MD SB0041.Drumgoole. Testimony.pdf
Uploaded by: Christine Drumgoole
Position: FAV

Christine J. Drumgoole

5220 Bangert Street
White Marsh, Maryland 21162
410-952-1868 (cell), btsurvivor@outlook.com

January 24, 2022

SENATOR SUSAN LEE

SENATE JUDICIAL PROCEEDINGS COMMITTEE
2 EAST
MILLER SENATE OFFICE BUILDING
ANNAPOLIS, MARYLAND 21401

RE: **SBOO41** CHILD CUSTODY AND VISITATION

I am a well-educated, emotionally healthy protective parent, intimate partner violence/betrayal trauma survivor, and family court reform advocate. I hold a favorable position as to SB0041 -FAMILY LAW – CHILD CUSTODY AND VISITATION.

I would like to offer suggestions to this Senate Bill. My own experience with Family Court has been quite difficult, given the vague requirements of custody and visitation when abuse is present. There is little to no guidance for what constitutes "supervised" custody and what metrics or professionals decide the likelihood of abuse occurring in the future.

In my divorce/custody case, my former spouse had a long history of emotional, psychological, sexual, physical, and financial abuse against me and our children. The court often defers to professionals, such as social workers, therapists, and academics when trying to determine if an abuser will abuse again- the likelihood of future abuse. Child sexual abuse perpetration is an especially difficult construct to ascertain. There are diagnostic criteria for "pedophilia" in the DSM V and ICD 11, but an abuser need not be diagnosed as a pedophile (specific, sustained attraction to minors) to have committed an act of sexual abuse. Further, any lack or presence of a diagnosis does not necessarily determine the likelihood of abuse in future. In the case of my former spouse, he identified as a sex and pornography addict, admitted to illegal sexual perpetrations, viewing child pornography, sexually abusing our daughter, and yet had no specific target or sexual attraction for his abuse. In short, he is an equal opportunity sexual predator. Professional without specific, certified credentials in the areas of child sexual abuse, emotional trauma, and/or compulsive

sexual behavior and pornography viewing would not be able to make a professional determination; let alone an educated and credentialed opinion as to the likelihood of abuse. In cases of abuse, it is best to always believe the victim (especially victims of child sexual abuse) and protect the victim from any likelihood. A low likelihood of reoffending is NOT no likelihood of reoffending.

Secondly, when the perpetrator's family members are tasked with overseeing supervised visitation, especially overnights, they should be required to complete the following:

1. Notification of the abuse that has occurred to warrant the supervision requirement by a trained professional.
2. Required to communicate with the safe parent to confirm attendance for supervision.
3. Be required to follow safety measures as set forth by child sexual abuse professionals, such as Dr. Mel Lanston.
4. Held responsible if they do not meet the requirements of supervision.

I appreciate your time and assistance. I remain supporter of this proposed bill and am available for further discussion. I apologize for the brevity of this letter of support, but I wrote this in less than ten minutes. This is a very important cause.

SINCERELY,

CHRISTINE J. DRUMGOOLE
Healthy, protective parent, intimate partner violence/betrayal trauma survivor, and advocate.

CPD Written Testimony SB 11.pdf
Uploaded by: Hanna Abrams
Position: FAV

BRIAN E. FROSH
Attorney General

ELIZABETH F. HARRIS
Chief Deputy Attorney General

CAROLYN QUATTROCKI
Deputy Attorney General

WILLIAM D. GRUHN
Chief
Consumer Protection Division

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION

January 26, 2022

TO: The Honorable Delores G. Kelley, Chair
Finance Committee

FROM: Hanna Abrams, Assistant Attorney General

RE: Senate Bill 11 – Maryland Online Consumer Protection and Child Safety Act – SUPPORT

The Office of the Attorney General supports Senate Bill 11 ("SB 11"), sponsored by Senator Lee, which gives Marylanders insight into the use of, and control over, their personal information.

The issues surrounding the use of personal data reach well beyond traditional notions of privacy – to issues like discrimination, algorithmic fairness, and accountability.[1] Consumers need a clear and consistent privacy law that they can rely on to protect them. Other states, including California, Virginia, and Colorado have already given their citizens privacy rights that allow them to control their personal information. As a result, large companies – SB 11's impact is limited to large businesses[2] – already have the mechanisms in place to allow consumers in those states to control their information. It is time for businesses to give Marylanders the same control.

SB 11 provides consumers with necessary rights that would allow consumers to control and choose how companies collect and use their information, including:

- Right to Transparency
- Right to Know
- Right to Delete
- Right to Opt out of Sale/Third Party Disclosure
- Right to Non-Discrimination[3]

Right now, companies are collecting and selling increasing amounts of sensitive information about our lives *without our knowledge or consent***.** And if consumers want to attempt

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

[2] § 14-401(c) limits the law's application to companies that either (1) have an annual gross revenue of $25,000,000, or (2) buy and sell personal information of at least 100,000 consumers, households or devices, or (3) make at least 50% of its annual revenue from selling consumers' personal information.

[3] These rights are explained more fully in Appendix A.

to decipher how companies collect and use their data, they need to read hundreds of lengthy privacy policies – often confusing, incomplete, or from companies they have never heard of.

The tech industry exploits and sells this sensitive information about our private lives. Companies are collecting information that gives strangers personal information about us including 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.[4] 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.

There are real consequences to the collection of information. For example, personal information has caused the loss of jobs, has been used to limit individuals' access to loans and professional opportunities, and has led to threats to personal safety:

- Individuals have been forced to resign after being outed as gay based on the data collected and shared by the dating app Grindr.[5]
- Social media profiles and internet usage may be used to determine creditworthiness.[6] Companies are determining creditworthiness or social class based on an individual's social network contacts, number of gadgets owned, how much the user uses the internet, and location data.[7] In other words, companies are collecting data about how you use the internet and deciding based on that whether you are eligible for a loan.
- Employers have consciously targeted advertisements at younger men to keep older workers and females from learning of certain job opportunities,[8] and landlords have prevented racial minorities from seeing certain housing advertisements.[9]
- The secondary use and sharing of location data creates a serious safety risk, particularly for survivors of intimate partner violence, sexual assault, and gender-based violence. The National Network to End Domestic Violence (NNEDV) advises survivors who are concerned they may be tracked to consider leaving

---

[4] 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.

[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] Katie Lobosco, *Facebook friends could change your credit score*, CNN.com (August 27, 2013) http://money.cnn.com/2013/08/26/technology/social/facebook-credit-score/index.html;
Matt Vasilogambros, *Will Your Facebook Friends Make You a Credit Risk?* The Atlantic (August 7, 2015), https://www.theatlantic.com/politics/archive/2015/08/will-your-facebook-friends-make-you-acredit-risk/432504/.

[7] Nizan Geslevich Packin, Social Credit: Much More Than Your Traditional Financial Credit Score Data, Forbes (Dec. 13, 2019), https://www.forbes.com/sites/nizangpackin/2019/12/13/social-credit-much-more-than-your-traditional-financial-credit-score-data/?sh=6de89d55a824.

[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] 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.

their phones behind when traveling to sensitive locations or turning their phones off altogether.[10]

The lack of an overarching privacy law to protect Marylanders has resulted in the regular collection and use of personal information without consent. Users are often unaware that using an app or technology will result in the disclosure of personal information to third parties. For example, health apps market themselves as being a cheaper, effective, and more accessible means for obtaining treatment for health conditions including mental health concerns and smoking cessation. Consumers who access these apps to help alleviate their depression, post-traumatic stress disorder, eating disorders, or other serious mental health concerns assume that these apps have confidentiality obligations similar to psychologists or doctors. Instead, these apps frequently share data for advertising or analytics with Facebook or Google without even disclosing this to users.[11]

SB 11 protects Marylanders by ensuring that companies disclose what data they are collecting and allows consumers to decide whether to opt out of having their information collected, maintained, and sold. SB 11 ensures that consumers have control over their data and the choice over how it is used.

We urge a favorable report.

Cc: Members, Finance Committee
The Honorable Susan Lee

[10] *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.

[11] Forbrukerrådet, *Out of Control* (Jan. 13, 2020) at 5-7. https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf.Kit Huckvale, et. al., *Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation*, *JAMA Netw Open.,* 2019;2(4):e192542.

APPENDIX A

CONSUMER RIGHTS UNDER SB 11

The Right of Transparency

Transparency is the first critical step – it allows consumers to make informed decisions. SB 11 will establish that, prior to collecting a consumer's information, a business must tell the consumer, generally: (1) what information it will collect; (2) how it will use the data; (3) the types of third parties it will give your information to; (4) why it will give the third parties your information; and (5) their rights (which are described below).[12] Businesses will also include the same information in their online privacy policies.[13]

The Right to Know

The consumer may also ask a business to provide specific information, twice a year, describing: (1) the specific personal information the business collected about the consumer; (2) the source of the information; (3) with whom the business shared the consumer's data; and (4) why it shared the data.[14] Businesses must provide accessible methods of making requests for this information.[15]

The Right to Delete

The most important aspect of consumer control is the right to request that their personal information be deleted. SB 11 would require businesses to honor consumer requests to delete personal information the business collected about them.[16] It makes ample exceptions, to allow businesses to keep information for research purposes, and where required by law.[17]

The Right to Opt Out of Sale/Third Party Disclosure

In some cases consumers will not choose to be fully forgotten, where they may still seek services from the business that collected their information. There is a lesser step they can take to protect themselves – they can exercise the right to not be sold. Exercising this right means that the business that collected a consumer's information can maintain it, but cannot share it with third parties.[18] Consumers will be able to exercise this right via a clear and conspicuous link on the business' website.[19]

The bill provides further protection to minors, barring businesses from disclosing their information to third parties.[20]

The Right of Non-Discrimination

[12] Section 14-4202.
[13] Section 14-4204(d).
[14] Section 14-4203.
[15] Section 14-4204.
[16] Section 14-4205.
[17] Section 14-4205(d).
[18] Section 14-4206.
[19] Section 14-4206(d).
[20] Section 14-4206(b).

The bill takes an important step – it bans discrimination against anyone who exercises one of the above-described rights.[21] That is critically important, because if a business could deny service or charge different prices based on a consumer exercising their rights, it would render the protections meaningless.

The Bill Still Allows a Wide Berth for Use of Consumer Data for Research Purposes

This bill does not impede the ability of businesses to use personal information for research purposes for the public good. It allows a business to ignore a consumer's request to delete information if keeping the information is necessary to engage in public or peer-reviewed scientific, historical, or statistical research in the public interest.[22]

The Businesses Impacted by SB 11 Comply with Similar Requirements in Other Statutory Schemes

SB 11 has revenue and population threshold minimums. Only businesses that have an annual gross revenue of over $25 million; annually buy, receive, or share the personal information of 100,000 or more consumers; or derive at least half of their annual revenue from selling consumer personal information are required to comply with SB 11.[23] Moreover, the impact of SB 11 is further limited as many companies that meet these thresholds already comply with the California Consumer Privacy Act ("CCPA") which went into effect in January 2020.[24] And some companies have decided to implement those protections nationwide. To the extent that there are Maryland businesses that meet the thresholds, but presently have no compliance requirements under the CCPA, we have been unable to identify them. Repeated requests for information regarding any relevant businesses have produced no response from industry.

Definition of Consumer

SB 11 defines "consumer" as "an individual who resides in the state."[25] This is broader than other consumer protection statutes to accommodate the way in which companies collect and intermingle data. Because apps and other technology collect data constantly, the data of a sole proprietor of a small business will be collected, collated, processed, shared, and sold without distinguishing between their personal and business capacity. Technology does not distinguish between their dual roles in the collection of personal information, therefore the statute must protect the individual's privacy as a whole.

Exemptions

SB 11 incorporates several exemptions, including for personal information collected pursuant to the federal Gramm-Leach-Bliley Act ("GLBA") and implementing regulations.[26] The exemption focuses on the information, rather than the entity that is covered by the GLBA because not all information collected by financial institutions is governed by the GLBA. For example, the

[21] Section 14-4207.
[22] Section 14-4205(d)(5); *see also* Section 14-4209 (requiring privacy and security protections for personal information used for research purposes).
[23] Section 14-4201(d).
[24] Businesses that operate in Europe also comply with the General Data Protection Regulation ("GDPR") which limits the collection and use of personal information through an opt-in regime, rather than an opt-out structure like that of SB 11 and the CCPA.
[25] Section 14-4201(g).
[26] Section 14-4208(b)(8).

GLBA does not apply when a financial institution collects information from an individual who is not applying for a financial product, such as the data that is collected from a person who visits a financial institution's website who does not have and is not seeking a relationship with the institution. The existing language addresses this gap. To the extent that the activities of a financial institution are covered by the GLBA or other laws, SB 11 does not alter those regulations. Financial institutions have the same obligation to protect personal information under the California Consumer Privacy Act.[27]

[27] Cal. Civ. Code §§ 1798.100-199.

SB0011_Irene Ly, Common Sense Media, Fav Written T

Uploaded by: Irene Ly

Position: FAV

Written Testimony of Irene Ly

Policy Counsel, Common Sense Media

Before the Maryland Senate Finance Committee on

"Maryland Online Consumer Protection and Child Safety Act"

Bill No: SB0011

Position: Favorable

January 26, 2022

My name is Irene Ly, and I am a Policy Counsel for Common Sense Media, where I work on privacy and platform accountability issues. Common Sense 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 harness the power of media and technology as a positive force in all kids' lives. That work often revolves around ensuring children and families' privacy as they interact with devices and corporate interests that are eager to collect, sell, and share their information, often in ways children and parents do not expect or understand.

My testimony will focus on the harms of surveillance advertising, which is powered by data, and how children and teens are uniquely vulnerable to this kind of advertising, necessitating a privacy law that protects these groups.

I. The Harms of Surveillance Advertising

Surveillance advertising, also known as behavioral advertising, is a practice in which companies micro-target advertisements to consumers through inferences about their interests and demographics based on data they have collected from tracking them over time.[1] It can rely on web browsing behavior such as the pages visited, searches performed, and links clicked. Users can interact with these ads in a variety of places, from the internet generally, to social media platforms, user-created content, video games, mobile apps, virtual or augmented reality, virtual assistants, and internet-connected toys.

Online platforms no longer display information chronologically by default as they used to. Companies use algorithms that amplify certain content they think will be of interest to the user

[1] Susan Grant, Factsheet: Surveillance Advertising: What is it?, Consumer Federation of America (Aug. 26, 2021).

based on inferences from their data in an effort to get them to spend more time and engage more on their platforms. In the case of social media platforms like Instagram and TikTok, this curates a specific feed of content for each user based on what they have been looking at and interacting with.

