

OAG_FAV_SB957

Uploaded by: Abrams, Hanna

Position: FAV

BRIAN E. FROSH
Attorney General

WILLIAM D. GRUHN
Chief

ELIZABETH F. HARRIS
Chief Deputy Attorney General



CAROLYN QUATTROCKI
Deputy Attorney General

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL

FACSIMILE NO.

WRITER'S DIRECT DIAL NO.

(410) 576-6566 (F)

(410) 576-7296

February 19, 2020

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

FROM: Hanna Abrams, Assistant Attorney General

RE: Senate Bill 957 – Maryland Online Consumer Protection Act (SUPPORT)

The Office of the Attorney General supports Senate Bill 957 (“SB 957”), which gives Marylanders back control over their personal information.

Americans want privacy protection. In a November 2019 poll by Pew Research, three quarters of Americans said there should be new regulation of what companies may do with personal data.¹ The same study found that “79% of adults assert they are very or somewhat concerned about how companies are using the data they collect about them,” and 75% of respondents said they are “not too or not at all confident that companies will be held accountable by government if they misuse data.”² Senate Bill 957 would address those concerns.

Right now, companies are collecting and selling increasing amounts of sensitive information about our lives without our knowledge or consent. Data breaches occur on a seemingly daily basis, and the unencumbered collection and use of our personal information, including precise location information, poses serious privacy and physical safety threats. Headlines involving tens of millions or more people being exposed online have become commonplace. Consider the revelations involving Facebook and Cambridge Analytica for example. Facebook allowed sensitive and deeply personal information to be collected from over 50 million people without their knowledge or consent. This isn't an anomaly. The tech industry exploits and sells the most sensitive details about our private lives, including details beyond what we reveal willingly. Companies are collecting information that gives strangers personal information about us including gender, religious beliefs, sexual preferences, and even our precise location. 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.

¹ Pew Research Center, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information* (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americansand-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

² *Id.*

Companies collect data from a variety of sources: web browsing trackers, social media companies, household electronic appliances, apps, public records, and many others. Everything from music streaming to weather apps collect your data and you don't even have to be awake; smartphone apps continue to collect information and disseminate it while you sleep.³

The adtech industry is out of control in its data sharing, selling, and processing practices and it shows no signs of self-policing. 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 lack of an overarching privacy law to protect Marylanders has resulted in the regular collection and use of personal information without consent. A constant stream of discoveries shows how this data is being monetized:

- A New York Times investigation found that many of the apps that collect location information for localized news, weather, and other location services repurpose or share that information with third parties for advertising and other purposes. The investigation also suggested that users believe they are sharing location data only for a specific service, not giving free rein for any use sharing.⁵
- General Motors bragged to an association of advertisers that the company had secretly gathered data on driver's radio-listening habits and where they were when listening "just because [they] could."⁶ This data was exfiltrated from cars using built-in wireless network, which consumers could only use if they agreed to GM's terms of service, but consumers were never informed about this data collection.
- Madison Square Garden deployed facial recognition technology purportedly for security purposes, while vendors and team representatives said the system was most useful for customer engagement and marketing.⁷
- The application developer Alphonso created over 200 games, including ones targeting children, that turn on a phone's microphone solely for marketing purposes.⁸

³ Geoffrey Fowler,, *It's the middle of the night. Do you know who your iPhone is talking to?*, Wash. Post. (May 28, 2019), <https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/> (reporting that in a single week, he encountered over 5,400 trackers, mostly in the form of smartphone apps).

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 Jennifer Valentino DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times, (Dec. 10, 2018), <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html>.

⁶ Cory Doctorow, *Every Minute for Three Months, GM Secretly Gathered Data on 90,000 Drivers' Radio Listening Habits and Locations*, BoingBoing (Oct. 23, 2018), <https://boingboing.net/2018/10/23/dont-touch-that-dial.html>.

⁷ Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, N.Y. Times, (Mar. 13, 2018), <https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html>.

⁸ Sapna Maheshwari, *That Game on Your Phone May Be Tracking What You Watch on TV*, N.Y. Times (Dec. 28, 2017), <https://www.nytimes.com/2017/12/28/business/media/alphonso-app-tracking.html>.

