Irene Ly

Policy Counsel, Common Sense Media

Before the Senate Finance Committee

"Online and Biometric Data Privacy Act"

Bill No: SB 698

Position: Favorable

March 8, 2023

My name is Irene Ly, and I am a Policy Counsel for Common Sense Media, where I work on privacy and platform accountability issues at the state and federal level. Common Sense Media is the leading organization dedicated to helping kids and families thrive in a rapidly changing digital world. We help parents, teachers, and policymakers by providing unbiased information, trusted advice, and innovative tools to help them utilize the power of media and technology as a positive force in all kids' lives.

Testimony Summary: Maryland must pass a strong privacy law that reduces harms against children online. Children are uniquely vulnerable because their brains are still developing, and their brain structures are fundamentally different from adults. These developmental vulnerabilities subject children to more harm from practices like targeted advertising and the algorithmic recommendation of content. Companies successfully engage in such practices by collecting billions of data points from users. Senator Augustine's SB 698 provides strong and needed protections for all consumers, and for children in particular, by imposing data minimization principles and requiring companies to obtain opt-in consent from teens before serving them targeted ads or selling their data. SB 698 should be further strengthened by amending the knowledge standard, and banning targeted advertising to children altogether. It is time for Maryland residents, and particularly Maryland children, to have their privacy truly protected online.

Thank you for the opportunity to offer comments on this important matter.

I. Absent Federal Legislation, Maryland Must Pass a Strong Comprehensive Privacy Law to Protect its Children

A. Existing Laws are Insufficient to Protect Consumers Online, and There is No Guarantee Federal Privacy Legislation Will Pass

The internet looks completely different from how it did just ten years ago. Platforms collect billions of data points of personal information about users that go far beyond their birthdate, home address, and phone number. As soon as users are on a platform, it is recording their online activity: which websites they visit and for how long, what information they looked for and the search terms they used, and which ads and other user posts elicited a response. With the use of emerging technologies like machine learning, platforms draw inferences about users based on these data points to hypertarget them with specific ads and content in an effort to maximize user engagement and profit. Strong privacy legislation is essential to protecting people online, particularly children, who have unique vulnerabilities, by cutting off the firehose of data that companies are unnecessarily but intentionally collecting on everyone.

Over the last two decades, there have been many attempts to pass a federal comprehensive online privacy law to no avail, leaving states to take the initiative. To date, five states have passed – to varying degrees of strength/or adequacy – an online privacy law: California, Colorado, Connecticut, Virginia, and Utah.

If an individual does not live in one of these five states, they do not have any privacy protections over their online personal information except when their data is subject to specific federal laws, such as the Children's Online Privacy Act (COPPA) and the Health Insurance Portability and Accountability Act (HIPAA). COPPA, which protects children's online data by requiring a company to obtain parental opt-in consent before collecting information from a child under 13 years old, was passed over two decades ago. For more than a decade, legislators and advocates have called for it to be updated to reflect what the internet, and the harms associated with it, look like today.

Last year, the Senate Commerce Committee passed the Children and Teens' Online Privacy Protection Act (COPPA 2.0) and the Kids Online Safety Act, and the House Energy and Commerce Committee passed the American Data Privacy and Protection Act. Although all three bills had strong bipartisan support, they did not get a floor vote. The Senate and House will likely reintroduce these three bills this session, but it takes more than strong bipartisan interest to pass legislation.

Consequently, it is left to states to protect children from the harm we know is associated with its unnecessary collection, storage and sharing. State legislatures should also, in tandem but not in place of privacy legislation, push for platform design and safety legislation, like Senators Kramer and West's SB 844, the Maryland Age-Appropriate Design Code Act. These are two distinct

types of legislation that are complementary, not synonymous with one another. Strong privacy legislation like Senator Augustine's SB 698 is needed to limit the amount of data companies can collect and use from consumers in the first place, and then platform design legislation like SB 844 is needed to address the harmful design practices companies engage in to keep young users engaged, such as utilizing algorithmic recommendation systems, endless scroll, and push alerts.

B. Without Privacy Legislation, Children Will Keep Being Harmed Online

1. The Structural Disparities Between Children and Adults' Brains Make Children More Vulnerable to Online Harms

Although people of all ages may face a range of harms online, children are particularly vulnerable. Individuals' brains gradually develop as they go through adolescence. It takes time for kids to learn key skills like critical thinking, and taking a step back before acting. As a result, children are impressionable and companies more easily manipulate them with tactics like targeted advertising, addictive platform design, and social pressure. For example, most kids cannot distinguish an ad from content, or recognize the persuasive intent of ads, until they are at least 8 years old.¹ Even tweens and teens 12 to 15 years old still have trouble identifying ads and their persuasive intent.² These vulnerabilities make kids and teens largely defenseless against advanced and personalized techniques like targeted advertising.³

Children's developmental vulnerabilities stem from the structural differences between the brains of adults and adolescents that cause kids and teens to respond to stimuli differently from adults.⁴ The limbic system and the prefrontal cortex of our brains grow synchronously, but at different speeds.⁵ The limbic system is associated with survival and contains the part of our brain that controls certain emotional responses such as our "fight or flight" response.⁶ Meanwhile, the prefrontal cortex is associated with higher-level functions such as planning, problem solving, reasoning, and impulse control, and will not mature until closer to adulthood.⁷ Before the prefrontal cortex is fully matured and able to counterbalance the limbic system, kids and teens

¹ American Psychological Association, Report of the APA Task Force on Advertising and Children 5 (Feb. 2004).

² Ofcom. (Nov. 2016). Children and parents: Media use and attitudes report, 86 (stating only 38 percent of 12 to 15-year-olds correctly identified sponsored links on Google as advertising despite their being distinguished by an orange box with the word "ad" on it. See also Samantha Graff, Dale Kunkel, and Seth E. Mermin, Government Can Regulate Food Advertising to Children Because Cognitive Research Shows That It Is Inherently Misleading, 31 Health Affairs 2, 392–98 (2012); Owen B.J. Carter et al., Children's Understanding of the Selling Versus Persuasive Intent of Junk Food Advertising: Implications for Regulation, 72 Social Sci. & Med. 6, 962–68 (2011).

³ Common Sense Media, AdTech and Kids: Behavioral Ads Need a Time-Out (May 13, 2021).

⁴ See Brief for Common Sense Media and Frances Haugen as Amici Curiae Supporting Respondents 6–9, *Gonzales v. Google*, ___ U.S. ___ (2022) (No. 21-1333) (discussing the structural disparities between the adult and adolescent brain and how they lead adults and adolescents to respond to stimuli differently).

⁵ B.J. Casey et al., *The Adolescent Brain*, 28 DEVELOPMENTAL REV. 62, 63 (2008).

⁶ See Velayudhan Rajmohan and Eladath Mohandas, *The Limbic System*, 49 INDIAN J. OF PSYCHIATRY 132–39 (2007) (providing an overview of the components and functions of the limbic system).

⁷ Edward E. Smith and John Jonides, *Storage and Executive Processes in the Frontal Lobes*, 283 SCIENCE 1657, 1659–60 (1999).

are less equipped than adults to make rational decisions, consider long term consequences, and control impulses.⁸

These structural disparities help explain why kids more often fail to stop and think before giving into impulses or temptation. Kids are not simply being difficult: their brains are biologically less capable than adults of mulling over the long-term consequences of their decisions.

2. *Children Face a Wide Range of Online Harms From Targeted Advertising and Algorithmic Recommendations Powered by Online Data*

Data is what makes online platforms so powerful. By the time a child turns 13 years old, adtech firms have compiled more than 72 million data points on that child.⁹ The more data companies have, the more information they have to utilize for practices like (1) targeted advertising and (2) algorithmically recommending content on their online platforms. Both these practices impose great harm on children, and demonstrate the imminent need for privacy legislation that would cut off companies' access to this incessant amount of data.

With targeted advertising, firms track children's activities online, collecting tens of millions of data points to make inferences about them. They use these inferences to create a behavioral profile for each child. Then, based on these profiles, marketers create any number of ads, with each customized to appeal to a group of kids with similar profiles. Most children are not aware that ads may be tailored to them, and researchers have concluded that they are even less equipped to identify targeted ads compared to traditional ads.¹⁰ This inability to identify ads and their intent makes kids much more susceptible to these ads' influence.

Targeted advertising can push kids towards unhealthy products or behaviors such as vaping. For example, one in four teens in a 2019 survey responded that they first learned about vaping predominantly through targeted ads and sponsored content while on social media.¹¹ In a 2016 report, middle school students were shown to be three times more likely and high schoolers two times more likely to use e-cigarettes than their peers when they routinely saw ads for the product

⁸ See Angela Griffin, *Adolescent Neurological Development and Implications for Health and Well-Being*, 5 HEALTHCARE 62, 63 (2017) (describing how the prefrontal cortex is late-evolving and enables individuals to learn how to manage long term planning, monitor what is going on, and adjusting smoothly to surroundings while keeping emotions and behaviors context-appropriate).

⁹ Tim Cross, *Ad Tech collects 72 million data points on the average American child by age 13*, VideoWeek (Dec. 14, 2017), <https://videoweek.com/2017/12/14/ad-tech-collects-72-million-data-points-on-the-average-american-child-by-age-13/>. This number is from 2017, so it is likely a substantial underestimate today.

¹⁰ Kaiwen Sun, Carlo Sugatan, Tanisha Afnan, Hayley Simon, Susan A. Gelman, Jenny Radesky, and Florian Schaub. 2021. "They See You're a Girl if You Pick a Pink Robot with a Skirt": A Qualitative Study of How Children Conceptualize Data Processing and Digital Privacy Risks. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 687, 1–34. DOI:<https://doi.org/10.1145/3411764.3445333>.

¹¹ Common Sense Media, *Vaping and Teens: Key Findings and Toplines*, 2019. More than half of teens on TikTok saw vaping-related posts.

online.¹² This push towards unhealthy products and behaviors can be covert as well. In 2019, Facebook was revealed to have categorized 740,000 kids under 18 years old as being interested in gambling, and 940,000 kids as being interested in alcoholic beverages.¹³ While advertisers cannot target minors with ads for products illegal for them, they can still use this knowledge in a way that harms children, such as by advertising games that contain gambling elements.¹⁴

Further, when kids know they are being monitored by surveillance technology, they are less likely to engage in critical thinking, political activity, or questioning of authority.¹⁵ Knowing ads are being targeted to them can chill kids' expression, because they are afraid these ads could expose parts of their lives they want to keep private or share on their own terms.¹⁶ For example, a kid may be afraid that ads for LGBTQ+ resources will show up on a shared device, outing a child to their family instead of giving them the autonomy to come out on their own accord.¹⁷

Social media platforms like Instagram and TikTok also use algorithmic recommendation systems to curate an endless feed of content for users based on data and analytics from online activity like who the user follows and the content they have consumed and engaged with, such as by liking or commenting. However, these algorithms can take users down dark rabbit holes – and these companies not only know about it, but often continue to push that content to users anyway. Online platforms recommend content promoting self-harm and suicide, eating disorders, and dangerous physical challenges that pose grave physical and mental health harm to kids and teens.

Young users can find an alarming amount of content promoting self-harm and suicidal ideation online. In 2017, 14-year-old Molly Russell killed herself after falling into a vortex of despair on social media the last year of her life.¹⁸ An inquest into her life concluded that she died from "an act of self-harm while suffering from depression and the negative effects of online content."¹⁹ Of 16,300 pieces of content Molly saved, liked, or shared on Instagram in the six months before she died, 2,100 were related to suicide, self-harm, and depression.²⁰ The more of this content she consumed, the more the algorithm bombarded her with similar content. The content was so

¹² Lisa Rapaport, Reuters Health Report, Teens Most Drawn to E Cigarettes by Online Ads, Reuters (Apr. 2016), <http://www.reuters.com/article/us-health-ecigarettes-internet-advertisi-idUSKCN0XM08T>.

¹³ Alex Hern and Frederik Hugo Ledegaard, Children 'interested in' gambling and alcohol, according to Facebook, The Guardian (Oct. 9, 2019), <https://www.theguardian.com/technology/2019/oct/09/children-interested-in-gambling-and-alcohol-facebook>.

¹⁴ *Ibid.*

¹⁵ D.H. Brown & N. Pecora, Online Data Privacy as a Children's Media Right: Toward Global Policy Principles, *Journal of Children and Media*, 8(2), 201–207 (2014).

¹⁶ *Supra* note 3, at 5 (adtech explainer).

¹⁷ *Id.*

¹⁸ John Naughton, *Molly Russell was Trapped by the Cruel Algorithms of Pinterest and Instagram*, The Guardian (Oct. 1, 2022), <https://www.theguardian.com/commentisfree/2022/oct/01/molly-russell-was-trapped-by-the-cruel-algorithms-of-pinterest-and-instagram>.