However, these algorithms often amplify harmful content for users to see. Users can look at seemingly innocuous content such as healthy eating content, then quickly be led down a rabbit hole that escalates to receiving content promoting eating disorders, self-harm, and suicide ideation. For example, after watching one video by a fitness influencer on TikTok and following her, a teen user named Lauren started receiving a lot of the same pages.[2] She stopped seeing funny dance videos and other fun content, and her feed became dominated by content focused on keeping up a so-called "healthy" lifestyle that pushed her to the viral trend of meticulously tracking how many calories they eat.[3] She stated she had previously never had many negative thoughts about her body, until she started seeing videos of people saying they hated their body, and would cry about it every night.[4] Four months later, she was diagnosed with an eating disorder.[5] She is not alone, and many others have been led down this same path.[6]

The speed at which this harmful content can show up and take over someone's feed is alarmingly quick. Within a day of U.S. Senator Richard Blumenthal's office creating a fake Instagram account for a 13-year-old girl and following accounts with disordered eating and dieting content, the platform began serving endless content promoting eating disorders and self-harm.[7] It also only took the office one minute to find TikTok videos promoting illegal steroids.[8]

Seeing harmful content that is amplified by these algorithms is taking a toll on kids' and teens' mental health, escalating into what the U.S. Surgeon General and many other medical and psychological professionals have called a mental health crisis.[9] Teens have shown a two percent increase in depressive symptoms for every increased hour they spent using social media.[10] Facebook's own internal research, which whistleblower Frances Haugen leaked in fall 2021, found that teens blamed Instagram for increases in the rate of anxiety and depression, and that

---

[2] Avani Dias et. al, The TikTok spiral, ABC News Australia (Jul. 25, 2021).
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] Protecting Kids Online: Snapchat, TikTok, and YouTube: Hearing Before the Subcommittee on Consumer Protection, Product Safety, and Data Security, Oct. 26, 2021 (Statement of Richard Blumenthal); s*ee 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)
[8] *Id.*
[9] Press Release, U.S. Surgeon General Issues Advisory on Youth Mental Health Crisis Further Exposed by COVID-19 Pandemic, U.S. Department of Health & Human Services (Dec. 7, 2021).
[10] Boers E, Afzali MH, Newton N, Conrod P. Association of Screen Time and Depression in Adolescence. *JAMA Pediatr*. 2019;173(9):853-859. doi:10.1001/jamapediatrics.2019.1759.

Instagram made body image issues worse for one in three teen girls.[11] The same research showed that among teens who reported suicidal thoughts, 13 percent of British users and six percent of American users traced the desire to commit suicide to Instagram.[12] Other studies have found similar disturbing results. In one study, young women showed decreased body satisfaction, decreased positive affect, and increased negative affect after browsing Instagram for just seven minutes, compared to those who browsed Facebook or played a simple video game for the same amount of time.[13]

The harm from surveillance advertising reaches a large audience too. More and more children are using social media, and starting at increasingly younger ages. About one-third of 7- to 9-year olds and almost half of 10- to 12-year old children use social media apps.[14] Ninety percent of teens ages 13 to 17 have used social media.[15]

Platforms know the harms these algorithms inflict on large numbers of kids and teens, and they are acting intentionally. In 2017, a Facebook internal report was leaked that showed Facebook boasting to advertisers that they have the capacity to monitor posts and photos in real time to identify the exact moment in which teenagers feel "insecure," "worthless," and "in need [of] a confidence boost," amongst other negative emotions.[16] This enabled them to attack kids with ads at the exact moments they were feeling most vulnerable and thus most likely to fall prey to commercial manipulation. Although Facebook announced it was restricting ad targeting to teens under 18 in July 2021,[17] the Tech Transparency Project found in experiments that September that the platform was still approving advertisements that promote harmful content to teens, in as little as less than an hour.[18]

II. Children and teens are uniquely vulnerable to being manipulated and harmed by surveillance advertising

Surveillance advertising is particularly harmful to kids and teens because of their unique vulnerabilities that make them easier to manipulate. This practice's method of tracking and profiling consumers exploits the vulnerable, developing brains of kids and teens, constrains and

---

[11] Georgia Wells, Jeff Horwitz, Deepa Seetharaman, "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show," *The Wall Street Journal*, (September 14, 2021).
[12] *Id.*
[13] Engeln R, Loach R, Imundo MN, Zola A. "Compared to Facebook, Instagram use causes more appearance comparison and lower body satisfaction in college women," *Body Image*. 2020; 34:38-45. https://doi.org/10.1016/j.bodyim.2020.04.007.
[14] University of Michigan School of Medicine, National Poll: 1/3 of children ages 7-9 use social media apps, American Association for the Advancement of Science (Oct. 18, 2021).
[15] Facts for Families: Social Media and Teens, American Academy of Child & Adolescent Psychiatry (Mar. 2018).
[16] Sean Levin, Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless', The Guardian (May 1, 2017).
[17] Giving Younger People a Safer, More Private Experience on Instagram, Facebook Newsroom (Jul. 27, 2021).
[18] Facebook's repeat fail on harmful teen ads, Tech Transparency Project (Oct. 1, 2021).

shape their choices and autonomy, and can perpetuate racial, gender, and socioeconomic discrimination.[19]

Kids and teens are largely defenseless against advanced advertising techniques. Most children younger than 8 years old cannot identify ads.[20] Over 75 percent of 8- to 11-year olds still cannot distinguish ads from other content, or understand the persuasive intent behind them.[21] This makes kids more prone to accepting advertiser messages as being truthful, accurate, and unbiased.[22] Most children do not know that ads can be customized to each individual either.[23] Researchers have concluded that children are not equipped to identify targeted ads that exploit their tracked activity data from traditional advertising.[24]

This enables marketers to create profiles of a child or teen's interests and fine-tune sales pitches to these impressionable groups without them even understanding that they are looking at ads. Even when kids and teens can recognize advertising, they are often not able to resist it due to their immature and developing critical thinking skills and impulse inhibition, especially when it is embedded within trusted social networks, encouraged by celebrity influencers, or delivered next to personalized content.[25] This is particularly problematic for kids and teens, because evidence suggests that exposure to advertising is associated with unhealthy behaviors, such as consumption of high-calorie, low-nutrient food and beverages, use of tobacco products and electronic cigarettes, use of alcohol and marijuana, and indoor tanning.[26]

Kids and teens also do not want or like surveillance ads.[27] They express negative attitudes about data collection and sharing, especially when this data is collected and shared surreptitiously, and dislike when apps can monitor or collect private information about them.[28] Parents do not want their kids to receive these ads either, with 88 percent of parents believing

---

[19] *See* Common Sense Media, AdTech and Kids: Behavioral Ads Need a Time Out (May 13, 2021).
[20] Zhao, J., Wang, G., Dally, C., Slovak, P., Childs, J. E., Van Kleek, M., & Shadbolt, N. (May 2019). "I make up a silly name": Understanding children's perception of privacy risks online. CHI Conference on Human Factorsin Computing Systems Proceedings 2019, p. 2.
[21] Ofcom. Children and Parents: Media Use and Attitudes Report 2017 (Nov. 29, 2017).
[22] American Psychological Association. Advertising leads to unhealthy habits in children; says APA task force. [Press release] (Feb. 23, 2004).
[23] 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.
[24] Zhao et. al *supra* note 20.
[25]Jenny Radesky, Yolanda (Linda) Reid Chassiakos, Nusheen Ameenuddin, Dipesh Navsaria, Council on Communications and Media; Digital Advertising to Children. *Pediatrics* July 2020; 146 (1): e20201681. 10.1542/peds.2020-1681.
[26] *Id.*
[27] *Id.*
[28] Sun et. al *supra* note 23.

that the practice of tracking and targeting kids with ads based on their data should be prohibited.[29]

The profiling of surveillance advertising can harm kids' and teens' development and constrain and shape their choices and autonomy. Kids are encouraged by society to explore new things and not worry about making mistakes during childhood. And yet, surveillance advertising's constant profiling and targeting of kids does a disservice to them by potentially labeling and limiting them from a very young age.[30] Kids should be exploring a range of interests, yet based on their behavior, they may be profiled as gamers, impulsive purchasers, or anxious oversharers, then unfairly targeted by ads that encourage more of these behaviors.[31] This profiling can also make kids hold themselves back, with kids who know they are being monitored by surveillance technology less likely to engage in critical thinking, political activity, or questioning of authority.[32] Knowing they receive targeted ads can chill their expression too, out of fear these ads could expose aspects of their lives they want to keep secret or share on their own terms, such as through ads involving sex, drugs, or professional interests.[33] For example, ads for LGBTQ+ resources showing up on a shared device could out a child instead of giving them the autonomy to do so on their own accord.[34]

Finally, surveillance advertising can perpetuate discrimination towards kids, teens, and adults alike. Businesses can constrain kids' and teens' choices and autonomy by utilizing coercive techniques that only show them certain opportunities and algorithmic profiling that builds in bias in decision making, such as when to admit students into educational programs.[35] This can disadvantage kids by restricting the number of opportunities they receive or even see, based on characteristics like their race or ethnicity, socioeconomic status, or location.

One clear example of how surveillance advertising can be used to perpetuate discrimination is seen with Naviance, a software that nearly two-thirds of American high schoolers use in the college application process to learn information about colleges and see which is a good fit for them.[36] Naviance allows admissions officials to select what kinds of students will see their recruiting messages based on factors like the students' location, academic credentials, the majors they are interested in, and most concerningly, their race.[37] TheMarkup found that one university deliberately advertised only to white students on Naviance, and many other schools targeted

---

[29] Accountable Tech, 2021 Accountable Tech Frequency Questionnaire 2021 (Jan. 28, 2021).
[30] Common Sense Media *supra* note 19.
[31] *Id.*
[32] Brown, D. H., & Pecora, N. (2014). Online data privacy as a children's media right: Toward global policy principles. Journal of Children and Media, 8(2), 201–207.
[33] Common Sense Media *supra* note 19.
[34] *Id.*
[35] *Id.*
[36] Todd Feathers, College prep software Naviance is selling advertising access to millions of students, The Markup (Jan. 13, 2022).
[37] *Id.*

students of all races in some states but only white students in other states.[38] Although students can receive messages on Naviance about schools that may be a good fit for them, some of those messages are advertisements the schools paid for.[39] This kind of social engineering can, at worst, close teens off from having access to viewing certain educational opportunities at all, and at best, make them more likely to constrain themselves and believe a school is not a good fit for them.

Surveillance advertising's harmful effects can be inflicted and felt by anyone, including adults. However, kids' and teens' unique vulnerabilities makes them even more susceptible to this advertising practice. Despite the many harms surveillance advertising imposes, it is also not significantly more profitable than other advertising practices,[40] such as contextual advertising, which involves placing advertisements based on the content of the web page the user is on.[41]

III. Enacting a strong privacy law that protects kids and teens cuts off businesses' access to data, which will weaken the power of these algorithms

Surveillance advertising is made possible by the troves of data businesses collect from tracking users. Kids today have the largest data footprints in history. In 2017, adtech company SuperAwesome reported that companies have an average of 72 million data points for a 13-year-old, all gathered "unintentionally" through adult-oriented adtech.[42]

In the absence of a ban on surveillance advertising, the most effective way to weaken the power and impact of this advertising, particularly to kids and teens, is to pass a strong privacy law that protects users' data privacy and prohibits certain data collection. This cuts off at least some of the access to data businesses need for their algorithms to target ads to users. Then, platforms like Instagram and Facebook could not disclose data on kids and teens to third-party advertisers to target their ads. For example, it would prevent another situation like the one in which Instagram allowed one of its preferred marketing partners, HYP3R, to flout its privacy rules and scrape as many as one million posts a month from millions of public users' profiles in 2019, including Instagram stories that are meant to disappear after 24 hours.[43]

The Maryland Online Consumer Protection and Child Safety Act would allow a consumer to opt out of third party disclosure at any time, and prohibit businesses from disclosing the personal information of a consumer to a third party if the business has actual knowledge or willfully

---

[38] *Id.*
[39] *Id.*
[40] Keach Hagey, Behavioral ad targeting not paying for publishers, study suggests, The Wall Street Journal (May 29, 2019).
[41] *See* Jessica Davies, After GDPR, The New York Times cut off ad exchange in Europe – and kept growing ad revenue, Digiday (Jan. 16, 2019).
[42] Ad Tech collects 72 million data points on the average American child by age 13, VideoWeek (Dec. 14, 2017).
[43] Devin Coldeway, Instagram ad partner secretly sucked up and tracked millions of users' locations and stories, TechCrunch (Aug. 7, 2019).

disregards the fact that the consumer is under 16 years old. This would provide protection to teens 13-15 years old who are currently not protected under the federal Children's Online Privacy Protection Act (COPPA), and consistent with the proposed amendments to COPPA some legislators are pushing and advocacy organizations like Common Sense hope to see passed. If this bill were passed, Maryland kids' and teens' data would be better protected and the impact of surveillance advertising on them could be significantly weakened.

IV. Conclusion

Children and teens' unique vulnerabilities make them particularly easy to be manipulated and harmed by surveillance advertising. Cutting off companies' access to data on these groups, as this bill would do, is a necessary step to weakening the harm surveillance advertising can inflict on kids and teens and better protect them online. Thank you Senator Lee for your work on this bill.

JNM1_MD_SB11_WrittenTestimony_DrJeannaMatthews_202
Uploaded by: Jeanna Matthews
Position: FAV

January 23, 2022

I am writing in support of Maryland Senate Bill SB11, the Maryland Online Consumer Protection and Child Safety Act. I also plan to offer oral testimony to the Maryland Senate Finance Committee on January 26, 2022.

I am a Professor of Computer Science at Clarkson University in Potsdam, New York with a Ph.D. in Computer Science from University of California Berkeley. I am also co-chair of the IEEE-USA AI Policy Committee and a member of the ACM US Technology Policy Committee (ACM US-TPC) and a co-chair of their AI and Algorithms Subcommittee.

I am providing copies of 4 documents relevant to this bill.

- An article I wrote that appears in The Conversation on January 12, 2022, "**Radicalization pipelines: How targeted advertising on social media drives people to extremes** "
- The IEEE-USA Policy Statement "**Privacy, Equity, and Justice in Artificial Intelligence",** adopted by the IEEE-USA Board of Directors in November 2021.
- The IEEE-USA Policy Statement "**Democratic Use of Artificial Intelligence",** adopted by the IEEE-USA Board of Directors in November 2021.
- A policy statement issued by the ACM US-TPC in January 2017, "**Statement on Algorithmic Transparency and Accountability**"

I congratulate the Maryland Senate for working to protect the rights of Marylanders with SB 11. This is an important and difficult policy area and I commend you for rising to the challenge. Through this bill Maryland has an opportunity to take a leadership role in the national debate over data privacy protections. As is stated in the IEEE USA Policy Statement "**Privacy, Equity, and Justice in Artificial Intelligence"**, "Equitable AI practices require a clear legislative framework for data ownership, confidentiality of data, and rights of access to data used in and by AI systems--essential to protecting privacy and autonomy. Moreover, *the absence of a comprehensive data protection law at the federal level in the U.S. is a missed opportunity for the U.S. to globally shape and address data rights, practices, and privacy*."

IEEE-USA recommends policies that enact clear and comprehensive data protection laws, establish data collection and data use limitations, contain data quality standards and security safeguards, require clearer notice of data collection practices with truly effective opportunities to consent (or not) to such data collection, and mandate transparency and user control in use of individual data.

I would like to comment especially on the aspects of de-identification, re-identification, and pseudonymization mentioned in SB 11. Many people are surprised to realize the degree to which seemingly anonymous data can be linked to them personally. For example, if an application or web service is capable of tracking someone's location over time, then it is usually possible to uniquely

Jeanna Matthews, Professor, Department of Computer Science
Clarkson University • PO Box 5815 • Potsdam, NY 13699-5815
315-268-6288 • Fax 315-268-2371 • e-mail jnm@clarkson.edu

identify that person even without direct personal information like name or phone number. Simple algorithms systems can conclude that a person's most frequent location at night is likely their home and their most frequent location during the day is likely their work. The combination of where you live together with where you work can be enough to uniquely identify you from publicly available data sources. More sophisticated algorithms can use additional seemingly anonymous location data, including whether you frequent a gym, have regular medical appointments, the location of your children's school and more to draw a frighteningly accurate picture of you and your family. In addition, the mobility patterns for people are highly predictable so with past location data is possible to predict where you will be an hour from now with a high degree of accuracy.