Apps frequently share information that is wholly unconnected to the service that the consumer initially signed up for. For example, makeup filter apps may share the precise GPS coordinates of its users; ovulation, period and mood-tracking apps share users' personal information with Facebook and Google; dating apps exchange user data with each other, and also share sensitive user information with third parties.⁹

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 to Facebook or Google without even disclosing this to users.¹⁰ The collection of information is not limited to apps; studies found that voice assistants such as Alexa and Google Assistant listen and record even when you are not speaking to them. In many instances, the recorded conversation was sent not just to Amazon's and Google's servers, but also to third-party developers.¹¹ In other words, if you have a smart speaker, it may be spying on you inside your home, recording your conversations, and even disseminating them to third parties unbeknownst to you.

In many instances, the personal information that companies are collecting can be used in ways that have resulted in real world harm beyond privacy concerns. For example, personal information has been used to limit individuals' access to opportunities or threaten their safety:

- Employers have consciously targeted advertisements at younger men to keep older workers and females from learning of certain job opportunities,¹² and landlords have prevented racial minorities from seeing certain housing advertisements.¹³
- 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 their phones behind when traveling to sensitive locations or turning their phones off altogether.¹⁴

⁹ 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>.

¹⁰ 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.

¹¹ Ben Fox Rubin, *Amazon Looks to Expand Alexa's World Amid Growing Privacy Concerns*, CNET (Sept. 23, 2019), <https://www.cnet.com/news/amazon-looks-to-expand-alexa-world-amid-growing-privacy-concerns/>.

¹² 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>.

¹³ 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>.

¹⁴ 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>.

- A Motherboard investigation found that bounty hunters could access detailed location data sold by ISPs.¹⁵

Consumers do not want their personal data being used for purposes beyond providing the service they signed up for. SB 957 is designed to give Marylanders control over their personal information. It forces companies to disclose what data they are collecting and allows consumers to decide whether to opt out of having their information collected, maintained, or sold. This ensures the protection and safety of Marylanders.

The tools that we currently have in place come into play after a breach has already occurred. The Maryland Personal Information Protection Act (“MPIPA”) is the Attorney General’s Office’s main tool in this area. After a breach, we investigate whether the company had taken reasonable steps to protect personal information, and whether they should have prevented the breach. If they were at fault, we pursue MPIPA enforcement actions against them to hold them accountable.¹⁶

But this bill provides something more – it is preventative. It gives consumers the ability to protect themselves. It is a proactive step to limit the amount of consumers’ personal information that is available for hackers to find.

SB 957 shines a light on what happens with consumer data, and gives consumers control over their data. This is the best way to protect Marylanders from the harms of data breaches.

CONSUMER RIGHTS UNDER SB 957

The Right of Transparency

Transparency is the first critical step – it allows consumers to make informed decisions. SB 957 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).¹⁷ Businesses will also include the same information in their online privacy policies.¹⁸

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.¹⁹ Businesses must provide accessible methods of making requests for this information.²⁰

¹⁵ Joseph Cox, *I gave a bounty hunter \$300. Then he located our phone*, Motherboard (Jan. 8, 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phonemicrobilt-zumigo-tmobile.

¹⁶ Misuse of consumer data could also violate the Consumer Protection Act, Md. Code Ann., Com. Law §§ 13-101, *et seq.*

¹⁷ Section 14-4202.

¹⁸ Section 14-4204(d).

¹⁹ Section 14-4203.

²⁰ Section 14-4204.

The Right to Delete

The most important aspect of consumer control is the right to request that their personal information be deleted. SB 957 would require businesses to honor consumer requests to delete personal information the business collected about them.²¹ It makes ample exceptions, to allow businesses to keep information for research purposes, and where required by law.²²

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.²³ Consumers will be able to exercise this right via a clear and conspicuous link on the business’ website.²⁴

The bill provides further protection to minors, barring businesses from disclosing their information to third parties.²⁵

The Right of Non-Discrimination

The bill takes an important step – it bans discrimination against anyone who exercises one of the above-described rights.²⁶ 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

Unlike consumers’ feelings toward a business using their personal information to make a profit, studies have indicated that most consumers (78%) are willing to allow their personal information to be used for research for the public good.²⁷ This bill reflects that, and 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.²⁸

The Businesses Impacted by SB 957 Comply with Similar Requirements in Other Statutory Schemes

SB 957 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

²¹ Section 14-4205.

²² Section 14-4205(d).

²³ Section 14-4206.

²⁴ Section 14-4206(d).

²⁵ Section 14-4206(b).

²⁶ Section 14-4207.