¹⁹ *Id.*

²⁰ *Id.*

disturbing that at a hearing in a London coroner court, a consultant child psychiatrist said he could not sleep well for weeks after viewing the content Molly had seen right before she died.²¹ The coroner even considered editing footage for the court because of how distressing the content is, but decided against it because Molly herself had no such choice.²²

Eating disorder content is also rampant on social media. A report by the children's advocacy watchdog group Fairplay showed that Meta, formerly Facebook, knowingly profited from pushing pro-eating disorder content to children on Instagram since at least 2019.²³ This pro-eating disorder bubble on Instagram includes 90,000 unique accounts that reach 20 million unique followers, with at least one-third of the followers in this bubble being underage.²⁴ This targeting happens quickly, too. Within a day of U.S. Senator Richard Blumenthal (D-CT)'s office creating a fake Instagram account for a 13-year-old girl and following accounts with content related to disordered eating and dieting, the platform began serving content promoting eating disorders and self-harm.²⁵

*Additionally, many dangerous physical challenges like the "blackout challenge," where people choke themselves until they pass out on camera, have become viral online.*²⁶ The blackout challenge, which went viral on TikTok, has now killed seven kids.²⁷ Although platforms do not allow content that encourages dangerous or illegal activities, new dangerous challenges pop up and become amplified.

With strong privacy legislation in place, online platforms would not be able to serve up targeted ads or algorithmic recommendations with as extreme precision, helping to prevent kids from falling into dark rabbit holes that harm their physical and mental health.

II. SB 698 Provides Strong and Needed Protections for All Consumers and Children, And It Could Be Even Stronger with a Few Reasonable Modifications

Maryland residents deserve true privacy protections. Senator Augustine's SB 698 moves beyond the "notice and consent" model that existing privacy legislation has long adhered to to begin providing more meaningful online protections.

²¹ *Id.*

²² Molly Russell Inquest: Instagram Clips Seen by Teen "Most Distressing," BBC News (Sept. 23, 2022), <https://www.bbc.com/news/uk-england-london-62998484>.amp.

²³ Fairplay, Designing for Disorder: Instagram's Pro-eating Disorder Bubble (Apr. 2022), https://fairplayforkids.org/wp-content/uploads/2022/04/designing_for_disorder.pdf.

²⁴ *Id.*

²⁵ See also Adam Westbrook, Lucy King, and Jonah M. Kessel, *What's One of the Most Dangerous Toys for Kids? The Internet*, New York Times (Nov. 24, 2021), <https://www.nytimes.com/2021/11/24/opinion/kids-internet-safety-social-apps.html>.

²⁶ Fairplay, Dared by the Algorithm: Dangerous Challenges Are Just a Click Away (Sept. 29, 2022), <https://fairplayforkids.org/wp-content/uploads/2022/09/Dangerous-Challenges.pdf>.

²⁷ Mitchell Clark, *The TikTok 'Blackout Challenge' Has Now Allegedly Killed Seven Kids*, The Verge (Jul. 7, 2022), <https://www.theverge.com/2022/7/7/23199058/tiktok-lawsuits-blackout-challenge-children-death>.

A. Through a Combination of Data Minimization and Consumer Rights, SB 698 Would Protect All Consumers' Data

The most effective way to limit privacy harms is to limit the amount and type of data that companies collect from consumers in the first place. Under SB 698, a controller shall limit the collection of personal data to what is (i) adequate, relevant, and reasonably necessary to collect for the purposes for which the data is processed; and (ii) disclosed to the consumer. This creates a data minimization regime, instead of the notice and consent-based regime where companies overwhelm consumers with long, convoluted terms of service and privacy policies, which leads to more data collection.

This bill also recognizes the extreme sensitivity of biometric data, such as our fingerprints, voiceprints, or eye retinas or irises, by imposing restrictions on this data. For example, companies are prohibited from selling, leasing, or trading a consumer's biometric data, and prohibited from collecting, using, disclosing, or redisclosing it except in specific circumstances.

The consumer rights SB 698 provides, such as the right to opt out of profiling, are also more meaningful because of the global opt out language. Every online service is different, and some websites, both intentionally and unintentionally, make it burdensome to navigate the opt-out process, and every consumer uses a countless number of websites and apps. Allowing consumers to utilize global opt out signals such as browser extensions or global device settings greatly simplifies the opt-out process so that consumers can easily exercise their data rights.

B. SB 698 Extends Needed Privacy Protections to Teens

SB 698 would provide protections teens do not currently have under federal COPPA by requiring companies to obtain opt-in consent from teens over the age of 13 and under the age of 16 years old before serving them targeted advertising or selling their data. In combination with the bill's data minimization principle, SB 698 would help decrease the amount of data companies collect on kids and teens.

Requiring a teen's opt-in consent creates an affirmative action that teens have to take that would help them to better understand the fact that companies are collecting and using their personal information. Common Sense Media recognizes the paradox in requiring companies to obtain consent from teens whose sense of judgment is not yet fully formed. However, adolescence is a time when teens are expected and should be allowed to become increasingly independent. For teens' consent to be informed and effective though, companies must provide terms of service and privacy policies in a format they can understand.²⁸ Section 14-4508(A)(1) addresses this by

²⁸ In a 2018 UK Children Commissioner's report, a privacy lawyer rewrote Instagram's terms of service in child-friendly language by taking its original 17-page, roughly 5,000 word form and boiling it down to a single 800 word page. One 13-year-old girl who read the revised policy stated that if such notices were easier to read, "then people would actually read it and think twice about the app." The report also found that only people with postgraduate levels of education – which is only about 13.1 percent of U.S. adults – could probably understand the

requiring a company to provide a consumer with a "reasonably accessible, clear, and meaningful privacy notice..." and lays out the information a notice should include. This section should better ensure privacy notices are easy for consumers to understand by adding language further specifying what makes a notice "accessible, clear, and meaningful." For example, the section could state notices should be no longer than a certain number of pages (and if they must be longer, offer a shorter-form version), and written at no higher than a middle school reading level, so teens can provide informed opt-in consent.

C. Specific Amendments Would Make SB 698 Even Stronger

Crafting strong privacy legislation that effectively protects all consumers is a challenging endeavor. SB 698 is already a strong bill, but there is opportunity to strengthen it further, and we look forward to working with Senator Augustine and the committee to do so. In particular, we have two recommendations for the teens' protection section:

1. Amend the knowledge standard

The effectiveness of any children's privacy protections rests largely on the knowledge standard that determines when a company must comply with the law. To ensure that the teen opt-in protections are as effective as possible, the knowledge standard should be amended.

One major weakness of federal COPPA is that the current knowledge standard creates a loophole for companies to turn a blind eye to young users on their platform and avoid compliance. Companies are only required to comply with COPPA if their online service is directed to children, or when they have "actual knowledge" that a user is a child. This enables bad actors to bury their heads in the sand and claim their services are directed to a general audience, often while touting to advertisers that they can target kids. One of the most prominent companies that has exploited this loophole is YouTube, which settled with the Federal Trade Commission in 2019 for collecting data from children in violation of COPPA.²⁹ While the Commission ultimately fined YouTube, the Commission had to waste time and money to gather evidence confirming the obvious: YouTube knew kids were on its platform, and proceeded to collect information from them in violation of COPPA anyway. The knowledge standard must be updated to reflect today's reality: companies already collect large amounts of data, and some of this data can be used to infer the age of users.

original 17-page version. Children's Commissioner, Growing Up Digital: A Report of the Growing Up Digital Taskforce (Jan. 2017), https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf.

²⁹ Press Release, Federal Trade Commission, Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children's Privacy Law (Sept. 4, 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law>.

SB 698 aims to strengthen the knowledge standard by eliminating the reference to "actual knowledge," and more simply stating that a controller shall not "process the personal data of a consumer that the processor *knows* is at least 13 years old and under the age of 16 years old without the consumer's consent." However, courts have interpreted "knows" by its plain meaning, which here would likely be actual knowledge.

We strongly recommend amending the provision to state, a controller shall not "**process the personal data of a consumer that the processor *knew or should have known* is at least 13 years old and under the age of 16 years old without the consumer's consent.**" This amendment would ensure that companies have to look at the data they already have, such as data collected directly from users or from parental complaints, and cannot turn a blind eye when they know children are on their site.

2. *Ban targeted advertising to minors*

In addition to teen opt-in protections, another baseline protection teens should have is a ban on targeted advertising to minors altogether. Because kids and teens' brains are still developing, they are incapable of defending themselves against targeted advertising. As a result, targeted advertising imposes a wide range of harm on kids and teens, as discussed in section I.B.

There is widespread bipartisan support behind the proposal. At the federal level, both the bipartisan American Data Privacy and Protection Act and COPPA 2.0 bills prohibit targeted advertising to minors under 17 years old. In addition, for two years in a row, President Biden has called for the ban of targeted advertising to minors in his State of the Union address.³⁰ Although requiring teens' opt-in consent for targeted advertising and sale of data is a step in the right direction, banning targeted advertising would be an even more significant step towards reducing harms to youth online.

III. Conclusion

Kids and teens are increasingly losing control of their privacy online and are facing harm to their mental health and overall well-being at the hands of companies' data and advertising practices. With each year we fail to pass privacy and platform accountability legislation, more youth are harmed. All Maryland residents, and particularly Maryland children, deserve to finally have their privacy protected online. Thank you Chair Griffith and Vice Chair Klausmeier for the opportunity to comment on this matter, and we look forward to working with you, Senator Augustine, and members of the Committee to get SB 698 across the finish line.

³⁰ Alfred Ng, *Biden Calls for Ban of Online Ads Targeting Children*, Politico (Feb. 7, 2023), <https://www.politico.com/news/2023/02/07/biden-calls-for-ban-of-online-ads-targeting-children-00081731>.

(3.7) SB 698 - Consumer Protection - Online and Bi

Uploaded by: Tonaeya Moore

Position: FAV



SB 698 - Consumer Protection - Online and Biometric Data Privacy
Senate Finance Committee
March 8th, 2023
SUPPORT

Chairman Griffith, Vice-Chair, and members of the committee, thank you for the opportunity to submit testimony in support of Senate Bill 698. This bill will increase consumer protections around biometric data and create the Task Force to Study Online Data Privacy.

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 biometric 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 2022, Maryland had over 1000 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.

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. This can result in consumers becoming victims of identity fraud.

SB 698 will also establish the Task Force to Study Online Data Privacy. This task force would study how data is shared between health and social care providers, ways to protect children, and how to reduce bias in using biometric, and other topics concerning online data privacy.

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.

For these reasons, we encourage a favorable report on SB 698.

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

SB698_USM_FWA.pdf

Uploaded by: Andy Clark

Position: FWA



SENATE FINANCE COMMITTEE
Senate Bill 698
Consumer Protection – Online and Biometric Data Privacy
March 8, 2023
Favorable with Amendment

Chair Griffith, Vice Chair Klausmeier and committee members, thank you for the opportunity to share our thoughts on Senate Bill 698. The bill makes broad changes to the structure of privacy across the State of Maryland. The University System of Maryland (USM) recognizes the sensitivity of the information we are entrusted to hold and the importance of keeping that information private. With that in mind, the USM worked during the 2020 legislative session to pass a Maryland higher education privacy law that is appropriate for higher education institutions (2020 HB1122/SB588). The bills that passed in the 2020 session are set to go into effect in October 2024, and all USM institutions are currently working to implement the 2020 requirements.

USM institutions, and all public higher education institutions in general, operate very differently from the agencies of the executive branch or private enterprises. Public higher education institutions function much more like small cities than business entities. Public higher education institutions operate broad and wide-ranging education and research enterprises, covering a multitude of topic areas and types of information. Public higher education institutions also conduct activities related to many other verticals including (but not limited to) healthcare, housing, food service, guest services, and event management. Lastly, the USM institutions all have a unique and varied educational research function that carries its own set of unique compliance and cybersecurity requirements. The varied, city-like nature of the operations of public higher education means that public higher education institutions hold many categories of information.

Senate Bill 698 exempts various categories of information that could apply to an educational institution such as education records, health records, and human subjects research information; but public higher education institutions have many types of information that are not expressly carved out of Senate Bill 698. As written, Senate Bill 698 would cause public higher education institutions to have two, in some cases conflicting, privacy laws to have to comply with and manage.

Given that the USM and public higher education in general already have their own information privacy law, we respectfully request that the definition of public higher education institutions from the 2020 higher education privacy law be used to exempt public higher education institutions from the requirements of Senate Bill 698 in section 14-4503(A) (SB698 - page 11/line 5).

Thank you for allowing the USM to share these concerns regarding Senate Bill 698.



About the University System of Maryland

The University System of Maryland (USM)—one system made up of twelve institutions, three regional centers, and a central office—awards eight out of every ten bachelor’s degrees in the State of Maryland. The USM is governed by a Board of Regents, comprised of twenty-one members from diverse professional and personal backgrounds. The chancellor, Dr. Jay Perman, oversees and manages the operations of USM. However, each constituent institution is run by its own president who has authority over that university. Each of USM’s 12 institutions has a distinct and unique approach to the mission of educating students and promoting the economic, intellectual, and cultural growth of its surrounding community. These institutions are located throughout the state, from western Maryland to the Eastern Shore, with the flagship campus in the Washington suburbs. The USM includes Historically Black Colleges and Universities, comprehensive institutions, research universities, and the country’s largest public online institution.

USM Office of Government Relations - Patrick Hogan: phogan@usmd.edu

SB698 CDIA FWA.pdf

Uploaded by: Chris DiPietro

Position: FWA

March 8, 2023

The Honorable Melony Griffith
Chair, Senate Finance Committee
Annapolis, MD 21401

Re: Amend SB698: Consumer Protection - Online and Biometric Data Privacy

Dear Chair Griffith,

This bill, SB698, is intended to protect the rights of consumers in the State of Maryland. We strongly support that goal, which is why CDIA is requesting that your committee amend some of the technical provisions to align with long-standing federal and state law. I write on behalf of the Consumer Data Industry Association (“CDIA”)¹ to respectfully request that amendment.