I recommend that you use SB 11 as opportunity to provide increased protections for the citizens of Maryland from intrusive data collection and an opportunity to influence the strengthening of protections at the federal level.

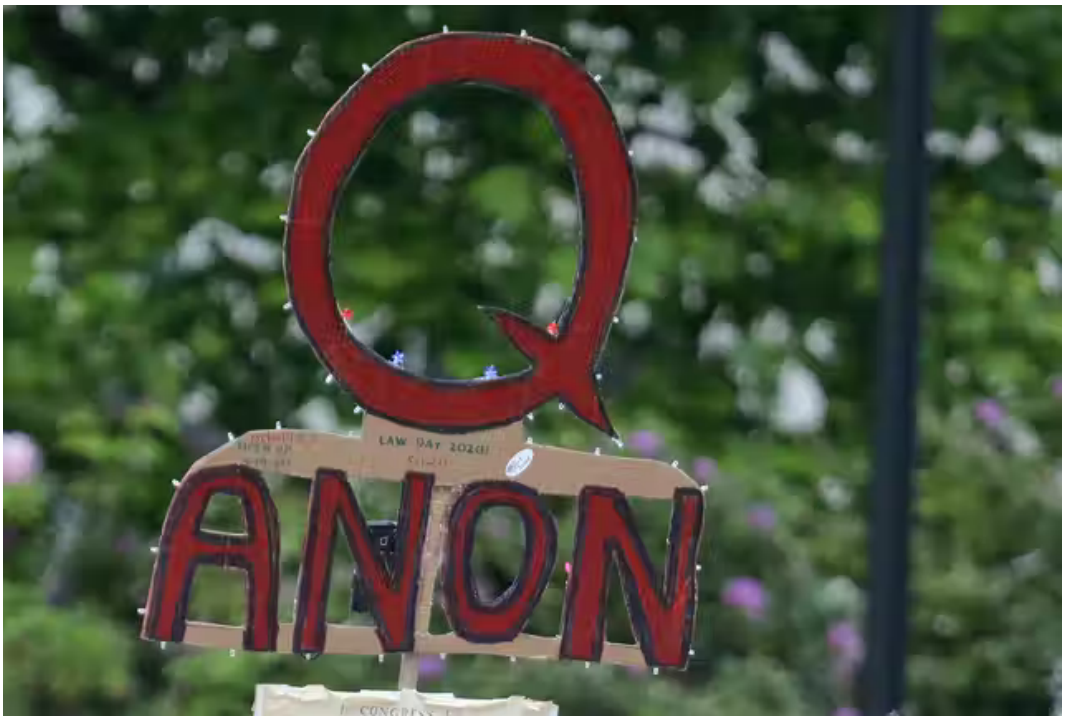
I am honored to have the opportunity to provide input to the Maryland Senate in their deliberations of this important bill

Dr. Jeanna Matthews
Professor of Computer Science, Clarkson University
IEEE USA AI Policy Committee, Co-Chair
ACM Technology Policy Council, ACM US Technology Policy Committee, AI and Algorithms Subcommittee Co-Chair

JNM2_JeannaMatthews_TheConversation_Radicalization
Uploaded by: Jeanna Matthews
Position: FAV

THE CONVERSATION

Academic rigor, journalistic flair



Many people are led to conspiracy theories and extremist views from less extreme positions. AP Photo/Ted S. Warren

Radicalization pipelines: How targeted advertising on social media drives people to extremes

January 12, 2022 8.37am EST

Jeanna Matthews

Professor of Computer Science, Clarkson University

Have you had the experience of looking at some product online and then seeing ads for it all over your social media feed? Far from coincidence, these instances of eerily accurate advertising provide glimpses into the behind-the-scenes mechanisms that feed an item you search for on Google, "like" on social media or come across while browsing into custom advertising on social media.

Those mechanisms are increasingly being used for more nefarious purposes than aggressive advertising. The threat is in how this targeted advertising interacts with today's extremely divisive political landscape. As a social media researcher, I see how people seeking to radicalize others use targeted advertising to readily move people to extreme views.

Advertising to an audience of one

Advertising is clearly powerful. The right ad campaign can help shape or create demand for a new product or rehabilitate the image of an older product or even of an entire company or brand. Political campaigns use similar strategies to push candidates and ideas, and historically countries have used them to wage propaganda wars.

Advertising in mass media is powerful, but mass media has a built-in moderating force. When trying to move many people in one direction, mass media can only move them as fast as the middle will tolerate. If it moves too far or too fast, people in the middle may be alienated.

The detailed profiles the social media companies build for each of their users make advertising even more powerful by enabling advertisers to tailor their messages to individuals. These profiles often include the size and value of your home, what year you bought your car, whether you're expecting a child, and whether you buy a lot of beer.

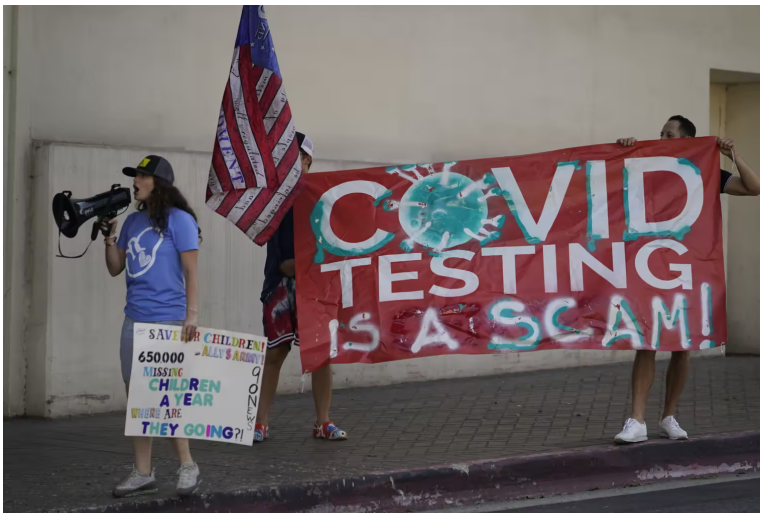
Consequently, social media has a greater ability to expose people to ideas as fast as they individually will accept them. The same mechanisms that can recommend a niche consumer product to just the right person or suggest an addictive substance just when someone is most vulnerable can also suggest an extreme conspiracy theory just when a person is ready to consider it.

It is increasingly common for friends and family to find themselves on opposite sides of highly polarized debates about important issues. Many people recognize social media as part of the problem, but how are these powerful customized advertising techniques contributing to the divisive political landscape?

Breadcrumbs to the extreme

One important part of the answer is that people associated with foreign governments, without admitting who they are, take extreme positions in social media posts with the deliberate goal of sparking division and conflict. These extreme posts take advantage of the social media algorithms, which are designed to heighten engagement, meaning they reward content that provokes a response.

Another important part of the answer is that people seeking to radicalize others lay out trails of breadcrumbs to more and more extreme positions.



Many people feel that they have 'figured out' conspiracy theories for themselves, but in many cases they've been deliberately led to them. AP Photo/Damian Dovarganes

These social media radicalization pipelines work much the same way whether recruiting jihadists or Jan. 6 insurrectionists.

You may feel like you're "doing your own research," moving from source to source, but you are really following a deliberate radicalization pipeline that's designed to move you toward more and more extreme content at whatever pace you will tolerate. For example, after analyzing over 72 million user comments on over 330,000 videos posted on 349 YouTube channels, researchers found that users consistently migrated from milder to more extreme content.

The result of these radicalization pipelines is apparent. Rather than most people having moderate views with fewer people holding extreme views, fewer and fewer people are in the middle.

How to protect yourself

What can you do? First, I recommend a huge dose of skepticism about social media recommendations. Most people have gone to social media looking for something in particular and then found themselves looking up from their phones an hour or more later having little idea how or why they read or watched what they just did. It is designed to be addictive.

I've been trying to chart a more deliberate path to the information I want and actively trying to avoid just clicking on whatever is recommended to me. If I do read or watch what is suggested, I ask myself "How might this information be in someone else's best interest, not mine?"

[*Over 140,000 readers rely on The Conversation's newsletters to understand the world.* Sign up today.]

Second, consider supporting efforts to require social media platforms to offer users a choice of algorithms for recommendations and feed curation, including ones based on simple-to-explain rules.

Third, and most important, I recommend investing more time in interacting with friends and family off of social media. If I find myself needing to forward a link to make a point, I treat that as a warning bell that I do not actually understand the issue well enough myself. If so, perhaps I have found myself following a constructed trail toward extreme content rather than consuming materials that are actually helping me better understand the world.

Editor's note: The Conversation has replaced the lead image of this story to avoid associating any particular political viewpoint with conspiracy theorists.

JNM3_IEEEUSA_202111_Privacy_Equity_ Justice.pdf
Uploaded by: Jeanna Matthews
Position: FAV

IEEE-USA

POSITION STATEMENT

Privacy, Equity, and Justice in Artificial Intelligence

Adopted by the IEEE-USA
Board of Directors (November 2021)

AI's ubiquitous presence in society has challenged our ability to protect privacy and ensure equity and justice. The foundational principles below provide a legal, technical, and policy framework to address these challenges going forward and resolve problems embedded in existing AI uses and systems, such as when AI systems are trained with past data embedded with patterns of inequality and human bias. Building this framework requires updating, harmonizing, and streamlining federal laws, policies, and guidelines as follows:

1. Data ownership, data rights, and privacy

Equitable AI practices require a clear legislative framework for data ownership, confidentiality of data, and rights of access to data used in and by AI systems--essential to protecting privacy and autonomy. Moreover, *the absence of a comprehensive data protection law at the federal level in the U.S. is a missed opportunity for the U.S. to globally shape and address data rights, practices, and privacy.* The current patchwork of federal and state laws lacks coherence and is insufficient.[1]

- ***Enact clear and comprehensive data protection law(s) at the federal level*** Internet and other communication-related platforms, apps, and devices routinely collect or infer health, financial, and biometric information without user knowledge, control, or consent. The U.S. sectoral approach to data regulation leaves vast swaths of individuals' intimate data unprotected and fails to provide a clear framework of permissible operation for AI

[1] Our current federal and state patchwork of data laws lends to confusion and inefficiencies and precludes the U.S. from shaping private and government sector data practices on a national and international level. At the federal level, there is a sectoral-based approach to data regulation by both public and private sectors (e.g., health – Health Insurance Portability and Accountability Act; and financial – Gramm-Leach-Bliley Act). Given current data collection practices (communication platforms, apps, and devices routinely collect health, financial, and biometric data, and PII), the existing sectoral approach leaves vast swaths of individuals' intimate data unprotected in the current federal legislative scheme. At the state level, all 50 states have passed varying forms of data breach laws and a myriad of states have enacted comprehensive data regulation and biometric laws, such as the California Consumer Privacy Act (CCPA) and the Illinois Biometric Information Privacy Act. California, via CCPA, and the European Union's General Data Protection Regulation Act (GDPR) both provide legislative frameworks that have altered private sector data practices on a global scale.

systems and their operators, leading to inefficiencies and confusion. Comprehensive data regulation through legislative action should incorporate principles like Fair Information Practice Principles (FIPPs) that:

- **Establish data collection and data use limitations, data quality standards, and security safeguards.**
- **Require clearer notice of data collection practices with truly effective opportunities to consent (or not) to such data collection.**
- **Mandate transparency and user control in use of individual data**. Consumers are often unaware of how their data is collected and used; long, complex Terms of Use and privacy policies obscure actual data practices. Mandate that users have the right to access, review, store, and delete personal user data, including behavioral data used for tracking and AI recommendation systems, and require an option to opt-out of tracking.

2. **Mitigate disparate impacts of AI**

When AI systems are developed and deployed, objectives of accuracy and lack of algorithmic bias towards marginalized or vulnerable groups can conflict, resulting in disparate impacts and lack of public confidence. To mitigate, objectives must be balanced by means that require clarity, transparency, and protection of all stakeholders.

- ***Establish and mandate metrics and standards.*** AI systems and their operators must comply with standards for fairness, privacy, safety, and security.
- ***Establish transparency mechanisms for stakeholders.*** For example, require third-party access to data in standardized, machine-readable format.
- ***Create research investments on how the use of algorithms may disparately impact or disadvantage certain individuals and groups.***

3. **Ongoing verification and validation of AI systems**

Increasingly, AI systems directly impact human life, individual rights and societal well-being and, like other systems that do so, must be evaluated throughout their lifecycle, i.e., design, implementation, and deployment. When AI systems are deployed in critical applications such as employment, credit/finance, criminal justice, health systems, and allocation of public resources:

- ***Require transparency about the training data and other developmental inputs.***
- ***Require mechanisms for (and permit) independent verification and validation***.

4. **Redress**

When AI systems make life-impacting decisions, preserving privacy, equity, and justice requires that individuals be informed about, and permitted to, question decisions and have access to systems that enable redress.

- **Define pathways for all stakeholders to report problems, question results, provide additional information relevant to automated decision making, and receive redress when they are harmed.**
- **Define pathways for individuals to review, verify and question input data about them as individuals.**

- **Require human teams be tasked to investigate errors with clear pathways for stakeholders to communicate with teams and require timely response.**
- **Require systems to produce explanations of their output that can be examined by human decision makers and other stakeholders.**
- **Provide clear statutory culpability and means of civil redress for entities in the AI supply chain responsible for harm to individuals, groups, or the environment.**

5. Baseline Standards for Platform Governance

AI systems are ubiquitous, and access to and use of online platforms is a requirement to be an effective citizen of the modern world (education, taxes, banking - all require online participation with platforms, devices, and apps that operate with and rely upon AI systems). **To protect both domestic and national security interests and the constitutional rights (speech and privacy) of users**, baseline standards should be created for: verification procedures for account creation; when accounts can or should be removed or deactivated for a period of time; and when content can or should be removed or labeled with warnings

6. Anti-Manipulation

When AI systems are built with detailed, fine-grained information about individuals, they can use this information to deliver customized suggestions to individuals. Without limitations, microtargeting and behavioral advertising can permit and enable manipulation outside a user's awareness and explicit control (e.g., *delivering a suggestion* for unhealthy food or addictive substances or conspiracy theories *exactly when a person is vulnerable to them*), thus, enabling systems or human operators to exploit, manipulate, and radicalize others. *Subtle-to-the-user practices have huge societal impacts*, e.g., voting misinformation and voting messaging (how "my friends" voted) sways elections; having an autoplay feature in YouTube (enables seamless radicalization of viewers). Legislation to mitigate such effects would:

- ***Require clear information about why a suggestion is being offered to an individual and about who is paying to deliver that suggestion.***
- ***Require disclosure of actor*** (human or AI) with whom the user is interacting.
- ***Require proactive steps to prevent harmful manipulation and abuse.***
- ***Require data and access necessary for independent research/evaluations of anti-manipulation measures.***
- ***Require verified identity for entities/persons paying for content or ad distribution.***

This statement was developed by IEEE-USA's Artificial Intelligence Policy Committee and represents the considered judgment of a group of U.S. IEEE members with expertise in the subject field. IEEE-USA advances the public good and promotes the careers and public policy interests of the nearly 150,000 engineering, computing and allied professionals who are U.S. members of IEEE. The positions taken by IEEE-USA do not necessarily reflect the views of IEEE, or its other organizational units.