²⁷ *See, e.g.,* Personal Data for the Public Good: New Opportunities to Enrich Understanding of Individual and Population Health, Final Report of the Health Data Exploration Project, UC Irvine and UC San Diego (2014).

²⁸ Section 14-4205(d)(5); *see also* Section 14-4209 (requiring privacy and security protections for personal information used for research purposes).

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 957.²⁹ Moreover, the impact of SB 987 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 2020.³⁰ 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 thus far.

Definition of Consumer

SB 957 defines “consumer” as “an individual who resides in the state.”³¹ 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 957 incorporates several exemptions, including for personal information collected pursuant to the federal Gramm-Leach-Bliley Act (“GLBA”) and implementing regulations.³² 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 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 957 does not alter those regulations. Financial institutions have the same obligation to protect personal information under the California Consumer Privacy Act.³³

Privacy legislation must (1) provide individual rights to access, correct, delete, and port personal information; (2) require reasonable data security and corporate responsibility; (3) prohibit unfair data practices, particularly the repurposing or secondary use of sensitive data, with carefully scoped exceptions; (4) prevent data-driven discrimination and civil rights abuses; and (5) provide robust and rigorous enforcement. SB 957 provides these protections to Marylanders.

We urge a favorable report.

Cc: Members, Finance Committee

The Honorable Susan Lee

²⁹ Section 14-4201(d).

³⁰ 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 957 and the CCPA.

³¹ Section 14-4201(g).

³² Section 14-4208(b)(8).

³³ Cal. Civ. Code §§ 1798.100-199.

SB957_FAV_Lee

Uploaded by: Senator Lee, Senator 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 Emeritus
Maryland Legislative Asian American
and Pacific Islander Caucus

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



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

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

February 19, 2020

Senate Finance Committee

Senate Bill 957 – Maryland Online Consumer Protection Act

SB 957 is landmark online privacy legislation that will empower Marylanders to better understand, protect and control what personal data is collected about them and how businesses utilize personal information to analyze your individual activities. Algorithms are the new temples that everyone from business, government and non-profits worship at the altar. While these devices have utility, they encourage data harvesting and packaging of individuals' information to a level of preciseness that they can predict and even modify your behavior.

Privacy is dying and our democratic institutions have been infected. Our values seem to carry less value than our purchasing power, or our social media connections. It is time to take back data ownership, it is time to take back our privacy. SB 957 is the privacy bill Marylanders require and a bill that should be easy for companies to implement because they already apply the same provisions to Californians. Is comprehensive personal information about Marylanders less important? Do we expect Congress to act?

Data recently surpassed oil as the most valuable asset in the world, because the personal data that businesses collect about us allow them to peer into even the most intimate and sensitive facets of our lives to market consumer goods and policy proposals to; but for all its value and sensitivity, the collection and sharing of Marylanders' personal information is not governed by comprehensive privacy protections beyond bare bones data breach notification laws that only touch personally identifiable information that traditionally was used to steal an identity. California recently enacted a more comprehensive law that has had an impact across the country, but some large corporations are limiting the benefits so they don't reach Marylanders. Not because they can't extend those benefits, but because they don't want to stop monetizing your

data, and can't be bothered to take measures to protect your privacy. We have worked with them to try and find compromise language but there is an ideological divide about the role of state government in the solution.

Many individuals around the globe already have protections to strengthen data ownership and consumer protection from digital advertising firms. Jurisdictions outside of Maryland have established rules of the road in this space, and those rules are already being enforced. In Europe, the General Data Privacy Regulation (GDPR) was implemented in 2018, and enforcement of a similar initiative in California, the California Consumer Protection Act (CCPA), began on January 1 of this year. The CCPA was used as a model for this legislation, and will be fully enforceable July 1st of this year, so we are waiting for final regulations, but we know the lay of the land already and don't need to wait for all of the details to fall into place to start policing this space. Elected officials around the world are taking action to give consumers the tools to protect themselves in the digital Wild West; it's time we do the same for consumers in Maryland.

The Maryland Online Consumer Privacy Act (MOCOPA) affords Marylanders five basic rights in the digital landscape:

1. Marylanders will have the **right to know what categories of personal information a business will collect about them**, at or before the point of collection;
2. Marylanders will have the **right to obtain the specific personal information that businesses have collected** about them;
3. Marylanders will have the **right to know what personal information collected about them has been shared, sold or otherwise disclosed, to a third party**, and why that information was disclosed;
4. Marylanders will have the **right to request that a business delete the personal information they have collected** about that consumer;
5. Marylanders will have the **right to opt-out of future disclosure of their personal information to a third party**;

I want to highlight a few important sections and provisions in the bill that expand on these basic rights. Please walk through the bill with me, so I can help demystify these provisions one-by-one. Privacy is a complicated subject, but don't let the opposition muddy the waters, this is not rocket science.