For over 110 years, CDIA and its members have stood to help protect the American economy and the American public. Since 1970, the federal Fair Credit Reporting Act (“FCRA”) has stood as a strong legal floor for background checks in the U.S. Maryland has its own version of the FCRA in the Commercial Law article since 1976. Among other things, these laws demand accuracy in background check processes and afford legal rights to consumers.

It is critically important for a state privacy law to recognize consumer protections that currently exist under federal privacy law. Any state privacy law should include clear and concise language exempting consumer data already regulated under the federal Fair Credit Reporting Act (FCRA)

The FCRA exemption on p.12 lines 28-33 is not sufficient. It only covers the exchange of information “to or from” a CRA and would not cover information held by a CRA or user not covered by GLBA or other data flows part of the consumer reporting ecosystem.

We suggest language substantially similar to:

This [act] [title] [chapter] does not apply to an activity involving personal information governed by the Fair Credit Reporting Act, section 1681 et seq., Title 15 of the United States Code, or otherwise used to generate a consumer report, by a consumer reporting agency, as defined by [15 U.S.C. Sec. 1681a\(f\)](#), by a furnisher of information, or by a person procuring or using a consumer report.

The Gramm-Leach-Bliley Act (GLBA) is, in significant part, a national financial privacy law. The law imposes requirements on businesses to limit the disclosure of information and allows consumers to opt-out of certain information sharing. We are happy to see some

¹ CDIA is the voice of the consumer reporting industry, representing consumer reporting agencies, including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity all over the world, helping ensure fair and safe transactions for consumers, facilitating competition, and expanding consumers’ access to financial and other products suited to their unique needs.

protections included on p. 11 lines 15-16. However, This Entity-level GLBA exemption includes “in compliance with” language. There is no data-level exemption. The entity level only covers financial institutions and their affiliates, this is not sufficient because it would not reach third-party recipients holding GLBA-regulated and limited data.

We suggest an amendment substantially similar to:

This [act] [title] [chapter] does not apply to a financial institution as defined by [15 U.S.C. Sec. 6809\(3\)](#), or to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act ([Public Law 106-102](#)).

Finally, with regard to the definition of “publicly available information” found on page 8 lines 4-9. CDIA requests that “and” be changed to “or” to be more consistent with the data privacy laws passed in other states (see below) or use our model public records exemption language.

(W) “PUBLICLY AVAILABLE INFORMATION” MEANS INFORMATION THAT:
(1) IS LAWFULLY MADE AVAILABLE THROUGH:
(I) FEDERAL, STATE, OR LOCAL GOVERNMENT RECORDS; OR
(II) WIDELY DISTRIBUTED MEDIA; ~~AND~~ **OR**
(2) A CONTROLLER HAS A REASONABLE BASIS TO BELIEVE A CONSUMER HAS LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC.

I am happy to answer any questions you may have. I thank you in advance for your consideration.

Sincerely,

Mike Carone
Manager of Government Relations

MD-SB0698-testimony-Insights_Association-AMD-3-8-2

Uploaded by: Howard Fienberg

Position: FWA



March 8, 2023

Senate Finance Committee**S.B. 698 (Online and Biometric Data Privacy Act)****Written testimony for hearing, submitted by the Insights Association**

The Insights Association (IA), the leading nonprofit trade association for the market research and data analytics industry, writes to comment on comprehensive privacy legislation before your committee today, the Online and Biometric Data Privacy Act (S.B. 0698), on behalf of our more than 150 members in Maryland, and to propose amendments.

Our more than 7,100 overall members are the world's leading producers of intelligence, analytics and insights defining the needs, attitudes and behaviors of consumers, organizations and their employees, students and citizens. With that essential understanding, leaders can make intelligent decisions and deploy strategies and tactics to build trust, inspire innovation, realize the full potential of individuals and teams, and successfully create and promote products, services and ideas.

The Insights Association supports comprehensive federal privacy legislation that moves beyond the old-school notice-and-choice model, instead of a patchwork of conflicting state privacy laws built on those old models. A study¹ conducted by our member companies Research Narrative and Innovate MR, on behalf of Privacy for America, revealed that nearly all Americans surveyed (92 percent) believe it is important for Congress to pass new legislation to protect consumers' personal data, and a majority (62 percent) prefer federal regulation over individual state regulations. Four out of five voters (81 percent) support a national standard that outright prohibits harmful ways of collecting, using, and sharing personal data. Congress made some progress on that front in 2022, and we are pushing hard for a federal law this year.

However, should you and your fellow legislators decide to move forward with S.B. 0698, IA urges you to consider several important improvements:

- 1. Ensuring that targeted advertising does not include independent audience measurement:** Audience measurement, particularly independent audience measurement, builds the currency upon which advertising and other content, online and off, is valued, and collects covered data about individuals for the purpose of understanding groups. Advertisers, for

¹ New Study Shows Overwhelming Bipartisan Support for U.S. Federal Privacy Legislation. DECEMBER 1, 2021. <https://www.insightsassociation.org/News-Updates/Articles/ArticleID/289/New-Study-Shows-Overwhelming-Bipartisan-Support-for-U-S-Federal-Privacy-Legislation>

example, pay based on the number of "impressions" for online ads, and independent measurement verifies that the number of impressions is accurate. Local Maryland businesses would bear the burden of these elevated costs for every impression inaccurately added to the count. Independent measurement also allows content creators to know their actual viewership in relation to the marketplace thus allowing for accurate programming decisions. The exception would still require that the data would be limited "solely" to measurement, preventing its use for other purposes. Therefore, IA encourages you to clarify that this exception covers independent measurement, and content as well as advertisement, just like the language in the federal privacy bill ADPPA that passed committee in the House in 2022, by tweaking § 14–4501 (z)(2)(iv) as follows (with additions in bold): *“processing personal data solely to measure or report advertising **or content** performance, reach, or frequency, **including independent measurement.**”* This is a slightly expanded provision from the targeted advertising definitions in recent privacy laws in Colorado, Connecticut, Utah and Virginia.²

2. **Protect market research and/or audience measurement more broadly:** To protect the essential production of insights while still protecting consumers, IA urges you to add a new exemption to the list in § 14–4503 (B) for market research -- *“information for purposes of investigating the market for or marketing of products, services, or ideas, where the information is not: (i) integrated into any product or service; (ii) otherwise used to contact any particular individual or device; or (iii) used to advertise or market to any particular individual or device.”*³ – and/or a new exemption to the list for audience measurement – *“information for purposes of independently measuring or reporting advertising or content performance, reach, or frequency pursuant to a contract with a controller that collected personal information in accordance with this act.”*⁴
3. **Tighten the definition of “sensitive data”:** The current definition of “sensitive data” in § 14–4501 (Y) includes relatively common demographic data, especially data revealing “racial or ethnic origin”– data so common that it is asked by the decennial census. If you should choose not to accept our recommendations above to protect market research and audience measurement, the Insights Association urges you even more so to avoid imperiling even the most basic of research studies by amending § 14–4501 (Y)(1) with language at the end: *“, except to the extent such data is used solely for purposes of determining participation of an individual in market research.”* A new definition of “market research” could then be added to § 14–4501 to mean: *“the collection, use, maintenance, or transfer of personal data as*

² See 2021 Colorado S.B. 190 (“processing personal data solely for measuring or reporting advertising performance, reach, or frequency”), 2022 Connecticut S.B. 6 (“processing personal data solely to measure or report advertising frequency, performance or reach”), 2021 Virginia S.B. 1392 (“Processing personal data processed solely for measuring or reporting advertising performance, reach, or frequency”), and 2022 Utah S.B. 227 (“processing personal data solely to measure or report advertising: (A) performance; (B) reach; or (C) frequency”).

³ This definition of market research is used by the model federal privacy legislation put forward by Privacy for America in Part I, Section 1, R: <https://www.privacyforamerica.com/overview/principles-for-privacy-legislation-dec-2019/> and also by the federal privacy bill passed out of committee in 2022, ADPPA.

⁴ This exemption was used in Florida H.B. 9 in 2022.

reasonably necessary to investigate the market for or marketing of products, services, or ideas, where the information is not: (i) integrated into any product or service; (ii) otherwise used to contact any particular individual or device; or (iii) used to advertise or market to any particular individual or device.”

4. **Ensure that discrimination provisions do not impede participant incentives for research subjects:** IA is concerned that choosing research subjects for participation in market research, when it involves a participant incentive, could be misconstrued as discrimination under § 14–4507(E). Participant incentives are an important tool in the insights industry toolkit to encourage research subjects’ involvement in market research involving their covered data, as response rates have declined. Participant incentives are particularly key to research in which the research subject has affirmatively consented to participate. Research subjects are sought in certain segments and numbers for market research studies, with the samples varying depending on the needs and scope of the study. For example, a study may oversample or focus entirely on black homosexual women in their 30s and 40s – if a participant incentive is involved, would other potential research subjects disqualified from participation potentially have been discriminated against? To preserve the ability to conduct market research and to adequately include any necessary populations, IA urges you to add a new clause (3) in § 14–4507(F) to clarify the continued legality of participant incentives for research subjects in face of the bill’s discrimination provisions: *“Prevent a controller from offering a financial incentive or other consideration to an individual for participation in market research as a research subject, defined as the collection, use, maintenance, or transfer of personal data as reasonably necessary to investigate the market for or marketing of products, services, or ideas, where the information is not: (i) integrated into any product or service; (ii) otherwise used to contact any particular individual or device; or (iii) used to advertise or market to any particular individual or device.”*
5. **Limit the use of an authorized agent to only where necessary:** § 14–4506 of the Act would not tangibly limit the exercise of an opt out by an authorized agent of the consumer; anyone could submit a request through an authorized agent. This option will be unnecessary in most cases, increase paperwork associated with the verification process, and open the door for fraudulent requests. Except in cases where the consumer is a minor, or someone who genuinely needs an authorized agent to submit a request (such as an elderly or incapacitated individual), requiring requests to be submitted by consumers themselves would better serve the purpose of S.B. 0698.

The Insights Association and our members support strong consumer privacy protections within a regulatory framework that still allows for the pursuit of insights, as we’ve discussed above. We look forward to talking with you and your fellow legislators and staff further, and providing more information regarding these issues and Maryland’s Online and Biometric Data Privacy Act (S.B. 0698).

Sincerely,

Howard Fienberg
Senior VP, Advocacy
Insights Association

P R O T E C T ◆ C O N N E C T ◆ I N F O R M ◆ P R O M O T E

SB 698_EconAction_FAV (2023).pdf

Uploaded by: Marceline White

Position: FWA



Testimony to the Senate Finance Committee
SB 698: Consumer Protection-Biometric Data Privacy
Position: Favorable

March 8, 2023

The Honorable Melony Griffith, Chair
Senate Finance Committee
3 East, Miller Senate Office Building
Annapolis, Maryland 21401
cc: Members, Senate Finance Committee

Honorable Chair Griffith and Members of the 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.

We are writing in support of SB 698 and urge a favorable report.

Biometric identifiers (palm, fingerprint, iris, voice, face) are increasingly being used by law enforcement, airports, property management firms, and employers. Currently there are few restrictions on how companies collect, analyze, store, share, or sell our personal biometric identifiers. Unlike a credit card, we can't get new biomarkers.

While some consumers may choose to use biometrics to, for example, open their smartphone with their fingerprint, it is their choice to do so for security and/or ease. In other cases, the individual may not be aware that their biometric data is being collected and stored.

SB 698 establishes reasonable limits on the collection, use, and storage of biometric data. It prohibits businesses from collecting biometric data without consumer consent. It also prohibits businesses from selling or sharing consumer biometric data.

In addition, SB 698 requires that biometric information be destroyed when it is no longer in use. Several other states have already enacted laws to protect consumers' biometric information, including California, Illinois, Texas, and Washington. These protections are particularly important given the



uniqueness of biometric identifiers. Unlike account numbers, once biometric data has been breached, it is compromised forever—you cannot change your fingerprint or iris if it gets stolen.

Data thieves have already begun to target biometric data; in 2019, data thieves breached an international database and gained access to more than a million fingerprints and other sensitive data, including photographs of people and facial recognition data.

Like the laws already in effect in Illinois and California, SB 698 provides for a private right of action. Given the high cost when an individual's biometrics are compromised, businesses must be held accountable if they sell or misuse an individual's biometric data.

For all these reasons, we support SB 698 and urge a favorable report.

Best,

Marceline White
Executive Director

SB 698 Data Privacy SWA 03082023 APCIA .pdf

Uploaded by: Nancy Egan

Position: FWA



Testimony of
American Property Casualty Insurance Association (APCIA)
Senate Finance Committee
SB 698 Consumer Protection - Online and Biometric Data Privacy
March 8, 2023

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 62.7 percent of total property and casualty insurance sold in Maryland. APCIA appreciates the opportunity to provide written comments regarding Senate Bill 698.

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 Senate Bill 698 **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: (pg 11-Lines 15-16)

15 (III) AN ENTITY, OR AN AFFILIATE OF AN ENTITY, **OR DATA** SUBJECT TO
16 AND IN COMPLIANCE WITH THE FEDERAL GRAMM–LEACH–BLILEY ACT;

Once again, thank you for the opportunity to provide comments and request this simple amendment to Senate Bill 698.