JNM4_IEEEUSA_202111_Democratic use of AI.pdf
Uploaded by: Jeanna Matthews
Position: FAV

IEEE-USA

POSITION STATEMENT

Democratic Use of Artificial Intelligence

Adopted by the IEEE-USA
Board of Directors (November 2021)

IEEE-USA believes that AI systems can increase quality of life, improve government efficiency, and promote societal well-being. However, when used improperly or by malicious actors, AI systems can jeopardize human rights, violate the U.S. Constitution, create and amplify harmful mis- and disinformation, and pose severe threats to individual and collective privacy. US government action and collaboration with like-minded states can help ensure that AI systems promote rather than threaten democratic values. IEEE-USA recommends that the U.S. government:

1. **Encourage international standards, diplomacy, and agreements to uphold human rights, promote innovation and commerce, and govern AI systems and techniques.**[1] While there has been considerable progress in declarations on the ethical use of AI systems by governments, corporations, and international organizations, there is a need for an overall framework that links national and global efforts to address the use of AI in ways that support democracy. We recommend that the U.S. government:

    - Lead the development of such a framework as well as promote its use and further development among allies and like-minded nations. This can be achieved through:
        - Existing and evolving standards;
        - Diplomatic efforts;
        - Strong domestic and international intellectual property policy; and,
        - Strengthening both domestic and international agreements on the ethical uses of AI systems; as well as how data is collected, used, and retired; and,
    - Undertake and promote collaboration with companies, academics, and stakeholders in relevant technical and social scientific fields within the context of this common framework.

[1] See the IEEE-USA position statement on "Accelerating Inclusive AI Innovation by Building Trust," https://ieeeusa.org/wp-content/uploads/2021/03/AIPC_BuildingTrustInAI.pdf.

2. **Promote transparency, human agency, and accountability in AI systems to reduce the promotion of extremism, misinformation, and disinformation.** The AI systems that drive content recommendation systems used by online platforms can create echo chambers that are harmful to society. To mitigate the harmful impacts of these systems, we recommend that the U.S. government:

    - Establish clear transparency standards that allow users to understand why they were shown certain content, particularly when it may be the result of commercial or foreign entities;
    - Invest in increasing technical literacy to improve public understanding of personal information that AI systems may infer about them, and how these systems could influence their thinking; and,
    - Partner with allies and like-minded nations to establish transparent ethical guidelines for the use and accountability of AI systems that could manipulate individuals or influence public opinion so that the public can understand who is attempting to influence them and how they are doing it.

3. **Support human rights and democratic governance of AI through the rule of law and the right to privacy.** To encourage the development and implementation of AI systems that respect and further human rights, we recommend that the U.S. government:

    - Establish principles for the design and operational use of AI systems to prevent violations of human rights and the U.S. Constitution;
    - Create, where possible, accountability mechanisms for groups deploying AI systems that have the potential to violate human rights principles or the U.S. Constitution;
    - Require the disclosure of when AI and automated decision systems are used, and how their use may impact users; and,
    - Increase investments in research on the human rights impacts of AI systems.

    To ensure that AI systems used by popular online platforms promote democracy, we recommend that the U.S. government:

    - Create partnerships between government, industry, and academia to monitor the spread and impacts of mis- and disinformation, extremist content, and foreign malign influence on internet platforms, subject to appropriate legal and constitutional limitations; and,
    - Place restrictions on the personal data that foreign-operated internet platforms can collect about U.S. users, preventing anti-democratic actors from performing sophisticated microtargeting of propaganda.

To promote the democratic governance of AI systems,[2] we recommend that the U.S. government:

- Increase investment in public education about potential impacts of AI (including both its capabilities and limitations); and,
- Develop mechanisms for soliciting broad public input on the governance of AI, particularly from marginalized or vulnerable communities.

4. **Protect intellectual property (IP) from manipulation including theft, excessive patent filing, and abuse caused by incorporating patented technology into international standards.** IP policy should be recognized as a national priority with special commitment to IP policy enhancement around AI-related emerging technologies. We recommend that the U.S. government:

   - Combat any actions that would directly or indirectly negatively influence international standards settings;
   - Combat the injection of a large body of low-quality prior art that would adversely impact the United States Patent and Trademark Office; and,
   - Continue and expand efforts to counter and sanction the foreign theft of intellectual property through hacking, espionage, blackmail, and illicit technology transfer.

5. **Clarify the lines between free speech and censorship in content moderation.** Internet platforms use AI systems to select, target, and promote content. These systems often amplify content that many consider to be false or manipulative. Given the exponentially increasing quantity of content and lack of knowledge of speaker identity, individuals using these platforms are disadvantaged in verifying the accuracy of content and sources. However, actions and mechanisms to rectify these problems must be carefully balanced with the freedom of expression. Without affecting individuals' right to freedom of expression, we recommend that the U.S. government:

   - Establish guidelines for transparent content moderation policies that limit:
     - the ability to create fake accounts to promote or amplify messages at large scale;
     - the ability to spread artificially generated harmful audio, video or photographic material that appropriate or mimic real people without consent ("deepfakes"); and
     - the ability to spread messages that are factually incorrect or carefully crafted to manipulate and mislead;
   - Establish guidelines clarifying content moderator's rights and responsibilities for regulating speech that balance openness,

[2] See also the IEEE-USA position statement on "Effective Governance of AI."

transparency, and free speech with platforms' right to control their products.

- Require that AI systems, which are limited in their ability to accurately and transparently detect harmful content, not be exclusively relied upon for content moderation;
- Require that internet platforms provide, subject to appropriate privacy restrictions, the data necessary for researchers and the public to independently evaluate the extent of possible manipulation or abuse; and,
- Scale guidelines for accounts and platforms so that they increase with the size of their audiences and reach.

This statement was developed by IEEE-USA's Artificial Intelligence Policy Committee and represents the considered judgment of a group of U.S. IEEE members with expertise in the subject field. IEEE-USA advances the public good and promotes the careers and public policy interests of the nearly 150,000 engineering, computing and allied professionals who are U.S. members of IEEE. The positions taken by IEEE-USA do not necessarily reflect the views of IEEE, or its other organizational units.

JNM5_ACM_USTPC_2017_statement_algorithms.pdf
Uploaded by: Jeanna Matthews
Position: FAV

Association for Computing Machinery
US Public Policy Council (USACM)

usacm.acm.org
facebook.com/usacm
twitter.com/usacm

January 12, 2017

Statement on Algorithmic Transparency and Accountability

Computer algorithms are widely employed throughout our economy and society to make decisions that have far-reaching impacts, including their applications for education, access to credit, healthcare, and employment.[1] The ubiquity of algorithms in our everyday lives is an important reason to focus on addressing challenges associated with the design and technical aspects of algorithms and preventing bias from the onset.

An algorithm is a self-contained step-by-step set of operations that computers and other 'smart' devices carry out to perform calculation, data processing, and automated reasoning tasks. Increasingly, algorithms implement institutional decision-making based on analytics, which involves the discovery, interpretation, and communication of meaningful patterns in data. Especially valuable in areas rich with recorded information, analytics relies on the simultaneous application of statistics, computer programming, and operations research to quantify performance.

There is also growing evidence that some algorithms and analytics can be opaque, making it impossible to determine when their outputs may be biased or erroneous.

Computational models can be distorted as a result of biases contained in their input data and/or their algorithms. Decisions made by predictive algorithms can be opaque because of many factors, including technical (the algorithm may not lend itself to easy explanation), economic (the cost of providing transparency may be excessive, including the compromise of trade secrets), and social (revealing input may violate privacy expectations). Even well-engineered computer systems can result in unexplained outcomes or errors, either because they contain bugs or because the conditions of their use changes, invalidating assumptions on which the original analytics were based.

The use of algorithms for automated decision-making about individuals can result in harmful discrimination. Policymakers should hold institutions using analytics to the same standards as institutions where humans have traditionally made decisions and developers should plan and architect analytical systems to adhere to those standards when algorithms are used to make automated decisions or as input to decisions made by people.

This set of principles, consistent with the ACM Code of Ethics, is intended to support the benefits of algorithmic decision-making while addressing these concerns. These principles should be addressed during every phase of system development and deployment to the extent necessary to minimize potential harms while realizing the benefits of algorithmic decision-making.

[1] Federal Trade Commission. “Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues.” January 2016. https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report.

Principles for Algorithmic Transparency and Accountability

1. Awareness: Owners, designers, builders, users, and other stakeholders of analytic systems should be aware of the possible biases involved in their design, implementation, and use and the potential harm that biases can cause to individuals and society.

2. Access and redress: Regulators should encourage the adoption of mechanisms that enable questioning and redress for individuals and groups that are adversely affected by algorithmically informed decisions.

3. Accountability: Institutions should be held responsible for decisions made by the algorithms that they use, even if it is not feasible to explain in detail how the algorithms produce their results.

4. Explanation: Systems and institutions that use algorithmic decision-making are encouraged to produce explanations regarding both the procedures followed by the algorithm and the specific decisions that are made. This is particularly important in public policy contexts.

5. Data Provenance: A description of the way in which the training data was collected should be maintained by the builders of the algorithms, accompanied by an exploration of the potential biases induced by the human or algorithmic data-gathering process. Public scrutiny of the data provides maximum opportunity for corrections. However, concerns over privacy, protecting trade secrets, or revelation of analytics that might allow malicious actors to game the system can justify restricting access to qualified and authorized individuals.

6. Auditability: Models, algorithms, data, and decisions should be recorded so that they can be audited in cases where harm is suspected.

7. Validation and Testing: Institutions should use rigorous methods to validate their models and document those methods and results. In particular, they should routinely perform tests to assess and determine whether the model generates discriminatory harm. Institutions are encouraged to make the results of such tests public.

SB 11 Consumer Reports fav.pdf
Uploaded by: Maureen Mahoney
Position: FAV

January 24, 2022

The Honorable Delores G. Kelley, Chair
Maryland Senate Finance Committee
Miller Senate Office Building, 3 East Wing
11 Bladen Street
Annapolis, MD 21401-1991

Re: SB 11, Maryland Online Consumer Protection and Child Safety Act — FAVORABLE

Dear Chair Kelley,

Consumer Reports[1] writes in support of the Maryland Online Consumer Protection and Child Safety Act (SB 11), which outlines a strong framework to protect consumer privacy. Though consumers in Europe and California enjoy baseline privacy protections, Maryland residents currently do not have similar basic privacy rights. SB 11 would address this by extending to Maryland consumers the right to access, delete, and stop the sale of their personal information, including through a global opt out.

These protections are long overdue: consumers are constantly tracked, and information about their online and offline activities are combined to provide detailed insights into a consumers' most personal characteristics, including health conditions, political affiliations, and sexual preferences. This information is sold as a matter of course, is used to deliver targeted advertising, facilitates differential pricing, and enables opaque algorithmic scoring—all of which can lead to disparate outcomes along racial and ethnic lines.

Privacy laws should set strong limits on the data that companies can collect and share so that consumers can use online services or apps safely without having to take any action, such as opting in or opting out. We recommend including a strong data minimization requirement that limits data collection and sharing to what is reasonably necessary to provide the service

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

requested by the consumer, as outlined in our model bill.[2] A strong default prohibition on data sharing is preferable to an opt-out based regime which relies on users to hunt down and navigate divergent opt-out processes for potentially thousands of different companies. Consumer Reports has documented that some California Consumer Privacy Act (CCPA) opt-out processes are so onerous that they have the effect of preventing consumers from stopping the sale of their information.[3]

But in the absence of strong data minimization requirements, at the very least, consumers need tools to ensure that they can better exercise their opt-out rights, such as a global opt out, which is provided by this bill. We appreciate that SB 11 requires companies to honor browser privacy signals as an opt out signal. Privacy researchers, advocates, and publishers have already created a "Do Not Sell" specification, the Global Privacy Control (GPC),[4] which could help make the opt-out model more workable for consumers.[5]

In addition, we support several other key provisions in the bill:

- *Strong enforcement*. We applaud you for including a private right of action. Given the AG's limited resources, a private right of action is key to incentivizing companies to comply. Further, it's appropriate that consumers are able to hold companies accountable in some way for violating their rights. We also appreciate that there is no "right to cure" provision in administrative enforcement: this "get-out-of-jail-free" card ties the AG's hands and signals that a company won't be punished for breaking the law.

- *Non-discrimination.* SB 11 has strong non-discrimination language. The non-discrimination language in SB 11 clarifies that consumers cannot be charged for exercising their rights under the law. We appreciate the work that has been done to ensure that privacy protections aren't just for those who can afford them.

- *Authorized agent rights.* We also appreciate that SB 11 allows consumers to delegate to third parties the ability to submit opt-out requests on their behalf—allowing for a practical option for consumers to exercise their privacy rights in an opt-out framework. Consumer Reports has already begun to experiment with submitting opt-out requests on

[2] *Model State Privacy Act*, CONSUMER REPORTS (Feb. 23, 2021), https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/.
[3] *Consumer Reports Study Finds Significant Obstacles to Exercising California Privacy Right*s, CONSUMER REPORTS (Oct. 1, 2020), https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-significant-obstacles-to-exercising-california-privacy-rights/.
[4] Global Privacy Control, https://globalprivacycontrol.org.
[5] Press release, Announcing Global Privacy Control: Making it Easy for Consumers to Exercise Their Privacy Rights, Global Privacy Control (Oct. 7, 2020), https://globalprivacycontrol.org/press-release/20201007.html.

consumers' behalf, with their permission, through the CCPA's authorized agent provisions. We found that consumers are enthusiastic about this option.[6]

For these reasons, we support SB 11. Thank you for your consideration.

Sincerely,

Maureen Mahoney
Senior Policy Analyst

cc: Members, Senate Finance Committee
The Honorable Susan Lee

[6] Ginny Fahs, *Putting the CCPA into Practice: Piloting a CR Authorized Agent*, DIGITAL LAB AT CONSUMER REPORTS (Oct. 19, 2020), https://medium.com/cr-digital-lab/putting-the-ccpa-into-practice-piloting-a-cr-authorized-agent-7301a72ca9f8; Maureen Mahoney et al., *The State of Authorized Agent Opt Outs Under the California Consumer Privacy Act*, CONSUMER REPORTS (Feb. 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_AuthorizedAgentCCPA_022021_VF_.pdf.

SB11_SenatorLee_favorable.pdf
Uploaded by: Susan Lee
Position: FAV

Susan C. Lee
Legislative District 16
Montgomery County

Majority Whip

Judicial Proceedings Committee

Joint Committee on
Cybersecurity, Information Technology,
and Biotechnology

Chair
Maryland Legislative Asian American
and Pacific Islander Caucus

President Emeritus
Women Legislators of the
Maryland General Assembly, Inc.

THE SENATE OF MARYLAND
Annapolis, Maryland 21401

James Senate Office Building
11 Bladen Street, Room 223
Annapolis, Maryland 21401
410-841-3124 · 301-858-3124
800-492-7122 *Ext.* 3124
Susan.Lee@senate.state.md.us

January 26, 2022

Sponsor Testimony - FAVORABLE - SB11

The Maryland Online Consumer Protection and Child Safety Act

SB11 is essential 21st century online privacy legislation that will enable Marylanders to better understand, protect and control what and how their personal data is being collected, shared, sold, or used by private companies. Most importantly, the bill will protect the personal information being collected on children, our most precious and vulnerable resource.