Page 2 of the bill contains the definitions under Section 14-4201. Note that aggregate information that is not individualized is not subject to the provisions of the bill. The bill only applies to businesses that either have gross revenues in excess of \$25 million, touches 100,000 consumers or households, or derives at least half of its annual revenues from selling consumers' personal information. A "consumer" is defined on the top of page 2 as an individual who resides in the state. There is an explicit business to business exception through this definition of consumer to be an individual who resides in Maryland. Page 5 contains the definition of

“personal information” and explicitly clarifies that de-identified consumer information is not included, nor is aggregate or publicly available information.

On page 7, Section 14-4202 is the notice provision and establishes the right of a consumer to know what personal information will be collected about them. This essentially codifies what any responsible business already discloses in their privacy policy, and adds that a business must notify a consumer of their new rights under this bill, namely, the right to request a copy of personal information, the right to delete that personal information, and the right to opt-out of third-party disclosure of personal information. The section also requires that a business notify a consumer before beginning to collect additional personal information from that consumer.

On page 8, Section 14-4203 establishes the right of a consumer to obtain their own personal information from a business. A business is required to 1) disclose all pieces of personal information that a business has collected about that consumer, 2) disclose how that information was collected, and 3) disclose what third-parties that information has been disclosed to, and for what purpose that information was disclosed. All of this information is to be provided free of charge to the consumer once every six months upon request; businesses are allowed to charge a reasonable fee or deny a request for subsequent requests made in a six-month period. This provision protects companies from excessive and repetitive compliance costs. There is a carve-out so that companies are not required to share the personal data of a consumer to that consumer if that disclosure would adversely affect the legal rights of another consumer. Further, none of the information detailed above is to be disclosed without a **verifiable consumer request** for that information.

“Verifiable consumer request” is an important item to understand, as it is required for a consumer to exercise many of the rights enshrined in this bill. Our bill doesn’t define verifiable consumer request clearly, instead, we defer to the Attorney General to develop those regulations. The California Consumer Protection Act uses the exact same language as we do in our bill, and the California Attorney General has been able to define verifiable consumer request effectively and with nuance to require different levels of verification for access to data of different sensitivities. By requiring a verifiable consumer request, we protect consumers and companies from others fraudulent access or deletion of their data.

On page 11, Section 14-4205 establishes the right of a consumer to request that a business delete their personal information. We include a robust set of carve-outs that mirror the California law to ensure that we balance the privacy interests of a consumer against the need of a business to maintain information to deliver services, engage in research, protect other consumers’ personal information, and comply with other legal obligations. This is the provision the banks and insurance companies don’t want to follow. They are going to argue they should be exempt as an institution because they don’t sell data to third parties under the federal banking and insurance law known as the Gramm-Leach-Bliley Act (GLBA). What they won’t tell you is that they don’t want to allow you to delete your data that is not covered under the federal GLBA. We have a

solution for them in the loyalty card section. The bill already explicitly carves out all information already covered under the GLBA, and their request is to be carved out of having to delete data that is unassociated with the GLBA information they are collecting, without even clarifying what they would use that data for in the future.

Jumping ahead a bit to page 15, subsection (6) of 14-4208 explicitly does not apply to personal information collected, processed, sold, or disclosed under the GLBA and implementing regulations. If there is personal information the banks have about you that is not covered under the GLBA, it should be covered under this legislation. There is no need for a carve out with the loyalty card exception language.

On page 12, Section 14-4206 establishes the right of a consumer to opt-out of all disclosure of their personal data to a third party. The section establishes a ban on the disclosure of the third-party disclosure of an individual under 16 years old, in line with the California provision. Section 14-4206 allows consumers to opt-out of third-party *disclosure*, this is a clarification from the California law that referred only to sales but has expanded the scope of that definition to cover entities like Facebook that argue they don't sell data. The goal of this section is to protect consumer privacy by preventing third-party access to consumer data; whether that data was sold or simply shared with the third-party by the collecting party is irrelevant for the purpose of the legislation. The industry groups see potential gaps in the law as loopholes to drive their organizations through safely without regulation, we must be vigilant to not allow the exceptions to gut the rule.