Nancy J. Egan,

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

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

MCPA-MSA_SB 698_Consumer Protection-Online-Biometr

Uploaded by: Andrea Mansfield

Position: UNF



Maryland Chiefs of Police Association

Maryland Sheriffs' Association



MEMORANDUM

TO: The Honorable Melanie Griffith, Chair and
Members of the Finance Committee

FROM: Darren Popkin, Executive Director, MCPA-MSA Joint Legislative Committee
Andrea Mansfield, Representative, MCPA-MSA Joint Legislative Committee
Natasha Mehu, Representative, MCPA-MSA Joint Legislative Committee

DATE: March 8, 2023

RE: **SB 698 – Consumer Protection – Online and Biometric Data Privacy**

POSITION: **OPPOSE**

The Maryland Chiefs of Police Association (MCPA) and the Maryland Sheriffs' Association (MSA) **OPPOSE SB 698**. This bill sets standards and mandates policies and procedures private entities must follow when handling biometric data but does so in an overly broad and restrictive manner that conflicts with recently established privacy laws under Title 17 of the Criminal Procedure Article and jeopardizes criminal investigations.

The MCPA and MSA are significantly concerned with the impact this bill could have on the ability of law enforcement to use advancements in DNA and ancestry technology to solve difficult criminal cases. In 2021, legislation was passed into law establishing important guardrails and protocols for law enforcement and ancestry databases that govern how biometric data can be used for the investigative process of Forensic Genetic Genealogy. The provisions in Title 17 of the Criminal Procedure Article were carefully worded to balance the need for privacy protections while allowing individuals to voluntarily share the DNA they have provided to ancestry databases with law enforcement to help solve crimes. SB 698 could override all those thoughtful provisions and prevent the effective use of Forensic Genetic Genealogy.

Some of the most concerning aspects of SB 698 are the definition of biometric data, the mandatory destruction protocols, and the various non-disclosure provisions. Among other things, these provisions require the mandatory destruction of all biometric data in the possession of private entities including DNA profiles that consumers have provided to certain ancestry search companies. The provisions do not reflect or account for the provisions in Title 17 or federal guidelines that were established to specifically deal with the sensitive nature of Forensic Genetic Genealogy.

Forensic Genetic Genealogy has been critical for solving decades-old cold cases. Most notably the technology was used to identify the Golden Gate Killer. It is important to note that DNA from ancestry databases can only be used for law enforcement purposes with the explicit consent of the individual submitting their DNA and that not all databases chose to partner with law enforcement. This process is truly voluntary and ensures that all parties involved are adhering to stringent privacy protections and biometric data management established under both Title 17 and US Department of Justice guidelines.

Local law enforcement is actively working on cases using Forensic Genetic Genealogy. For instance, the Prince George's County Police Department's Cold Case Homicide Unit in partnership with the Prince George's County State's Attorney's Office is currently working on 15 cold cases involving murder or sex offenses. The Prince George's State's Attorney's Office was awarded a \$470,000 grant to support the investigation of unsolved homicides and sex offense cases using recently developed forensic genealogy (FGG) processes. Local agencies across the state are even partnering with the FBI's Investigative Genealogy Unit on some of their cold cases. The passage of SB 698 as written would hinder the ability of the department to work locally or with their federal partners to use this innovative and burgeoning technology to solve these crimes and bring justice to the victims and their families.

DNA and Forensic Genetic Genealogy are extraordinary investigative tools for identifying violent offenders that would be crippled by the passage of this bill. It is critical to ensure that there are exemptions that allow for the continued use of Forensic Genetic Genealogy and the regulatory provisions already established under Title 17. For these reasons, MCPA and MSA **OPPOSE SB 698** and urge an **UNFAVORABLE** report.

SB 698_MDCC_Consumer Protection-Online and Biometr

Uploaded by: Andrew Griffin

Position: UNF



MARYLAND
Chamber of Commerce

LEGISLATIVE POSITION:

Unfavorable

Senate Bill 698

Consumer Protection – Online and Biometric Data Privacy

Senate Finance Committee

Wednesday, March 8, 2022

Dear Chairwoman Griffith 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 6,400 members and federated partners working to develop and promote strong public policy that ensures sustained economic recovery and growth for Maryland businesses, employees, and families.

Maryland Chamber of Commerce members place a high priority on consumer privacy and the business community is watching and learning from the experience of the five other states that have passed data privacy laws protecting biometric and other information. The Maryland General Assembly has considered versions of these laws in past sessions but has not reached a decision on a path forward for Maryland. SB 698 is a version of data privacy passed in four of those other states and contains strong consumer protections for a variety of data including biometric data, personal data, confidential data, and sensitive data.

However, SB 698 still maintains problematic provisions of SB 169 that will create significant hardships for Maryland employers and could result in stifling important advances in safety and security. As demonstrated from the business experience in the wake of the 2008 Illinois law, the threat and burden of frivolous class action litigation on local businesses will lead to a cooling effect in Maryland whereby Maryland companies will cease developing and utilizing pro-consumer, pro-privacy uses of biometric data like building security, user authentication, and fraud prevention. Interestingly, like mentioned above, four other states have passed versions of SB 698, but no other state has chosen to repeat the 2008 Illinois law. Further, there is currently strong consideration for repealing some of the provisions of that problematic policy.

It is important to note that while SB 698 and SB 169 calls for a “limited” private right of action, that will not prevent individuals from filing a suit, no matter the merit. Baseless actions will necessitate companies to defend themselves both in court and in public opinion. The need to show actual damages will not erase the legal fees, out-of-settlements, and damage in the public eye businesses will face. Again, the experience in Illinois bears out this truth with only one case ever

MDCHAMBER.ORG

60 West Street, Suite 100, Annapolis 21401 | 410-269-0642

being brought to trial in the nearly 1,000 filed suits. We strongly urge the committee to consider an alternative enforcement mechanism that has not created such burdensome and costly litigation.

Finally, it is important to mention the advantage and potential cost savings in considering the policies of neighboring states and avoiding a patchwork of regulation. In a call for federal action on data privacy, the Information Technology & Innovation Foundation released a January 2022 evaluation on the cost of compliance in a 50-state patchwork system of privacy laws. The cost of compliance for Maryland was estimated at \$4.2 billion with the burden being shared equally for in and out-of-state compliance.¹ This is a strong argument to find similarities in policy adoption across states without federal action.

SB 698 is a large and complex piece of legislation, but the policy is the product of thorough conversations and negotiations in other states. Maryland residents and employers deserve privacy protections that safeguard sensitive data while promoting innovation and job creation. The Maryland Chamber of Commerce remains committed to working alongside the bill sponsors, this committee, and impacted partners to address the issues surrounding the safety and security of personal data. Making good and useful policy is in the best interest of everyone involved.

For these reasons, the Maryland Chamber of Commerce respectfully requests an **unfavorable report** on **SB 698**, as introduced.

¹ <https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/>



SPSC - MD SB 698 (Omnibus & Biometrics) - Unfavora

Uploaded by: Andrew Kingman

Position: UNF

STATE PRIVACY & SECURITY COALITION

March 6, 2023

Chair Melony Griffith
Vice Chair Katherine Klausmeier
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

Re: SB 698 (Comprehensive Privacy & Biometrics) – Unfavorable

Dear Chair Griffith and Vice Chair Klausmeier,

The State Privacy & Security Coalition, a coalition of over 30 companies and six trade associations in the retail, automotive, technology, telecom, and payment card sectors, writes in opposition to SB 698, but with the hope that the bill can be amended to a place where we no longer oppose it. The bill includes provisions based on an outdated Illinois law, the Biometric Information Privacy Act (BIPA), that was passed in 2008 – less than a year after the smartphone was invented. The abuse of the private right of action (PRA) in the law, as well as the evolution of the online ecosystem, has led to bipartisan efforts in Illinois to reform the statute so as to eliminate the problems that have plagued it since its passage. It is also a primary reason why not a single other state has enacted this statute.

However, SB 698 also contains language based on the Connecticut privacy bill that passed in 2022, and is going into effect in July of this year. If SB 698 is amended to match that legislation, SPSC would not oppose the bill.

SPSC's members support strong protections for consumers' personal data. Effective privacy legislation should appropriately balance increased consumer control over their data and how it is used, while retaining the need for operational workability and cybersecurity.

Connecticut and other states such as Colorado have passed comprehensive privacy laws that cover a broad swath of personal data. These bills provide:

- strong, opt-in protections for consumers with regard to biometrics and other sensitive data;
- a greater number of consumer rights (access, deletion, correction, portability), opt-out of sale, targeted advertising, and profiling;
- strong obligations on businesses to document data processing activities that present a heightened risk of harm; and
- strong contractual requirements for entities that handle personal data – including biometrics – on behalf of the entities that collect the data.

Additionally, the Connecticut legislation – like all other comprehensive privacy bills that states have passed – has exclusive enforcement by the Attorney General for privacy violations, and

STATE PRIVACY & SECURITY COALITION

also has a Right to Cure. These are integral and critical parts of businesses being willing and able to institute these complex, expansive consumer privacy protections.

Connecticut's Treatment of Biometric Information

One of the many advantages that the Connecticut framework has over a sectoral approach is that it encompasses ***all data that is linked or reasonably linkable to an individual***. In other words, it covers not just one type of data like biometrics, but anything that is “reasonably linkable” to an individual.

However, since SB 698 attempts to also incorporate SB 169's biometrics language, we believe it is helpful to outline the protections consumers would have for biometric information under the Connecticut framework. These include:

- Classifying biometric data as “sensitive data,” along with precise geolocation data, health data, children’s data, among other sets of data.
- Establishing affirmative opt-in consent requirements for any collection or processing of biometric data.
- Requiring businesses to disclose the purposes for processing such data.
- Requiring businesses to obtain affirmative opt-in consent if the purposes for processing change.
- Requiring businesses to obtain affirmative opt-in consent if a business wants to use the biometric data for another purpose than that which it first told the consumer.
- Requiring businesses to document the processing of biometric data, and documenting both the risks and the benefits to such processing.
 - Documenting how the business intends to mitigate the risks from processing biometric data, if risks are identified.
- Requiring processors (vendors who provide services to the consumer-facing entities) to contractually agree to:
 - A duty of confidentiality with regard to processing the biometric data
 - Deleting or returning all of the biometric data to the controller once the contract is completed
 - Allow the controller to conduct assessments of the processor’s contractual compliance for handling biometric data.
- Providing the consumer with the rights to:
 - Confirm whether the controller is processing biometric data and access such data (unless there are security risks to providing the consumer with the actual biometric data);
 - Require the controller to delete biometric data;
 - Correct inaccurate data;
 - Port such data from one controller to another (again, unless there are security risks to providing the consumer with the actual biometric data)

STATE PRIVACY & SECURITY COALITION

As you can see, the Connecticut framework provides extensive protections and consumer rights with regard to biometric data (and, critically, all other types of data that are not already regulated by federal law such as the Health Insurance Portability and Accountability Act (HIPAA)).

We believe that this framework is a much stronger, more balanced approach that better serves consumers and is much clearer for businesses to comply with.

Notably, in the 15 years since BIPA's enactment in Illinois, ***not a single state has enacted it***. Connecticut, following Virginia, Colorado, and Utah, ***was the fourth state to enact a version of this law since 2021***, with a number of other states expected to pass a version of the law this year.

The Private Right of Action Will Make Consumers Less Safe

A critical component to add to SB 698's existing language is enforcement by the Attorney General, along with a right to cure. Retaining the private right of action will make this bill untenable, and would continue to create opposition from the business community. There are several reasons for this.

First, including a private right of action for statutory damages would create massive class action litigation exposure for any *alleged* violations of the law by commercial entities, significantly deterring uses of biometric data including for anti-fraud, authentication and other security purposes that benefit consumers. As in Illinois, the result would be to enrich trial lawyers without striking a balance that allows the use of biometric data for purposes that benefit Maryland residents. Put simply, a private right of action means businesses will be much less likely to offer services that keep Maryland residents' identities safe.

The litigation numbers bear this out: in the last five years, trial lawyers have filed *nearly 1000 class action lawsuits based on BIPA*. 14 years of experience with Illinois' law have shown that this approach leads businesses to decline to offer their full suite of services to state residents, or avoid offering their services in the state at all, due to the overzealous litigation this legislation catalyzed. For this reason, Illinois is considering amending the law in order to address this significant unintended consequence and bring beneficial services back to Illinois consumers.

This is because plaintiff trial lawyers' legal strategy to extract settlements does not rest on the merits of the case, but instead on the opportunity to inflict asymmetrical discovery costs on businesses both small and large – with a cost to defend these frivolous actions averaging \$500,000. These heavy costs to defend cases through summary judgment gives trial lawyers, who bear no or minimal discovery costs, huge negotiating leverage for nuisance settlements, even if the defendant is compliant with the law. In fact, ***only a single case has ever been brought to trial***.

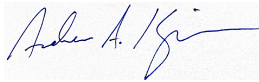
STATE PRIVACY & SECURITY COALITION

Furthermore, studies have revealed that private rights of action fail to compensate consumers ***even when a violation has been shown***, and instead primarily benefit the plaintiff's bar by creating a "sue and settle" environment.¹ This is not to say that Maryland lacks effective enforcement options outside the trial bar – to the contrary, it has a strong consumer protection statute that the Attorney General can use *right now* to punish bad actors. On the other hand, the PRA in Illinois has not only failed to meaningfully protect consumers, but actually made them less safe, as anti-fraud, convenient authentication, and other beneficial services leave the state because of abusive litigation risk.