After the General Data Privacy Regulation (GDPR) and the California Consumer Protection Act (CCPA) went into force in Europe and California respectively, Maryland's consumers are still left out in the cold, and to the whims of the tech giants. This bill will allow consumers to correct and delete personal information before it gets sold to third parties on the web, breached by domestic hackers, or stolen from state-sponsored actors. Most importantly, it will increase children's privacy protections by prohibiting the collection or sale of their data. The main focus of this bill is to give the consumers protections against unfair trade practices, and control over their data and corresponding privacy.

The current "notice and choice" systems provided by businesses utilize a complex language, which places significant burdens on the consumer to read and understand different privacy policies. This bill poses simple language and the clear choice to "opt out" to appear on the home page, or allow users to use third party programs to set their preferences across the board. There are many other provisions the directly mirror California's law, which is in force at this moment, without serious problems. This is not the first time this language has been proposed in Maryland, but there is one addition to make this more user-friendly for consumers and businesses. The global privacy control provision expressly provided in this bill allows third parties to be used for setting privacy preferences. This will make it easier for all to comply and has already been utilized successfully in California.

The rampant growth of data giants and their deliberate data selling techniques has led to an increase of identity theft, whereupon thieves use the information to induce harm to consumers

while creating havoc within communities. Unfortunately, there are little to no protections for consumers, who are unaware of the whereabouts of their personal information and the intentions of those who have in their position important personal information. Information is power, and corporations have valued personal information data more than all the oil in Earth. So why can't the true owners of their own data protect their own privacy? - Money and Power.

Cambridge Analytica was the catalyst for this legislation back in 2019, when I sponsored the first version of this legislation for Maryland, but so much has changed in the personal information landscape since that time, and since the passage of the federal standards. The internet is a beehive of activity for children and the collection of their information is unbridled by COPPA, which only extends to children under 13, despite the reality that most harmful activities children participate in likely fall within the cracks for children ages 13-15.

Cambridge Analytica focused on relatively broad info about a personality trait analysis, but you can determine that just based on their click pattern now as Gloria Mark from UC Irvine has been able to calculate up to an 80% accuracy. So all of the harm created with Brexit and the 2016 election could be done with more broadly available personal information, and much more targeted personal information is available to analyze your facial expressions to market items, or ideas. The concern is that the info is being collected without any friction from government. The Maryland State government currently treats this info as if it was completely harmless.

SB 11 bill brings us up to date with California and European countries that prioritize the protection of their children's data. This legislation accomplishes this goal in a uniquely Maryland manner through the existing authority of the Office of Attorney General Consumer Protection Division under title 13 of the Commercial Law Article. We merely expand that existing authority to online consumer protection that was not envisioned when title 13 was discussed as a legislative issue. There are many ways to move forward, but no reason to stand still. The time for pontification whether to act at the state level has passed. Other states are joining California, but not all laws are equal.

My oral testimony included a clip from The Social Dilemma to highlight one harm children suffer when their data is used against themselves. This is merely one avenue for targeted ads and manipulation of data to reach children, but certainly the most important one at this point in time because the amount they interact with the platform. Human phycology is being used to maximize profits, and the failure to recognize the components that go into that manipulation are tying governments' hands behind their backs. If the algorithms companies use are business confidential, shouldn't our info be personally confidential? If not shouldn't we at least acknowledge that children can't consent to a contract and shouldn't to info that can harm them?

If you have time, please review this preview as well because it highlights what damage can be done to average citizens with the corruption of their data for nefarious purposes. As The Great Hack highlights, Cambridge Analytica was horrifying because it demonstrated that enough data points can change behavior not only when it concerns commerce, but also political actions. The book "The Age of Surveillance Capitalism" – captures the profit seeking motives of data brokers and related digital platforms around the world in stark terms that should frighten us all. As China moves towards a heightened Surveillance Government, and most of the states and the federal government keep their heads in the sand, the advertisement bombardment is only the start. We are losing the war waged against the minds of our children and not even showing up to the battlefield. The states have the police powers to act, and COPPA clearly allows states to

increase enforcement, so why aren't we acting now, in 2022? Companies can comply with CCPA and the GDPR, so why can't they comply with the Maryland Online Consumer Protection and Child Safety Act?

Jeanna Matthews will join the hearing after the sponsor panel to explain her recent nationally syndicated article and how our bill would fit into the solution that social media drives people to extremes. Children are specifically vulnerable to manipulation, but the dangers spread to us all, as we have witnessed with the impacts to our health care system when false rumors are spread about vaccines and masks. January 6th marks a new reason to be concerned, as the actual historical facts of what lead up the attack are questioned to a degree only possible with social media, and the circular flow of information reinforces objectively fake news. When all your feeds reinforce what you already feel, the outrage competition seizes control of our political system. Cancel culture is also a part of this, because now people can be cancelled for posts they made when they were teenagers. Furthermore, anyone interested in state surveillance should be concerned about the ability to use state secrets to protect the collection of personal information from businesses that feed information to our intelligence agencies. Who has a check on them if our data isn't our own? Is this the world you want to raise a child?

We in the Maryland General Assembly have a responsibility to protect our citizens, especially our children, at a time when Congress has been unable to move forward on this and many other paramount pieces of legislation. Senate Bill 11 will make Maryland the leader in moving consumer protection into the 21st century, not only in our state, but nationwide. For these reasons, I respectfully request a favorable report on SB 11.

CASH_ SB 11- Maryland Online Consumer Protection a
Uploaded by: Tonaeya Moore
Position: FAV

SB 11- Maryland Online Consumer Protection and Child Safety Act
Senate Finance Committee
January 26, 2022
SUPPORT

Chairwoman Kelley, Vice-chair, and members of the committee, thank you for the opportunity to testify in support of SB 11. This bill will give the Office of the Attorney General the authority to regulate the collection and use of consumers' personal information by businesses.

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 to be aware of which businesses are using your personal data, why they are using it, and having the option to ask those businesses to delete your 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 2020, Maryland had over 900 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.

This bill will also regulate the ways in which consumers are notified about their data. Quicker, more efficient notifications, and more extensive attempts to notify consumers will position consumers to be able to respond to potential threats in a faster manner. This will also allow consumers to request their data be deleted at any point if necessary. These measures are necessary to ensure Maryland remains a national leader in consumer protection policy.

People must be very careful about who has access to their personal information. CASH supports legislation that provides an additional layer of consumer protection and allows the consumer to control information that is collected and tracked by merchants.

For these reasons, we encourage you to return a favorable report for SB 11.

[1] https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/breachnotices.aspx

MD SB 11 - RELX - Testimony FWA .pdf
Uploaded by: Caitlin McDonough
Position: FWA

January 26, 2022

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

Re: SENATE BILL 11 – THE MARYLAND ONLINE CONSUMER PROTECTION AND CHILD SAFETY ACT (Favorable with Amendments)

Dear Chair Kelley 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 11, 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) exemptions for entities currently regulated by federal law, (2) exemptions for fraud prevention and detection, (3) definitions of consumer and personal information, and (4) penalties and enforcement. 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 Lee for working with us on amendments to the proposed legislation in previous Sessions and we remain committed to continuing that work to develop and implement 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

2022-SB11_PHI Oppose.pdf
Uploaded by: Alexis Gallagher
Position: UNF

An Exelon Company

An Exelon Company

January 26, 2022

112 West Street
Annapolis, MD 21401

OPPOSE - Senate Bill 11: Maryland Online Consumer Protection and Child Safety Act

Potomac Electric Power Company (Pepco) and Delmarva Power & Light Company (Delmarva Power) oppose **Senate Bill 11: Maryland Online Consumer Protection and Child Safety Act.** Senate Bill 11 is a comprehensive bill that includes various requirements for businesses that collect consumer information and how that information can be disclosed or be prohibited from being disclosed at a consumer's request. Consumer information applicable to provisions within this bill includes account information, social security numbers, driver license numbers and forms of tracking data, which could include electricity consumption data and other data that could impact the security of Maryland's transmission and distribution grid collected by Pepco and Delmarva Power.

Pepco and Delmarva Power understand the concerns surrounding data privacy breaches, however Maryland has historically exempted utilities from disclosing to its customers critical electric infrastructure information in order to protect the security and integrity of the electric grid. The process of how information that impacts critical electric infrastructure information is disseminated and to whom continues to evolve through an existing Cyber-Security Reporting Work Group regulatory process at the Public Service Commission. Any policy impacting critical electric infrastructure information must be developed in a way that does not add unnecessary security risks to the electric system while protecting the electric utility's ability to service the needs of its customers.

We believe consumer privacy is an important issue. However, State-by-State regulation of consumer privacy will create an unworkable patchwork that will lead to consumer confusion. That is why we strongly support ongoing efforts to develop a uniform national approach to consumer privacy. The stakes involved in consumer privacy legislation are high and taking the wrong approach could have serious consequences for consumers, innovation, and competition.

Ensuring the energy safety of Maryland's residents must be paramount when considering legislation of this nature. We look forward to working with the sponsors and stakeholders to ensure the security of Maryland's energy infrastructure remains resilient against cyber-attacks.

Contact:
Alexis Gallagher
State Affairs Manager
609-412-6345
Alexis.gallagher@exeloncorp.com

Katie Lanzarotto
Senior Legislative Specialist
202-872-3050
Kathryn.lanzarotto@exeloncorp.com

BGE - SB 11 Maryland Online Consumer Protection -
Uploaded by: Allyson Black
Position: UNF

BGE
An Exelon Company

Position Statement

OPPOSE
Senate Finance Committee
1/26/2022

Senate Bill 11 Maryland Online Consumer Protection and Child Safety Act

Baltimore Gas and Electric Company (BGE) opposes *SB 11 Maryland Online Consumer Protection and Child Safety Act*. Senate Bill 11 would establish requirements for businesses that collect consumer information, including how or if information can be disclosed without the consumers consent. Consumer information applicable under this bill would include account information, social security numbers, driver license numbers and forms of tracking data, which could include electricity consumption data and other data by BGE for billing purposes, as well as data that could impact the security of Maryland's transmission and distribution grid collected by BGE.

BGE understands the concerns regarding data privacy breaches; however, Maryland has historically exempted utilities from providing customers with disclosure of sensitive information in order to protect disclosure of critical electric infrastructure information.

The process of how information that impacts critical electric infrastructure information is disseminated and to whom continues to evolve through an existing Cyber-Security Reporting Work Group regulatory process at the Public Service Commission. Any policy impacting critical electric infrastructure information must be developed in a way that does not add unnecessary risk to the electric system, while protecting the electric utility's ability to service the needs of its customers.

Rather than pursue varying and disparate state-by-state regulations to address consumer privacy issues, we believe a more efficient and productive approach is the existing efforts to develop a uniform federal policy regarding consumer privacy.

We look forward to working with the sponsors and stakeholders to ensure the security of Maryland's energy infrastructure remains resilient against cyber-attacks.

For these reasons, BGE urges an unfavorable vote on this bill.

Sandy Grace | Charles Washington | Allyson Black | 410.269.5281

SB0011 -- Maryland Online Consumer Protection and

Uploaded by: Brian Levine

Position: UNF

Senate Bill 11 -- *Maryland Online Consumer Protection and Child Safety Act*
Senate Finance Committee
January 26, 2022
Oppose

The Montgomery County Chamber of Commerce (MCCC), the voice of business in Metro Maryland, opposes Senate Bill 11 – *Maryland Online Consumer Protection and Child Safety Act*.

MCCC is concerned that Senate Bill 11 will be costly and confusing for businesses, especially those that are small and do not have the infrastructure to address difficult new requirements. The bill's costs of compliance may be staggering for companies of all sizes, including small and startup businesses.

Senate Bill 11 imposes new requirements on businesses that are already struggling with the impact of the COVID-19 pandemic. Businesses continue to adjust to the new realities of a pandemic economy, which now are exacerbated by supply chain issues, inflation, and a historically tight and evolving labor market.

While Senate Bill 11 seeks to address consumer protection, MCCC contends that this specific type of issue should be addressed on the federal level. Without federal action, differing consumer protection requirements in multiple states will lead to businesses contending with a patchwork of difficult and confusing obligations.

For these reasons, the Montgomery County Chamber of Commerce opposes Senate Bill 11 and respectfully requests an unfavorable report.

The Montgomery County Chamber of Commerce, on behalf of our nearly 500 members, advocates for growth in business opportunities, strategic investment in infrastructure, and balanced tax reform to advance Metro Maryland as a regional, national, and global location for business success. Established in 1959, MCCC is an independent non-profit membership organization and a proud Montgomery County Green Certified Business.

Brian Levine / Vice President of Government Affairs
Montgomery County Chamber of Commerce
51 Monroe Street / Suite 1800
Rockville, Maryland 20850
301-738-0015 / www.mcccmd.com

Online Privacy Bill SB11.pdf
Uploaded by: cailey locklair
Position: UNF

SB11: Maryland Online Consumer Protection and Child Safety Act
Senate Finance Committee
January 26, 2022

Position: Unfavorable

Background: SB11 regulates the collection and use of consumers' personal information by businesses; establishing the right of a consumer to receive information regarding collection practices, have personal information deleted by a business, and prohibit the disclosure of personal information by a business; requiring businesses to provide certain notices to consumers and include certain information in online privacy policies; and authorizing the Office of the Attorney General to adopt regulations to carry out the Act.

Comments: The Maryland Retailers Association has numerous concerns with the legislation as outlined below.

1. **California's Privacy Model is the Wrong Model for Maryland**: S.B. 11, exclusively regulates "businesses" (e.g., retailers and other consumer-facing Main Street businesses) while exempting service providers and third parties who also handle the majority of consumer data. In this respect, it is following a California privacy law model, but it also goes beyond it in some respects. Maryland should be looking toward a more balanced law that obligates <u>all parties</u> that handle data to protect it and honor consumers' choices with respect to it.
    a. **MD Should Consider the VA Model**: Virginia's Consumer Data Protection Act (CDPA) was broadly supported by industry. It was adopted last spring and will take effect on January 1, 2023. It was the model for the only two state privacy bills to be enacted in 2021: in Virginia and Colorado. Unlike SB11, the VA privacy law balances the particular obligations between businesses and service providers. Additionally, with VA bordering Maryland and DC, it would make much more sense in this region to have a more harmonized privacy law – the same obligations for businesses and identical rights for consumers – across the three jurisdictions in light of consumers traversing these state and district lines daily and retailers being located in three separate jurisdictions in one metropolitan region.

2. **S.B. 11 Would Outlaw Retailers' Customer Loyalty Plans Unless Robust Savings Clauses Are Adopted**: Retailers are heavily invested in customer loyalty programs. The business incentive for loyalty programs is to reward repeat customers who sign up for the program for their shopping loyalty, and to create incentives for customers to shop at a particular brand repeatedly. Forrester Research released a report a few years ago that confirmed how popular such loyalty programs are with consumers: approximately 80% of adults participate in loyalty programs, and the average adult participant is signed up

for nine programs. Despite consumers supporting and opting into these programs, the current nondiscrimination language in S.B. 11 (p. 14, l. 21 – p. 15, l. 2) would render unlawful the normal functioning of retailers' customer loyalty programs. The programs are intended to benefit the loyal customers participating in them by offering them better prices and levels of service compared to those customers who do not participate in the programs.

For example, a consumer may exercise a right to opt-out of third party disclosure under the bill, but if such third party disclosure is necessary for the tracking of the customer's activity and/or the delivery of the loyalty plan benefits under the program, then the customer would not be able to participate in the loyalty program. That customer who opted out (i.e., exercising a privacy right) could then claim a violation of the bill's nondiscrimination provision if other customers who continue to participate in the plan receive better prices or different levels of quality of good or services by being in the plan. Retailers have therefore actively opposed similar nondiscrimination provisions in other states unless and until a loyalty plan savings clause has been adopted to preserve the loyalty programs that consumers overwhelmingly desire to have. We would strongly recommend S.B. 11 be revised to add the same savings clauses, to ensure that retailers have loyalty plan protections.

a. **Language Recommendations**: Although Virginia language could be used to rectify this deficiency, we would recommend using the following language from Ohio's legislation:

> **Sec. 1355.09.** (A) Subject to divisions (B) and (C) of this section, a business shall not discriminate against a consumer for exercising the rights provided to a consumer under this chapter.
> (B) A business may charge different prices or rates for goods or services for individuals who exercise their rights under this chapter for legitimate business reasons or as otherwise permitted or required by applicable law.
> (C) A business's denial of a consumer's request in compliance with this chapter shall not be considered discrimination against the consumer.
> (D) Nothing in this section shall be construed as doing either of the following:
> (1) Requiring a business to provide a product or service that requires the personal data of a consumer that the business does not collect or maintain or requiring a business to provide a product or service if the consumer has exercised the right to opt-out pursuant to section 1355.08 of the Revised Code;
> (2) Prohibiting a business from offering a different price, rate, level, quality, or selection of goods or services

to a consumer, including offering goods or services for no fee, if the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

3. **S.B. 11 Does Not Place Any Obligations on Service Providers or Third Parties Who Handle the Most Consumer Data.** As noted in the first point above, S.B. 11 exclusively regulates "businesses" (e.g., retailers and other consumer-facing Main Street businesses) while exempting "service providers" and "third parties" who handle the majority of consumer data. As a result, all liability for violations of the bill – even violations that arguably are the fault of a service provider – will land on the businesses that contracted the service provider, even if that business itself has done everything required of it under the law.
    a. **Example of How Retailers May be Vicariously Liable for Service Providers' Privacy Failures Under the Bill.** For example, if a consumer exercises a privacy right (e.g., delete consumers' personal information upon request), it is the obligation of the business under S.B. 11 to fulfill that obligation alone, even if it requires the assistance or performance by a service provider (e.g., cloud services) in order to complete the request. In subsection 14-4406(C) (p. 12, l. 15), for instance, it states: "(C) A **BUSINESS** THAT RECEIVES A VERIFIABLE CONSUMER REQUEST FROM A CONSUMER TO DELETE THE CONSUMER'S PERSONAL INFORMATION UNDER SUBSECTION (A) OF THIS SECTION **SHALL DELETE** THE PERSONAL INFORMATION FROM ITS RECORDS **AND DIRECT SERVICE PROVIDERS** TO DELETE THE PERSONAL INFORMATION FROM THE SERVICE PROVIDERS' RECORDS." Notably, the obligation in S.B. 11's section here is on the business alone to delete the personal information (PI) -- and to "direct" service providers to delete the PI as well – but there is no obligation in S.B. 11 on the service provider to actually delete the PI (i.e., the bill does not say the service provider "shall" delete) and the service provider is not even obligated to assist the business in fulfilling the obligation to delete where it is necessary to do so (i.e., where the PI is in service providers' database or cloud, for instance, that is controlled by the service provider). This means that if the service provider fails to take action and does not delete the PI in the database or cloud, the business "directed" it to, it will be the business (not the service provider that failed) who is liable under the statute for that failure if a consumer claims harm from continued accessibility to his/her PI in the database or cloud after making the deletion request and the AG then takes action to address it. In order to place liability where it belongs – on the service provider in this example – S.B. 11 would need to have obligations, such as those in VA and CO, that require the service provider (defined as a "processor" in those laws) to assist the business in meeting its obligations. We strongly recommend that S.B. 11 be revised to adopt provisions such as those in

the newly enacted VA and CO privacy laws, modeled on language in the WA privacy bill, that creates important obligations for data processors. This language protects both consumers and businesses alike in the handling of customers' PI by establishing the necessary statutory requirements for service providers to abide by consumers' privacy rights requests. Virginia's service provider (a.k.a. processor) language would rectify this deficiency.

- **Minimum Requirements of Other Providers:** Common-sense, minimum requirements for service providers (i.e., data processors) similar to those adopted in other state privacy laws should be added. This language would ensure that S.B. 11 protects consumers' personal information where the majority of consumer data processing occurs, by requiring such data processors to honor consumers' rights requests, protect consumer data provided to it by a business, and abide by other standard processor privacy obligations (listed in bullet form below). It would also ensure that privacy obligations do not fall exclusively on Main Street businesses such as retailers when the majority of data processing occurs among their service providers. Presently, S.B. 11 fails to protect consumers comprehensively by omitting privacy obligations for service providers to protect consumers' personal information and/or to honor their privacy rights requests. The language from WPA (in the form that passed the Washington Senate by a vote of 48-1 in 2021) included the following basic data processor obligations that were enacted in two other state laws and that also have applied to many U.S.-based global data processors under the EU's GDPR since 2018 – they require service providers (i.e., defined as "processors" under the state laws and GDPR) to:
  - fulfill the business's obligation to respond to consumer privacy rights requests and provide security in processing required by the act;
  - assist the business in meeting its obligations in relation to the security of processing the personal information and in relation to the notification of a security breach;
  - ensure each person processing personal information at the service provider is subject to a duty of confidentiality with respect to the data;
  - require any subcontractor of the service provider, pursuant to a written contract, to meet the service providers' obligations to the business with respect to the data;
  - implement appropriate technical and organizational measures to ensure the service provider adopts a level of security appropriate to the risk;
  - delete or return to the business, at the business's direction, all personal information in the possession of the service provider at the end of the provision of services;

- § make available, upon the reasonable request of a business, all information necessary to demonstrate the service provider's compliance with the act; and
- § cooperate with reasonable audit assessments by the business or its designator auditor of the service provider's policies and technical and organizational measures in support of the act's obligations for businesses and service providers.

- o **Suggested revision to text of S.B. 11:** Add to S.B. 11 the processor obligations found in Section 106 of S.B. 5062, the Washington Privacy Act (WPA) *(in the form that passed the Washington Senate by a vote of 48-1 in the 2021 session)*. (Note, the text of the WPA would first need to be modified by replacing all instances of the WPA-defined term "controller" with the term "business" (as defined in S.B. 11), replacing all instances of the WPA-defined term "processor" with "service provider" (as defined in S.B. 11), and making similar technical corrections to ensure the language works with S.B. 11's definitions of "personal information.")

For these reasons as well as the aggressive Title 13 penalties even for retailers following the law and broad exceptions included in the bill, we must again urge an unfavorable report on this legislation. Thank you for your consideration.

SIFMA SB 11 Testimony (01.26.22).pdf
Uploaded by: Chris DiPietro
Position: UNF

Statement of

Securities Industry and Financial Markets Association

Senate Committee on Finance Regarding

SB 11, the Maryland Online Consumer Protection and Safety Act

January 26, 2022

RE: SB 11 – The Maryland Online Consumer Protection and Child Safety Act– Unfavorable

Dear Chair Kelley and Members of the Senate Finance Committee:

On behalf of the Securities Industry and Financial Market Association (SIFMA)[1], we are writing to suggest amendments to SB 11, which would create the Maryland Online Consumer Protection and Child Safety Act. SIFMA brings together the shared interests of hundreds of securities firms, banks and asset managers located throughout Maryland and across the country. In fact, more than 94,000 people work in the finance and insurance industries, more than 16,800 of them work at securities firms, and 41 broker-dealer main offices call Maryland home.

SIFMA commends you for your commitment to protecting the privacy of Marylanders. The business community has been and remains committed to adhering to effective and reasonable privacy laws. However, SIFMA, along with many business groups and financial services firms, does not believe SB 11 offers the best solution to protecting data, and would not harmonize with federal privacy laws.

There are many provisions in this privacy proposal that are important to get right; today we will highlight just two that are important to our broker-dealers and financial services members. We are very interested in working with you on language that would better protect consumers without negatively impacting our members.

1. Gramm-Leach-Bliley Act Exemption: The Gramm-Leach-Bliley Act (GLBA) is an established and comprehensive federal privacy law that already provides protections for consumers and significant regulation on privacy and data security, including disclosure of privacy practices to customers, cybersecurity controls, and restrictions on the unauthorized sharing of non-public consumer financial information with significant oversight and enforcement by financial regulators. Financial institutions regulated by GLBA already have comprehensive privacy protections in place, and should be explicitly exempt from SB 11. The bill as currently written, would create several issues that have arisen from earlier state privacy law enactments. These issues include:

- **Consumer Protection**: Consumers likely do not know which data is collected under GLBA and which is not, but they do know when they are dealing with their financial institution (bank,

[1] SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate for legislation, regulation, and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.

brokerage firm, investment adviser, etc.). The differences will not matter to consumers, but they may still be told that some of their information may be subject to regulation under state law if this bill is enacted (and therefore able to be disclosed, corrected, or deleted), and other information may not be, depending on the reasons why it was collected.

- **Data treatment:** Financial institutions do not treat data differently based on how or why they collect it. Once they have data, they generally treat it in the same way as information collected under the GLBA for cybersecurity and data protection purposes as described above. Requiring the information to be dissected would impose a significant burden on financial institutions.

- **Issues with Data Level Exemption:** The exemption should attach to the entity and not to the data. Exempting only data collected under GLBA may leave open a door for fintech and other unregulated companies to use and share non-public personal financial information outside of the law. Such entities are not subject to GLBA or Regulation S-P[2] and therefore are not legally required to have the same levels of protections, disclosures, and cybersecurity practices.

  As such, a financial institution entity-level exemption is the best, most comprehensive way to protect consumer's data, as the entities are subject to GLBA and therefore have the policies and procedures in place to protect such information as required by federal law.

In order to prevent consumer confusion and disruption in the business community, SIFMA requests that you consider amending the current GLBA exemption to mirror the most recent privacy law enactment in the country, the Virginia Consumer Data Protection Act of 2021.[3] The GLBA exemption in VA reads:

> "this chapter shall not apply to any… *(ii) financial institution or data subject to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.)".*

This exemption language would allow for the financial services industry to provide consumers with meaningful privacy control in an efficient and effective manner.

2. Independent Contractor Exemption: In order to encompass the full labor pool of the securities industry, we ask that you broaden the exemption language to the definition of consumer to include independent contractors. Please see the below suggested changes which would sufficiently broaden the exemption for independent contractors.

> 5. "Consumer" an individual who reside in the state.
> "Consumer" shall not include any of the following:
> (A) a natural person known to be acting in a commercial or employment context;
> (B) a natural person in the course of acting as a job applicant to, an employee of, or former employee of, owner of, director of, officer of, medical staff member of, or contractor of a business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business.

In short, while we applaud your work to protect Marylander's data privacy, we would like to work with you to better align your proposal with federal law and the existing, robust financial services data protection

[2] Regulation S-P
[3] Chapter 35

policies and practices before advancing SB 11. We appreciate your willingness to consider our concerns. If you have any questions, please contact SIFMA's Maryland council, Chris DiPietro, of CDI Consulting at 410-243-5782 or Nancy Lancia, of SIFMA at (212) 313-1233 or nlancia@sifma.org.

MD_TechNet_Data Privacy SB 11-1.26.22.pdf
Uploaded by: Christopher Gilrein
Position: UNF

TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Northeast | Telephone 774.230.6685
One Beacon Street, Suite 16300, Boston, MA 02108
www.technet.org | @TechNetNE

January 25, 2022

The Honorable Senator Delores Kelly, Chair
The Honorable Senator Brian Feldman, Vice Chair
Senate Finance Committee
Miller Senate Office Building
Annapolis, Maryland 21401

Re: SB 11 – Maryland Online Consumer Protection and Child Safety Act

Dear Chair Kelly, Vice Chair Feldman, and members of the Committee:

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 four 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, Olympia, Sacramento, San Francisco, Silicon Valley, and Washington, D.C.

TechNet's member companies place a high priority on consumer 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 supports a federal standard that establishes a uniform set of rights and responsibilities for all Americans. The global nature of data demands a federal policy, and even the most well-designed state statute will ultimately contribute to a patchwork of different standards across the country, resulting in steep compliance costs and consumer confusion.

In the absence of a uniform standard, TechNet urges states considering their own legislation to consider interoperability with existing models as the default position. Specifically, states should look to the most recent examples of Virginia and Colorado, which have taken lessons learned from US and global privacy law and present a clearer, more explicit explanation of consumer rights and controller responsibilities.

SB 11 instead pulls from the California model, which even as we discuss this, remains a moving target. CA businesses and consumers currently live under a privacy regime enacted in 2018 and interpreted through a long series of rulemakings by the Attorney General's office. That regime will be supplanted in 2023 by a new authority, the California

TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

Privacy Protection Agency, tasked with enforcing a 2020 law, which is the subject of a current series of rulemakings by the new agency. Already this state of affairs has caused significant confusion for businesses and consumers alike, as the provisions in the new law and actions by the AG have differed, and occasionally contradicted one another.

TechNet members believe that privacy legislation should connect specific remedies to specific privacy harms. A truly effective privacy law is as explicit as possible – it should be clear what is expected of companies and what rights consumers can avail themselves of. The Virginia Consumer Data Protection Act (VCPDA) in particular improves upon the CA experience with tighter definitions and more explicit instruction in statute, leaving fewer details to be worked out administratively. TechNet believes the key definitions in the VCPDA more accurately reflect the current privacy landscape, including the different types of data and the critical delineations between controllers and processors of data.

Additionally, SB 11 places the enforcement of this new law under Title 13, which includes a private right of action. Experience in other states has shown that a private right of action in privacy statute can mean that any unintentional or perceived violation could result in ruinous liability for companies. The penalties imposed under the bill would enable class action firms to wield this law as a cudgel against well-meaning businesses to extract significant settlements from companies with little or no actual value delivered to the consumer. Central enforcement by the Attorney General with a right to cure period ensures that justice is meted out evenly, and that enforcement actions are targeted at those causing actual harm to Maryland residents, not just those that offer the opportunity for a lucrative settlement.

Thank you for your consideration. Please consider TechNet and our members a resource as the Committee addresses these complex issues.

Sincerely,

Christopher Gilrein
Executive Director, Northeast
TechNet
cgilrein@technet.org

SB11_AdTrades_UNF
Uploaded by: Christopher Oswald
Position: UNF

January 25, 2022

The Honorable Sen. Delores G. Kelley
Chair of the Maryland Senate Finance Committee
3 East Miller Senate Office Building
11 Bladen Street
Annapolis, MD 21401

The Honorable Sen. Brian J. Feldman
Vice Chair of the Maryland Senate Finance Committee
104 James Senate Office Building
11 Bladen Street
Annapolis, MD 21401

RE: Letter in Opposition to Maryland SB 11

Dear Senator Kelley and Senator Feldman:

On behalf of the advertising industry, we oppose the Maryland Online Consumer Protection and Child Safety Act ("SB 11").[1] We and the companies we represent, many of whom do substantial business in Maryland, agree that Maryland consumers deserve meaningful privacy protections supported by reasonable government policies. However, we strongly believe privacy should be the subject of preemptive federal legislation,[2] because passing privacy laws on a state-by-state basis provides uneven protections for consumers and creates a complex landscape for businesses across the country.