The Right to Cure is also a critical component of any comprehensive privacy enforcement mechanism. The right to cure helps all parties – the Attorney General's Office, consumers, and businesses. It helps the Attorney General's Office by streamlining compliance; all that is required to put a business on notice that it is in violation of the statute is a letter; in response, a business has a period of time to fix the violation and expressly state it will not commit the violation in the future. This helps the consumer by keeping their privacy protections in place with a short time for resolution, omitting the need for lengthy and costly litigation. Finally, it helps businesses by increasing cooperation with the Attorney General's office while still holding businesses accountable to the consumer.

Again, we would urge this committee to consider alternative, more modern, and more expansive data privacy protections for Maryland consumers that are more balanced, work across state lines, and do not create risks of frivolous litigation.

Respectfully,



Andrew A. Kingman
Counsel, State Privacy & Security Coalition

¹ Mark Brennan et al., *Ill-Suited: Private Rights of Action and Privacy Claims*, U.S. Chamber Institute for Legal Reform (July 2019).

SB 698 Privacy and Biometrics MRA Testimony.pdf

Uploaded by: cailey locklair

Position: UNF



SB 698 Consumer Protection - Online and Biometric Data Privacy

Section 14-4507. (note: text of paragraph (G) below begins on p. 25 and carries over to p. 26)

23 (G) (1) IF A CONSUMER’S DECISION TO OPT OUT OF THE PROCESSING OF
24 THE CONSUMER’S PERSONAL DATA FOR THE PURPOSES OF TARGETED ADVERTISING
25 OR THE SALE OF PERSONAL DATA THROUGH AN OPT-OUT PREFERENCE SIGNAL
26 SENT IN ACCORDANCE §14-4508(B)(4)(II) OF THIS SUBTITLE CONFLICTS WITH
27 THE CONSUMER’S EXISTING CONTROLLER-SPECIFIC PRIVACY SETTING ~~OR~~
28 ~~VOLUNTARY PARTICIPATION IN A CONTROLLER’S BONA FIDE LOYALTY, REWARDS~~
29 ~~PREMIUM FEATURES, DISCOUNTS, OR CLUB CARD PROGRAM,~~ THE CONTROLLER
30 SHALL COMPLY WITH THE CONSUMER’S OPT-OUT PREFERENCE SIGNAL.

31 (2) A CONTROLLER MAY:

1 (I) NOTIFY A CONSUMER OF THE CONFLICT BETWEEN AN
2 OPT-OUT PREFERENCE SIGNAL AND A CONTROLLER’S SPECIFIC PRIVACY SETTING;
3 AND

4 (II) PROVIDE TO THE CONSUMER THE CHOICE TO CONFIRM THE
5 CONTROLLER-SPECIFIC PRIVACY SETTING OR PARTICIPATION IN THE PROGRAM.

RETAILERS’ CONCERNS WITH TEXT OF SECTION 14-4507(G)(1) and (2)

- We recommend striking the highlighted text above of subparagraphs (G)(1) and (2) of HB 807 in order to avoid the significant anti-consumer effect of a new law that – in direct opposition to Maryland consumers’ specific and prior, voluntary opt-in choices – automatically cancels their participation in a customer loyalty program.
- Subparagraph (G) provides a mechanism for conflict resolution with an automatic or global opt-out option available to controllers (under section 14-4508(B)(4)(II) on p. 28, l. 3-8) “to allow consumers to opt-out...of targeted advertising, or any sale of data, through an opt-out preference signal” sent by a web browser or other mechanism. However, (G)(1) and (2) inappropriately includes in its text extra language related

to customer loyalty programs even though the opt-out signals are for other purposes.

- This raises significant concerns for retailers. Recent studies show that nearly 80% of all consumers participate in at least one customer loyalty program and American adults, on average, participate in nine. Consumers choose to voluntarily participate in loyalty programs; participation is not required as plans are offered on an opt-in basis. By participating, consumers typically earn points, discounts and/or higher levels of service that reward them for greater engagement with the business offering the program.
- Consumers would not expect a “privacy-promoting” web browser or other technology designed with signals to opt them out of “targeted ads” or “data sales” to also opt them out of a loyalty program they already voluntarily opted into. The highlighted text above of subparagraph (G)(1) upends consumers’ specific choices and threatens to cancel their customer loyalty accounts and points, well beyond the purpose of the signal.
- Additionally, subparagraph (G)(2) creates consumer confusion by forcing them to re-confirm their prior choices to avoid automatic cancellation of loyalty programs. If they fail to re-confirm that choice because they miss a notice or are confused by it, their account and points could be automatically terminated. It is likely consumers would be surprised the law overturns their prior opt-in choice by effectively creating a confusing and unnecessary “double opt-in” requirement for popular customer loyalty programs.

MD SB698 Testimony-Opposed Unless Amended - RELX.

Uploaded by: Caitlin McDonough

Position: UNF

March 8, 2023

The Honorable Melony Griffith
Chair, Senate Finance Committee
Miller Senate Office Building, 3 East
11 Bladen Street
Annapolis, MD 21401

Re: Senate BILL 698 – THE ONLINE AND BIOMETRIC DATA PRIVACY ACT (Oppose Unless Amended)

Dear Chair Griffith and Members of the Senate Finance Committee:

I am writing on behalf of LexisNexis Risk Solutions (“LexisNexis”), a leading provider of credential verification and identification services for government agencies, Fortune 1000 businesses, and the property and casualty industry, to express concerns with Senate Bill 698, as introduced. While LexisNexis appreciates and supports Maryland’s efforts to provide practical and effective consumer protections for personal information and data, we join with industry in seeking clarifications in the proposed law to ensure the inclusion of the most up to date definitions and provisions and preserve our ability to provide quality services to our customers, particularly in the area of supporting fraud detection and identity theft.

Specifically, LexisNexis respectfully requests that the Committee consider amending the proposed legislation to clarify provisions relating to (1) stronger exemptions for entities currently regulated by federal law, (2) stronger exemptions for fraud prevention and detection, (3) definitions of consumer and publicly available information, (4) penalties and enforcement, and (5) an outdated biometric data framework. We stand willing to work with the Sponsor and the Committee to develop language that achieves the intended privacy protections for consumers, while allowing industry participants to effectively comply and continue to provide valuable services.

LexisNexis takes this opportunity to thank Senator Augustine for her hard work in this space and we remain committed to further collaboration in the development and implementation of best practices for data privacy, based on our expertise and experience. Thank you for your consideration of LexisNexis’ feedback on the proposed legislation.

Please let us know if we can answer any questions or provide any additional information.

Respectfully submitted,

Jeffrey Shaffer
Manager, Government Affairs, Mid-Atlantic
RELX (parent company of LexisNexis Risk Solutions)
1150 18th Street, NW, Suite 600
Washington DC, 20036
Mobile: 202-286-4894
Email: Jeffrey.shaffer@relx.com

CHPA Oppose - SB 698.pdf

Uploaded by: Carlos Gutierrez

Position: UNF



CONSUMER
HEALTHCARE
PRODUCTS
ASSOCIATION

Taking healthcare personally.

March 7, 2023

Senator Melony Griffith, Chair
Senate Finance Committee
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

Re: SB 698 - Online and Biometric Data Privacy - Oppose

Dear Chair Griffith,

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, I'm writing to express opposition to SB 698 as it is currently drafted. While we are not opposed to the bill's goal of providing consumers with more control over their personal data, we do have concerns with how the legislation interacts with existing federal laws related to controlled substances. Considering this potential conflict between laws, we oppose SB 698 unless amended to account for existing federal requirements.

Controlled Substances Act

The Comprehensive Drug Abuse Prevention and Control Act, commonly known as the Controlled Substances Act (CSA), was passed by Congress in 1970 and establishes a federal policy to regulate the manufacturing, distribution, and use of regulated substances. To comply with 21 U.S.C. Section 830 of the Act, regulated "persons" who engage in a transaction involving a listed chemical (like sellers of allergy drug products containing ephedrine or pseudoephedrine) must collect and keep identifiable private records of these transactions. SB 698, however, does not exempt these transactions from its privacy requirements.

Amendment Recommendation

To avoid potential conflict with already existing federal law, CHPA recommends the following amendment in red be added to page 11 within Section 14-4503, beginning on line 17:

(B) THE FOLLOWING INFORMATION AND DATA IS EXEMPT FROM THIS
SUBTITLE:

(1) PROTECTED HEALTH INFORMATION UNDER THE FEDERAL
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996;

(2) PATIENT-IDENTIFYING INFORMATION FOR PURPOSES OF 42
U.S.C. § 290dd-2;

(3) IDENTIFIABLE PRIVATE INFORMATION THAT IS USED FOR PURPOSES OF
THE FEDERAL POLICY UNDER THE CONTROLLED SUBSTANCES ACT SECTION ON THE
REGULATION OF LISTED CHEMICALS 21 U.S.C. SEC. 830;

Conclusion

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

Respectfully submitted,



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
The Honorable Senator Malcom Augustine

SB0698_UNF_MTC_Consumer Protection - Online and Bi

Uploaded by: Drew Vetter

Position: UNF



MARYLAND TECH COUNCIL

TO: The Honorable Melony Griffith, Chair
Members, Senate Finance Committee
The Honorable Malcolm Augustine

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

DATE: March 8, 2023

RE: **OPPOSE UNLESS AMENDED** – Senate Bill 698 – *Consumer Protection – Online and Biometric Data Privacy*

The Maryland Tech Council (MTC) writes in **opposition unless amended** to *Senate Bill 698: Consumer Protection – Online and Biometric Data Privacy*. We are a community of over 700 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.

First and foremost, 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. Protecting a consumer's personal online data has become a topic of discussion and debate in states around the country. Senate Bill 698 is a lengthy and complicated proposal with lots of new language proposed for Maryland. The MTC's over-arching feedback, therefore, is for Maryland lawmakers to adopt a data privacy approach that is consistent with approaches in surrounding states. Many of the provisions of Senate Bill 698 appear adopted from the Connecticut Data Privacy Act. We have seen other states in the Mid-Atlantic and Northeast region adopt or discuss this approach. We encourage Maryland to adopt the Connecticut approach as well, in a manner that is as consistent as possible with the Connecticut law. Many of our member companies conduct online business across state lines. Therefore, it is extremely important to have a set of operating rules that is consistent and predictable from state to state or within a region.

We are also concerned that the bill creates a separate system of regulations for biometric data. Our reading of the bill is that consumer biometric data would be encompassed under the online data privacy section of the bill modeled after Connecticut. Setting up a distinct and parallel system for biometric data risks being duplicative and confusing. Therefore, we propose this section specific to biometric data be struck from the bill.

In addition, we are concerned about the potential for private rights of action connected to violations of the law. MTC believes that the bill should be made clear to ensure that the Attorney General bears the responsibility of enforcing the law, rather than creating the potential for any new private rights of action.

Our members are concerned that the threat of litigation for even minor violations poses significant risks and ongoing burdens and costs for technology companies.

We continue to maintain that the issue of data privacy is better addressed at the federal level or with a consistent approach among states throughout the region. As stated above, technology companies reach into numerous states, and it can be a significant practical challenge to comply with a patchwork of state policies. These inconsistencies and resulting confusion could deter innovative companies and start-ups from wanting to do business here. At the very least, we encourage Maryland to adopt an approach that is consistent with other states in the region.

MTC respectfully requests an unfavorable report unless amended as specified.

SB698_CTIA_Unfavorable.pdf

Uploaded by: Jake Lestock

Position: UNF



**Testimony of
JAKE LESTOCK
CTIA**

**In Opposition to Maryland Senate Bill 698
Before the Maryland Senate Finance Committee**

March 8, 2023

Chair Griffith, 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 698. 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. This bill regulates various components of consumer privacy, including biometrics, differently than other comprehensive state laws. In addition, the private right of action would place businesses under a strong threat of litigation. As currently drafted, CTIA opposes the bill.

Consumer privacy is an important issue and the stakes involved in consumer privacy legislation are high. State-by-state regulation of consumer privacy will create an unworkable patchwork that will also 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. Heterogeneous state regulations would only complicate federal efforts and impose serious compliance challenges on businesses, ultimately confusing consumers. Federal legislation is the only way to ensure clear, consistent privacy protection for consumers and certainty for businesses.

While federal consumer privacy law is ultimately the only way to ensure consumers' privacy is adequately protected, CTIA understands without federal action, states will continue to fill the void. We appreciate that SB 698 is largely aligned with the Connecticut consumer privacy law, which was enacted last year. This law set forth strong consumer privacy rights and protections, and imposes robust but clear obligations on businesses and addresses how businesses can use biometric data. By closely mirroring Connecticut, Maryland can ensure consistent privacy protections and interoperability with other state frameworks. This will promote consistent consumer protection and will help Maryland businesses with implementation.

In order to achieve this, the added biometrics provisions should be amended to better align with other state comprehensive privacy laws. As currently drafted, this component is modeled after a biometric privacy law in Illinois, enacted in 2008, which has led to a myriad of lawsuits and little consumer protection. Maryland should not look to replicate this problematic law. The private right of action contained within the biometrics provisions would



subject companies to the risk of expensive litigation that primarily benefits the plaintiffs' bar and offers little relief to consumers. Through September of 2021, according to a search of court filings, plaintiffs' lawyers have filed over 900 cases alleging violations under the BIPA law in Illinois.¹ Notably, to date no other state that has enacted a comprehensive privacy law that has included a private right of action over core privacy standards. Additionally, no other state has enacted a law similar to the problematic Illinois BIPA standard.