If the General Assembly nonetheless decides to continue its effort to pass a privacy law in Maryland, we encourage it to consider adopting an approach to privacy that aligns with recently enacted law in other states, such as the Virginia Consumer Data Protection Act ("VCDPA"), to foster harmonization across state privacy standards.[3] As presently written, SB 11 falls short of creating a regulatory system that will work well for Maryland consumers or business. We address the following non-exhaustive areas of concern with the bill in this letter:

- **Maryland Should Take Steps to Harmonize Its Approach to Privacy With Other State Laws**
- **SB 11's Proposed Global Opt Out Provisions Lack Reasonable Safeguards to Protect Consumer Choice**
- **Privacy Laws Should Be Subject to Attorney General Enforcement and Should Not Permit a Private Right of Action**

[1] SB 11 (Md. 2022), located here.
[2] *See* Privacy for America, *Principles for Privacy Legislation*, located here.
[3] *See* Virginia Consumer Data Protection Act, §§ Va. Code Ann. 59.1-571 et seq., located here.

- **SB 11's Disclosure Requirements Related to Third Parties Are Operationally Infeasible**
- **SB 11's Blanket Ban On Disclosures of Data Associated With Individuals Under Age 16 Would Impede Teens' Access to Online Resources**
- **The Data-Driven and Ad-Supported Online Ecosystem Benefits Maryland Consumers and Fuels Economic Growth**

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, is responsible for more than 85 percent of the U.S. advertising spend and drives more than 80 percent of our nation's digital advertising expenditures. Our group has more than a decade's 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 on further study of the proposal with an aim toward better aligning the wants of consumers with the needs of the Internet economy.

I. Maryland Should Take Steps to Harmonize Its Approach to Privacy With Other State Laws

Harmonization in state privacy law standards is in the interests of consumers and businesses alike. Uniformity across state requirements helps to ensure consumers are subject to similar privacy protections no matter where they live and businesses can take a more holistic approach to privacy law compliance. Maryland should not adopt an outdated, confusing, and burdensome privacy legal regime when alternative approaches exist that protect consumers while providing consistency across states. We encourage the General Assembly to examine more up-to-date consumer protection standards that are available for regulating data privacy, including the VCDPA, before moving forward with SB 11.

Efforts to emulate outdated privacy laws in Maryland will significantly and disproportionately impact the ability of small and mid-size businesses and start-up companies to operate successfully in the state. A standardized regulatory impact assessment of the California Consumer Privacy Act of 2018 ("CCPA"), for example, estimated *initial* compliance costs at 55 billion dollars.[4] This amount did not account for ongoing compliance expenses and needed resource allotments outside of the costs to businesses to bring themselves into initial compliance with the law. Additionally, that same report estimated that businesses with less than 20 employees would need to spend $50,000 each to begin their CCPA compliance journey, and businesses with less than 50 employees would need to spend approximately $100,000 each.[5] Other studies confirm the staggering costs associated with varying state privacy standards. One report found that state privacy laws could impose out-of-state costs of between $98 billion and $112 billion annually, with costs exceeding $1 trillion dollars over a 10-year period and small businesses shouldering a significant portion of the compliance cost burden.[6] Maryland should reconsider implementing outdated privacy law provisions and instead should work to harmonize SB 11 with the VCDPA.

---

[4] California Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act Regulations* at 11 (August 2019), located at https://www.tellusventure.com/downloads/privacy/calif_doj_regulatory_impact_assessment_ccpa_14aug2019.pdf.
[5] *Id*.
[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).

II. SB 11's Proposed Global Opt Out Provisions Lack Reasonable Safeguards to Protect Consumer Choice

SB 11 would require businesses to allow consumers to "exercise the right to opt out of the sale or disclosure of the consumer's personal information through a technology indicating the consumer's intent to opt out, including a preference or browser setting, browser extension, or global device setting."[7] Unfortunately, SB 11's current provisions surrounding such controls are not accompanied by sufficient safeguards to ensure a preference indicated by a setting is a true expression of a consumer's choice. We urge you to either amend this provision to provide adequate safeguards to ensure these controls do not unfairly disadvantage various market participants, or remove this provision from the bill for further consideration.

Such controls must be designed and implemented in a manner that ensures a preference expressed through the setting is enabled by a consumer, and does not unfairly disadvantage or advantage one business or model over another.[8] Otherwise, these settings run the risk of intermediary interference, as the companies that stand between businesses and consumers, such as browsers and others, can set such controls by default without requiring an affirmative consumer action to initiate the control. SB 11 would accelerate the unintended consequence of creating a new class of gatekeepers, which would undercut competition in the market. Unconfigurable, global opt out setting mechanisms have already been introduced in the market, making decisions for consumers by default without requiring them to affirmatively turn on the mechanisms.[9] These tools are not user-enabled, as they do not provide any assurance that consumers themselves are the ones making privacy choices. Consumers should be assured the ability to take an action to enable these settings, and such settings should be subject to specific parameters that ensure they do not unfairly advantage certain businesses at the expense of others. For these reasons, the global privacy control provisions should be removed from SB 11.

III. Privacy Laws Should Be Subject to Attorney General Enforcement and Should Not Permit a Private Right of Action

As presently drafted, SB 11 allows for private litigants to bring lawsuits by deeming violations of the bill to be unfair, abusive or deceptive trade practices within the meaning of the Maryland Consumer Protection Act.[10] We strongly believe private rights of action should have no place in privacy legislation. Instead, enforcement should be vested with the Maryland Attorney General ("AG"), because such an enforcement structure would lead to stronger outcomes for Maryland consumers while better enabling businesses to allocate funds to developing processes, procedures, and plans to facilitate compliance with new data privacy requirements. AG enforcement, instead of a private right of action, is in the best interests of consumers and businesses alike.

A private right of action in SB 11 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. Private right of action provisions are completely

---

[7] SB 11, Sec. 14-407(E)(1).
[8] *See,* California Privacy Rights Act of 2020, Cal. Civ. Code § 1798.185(a)(19)(A); Colorado Privacy Act, Colo. Rev. Stat § 6-1-1313(2).
[9] *See* Brave, *Global Privacy Control, a new Privacy Standard Proposal, now Available in Brave's Desktop and Android Testing Versions*, located here ("Importantly, Brave does not require users to change anything to start using the GPC to assert your privacy rights. For versions of Brave that have GPC implemented, the feature is on by default and unconfigurable.")
[10] SB. 11, Sec. 14-411(A)(1).

divorced from any connection to actual consumer harm and provide consumers little by way of protection from detrimental data practices.

Additionally, including a private right of action in SB 11 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. And, in many cases, the threat of an expensive lawsuit may force smaller companies to agree to settle claims against them, even if they are convinced they are without merit.

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 the bill and replace it with a framework that makes enforcement responsibility the purview of the AG alone.

IV. SB 11's Disclosure Requirements Related to Third Parties Are Operationally Infeasible

SB 11 would, upon a consumer's request, require a business that collects personal information to disclose to the consumer the "names" of all "third parties to which the business disclosed the consumer's personal information."[11] This requirement is operationally infeasible given the modern structure of the Internet, which enables seamless data transfers between businesses to the benefit of consumers. Businesses also may not be able to comply with such a requirement due to confidentiality provisions they may have in contracts with their business partners, which oftentimes help companies innovate together in ways they could not individually. From a consumer's perspective, SB 11's requirement to provide names of third parties would likely result in inordinately long disclosures. The length of such disclosures would likely diminish their effectiveness. The Maryland General Assembly should therefore take steps to align its disclosure requirements with other state privacy laws, such as the VCDPA, which require disclosure of the *categories* of third parties to whom personal information is disclosed and not the individual names of the third parties themselves.

V. SB 11's Blanket Ban On Disclosures of Data Associated With Individuals Under Age 16 Would Impede Teens' Access to Online Resources

Our organizations do not flatly oppose all forms of heightened protections for uses of data associated with teens. In fact, we are proponents of a national privacy framework that creates additional protections for these unique internet users.[12] However, SB 11 would take an extreme and onerous approach to establishing protections for transfers of data associated with individuals under age 16. Specifically, the bill would flatly prohibit a business from disclosing any personal information

[11] SB 11, Sec. 14-4404(A)(3).
[12] *See* Privacy for America, *Principles for Privacy Legislation*, located here.

associated with an individual under age 16 to a third party if the business has actual knowledge or willfully disregards the fact that the consumer is under 16 years of age.[13]

In this regard, SB 11 is out of step with every other state that has passed privacy legislation as well as sectoral privacy laws at the federal level that provide for sharing of this data where there is consent.[14] SB 11 provides no exceptions to its blanket ban on data transfers, even for consent. In addition, the bill could also prohibit a consumer under the age of 16 from sharing personal information via a business, such as through online collaboration tools where students interact and share information. The bill's ban on U-16 data transfers would severely limit Maryland teens' access to online services and vital information, as described in more detail in Section V below. If enacted, the bill's burdensome terms related to adolescents would likely lead to a chilling effect on teens' ability to access online resources at a time in their lives when they should enjoy wide access to the Internet to inform their education and development (everything from summer camp brochures to future school choices and myriad other opportunities which are part of American life). For these reasons, the provisions related to U-16 data transfers should be removed from SB 11.

VI. The Data-Driven and Ad-Supported Online Ecosystem Benefits Maryland Consumers and Fuels Economic Growth

Over the past several decades, data-driven advertising has created a platform for innovation and tremendous growth opportunities. A new study found that the Internet economy's contribution to the United States' gross domestic product ("GDP") grew 22 percent per year since 2016, in a national economy that grows between two to three percent per year.[15] 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.[16] Additionally, more than 17 million jobs in the U.S. were generated by the commercial Internet, 7 million more than four years ago.[17] More Internet jobs, 38 percent, were created by small firms and self-employed individuals than by the largest internet companies, which generated 34 percent.[18] The same study found that the ad-supported Internet supported 168,600 full-time jobs across Maryland, more than double the growth in Internet-driven employment from 2016.[19]

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.[20] One recent study found that "[t]he U.S. open web's independent publishers and

---

[13] SB 11, Sec. 14-4407(B).
[14] Children's Online Privacy Protection Act, 15 U.S.C. § 6502; California Privacy Rights Act of 2020, Cal. Civ. Code § 1798.120; California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.120; Virginia Consumer Data Protection Act, Va. Code Ann. §§ 59.1-572(D), 59.1-574(A)(5); Colorado Privacy Act, Colo. Rev. Stat § 6-1-1308(7).
[15] *See* John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 5 (Oct. 18, 2021), located https://www.iab.com/wp-content/uploads/2021/10/IAB_Economic_Impact_of_the_Market-Making_Internet_Study_2021-10.pdf.
[16] *Id*.
[17] *Id*.
[18] *Id*. at 6.
[19] *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).
[20] *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.

companies reliant on open web tech would lose between $32 and $39 billion in annual revenue by 2025" if third-party tracking were to end "without mitigation."[21] 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.[22] 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.[23] Data-driven advertising has thus helped to stratify economic market power, ensuring that smaller online publishers can remain competitive with large global technology companies.

B. Advertising Supports Maryland Consumers' 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 about COVID-19. Advertising revenue is an important source of funds for digital publishers,[24] and decreased advertising spends directly translate into lost profits for those outlets. Since the coronavirus pandemic began, 62 percent of advertising sellers have seen advertising rates decline.[25] Publishers have been impacted 14 percent more by such reductions than others in the industry.[26] Revenues from online advertising based on the responsible use of data support the cost of content that publishers provide and consumers value and expect.[27] Legislative models that inhibit or restrict digital advertising can cripple news sites, blogs, online encyclopedias, and other vital information repositories, thereby compounding the detrimental impacts to the economy presented by COVID-19. The effects of such legislative models ultimately harm consumers by reducing the availability of free or low-cost educational content that is available online.

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.[28] Additionally, in a recent Zogby survey conducted by the Digital Advertising Alliance, 90 percent of consumers stated that free content was important to the overall value of the Internet and 85 percent surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers

---

[21] *Id*. at 34.
[22] *Id*. at 15-16.
[23] *Id*. at 28.
[24] *See* Howard Beales, *The Value of Behavioral Targeting* 3 (2010), located at https://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.
[25] IAB, *Covid's Impact on Ad Pricing* (May 28, 2020), located at https://www.iab.com/wp-content/uploads/2020/05/IAB_Sell-Side_Ad_Revenue_2_CPMs_5.28.2020.pdf
[26] *Id*.
[27] *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.
[28] 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.

must pay for most content.[29] Indeed, as the Federal Trade Commission noted in its recent 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.[30]

During challenging societal and economic times such as those we are currently experiencing, 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 any future legislation'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.

* * *

[29] 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.
[30] 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.

We and our members support protecting consumer privacy. We believe SB 11 would impose new and particularly onerous requirements on entities doing business in the state and would unnecessarily impede Maryland residents from receiving helpful services and accessing useful information online. We therefore respectfully ask you to reconsider the bill.

Thank you in advance for consideration of this letter.

Sincerely,

Christopher Oswald
EVP, Government Relations
Association of National Advertisers
202-269-2359

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

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
703-220-5943

Lartease 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:

The Honorable Sen. Susan C. Lee
223 James Street Senate Office Building
11 Bladen Street
Annapolis, MD 21401

Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP

Ext. Comm. - Letter - 2022 - Maryland SB 11 - Priv
Uploaded by: Joshua Fisher
Position: UNF

January 24, 2022

The Honorable Delores Kelley
Chair, Senate Finance Committee
3 East, Miller Senate Office Building
Annapolis, Maryland 21401

RE: SB 11 - MARYLAND ONLINE CONSUMER PROTECTION ACT
POSITION: UNFAVORABLE

Dear Senator Kelley:

The Alliance for Automotive Innovation (Auto Innovators) is writing to inform you of **our opposition to SB 11**. Auto Innovators generally opposes efforts to enact state-level privacy laws and believes that the best way to protect consumers is through a single, national privacy framework. We are increasingly concerned that multiple states will enact privacy laws that provide inconsistent rights and obligations. A patchwork of state privacy laws not only make compliance difficult but will also create confusion among consumers about their privacy rights.

That is exactly what will happen if this bill, as currently drafted, were to become law. Colorado, California and Virginia have passed varying privacy laws. We are already facing a web of requirements in various states. We strongly urge the Maryland General Assembly to not add to this current patchwork. Alternatively, we recommend consideration of Virginia's privacy law to better ensure consistency among the states.

The Alliance for Automotive Innovation is the singular, authoritative, and respected voice of the automotive industry. Focused on creating a safe and transformative path for sustainable industry growth, the Alliance for Automotive Innovation represents automakers producing nearly 99 percent of cars and light trucks sold in the U.S., Tier 1 original equipment suppliers, as well as other automotive technology companies.