In closing, we reiterate our concern about the enactment of state laws that further fragment privacy legislation across the country. While the bill remains inconsistent with other state comprehensive privacy laws, CTIA respectfully opposes this legislation. We recommend further aligning with the Connecticut model and look forward to working with the sponsor to ensure parity among existing laws. Thank you for your consideration.

¹ <https://institutelegalreform.com/research/ilr-briefly-a-bad-match-illinois-and-the-biometric-information-privacy-act/>

Ext. Comm. - Letter - 2023 - Maryland SB 698 - Pri

Uploaded by: Joshua Fisher

Position: UNF



March 5, 2023

The Honorable Melony Griffith
Chair, Senate Finance Committee
Annapolis, Maryland 21401

RE: SB 698 - Online and Biometric Data Privacy
Position: Unfavorable

Chair Griffith:

The Alliance for Automotive Innovation (Auto Innovators) is writing to inform you of **our opposition to SB 698**, which establishes requirements & restrictions on private entities use, collection, & maintenance of biometric data.

From the manufacturers producing most vehicles sold in the U.S. to autonomous vehicle innovators to equipment suppliers, battery producers and semiconductor makers – Alliance for Automotive Innovation represents the full auto industry, a sector supporting 10 million American jobs and five percent of the economy.

Maintaining Consumer Privacy and Cybersecurity

The protection of consumer personal information is a priority for the automotive industry. Through the development of the “Consumer Privacy Protection Principles for Vehicle Technologies and Services,” Auto Innovators’ members committed to take steps to protect the personal data generated by their vehicles. These Privacy Principles provide heightened protection for certain types of sensitive data, including biometric data.¹ Consumer trust is essential to the success of vehicle technologies and services. Auto Innovators and our members understand that consumers want to know how these vehicle technologies and services can deliver benefits to them while respecting their privacy. Our members are committed to providing all their customers with a high level of protection of their personal data and maintaining their trust.

Unique Considerations for Vehicle Safety Technology

Privacy requirements of this nature require a standardized, nationwide approach so there is not a dizzying array of varied state requirements. Privacy protections regarding biometrics are being enforced by the Federal Trade Commission (FTC)¹. The FTC has been the chief regulator for privacy and data security for decades, and its approach has been to use its authority under Section 5 of the FTC Act to encourage companies to implement strong privacy and data security practices. As noted above, the auto industries “Privacy Principles” are enforceable under

¹ https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf

Section 5 of the FTC Act. We prefer this standard approach over individual states enacting disparate and conflicting laws.

SB 698 raises unique challenges for the auto industry. While the requirement to have a written policy that lays out a retention schedule conforms with the industry's existing Privacy Principles, the requirement to destroy the information no later than three years after the company's last interaction are arbitrary. A requirement to provide clear disclosure to consumers about how long such information will be maintained should be sufficient. Moreover, in practice, this requirement may prove challenging because, in the automotive case, manufacturers do not generally have visibility into who is driving or using a particular vehicle at a particular time and will therefore have no way of knowing when a particular customer last interacted with the vehicle.

Additionally, in the automotive context, a strict deletion requirement may interfere with automakers ability to evaluate the performance of the technology and federal requirements concerning vehicle recalls. Any deletion requirement should be accompanied by reasonable exceptions which recognize these concerns.

As written, SB 698 requires automakers to provide a service dependent on biometric data even if the consumer does not want his or her biometric data collected. It is common sense not to require a company to provide a service if the consumer is not willing to provide the data that is required to utilize said service.

Finally, under SB 698, businesses may very well find themselves in a position of facing severe penalties for alleged violations and even very minor and inadvertent infractions and where there are no actual damages. We think existing remedies under state law are sufficient to address these issues.

Thank you for your consideration of the Auto Innovators' position. For more information, please contact our local representative, Bill Kress, at (410) 375-8548.

Sincerely,



Josh Fisher
Director, State Affairs

ⁱ <https://www.ftc.gov/news-events/press-releases/2021/01/california-company-settles-ftc-allegations-it-deceived-consumers>

SB 698 SIA Oppose (MD).pdf

Uploaded by: K. Alexander Wallace

Position: UNF



March 7, 2023

Chair Griffith
Senate Finance Committee

Dear Chair Griffith, 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 opposition to Senate Bill 698 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 include the leading providers of biometric technologies available in the U.S. Privacy is important to the delivery and operation of many safety and security-enhancing applications of technologies provided by our industry, and our members are committed to protecting personal data, including biometric data.

We are concerned that SB 698, as introduced, is the wrong approach to protecting data privacy as it would import an outdated and problematic model from Illinois and patchwork it into a broader data privacy bill—creating unnecessarily duplicative and overly restrictive regulations which would negatively impact consumers and small businesses in Maryland.

No other state has adopted legislation similar to the Illinois Biometric Information Protection Act (BIPA), which has resulted in more harm to consumers and local businesses than protections. There, businesses have been extorted through abusive “no harm” class action lawsuits, and beneficial technologies have been shelved. In fact, many of our member companies that provide products utilizing biometric technologies have chosen not to make these products or specific functions available in Illinois.

Safeguarding biometric information is important, but it should be done in a way that both protects Marylanders and allows for the development and use of advanced technologies that benefit them.

Beyond opening the door to lawsuit abuse with enforcement through a private right of action, there are also very real consequences to consumers – including their privacy – for imposing unnecessary limits through overregulation.

If the committee decides to move forward with SB 698, key changes are critical for preventing negative impacts on Maryland businesses and consumers. Including BIPA-style carve outs for biometric data in this bill, which should be treated as all other personal data, only damages the integrity and intent of a broad consumer data privacy bill. We urge you not to approve the bill in its current form.

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

Respectfully submitted,

Colby Williams
Senior Manager, Government Relations
Security Industry Association
Silver Spring, MD
Cwilliams@securityindustry.org
www.securityindustry.org

2023-3-8_CCIA_Written Comments_MD SB 698 (Unfavora

Uploaded by: Khara Boender

Position: UNF



March 8, 2023

Senate Finance Committee
Attn: Tammy Kraft, Committee Manager
3 East Wing
Miller Senate Office Building
11 Bladen Street
Annapolis, Maryland 21401

Re: SB 698 - Consumer Protection - Online and Biometric Data Privacy (Unfavorable)

Dear Chair Griffith and Members of the Senate Finance Committee:

On behalf of the Computer & Communications Industry Association (CCIA)¹, I write to respectfully oppose SB 698, Consumer Protection - Online and Biometric Data Privacy.

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, including biometric data. However, as currently written SB 698 includes several provisions that raise concerns. We appreciate the committee's consideration of our comments regarding several areas for potential improvement.

1. Definitions 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

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>

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 definitions in SB 698 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 recently enacted Virginia Consumer Data Protection Act and alignment of key definitions to allow businesses to better practically operationalizable privacy protections across state borders.

2. Privacy protections should take a risk-based approach.

Privacy protections should be directed toward managing data collection and processing practices that pose a high risk of harming consumers or are unexpected in the context of a service. Consent mechanisms can be a powerful tool for promoting transparency and consumer control. However, it is important to recognize that the provision of many services, both online and offline, requires the collection and processing of certain user information. Requiring specific user consent for any data collection or processing would be inconsistent with consumer expectations, introduce unnecessary friction resulting in the degradation of user experience, and likely overwhelm consumers, resulting in "consent fatigue" that would lessen the impact of the most important user controls.³

3. Sufficient time is needed to allow covered entities to understand and comply with newly established requirements.

SB 698 fails to provide covered entities with a sufficient onramp to achieve compliance. A successful privacy framework should ensure that businesses have an appropriate and reasonable opportunity to clarify the measures that need to be taken to fully comply with new requirements. Recently enacted privacy laws in California, Colorado and Virginia included two-year delays in enforcement of those laws. CCIA recommends that any privacy legislation advanced in Maryland include a comparable lead time to allow covered entities to come into compliance and would therefore recommend amending the current October 1, 2023 effective date included in SB 698 to a later date.

4. Investing enforcement authority with the state attorney general and providing a cure period would be beneficial to consumers and businesses alike.

SB 698 permits consumers to bring legal action against businesses that have been accused of violating new regulations. By creating a new private right of action, the measure would open the doors of Maryland's courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury.

³ See Article 29 Data Protection Working Party, WP 259, *Guidelines on Consent Under Regulation 2016/679*, 17 (Apr. 10, 2018), ("In the digital context, many services need personal data to function, hence, data subjects receive multiple consent requests that need answers through clicks and swipes every day. This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing."), <https://ec.europa.eu/newsroom/article29/items/623051>.



Lawsuits also prove extremely costly and time-intensive – it is foreseeable that these costs would be passed on to individual consumers in Maryland, disproportionately impacting smaller businesses and startups across the state. Further, every state that has established a comprehensive consumer data privacy law – California, Colorado, Connecticut, Utah and Virginia – has opted to invest enforcement authority with their respective state attorney general. This allows for the leveraging of technical expertise concerning enforcement authority, placing public interest at the forefront.

CCIA recommends that the legislation include a cure period of at least 30 days. This would allow for actors operating in good faith to correct an unknowing or technical violation, reserving formal lawsuits and violation penalties for the bad actors that the bill intends to address. This would also focus the government’s limited resources on enforcing the law’s provisions for those that persist in violations despite being made aware of such alleged violations. Such notice allows consumers to receive injunctive relief, but without the time and expense of bringing a formal suit. Businesses would also be better equipped with the time and resources to address potential privacy changes rather than shifting focus to defending against litigation.

* * * * *

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

MD SB 698 Privacy_TechNet _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

March 6, 2023

The Honorable Melony Griffith
Miller Senate Office Building, 3 East Wing
11 Bladen Street, Annapolis, MD 21401

RE: SB 698 Consumer Protection - Online and Biometric Data Privacy

Dear Chair Griffith and Members of the Committee,

On behalf of TechNet's member companies, I respectfully submit this letter of opposition to SB 698.

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 five 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. Specific requirements on data collection, use, or retention should be narrowly focused on personally identifiable, highly sensitive, or proprietary information. Privacy laws should be limited to specific practices tied to specific harms and should also apply to government entities.

Undoubtedly, biometrics has a critical role to play in the security and anti-fraud spaces, and its protections are a top priority for our members; however, the language in this bill is reflective of the Illinois Biometric Information Privacy Act (BIPA). BIPA is outdated and has led to several hundred frivolous lawsuits in Illinois. TechNet would suggest shifting the focus from biometrics to other language in SB 698 which reflects the Connecticut model and incorporates biometrics protections under the omnibus privacy umbrella. These protections include affirmative opt-in consent requirements, the ability for consumers to correct, delete, or port their data, among several other provisions. This approach provides more protections to Maryland consumers and allows for flexible interoperability across state lines.

TechNet opposes the inclusion of a private right of action because any unintentional or perceived violation could result in damaging liability for companies. PRAs are not effective methods of enforcement, as they can very easily be misused and lead to frivolous lawsuits. Litigation leads to uneven and inconsistent outcomes. In turn, some business may choose to stop doing business in Maryland or be forced to cease operations altogether. The Attorney General is the only appropriate entity to enforce such action. By shifting the focus away from the threat of civil suits, companies will be able to devote resources to complying with privacy laws, as opposed to dealing with frivolous litigation.

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. We would welcome the opportunity to work with your office to address issues of privacy protection without unintended consequences. Please 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
Executive Director, Pennsylvania & the Mid-Atlantic
TechNet
mdurkin@technet.org

MD 2023 NAMIC letter SB698 Consumer Biometric data

Uploaded by: Matt Overturf

Position: UNF

SENATE FINANCE COMMITTEE

MARYLAND SB0698: Consumer Protection—Online and Biometric Data Privacy

UNFAVORABLE

March 8, 2023

Chairwoman Griffith 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 in opposition to Senate Bill 698.

NAMIC consists of more than 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

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 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

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.



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, today 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 HB 807, the exception should apply to both the data and entity subject to the GLBA as follows:

Nothing in this Act shall be deemed to apply in any manner to data or to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal "Gramm-Leach-Bliley Act of 1999," 15 U.S.C. s.6801 et seq. 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.

Private Right of Action

As drafted, Senate Bill 698 would establish a private right of action under Sec. 13-408. A private right of action distracts from the goal of meaningful and real privacy protections where a knowledgeable agency or regulator ensures that businesses is protecting data. Private lawsuits could sweep in technical non-compliance items, and it could further erode uniformity. The concept is extremely objectionable as it could add costs to doing business for everyone, including the consumer. NAMIC urges policymakers to avoid the pitfalls associated with inviting privacy class actions lawsuits.

The U.S. Chamber Institute for Legal Reform (ILR) 2019 paper highlights the superior consumer protection of regulator enforcement over a private right of action. It concluded:

... privacy statutes that are enforced by government agencies provide a robust process through which noncompliance with protected privacy interests can be identified, remedied, and monitored while promoting consistency, fairness, and innovation.⁴

Thank you for taking the time to consider our position on Senate Bill 698.

Sincerely,

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

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

⁴ https://www.instituteforlegalreform.com/uploads/sites/1/III-Suited_-_Private_Rights_of_Action_and_Privacy_Claims_Report.pdf

Joint Ad Trade Letter in Opposition to Maryland SB

Uploaded by: Travis Frazier

Position: UNF



March 6, 2023

Senator Malcom Augustine
214 James Senate Office Building
11 Bladen Street
Annapolis, MD 21401

Senator Melony Griffith
Chair of the Maryland Senate Finance Committee
3 East Miller Senate Office Building
11 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

RE: Oppose: SB 698

Dear Senator Augustine, Chair Griffith, and Vice Chair Klausmeier:

On behalf of the advertising industry, we oppose Maryland SB 698.¹ We and the companies we represent, many of whom do substantial business in Maryland, strongly believe consumers deserve meaningful privacy protections supported by reasonable government policies. However, we are concerned that state efforts to pass privacy laws will only add to the increasingly complex privacy landscape for both consumers and businesses throughout the country. We and our members therefore support a national standard for data privacy at the federal level. As presently drafted, SB 698 contains provisions that are out-of-step with privacy laws in other states and would create the potential for private litigants to bring lawsuits for violations of its terms. We therefore encourage Maryland legislature to update the bill so it aligns with recently enacted legislation in the majority of other states, such as the Virginia Consumer Data Protection Act (“VCDPA”).²

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 2020.³ Our group has more than a decade’s

¹ Maryland SB 698 (Gen. Sess. 2023) located [here](#).

² See, e.g., Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-575 et. seq.

³ 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->

worth of hands-on experience it can bring to bear on matters related to consumer privacy and controls. We would welcome the opportunity to engage with you further on our suggested amendments to the bill outlined here.

I. Maryland Should Take Steps to Harmonize its Approach to Privacy with Other State Laws

Instead of adopting SB 698, we encourage the legislature to consider a framework for data privacy that better aligns with recently enacted privacy legislation in other states, such as the VCDPA. In the current absence of a national standard for data privacy at the federal level, it is critical for legislators to seriously consider the costs to both consumers and businesses that will accrue from a patchwork of differing privacy standards across the states. Harmonization with existing privacy laws is critical to minimizing costs of compliance and fostering similar consumer privacy rights for consumers, particularly in localities like the DC-Maryland-Virginia area where individuals regularly cross state lines.

One way that SB 698 presently diverges from existing state privacy laws is that it does not address the concept of pseudonymous data. Most state privacy laws, including the VCDPA, 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 laws exempt this data from consumer rights to access, delete, correct, and port personal data, provided that this data is kept separately from information necessary to identify a consumer and is subject to effective technical and organizational controls to prevent the controller from accessing such information. Without an explicit exemption for pseudonymous data from consumer rights, controllers could be forced to reidentify data or to maintain it in identifiable form to ensure they can, for example, return such information to a consumer in response to an access request. Requiring companies to link pseudonymous data with identifiable information is less privacy protective for consumers than permitting and encouraging companies to keep such data sets separate. We ask you to amend SB 698 and harmonize it with other privacy laws to exempt pseudonymous data from consumer rights of access, correction, deletion, and portability.

Absent amendments to SB 698 to unify its approach with existing state privacy laws, the costs to facilitate compliance with divergent state privacy requirements would be significant. To make the point: a regulatory impact assessment of the California Consumer Privacy Act of 2018 (“CCPA”) concluded that the initial compliance costs to California firms for the CCPA *alone* would be \$55 billion.⁴ Additionally, a recent study on a proposed privacy bill in a different state found that the proposal would have generated a direct initial compliance cost of between \$6.2 billion to \$21 billion, and an ongoing annual compliance cost of between \$4.6 billion to \$12.7 billion for companies.⁵ Other

[content/uploads/2021/10/IAB_Economic_Impact_of_the_Market-Making_Internet_Study_2021-10.pdf](#) (hereinafter, “Deighton & Kornfeld 2021”).

⁴ See State of California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* at 11 (Aug. 2019), located at <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf>.

⁵ See Florida Tax Watch, *Who Knows What? An Independent Analysis of the Potential Effects of Consumer Data Privacy Legislation in Florida* at 2 (Oct. 2021), located at

studies confirm the staggering costs associated with different 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 small businesses shouldering a significant portion of the compliance cost burden.⁶ Maryland should not add to this compliance burden for businesses and should instead opt for an approach to data privacy that is in harmony with already existing state privacy laws.

II. The Bill Should Vest Enforcement Exclusively in the Maryland Attorney General

SB 698 also diverges from existing privacy laws in its approach to enforcement. As presently drafted, the bill would permit private litigants to bring lawsuits for violations of its terms. We strongly believe a private right of action is not an effective enforcement mechanism for privacy legislation. Instead, enforcement should be vested solely with the Maryland Attorney General (“AG”) alone. This enforcement structure would lead to effective compliance by businesses and strong outcomes for state residents, while better enabling businesses to allocate funds to develop processes and procedures 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.

A private right of action would create a complex and flawed compliance system without tangible privacy benefits for consumers. Allowing private actions would flood Maryland’s courts with frivolous lawsuits driven by opportunistic trial lawyers searching for technical violations, rather than focusing on actual consumer harm.⁷ Private right of action provisions are completely divorced from any connection to actual consumer harm and provide consumers little by way of protection from detrimental data practices.

Additionally, establishing 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 would not effectively address consumer privacy concerns or deter undesired business conduct. A private right of action would expose businesses to extraordinary and potentially enterprise-threatening costs for technical violations of law rather than drive systemic and helpful changes to business practices. It 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

<https://floridatagwatch.org/DesktopModules/EasyDNNNews/DocumentDownload.ashx?portalid=210&moduleid=34407&articleid=19090&documentid=986>.

⁶ 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).

⁷ 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, 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](#).

threat of an expensive lawsuit may force smaller companies to agree to settle claims against them, even if they are convinced the claims are without merit.⁸

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, 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 remove the private right of action from SB 698 and make enforcement responsibility the purview of the AG alone.

III. 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 tremendous growth opportunities. A 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.⁹ In 2020 alone, it 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.¹⁰ 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.¹¹ More Internet jobs, 38 percent, were created by small firms and self-employed individuals than by the largest Internet companies, which generated 34 percent.¹² The same study found that the ad-supported Internet supported 168,600 full-time jobs across Maryland, almost triple the number of Internet-driven jobs from 2016.¹³

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.¹⁴ 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

⁸ 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.*

⁹ Deighton & Kornfeld 2021 at 5.

¹⁰ *Id.*

¹¹ *Id.*

¹² *Id.* at 6.

¹³ *Compare id.* at 127 (Oct. 18, 2021), located [here](#) with John Deighton, Leora Kornfeld, and Marlon Gerra, *Economic Value of the Advertising-Supported Internet Ecosystem*, INTERACTIVE ADVERTISING BUREAU, 106 (2017), located [here](#) (finding that Internet employment contributed 61,898 full-time jobs to the Maryland workforce in 2016 and 168,600 jobs in 2020).

¹⁴ See John Deighton, *The Socioeconomic Impact of Internet Tracking* 4 (Feb. 2020), located at <https://www.iab.com/wp-content/uploads/2020/02/The-Socio-Economic-Impact-of-Internet-Tracking.pdf>.

mitigation.”¹⁵ 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.¹⁶ 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.¹⁷ 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.”¹⁸ 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.¹⁹ 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,²⁰ 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.²¹ 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 2016.²² Another study found that the free and low-cost goods and services consumers receive via the ad-supported Internet amount to approximately \$30,000 of value per year, measured in 2017 dollars.²³ 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.

¹⁵ *Id.* at 34.

¹⁶ *Id.* at 15-16.

¹⁷ *Id.* at 28.

¹⁸ J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 9 (2022), located [here](#).

¹⁹ *See id.* at 8.

²⁰ *See* Howard Beales, *The Value of Behavioral Targeting* 3 (2010), located at https://www.researchgate.net/profile/Howard-Beales/publication/265266107_The_Value_of_Behavioral_Targeting/links/599eceeaa6fdcc500355d5af/The-Value-of-Behavioral-Targeting.pdf.

²¹ *See* John Deighton & Peter A. Johnson, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the US Economy* (2015), located at <https://www.ipc.be/~media/documents/public/markets/the-value-of-data-consequences-for-insight-innovation-and-efficiency-in-the-us-economy.pdf>.

²² 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](#).

²³ J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 2 (2022), located [here](#).

C. Consumers Prefer Personalized Ads & 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.²⁴ 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.²⁵ Indeed, as the Federal Trade Commission noted in its comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.²⁶

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 therefore respectfully ask you to carefully consider SB 698'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 support protecting consumer privacy. We believe, however, that SB 698 takes the wrong approach to privacy enforcement and would impose requirements that would be misaligned with other state privacy laws. We therefore respectfully ask you to decline to advance the bill in its current form. We are eager and willing to work with you on alternative, comprehensive privacy legislation that balances consumer privacy and choice with preserving the benefits that come from the responsible use of data.

²⁴ Mark Sableman, Heather Shoenberger & Esther Thorson, *Consumer Attitudes Toward Relevant Online Behavioral Advertising: Crucial Evidence in the Data Privacy Debates* (2013), located at https://www.thompsoncoburn.com/docs/default-source/Blog-documents/consumer-attitudes-toward-relevant-online-behavioral-advertising-crucial-evidence-in-the-data-privacy-debates.pdf?sfvrsn=86d44cea_0.

²⁵ Digital Advertising Alliance, *Zogby Analytics Public Opinion Survey on Value of the Ad-Supported Internet Summary Report* (May 2016), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/ZogbyAnalyticsConsumerValueStudy2016.pdf.

²⁶ Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located at https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.



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
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's
202-355-4564

Lartase Tiffith
Executive Vice President for 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: Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP

CPPA Written Testimony, SB 698 (Online and Biometr

Uploaded by: Maureen Mahoney

Position: INFO

CALIFORNIA PRIVACY PROTECTION AGENCY

2101 Arena Blvd
Sacramento, CA 95834
www.cppa.ca.gov



Written Testimony of Maureen Mahoney
Deputy Director of Policy & Legislation, California Privacy Protection Agency
Comments on SB 698, Online and Biometric Data Privacy (Informational Only)
Maryland Senate Finance Committee

Chair Griffith, Vice Chair Klausmeier, and Members of the Senate Finance Committee, the California Privacy Protection Agency¹ (CPPA or Agency) thanks you for the opportunity to submit written testimony on SB 698 (Online and Biometric Data Privacy). Please note that these comments are being provided for informational purposes only, and are not intended to promote or oppose the introduction or enactment of any legislation. Our originating statute, the California Consumer Privacy Act (CCPA), directs the Agency to work with other entities with jurisdiction over privacy laws to “ensure consistent application of privacy protections.”² We are proud that states are leading the way on legislation to protect consumers’ privacy and data security. As of 2023, four states have adopted, and over half the states have considered, omnibus consumer privacy laws.³

The Agency is encouraged that SB 698 shares similarities with California’s approach. For example, SB 698, like the CCPA, not only provides consumers with the right to access, delete, correct, and stop the sale of information to third parties, with additional protections for sensitive data, but is intended to be easy for consumers to use. This reflects the concerns outlined in the California law’s findings, which pointed out the “asymmetry of information [that] makes it difficult for consumers to understand what they are exchanging[.]”⁴

Background

California has a long history of privacy and data protection legislation. In 1972, California voters established the right of privacy in the California Constitution, amending it to include privacy as one of Californians’ “inalienable” rights.⁵ In 2002, California became the first state to pass a data breach notification requirement, and in 2003, became the first state to require businesses to post privacy policies outlining their data use practices. In 2018, it became the first state in the nation to adopt a comprehensive commercial privacy law, the California Consumer Privacy Act. That measure went into effect on January 1, 2020, and the Attorney General began enforcing it on July 1, 2020.⁶

In November 2020, California voters ratified Proposition 24, the California Privacy Rights Act, which amends and expands the CCPA, including by creating the first authority with full administrative powers

¹ Established in 2020, the California Privacy Protection Agency was created to protect Californians’ consumer privacy. The CPPA implements and enforces the California Consumer Privacy Act. It is governed by a five-member board that consists of experts in privacy, technology, and consumer rights.

² Cal. Civ. Code § 1798.199.40(i).

³ National Conference of State Legislatures, 2022 Consumer Privacy Legislation (updated June 10, 2022), <https://www.ncsl.org/about-state-legislatures/2022-consumer-privacy-legislation>.

⁴ Proposition 24, The California Privacy Rights Act § 2 (2020), <https://vig.cdn.sos.ca.gov/2020/general/pdf/top1-prop24.pdf>.

⁵ Cal. Cons. Art. 1 § 1.

⁶ Cal. Civ. Code § 1798.100 et seq.

focused on privacy and data protection in the United States, the California Privacy Protection Agency. Proposition 24 added new substantive provisions to the CCPA, such as new limitations on businesses' collection, use, retention, and sharing of personal information, a right to correction, and additional protections for sensitive data, which went into effect on January 1, 2023. On April 21, 2022, rulemaking authority under the CCPA formally transferred to the Agency. Along with the Attorney General, the Agency is vested with the authority to undertake enforcement to protect Californians' privacy.

Overview of California law

The CCPA includes specific notice requirements for businesses, grants new privacy rights to consumers, and imposes corresponding obligations on businesses. The rights granted to consumers include the right to know what personal information businesses have collected about consumers and how that information is being used, sold, and shared; the right to delete personal information that businesses have collected from consumers; the right to stop businesses' sale and sharing of personal information; and the right to non-discrimination in service, quality, or price as a result of exercising their privacy rights. As of January 1, 2023, California consumers have the right to correct inaccurate personal information the business maintains about them, and the right to limit a business's use and disclosure of sensitive personal information about them to certain business purposes, among other protections.