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 are enforceable through the Federal Trade Commission and provide heightened protection for geolocation data and how drivers operate their vehicles.[1] With increasing vehicle connectivity, customer privacy must be a priority. Many of the advanced technologies and services in vehicles today are based upon information obtained from a variety of vehicle systems and involve the collection of information

[1] The complete Principles document can be found at www.automotiveprivacy.com

1050 K Street, NW
Suite 650
Washington, DC 20001
AutosInnovate.org

about a vehicle's location or a driver's use of a vehicle. 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.

Practical Concerns

With this in mind, we have significant concerns with the proposed legislation. SB 11 defines "personal information" far more broadly than what that term is commonly understood to include. The bill defines "personal information" as "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 …" (emphasis added). This emphasized language in particular would mean that essentially every piece of direct and indirect data about a person could be classified as "personal information." The bill's definition of de-identification creates ambiguity around determining if particular methods of de-identification are sufficiently "reasonable" to pass the standard. This one-size-fits-all approach, including the imposition of costly and poorly defined mandates on businesses for the fulfillment of access and deletion requests, to personal information raises serious concerns from both a compliance and enforcement perspective.

Automotive Specific Concerns

While the concerns noted above apply across all industries, their impacts raise unique problems for vehicle manufacturers. When looking at records tied to a vehicle, automakers may have little insight into who was driving or otherwise riding in the vehicle at the time that the information was collected. Allowing non-owners access and deletion rights may risk disclosure of personally identifiable information (PII) of others in the vehicle. For instance, residents involved in domestic disputes could use this data to spy on each other in regard to their usage of the vehicle. Such concerns are very real and serve as a detriment to privacy.

To comply with requests from non-owners, automakers might need to collect and process personal information beyond that needed to provide vehicle services. As a result, SB 11 may practically require that non-identified personal information that a business holds be matched with identifiable personal information to comply with an access or deletion request. This means that a business will need to collect more data from a consumer.

The definition of collection of data is extremely broad. There is no provision on how SB 11 might be applied to information that is collected on a vehicle and not immediately accessed by the manufacturer but could be accessed by the business at some point in the future. Automakers use vehicle-level data they collect for analysis related to motor vehicle safety, performance, and security to comply with the standards set forth by NHTSA. Moreover, this data is crucial to the development, training, implementation, and assessment of automated vehicle technologies, advanced driver-assistance systems, and other life-saving vehicle technologies.

Automakers need to share this information with affiliate companies within the organization that focus on specified tasks within the manufacturing ecosystem, such as R&D, manufacturing, and warranties. If automakers are required, in response to a deletion request, to delete all information that could reasonably be linked to a vehicle, or are forbidden form sharing such information internally, that would negatively result in automakers not being able to use the information to develop, test, and deploy vehicles and technologies that will save lives.

Automakers, independent dealerships, and suppliers share information for purposes that benefit consumers and the public. Sharing vehicle information enables dealerships to access full repair histories for vehicles, makes it easier for consumers to obtain services from multiple dealerships, enables suppliers to use vehicle-level data to improve safety, security, and performance for vehicle parts and systems, and allows suppliers and dealers to share vehicle- or part-related information with automakers for safety, security, warranty, or other purposes. California realized the importance of this and subsequently amended their allow to not allow consumers to opt-out of 'selling' or sharing their vehicle data to a third party when it is shared for the purpose of vehicle repair related to a warranty or a recall

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

SB 11 CTIA UNF.pdf
Uploaded by: Lisa McCabe
Position: UNF

Testimony of
LISA MCCABE
CTIA

Senate Bill 11

Before the
Maryland Senate Finance Committee
January 26, 2022

Chair Kelley, Vice Chair Feldman, and members of the committee, on behalf of CTIA®, the trade association for the wireless communications industry, thank you for the opportunity to provide this testimony on Senate Bill 11, which would establish state regulations to address an inherently national and global issue: the protection of personal data. A state law that sweeps too broadly, as these bills do, will create security risks and presents serious compliance challenges for businesses.

State legislation that sweeps too broadly could have a negative effect. This bill has some commonalities with a California privacy statute initially adopted in 2018, and exemplifies overly broad legislation that is difficult and costly to implement. Bills were passed by the California legislature in an attempt to clarify the statute in 2019 and again in 2020. Then a ballot measure – the California Privacy Rights Act – was passed in November 2020, which further changed the law, imposing new requirements effective 2023. And the statute called for implementing regulations, which have been voluminous, and additional regulations will follow as a result of the new requirements under the ballot measure. Even with the serial changes and extensive regulations, the scope of the statute remains broad and ambiguous, making

compliance difficult and expensive for business.

In 2021, Colorado and Virginia likewise passed comprehensive privacy laws that have yet to be implemented. We now truly have a patchwork of state laws that will confuse consumers and burden businesses. Maryland should not rush to follow other states down this path to the detriment of both consumers and businesses.

This bill, like the California statute, creates broad access requirements that are in tension with data security principles, as they may encourage companies to centralize—rather than segregate—customer data in one location, pool customer data about particular consumers in one location, and/or maintain customer data in personally identifiable form, all to be able to comply with customer requests.

Requirements like the ones included in SB 11 put more burdens on companies in their efforts to prevent unauthorized access to data, which can be an attractive target to identity thieves and cybercriminals. In the United Kingdom, a white hat hacker was able to get his fiancée's credit card information, passwords, and identification numbers by making a false request.[1] Similar scenarios will likely happen in Maryland if the state enacts SB 11.

The practical implications of requirements permitting consumers to delete their data are unclear. These requirements may undermine important fraud prevention activities by allowing bad actors to suppress information. Businesses may also have to delete data that will

[1] Leo Kelion, Black Hat: GDPR privacy law exploited to reveal personal data, BBC (August 8, 2019).

help them track the quality of service to improve their products.

Moreover, the broad opt-out provisions in the bill may jeopardize the availability or quality of free or low-cost goods and services, which rely on the use of personal data that is subject to safeguards, such as pseudonymization. Online news sites, content providers, and apps are often provided to consumers free of charge because they are supported by advertising. These content providers should not be forced to continue to offer free services to consumers who opt-out of disclosing online identifiers to advertisers. While consumers should always be provided meaningful notice and choice before their personal data is used, that choice should be balanced against the numerous benefits to consumers.

While it is clear that these provisions create risk for consumers and cost for businesses, it is not clear that their benefits outweigh these risks. In Europe, consumers get reams and reams of data when they submit access requests, and they are constantly bombarded with pop-up windows as they browse the internet. Does this enhance their privacy or make their data more secure?

The stakes involved in consumer privacy legislation are high. Being too hasty to regulate could have serious consequences for consumers, innovation, and competition. Regulation can reduce the data that is available for research and for promising new solutions by putting too many constraints on the uses and flow of data. We are starting to see indications of this in Europe, where sweeping new privacy regulations took effect in 2018 and investment

in EU technology ventures has declined.[2] Similarly, the United States leads Europe in the development of Artificial Intelligence, and experts believe that Europe's new data protection laws will increase this competitive disadvantage.[3]

The broad privacy law in the E.U. has resulted in confusion for both small businesses and consumers. For example, a hairdresser refused to provide a customer with the brand and type of hair color used due concerns over data protection and a paramedic was denied the medical history of an unconscious patient over privacy law concerns.[4]

Additionally, in order to address some of the unintended consequences of broad privacy regulations, in the U.K., which has a statute similar to that in the E.U., the government recently signaled its intention, following Brexit, to revisit the U.K. General Data Protection Regulation (UK GDPR). The reforms in the U.K. are aimed at reducing barriers to innovation; reducing burdens on businesses and delivering better outcomes for people; boosting trade and reducing barriers to data flows; delivering better public services; and reform of the UK regulator, the Information Commissioner's Office.[5]

Any new state privacy law will contribute to a patchwork of regulation that will confuse

---

[2] Jia, Jian and Zhe Jin, Ginger and Wagman, Liad, "The Short-Run Effects of GDPR on Technology Venture" Investment, *National Bureau of Economic Research* (November 2018).
[3] Daniel Castro and Eline Chivot, Want Europe to have the best AI? Reform the GDPR, IAPP Privacy Perspectives (May 23, 2019).
[4] Hairdresser told customer she couldn't get details about hair dye due to 'GDPR concerns', Independent.ie, November 19, 2021
[5] Significant Changes Proposed to UK GDPR, JD Supra, (September 23, 2021).

consumers and burden businesses that operate in more than one state. Should the data of consumers who live in border cities and towns be treated differently when they cross the Maryland border? Should businesses with operations in multiple states segregate the data of Maryland citizens?

Much of the focus in the privacy debate thus far has been on compliance costs and the impact on larger companies, but regulation impacts business of all sizes. As part of the California Attorney General's regulatory process, the office commissioned an economic impact study.[6] The study found that the total cost of initial compliance with the law would be approximately $55 billion or 1.8% of the state's gross domestic product.[7]

The study further found that "[s]mall firms are likely to face a disproportionately higher share of compliance costs relative to larger enterprises.[8] These compliance costs include new business practices, operations and technology costs, training requirements, recordkeeping requirements, and other legal fees. It goes on to further state that "conventional wisdom may suggest that stronger privacy regulations will adversely impact large technology firms … however evidence from the EU suggests that the opposite may be true."[9] The study found that many smaller firms have struggled to meet compliance costs. The EU regulation of privacy

---

[6] See Standardized Regulatory impact Assessment: California Consumer Privacy Act of 2018 Regulations, Berkeley Economic Advising and Research, LLC (August 2019).
[7] *Id* at 11.
[8] *Id* at 31.
[9] *Id* at 31.

seems to have strengthened the position of the dominant online advertising companies, while a number of smaller online services shut down rather than face compliance costs. SB 11 includes a threshold of applying to an entity that processes or maintains the personal information of 100,000 or more consumers, or devices during the course of a calendar year. This translates to just over 273 unique transactions per day, which would likely impact a small business in Maryland.

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 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. Taking the wrong approach could have serious consequences for consumers, innovation, and competition in Maryland. Moving forward with broad and sweeping state legislation would only complicate federal efforts while imposing serious compliance challenges on businesses and ultimately confusing consumers. As we support a comprehensive federal privacy law, we oppose further fragmentation that would also arise from passage of SB 11.

As mentioned, California is still a moving target and Virginia and Colorado have yet to implement their laws. It is simply not clear that we have found a good formula for regulating privacy. As such, CTIA opposes SB 11 and respectfully urges the committee not to move this bill.

SB 11_MDCC_Maryland Online Consumer Protection Act
Uploaded by: Maddy Voytek
Position: UNF

MARYLAND
Chamber of Commerce

LEGISLATIVE POSITION
Unfavorable
Senate Bill 11
Maryland Online Consumer Protection and Child Safety Act
Senate Finance Committee
Wednesday, February 26, 2022

Dear Chairwoman Kelley 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 5,500 members and federated partners working to develop and promote strong public policy that ensures sustained economic health and growth for Maryland businesses, employees, and families.

Senate Bill 11 creates numerous personal information privacy rights for consumers in the state. Specifically, the bill requires a business that collects a consumer's personal information to clearly and conspicuously notify a consumer of (1) the categories of personal information being collected; (2) the business purposes for which the information will be used; (3) the categories of third parties the business discloses information to; (4) the business purpose for the third party disclosure; and (5) the consumer's right to request a copy of the personal information collected, deletion of the personal information and to opt out of third party disclosure.

As referenced above, this bill uses "third-party disclosure" instead of "selling" and allows consumers to opt out of this. However, this definition is much broader than what "selling" means (i.e., releasing, transferring, making available, etc.) in other laws and goes beyond sharing personal information for monetary gain. This very broad definition goes beyond the California Consumer Privacy Act (CCPA)/California Privacy Rights Act (CPRA).

This legislation, as introduced, will have a significant negative impact on Maryland's business community. Although this bill does not have an explicit private right of action, the language does refer to Maryland's unfair/deceptive trade practices law, which does have private right of action.

For these reasons, the Maryland Chamber of Commerce respectfully requests an **Unfavorable Report** on Senate Bill 11.

NAMIC SB 11 letter.pdf
Uploaded by: Matt Overturf
Position: UNF

NAMIC
NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES

317.875.5250 | [F] 317.879.8408
3601 Vincennes Road, Indianapolis, Indiana 46268

202.628.1558 | [F] 202.628.1601
20 F Street N.W., Suite 510 | Washington, D.C. 20001

January 24, 2022

The Honorable Delores Kelley
Chair, Senate Finance Committee
3 East Miller Senate Office Building
11 Bladen Street
Annapolis, Maryland 21401

RE: Senate Bill 11 – Maryland Online Consumer Protection and Child Safety Act- UNFAVORABLE

Dear Chairwoman Kelley and Members of the Senate Finance Committee,

My name is Matt Overturf on behalf of the National Association of Mutual Insurance Companies (NAMIC). NAMIC is the nation's largest trade association with more than 1,400 members, 22 of which are domiciled in Maryland. NAMIC requests and unfavorable report on Senate Bill 11 (SB 11).

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. Insurers must collect and use personal information to perform essential business functions – for example, to underwrite applications for new insurance policies, and to pay claims submitted under these policies. 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. Therefore, the insurance industry would be uniquely affected by the establishment of new general privacy requirements at the individual state level.

Senate Bill 11 would add to the mix of existing privacy laws for insurers. While NAMIC is pleased to see Sec. 14-4402 (6) with the Gramm-Leach-Bliley Act (GLBA) exception, this working differs from what we have seen elsewhere, and we are still in the process of reviewing its possible implications. Because Maryland has also acted in this area with respect to insurers, this exception should be expanded to encompass the state-specific wording as well but adding something like: …and A financial institution or any of its affiliated companies that are subject to the rules and implementing regulations promulgated under the specifically reference state enabling law and implementing regulation Again, NAMIC is continuing to review for complexities and expense of implementation and possible conflicting scopes, definitions, notice requirement and consumer rights.

NAMIC appreciates the opportunity to provide our concerns with the committee and request an unfavorable report on SB 11.

Thank you,

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

sb11.pdf
Uploaded by: Sara Elalamy
Position: UNF

MARYLAND JUDICIAL CONFERENCE
GOVERNMENT RELATIONS AND PUBLIC AFFAIRS

Hon. Joseph M. Getty
Chief Judge

187 Harry S. Truman Parkway
Annapolis, MD 21401

MEMORANDUM

TO:	Senate Finance Committee
FROM:	Legislative Committee Suzanne D. Pelz, Esq. 410-260-1523
RE:	Senate Bill 11 Maryland Online Consumer Protection and Child Safety Act
DATE:	January 26, 2022 (1/26)
POSITION:	Oppose as drafted

The Maryland Judiciary opposes Senate Bill 11 as drafted. This bill creates new provisions regulating the use and collection of consumer's personal information.

The Judiciary has no position on the intent and majority of this legislation. The Judiciary is concerned only with the particular language on page 18, §14-4414 which provides "IF A SERIES OF STEPS OR TRANSACTIONS IS ENGAGED WHERE COMPONENT PARTS OF A SINGLE TRANSACTION ARE TAKEN WITH THE INTENT OF AVOIDING THE REQUIREMENTS OF THIS SUBTITLE, A COURT SHALL DISREGARD THE INTERMEDIATE STEPS OR TRANSACTIONS FOR PURPOSES OF CARRYING OUT THIS SUBTITLE." This language is confusing and the court is not sure what this language actually provides. The Judiciary would need clarification on this language to ensure the bill is implemented correctly if the bill were to pass.

cc. Hon. Susan Lee
Judicial Council
Legislative Committee
Kelley O'Connor