The CCPA provides additional protections for children under 16. Businesses are not permitted to sell the personal information of consumers if the business has actual knowledge that the consumer is under 16, unless the consumer, or the consumer's parent or guardian in the case of consumers who are under 13, has affirmatively authorized the sale of the consumer's information.

The CCPA covers information that identifies, relates to, or could reasonably be linked with a particular consumer or household—subject to certain exceptions. The measure applies to for-profit businesses that do business in California, collect consumers' personal information (or have others collect personal information for them), determine why and how the information will be processed, and meet any of the following thresholds: have a gross annual revenue of over \$25 million; buy, sell, or share the personal information of 100,000 or more California consumers or householders; or derive 50% or more of their annual revenue from selling or sharing California residents' personal information.

Businesses have corresponding duties, including with respect to:

- *Data minimization and purpose limitations*
 - Businesses' collection, use, retention, and sharing of personal information must be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected.
 - Businesses must not further process personal information in a manner that is incompatible with those purposes.
- *Dark patterns*
 - In obtaining consent from consumers, businesses are prohibited from using "dark patterns," which are defined to mean a user interface "designed or manipulated with the

substantial effect of subverting or impairing user autonomy, decisionmaking, or choice[.]”⁷

Overview of CPPA Rulemaking

The California Privacy Protection Agency is currently engaged in a formal rulemaking process to issue regulations to further the intent of the CCPA, as amended.⁸ On July 8, 2022, the Agency published its notice of proposed action in the California Regulatory Notice Register, beginning the formal rulemaking process. The proposed regulations primarily do three things: (1) update existing CCPA regulations to harmonize them with CPRA amendments to the CCPA; (2) operationalize new rights and concepts introduced by the CPRA to provide clarity and specificity to implement the law; and (3) reorganize and consolidate requirements set forth in the law to make the regulations easier to follow and understand. They place the consumer in a position where they can knowingly and freely negotiate with a business over the business’s use of the consumer’s personal information.

SB 698 and State Privacy Laws

As noted above, the Agency appreciates that SB 698 shares similarities with California’s approach. It’s important that consumers have effective tools to protect their privacy, as well as default protections that provide key privacy safeguards even without taking additional steps. For example, like California and other states, SB 698 has several provisions that help ensure this ease of use for consumers:

- **Global opt-out.** California, Colorado, and Connecticut each have a provision in their privacy laws requiring businesses receiving opt-out requests to honor requests submitted by browser privacy signals.⁹ The CPPA’s proposed regulations reiterate the requirements for an opt-out preference signal that consumers may use to easily opt-out of the sale or sharing of their personal information with all businesses that they interact with online. With the goal of strengthening consumer privacy, the regulations support innovation in pro-consumer and privacy-aware products and services and help businesses efficiently implement privacy-aware goods and services.

The California Attorney General is currently enforcing the browser privacy signal requirement in the existing CCPA regulations. Last year, it announced its first public case, against Sephora, alleging that Sephora failed to disclose to consumers that it was selling their personal information and failed to process user requests to opt out of sale via user-enabled global privacy controls in violation of the CCPA.¹⁰

⁷ Cal. Civ. Code § 1798.140(l).

⁸ For more information about the Agency’s work to implement the regulations, please see California Privacy Protection Agency, California Consumer Privacy Act Regulations, https://cppa.ca.gov/regulations/consumer_privacy_act.html.

⁹ See, Cal. Civ. Code § 1798.135(e).

¹⁰ Press release, *Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act* (Aug. 24, 2022), <https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement>. For information on additional AG enforcement activity, see State of California Department of Justice, CCPA Enforcement Case Examples (updated Aug. 24, 2022), <https://oag.ca.gov/privacy/ccpa/enforcement>.

- ***Prohibition on dark patterns.*** California, Colorado, and Connecticut all have a provision prohibiting businesses from using dark patterns, defined in California as “a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation[,]” in obtaining consent.¹¹ California’s proposed regulations set forth clear requirements for how businesses are to craft their methods for submitting consumer requests and obtaining consumer consent so that the consumer’s choice is freely made and not manipulated, subverted, or impaired through the use of dark patterns. They address not only narrow situations where consent must affirmatively be given, but general methods for submitting CCPA requests to address abuse by businesses who craft methods in ways that discourage consumers from exercising their rights.¹²
- ***No requirement for authentication to opt out.*** Like SB 698, neither the CCPA nor Connecticut’s privacy law require authentication of opt-out requests. Verification often creates friction for consumers, making it more difficult for consumers to exercise their rights. This is particularly important as online identifiers that are used for behavioral tracking cannot be easily accessed or verified by the consumer. Like SB 698, California and Connecticut do require identity verification for access, deletion, and correction requests, where consumer privacy could be undermined in the case of an unauthorized request.

However, there are some elements of California law that are not included in SB 698. For example:

- ***Broad definition of personal information.*** California has a broad definition of personal information, including “information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.” It also specifically identifies online identifiers, inferences, and pseudonymous identifiers as personal information.¹³
- ***Protections with respect to non-discrimination/loyalty programs.*** The CCPA prohibits businesses from discriminating against consumers for exercising any of the rights provided by the measure, including by denying goods or services, offering a different price or a different level of quality for goods or services, or retaliating against an employee. Businesses are permitted to charge a consumer a different price or rate, or provide a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer’s data. Businesses are not permitted to use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.¹⁴

Conclusion

We hope that our work in implementing the CCPA is helpful to you as you consider legislation. I am happy to answer any questions.

¹¹ Cal. Civ. Code § 1798.140(l)

¹² See, California Privacy Protection Agency, Draft Final Regulations Text at § 7004 (Feb. 3, 2023), https://coppa.ca.gov/meetings/materials/20230203_item4_text.pdf.

¹³ See, Cal. Civ. Code § 1798.140(v).

¹⁴ Cal. Civ. Code § 1798.125.

Written Testimony - SB 698.pdf

Uploaded by: Robert Dean

Position: INFO

AISHA N. BRAVEBOY
STATE'S ATTORNEY



JASON B. ABBOTT
PRINCIPAL DEPUTY STATE'S ATTORNEY

State's Attorney for Prince George's County
14735 Main Street, Suite M3403
Upper Marlboro, Maryland 20772
301-952-3500

March 8, 2023

Informational Testimony

SB 698 – Consumer Protection – Biometric Data Privacy

Dear Madame Chair and Members of the Committee:

This submission is to provide information on Senate Bill 698 and its potential negative impact on Maryland law enforcement efforts to solve open homicide and sex offense cases. This is provided on behalf of Aisha Braveboy, States Attorney for Prince George's County and the Maryland State's Attorney's Association. I am Robert Dean, Special Assistant State's Attorney for Prince George's County assigned to work with the Cold Case Homicide Unit of the Prince George's County Police Department. On February 8, 2023, I testified before this committee on a somewhat related bill, SB 169 and provided written testimony as well. This written testimony tracks the written testimony that I provided previously as our concerns are the same.

Our concern is the potential effect that this bill may have on important law enforcement activity should it become law as is - specifically the effect on the forensic genetic genealogical investigative process. We urge you to consider ways to accomplish your purpose in protecting biometric data privacy, yet at the same time preserving Maryland law enforcement's ability to utilize the forensic genetic genealogy investigative process which has become an essential tool in solving cold cases of homicide and sex offenses. As the bill stands now, it is flawed but we believe the flaws can be fixed.

One and a half years ago, our office was awarded a \$470,000 grant from the Department of Justice to support the investigation of unsolved homicides and sex offenses using forensic genetic genealogy. Working with the county police crime lab we have initially identified approximately 640 cases of unsolved homicides and sex offenses in Prince George's County where forensic genealogy investigation may be useful. (This process is also valuable in identifying human remains). We currently have 15 active cases utilizing the forensic genetic genealogy process and we anticipate increasing that number up to about 20 by the end of this year.

In 2021, the General Assembly enacted a comprehensive regulatory scheme covering some of this field in *Title 17 of the Criminal Procedure Code*. This comprehensive effort, the only one in the nation so far, governs in considerable detail how investigations utilizing forensic genetic genealogy are to proceed.

Title 17 establishes regulatory criteria, including judicial oversight of the investigative process, and rules governing the composition of the data bases available to law enforcement for this investigative purpose. There are rules requiring confidentiality and destruction protocols, as well as the establishment of regulatory criteria for those involved in the process.

Without getting into all the details of the *Title 17* requirements, our unit must follow the requirements of Title 17 as well as the *Department of Justice Interim Guidelines on Forensic Genetic Genealogy (2019)*. We currently have obtained judicial approval to proceed in approximately 15 cases that occurred from 1972 to 2006.

An initial step in developing leads for investigative purposes is to submit biological samples from the crime scene that are likely to originate from the offender. This sample must have already been submitted to the national CODIS data base to see if there is a match from samples of known offenders that have already been provided into the data base.

Once it is determined that there is no match, the Forensic Genetic Genealogy process involves sending the biological sample of a purported unidentified offender to a private laboratory that performs a SNP extraction (Single Nucleotide Polymorphism) which is then uploaded into a data base of DNA samples that have been voluntarily submitted by consumers to determine their ancestry. The donors to this data base have consciously opted into the database and agreed that their DNA sample could be made available to law enforcement.

Based upon the SNP upload of the suspect sample, a distant relative of the possible suspect may be identified based upon a calculation of familial DNA characteristics. At this point, a genealogist will construct a family tree based upon open-source information.

This process can be very time consuming. But it may provide leads for investigators to follow. In building the family tree, persons of interest may be revealed. Any leads that arise through this process will, of course, need further investigation based upon the specifics of the crime being investigated.

Our concern with SB 698 is that those private entities who develop the SNPs and those private entities that maintain the essential data bases of DNA profiles voluntarily submitted, will likely avoid accepting Maryland cases because of the potential reach of this bill as well as other similar bills proposed.

A reading of the bill as it defines and regulates biometric data by private entities and the destruction protocols imposed and the cause of action SB 698 affords individuals, has the very real potential of ending the forensic genetic genealogy investigative process in Maryland.

I have spoken to representatives of Othram and BODE technologies who have expressed concern over the potential that such legislation has.

In light of the already existing regulatory scheme of *Criminal Procedure Title 17*, and the chilling effect that this bill could have to the availability of this crime solving technique in Maryland, we urge this committee to consider an amendment to the proposed legislation to exclude from the bill's coverage those entities that have laboratories developing the appropriate DNA profiles necessary in the forensic genetic genealogy process as well as those entities that maintain those data bases essential to the forensic genetic genealogy process.

Title 17 section 17-101 (c) and *(g)* provides statutory definitions of those entities that provide the services necessary to the forensic genetic genealogy process. The operative definitions are: (c) Direct to Consumer genetic genealogy services; and (g) publicly available open-data personal genomics database.

Therefore, we urge that these entities and the essential process of Forensic Genetic Genealogy that they perform for law enforcement be excluded from the coverage of the law. The operative exclusion section for this legislation is 14-4503(A). Options for possible amendments which would address our concerns are provided in the attachment to this written testimony. In addition to an amendment to this section of the bill, the purpose clause can be amended to explain that nothing in this law should affect the investigative processes regulated in *Title 17 of the Criminal Procedure Article*.

I will be happy to answer any questions or discuss further.

Respectfully,

Robert Dean

Special Assistant State's Attorney

Prince George's County

rldean@co.pg.md.us

Attachment

March 2023

To: Interested Parties

From: Robert Dean – ASA – Prince George’s County State’s Attorney’s Office

Re: SB 698 (cross-filed with HB 807). – Options for Recommended Amendment.

Purpose: To exclude from coverage of SB 698 (and HB 807) those private entities that provide essential services to law enforcement investigating crimes pursuant to Criminal Procedure Article Title 17.

Options:

14-4503 (A) This subtitle does not apply to:

(7) Option 1 - Any entity providing services for and on behalf of law enforcement agencies conducting investigative activity covered by Title 17 of the Criminal Procedure Article.

Option 2 – Any entity or process as defined by Title 17 of the Criminal Procedure Article Section 17-101 (c) and Section 17- 101 (g) providing services for and behalf of law enforcement agencies conducting investigative activity covered by the aforesaid Title 17.

Option 3 - A contractor, subcontractor, or agent of a state agency or local unit of government when working for or on behalf of that State agency or a local unit of government.

Note: Current Language from Annotated Code of Maryland – Criminal Procedure Article - Title 17 Definitions: 17-101:

(c) “**Direct-to-consumer genetic genealogy services**” means genetic genealogy services that are offered by private companies directly to members of the public and law enforcement agencies rather than through clinical health care providers, typically via customer access to secure online websites.

(g) “**Publicly available open-data personal genomics database**” means a database in which persons voluntarily submit their genomics data or genetic profiles, typically processed through genetic genealogy services, for the purposes of comparison or searching against the genetic profiles of other individuals to evaluate potential familial relationships between the reference sample and other service user samples.

Note - Option 3 above is derived From Illinois (The Biometric Privacy Act)

740 ILCS 14/25)

Sec 25 Construction

.....

(e) Nothing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or a local unit of government.

(Source: P.A. 95-994, eff.10-3-08.)