But we are happy to extend certain protections such as the loyalty programs. We have an amendment to make it possible for businesses to have a loyalty program, which provides certain benefits to customers who want to waive their right under this section to be able to delete their information. This should satisfy the bank and insurance companies' main concerns that they don't want to have to delete information upon request. On page 13, Section 14-4207 importantly provides that a company cannot discriminate against a consumer for exercising any of the rights established above but for loyalty program there would be an exception for the right to delete provision.

These protections and provisions are akin to a consumer bill of rights for the 21st century.

I'm sure you've noticed that I've referenced California a number of times in my testimony, and that's because, for almost every intent and purpose other than strengthening the third-party opt-out under 14-4206, this bill is an attempt to mimic the thresholds within the California Consumer Protection Act.

There are ongoing discussions about federal data privacy legislation, but because many of those discussions center around preemption goal rather than protecting privacy and with Congress' general dysfunction, we don't see those efforts materializing anytime soon. Industry argues that if a federal privacy law does not preempt state action soon, a 50-state patchwork of different

privacy standards will develop. That patchwork, the argument goes, would stifle the innovative spirit of the internet because only the very largest companies would be able to navigate the complicated and expensive compliance costs associated with such a patchwork. What we are showing here in Maryland is that the states can follow California's lead and we don't have to wait for Congress to act. Why would we wait for **more than a few years** for Congress to compromise on what would almost certainly be **weaker privacy protections than those that already exist in California, when we can force companies that are already offering strong protections to Californians to simply extend those same protection to Marylanders too.**

A number of companies already allow non-Californians to exercise the rights established under the CCPA. Right now, it doesn't matter if you're a Marylander or a Californian, you can request that Amazon, Netflix, Facebook and Uber, among others, delete your personal information or not sell that information to a third-party, and those businesses will comply. However, if you're a Marylander and want to the same thing with the information that AT&T, Disney, eBay, Equifax, Marriott, Lyft and dozens of more companies, those businesses will not comply with your request, **even though they are complying with those same requests for consumers in California.** There are no compelling differences between these companies; on one side is Uber and Amazon, on the other is Lyft and eBay, the only difference is whether they have chosen to offer the same protections to all Americans that they are already required to offer to Californians.

The patchwork we should be concerned about isn't one that drives up compliance costs for businesses; it's one that allows business to offer strong privacy protections to some consumers and weak protections to others, simply because they can save a dime by doing so. By passing this bill, we can show Maryland consumers that their privacy is just as important as the privacy of California consumers, and we can show the federal government that the states can limit compliance costs for business without undercutting the strong protections California has enshrined.

As mentioned before, there are some amendments in your packet to clean up some drafting mistakes concerning the loyalty program and to provide additional consistency with the California Consumer Protection Act.

For all these reasons, I respectfully request a favorable report on SB957, as amended.

MCRC-White_Favorable_SB0957

Uploaded by: White, Marceline

Position: FAV



Maryland Consumer Rights Coalition

**Testimony to the Senate Finance Committee
SB 957: Online Consumer Protection Act
Position: Favorable**

February 19, 2020

Senator Delores Kelley, Chair
Senate Finance Committee
3 East Miller Senate Office Building
Annapolis, MD 21401
Cc: Members, Senate Finance

Honorable Chairwoman Kelley and Members of the Committee:

The Maryland Consumer Rights Coalition (MCRC) is a statewide coalition of individuals and organizations that advances financial justice and economic inclusion for Maryland consumers through research, education, direct service, and advocacy. Our 8,500 supporters include consumer advocates, practitioners, and low-income and working families throughout Maryland. We are writing today in support of SB 957, which would expand and create a series of crucial consumer protections for internet users.

In recent years, large and small web companies have demonstrated their willingness to exploit consumer trust for financial gain. Scandals over the past few years involving major tech companies – including Facebook, AOL, Google, and more – demonstrate a clear need for guardrails to protect consumers privacy and wellbeing.

While many of these significant online privacy breaches involve underlying technologies – like webcams, GPS, etc. – the heart of these troublesome disruptions are companies collecting personal data without the user's knowledge or consent and then either sharing it with third parties or simply failing to keep it safe.

There are major consequences to online firms failing to protect users' information. When websites neglect to adequately protect a consumer's personal information, identity theft and cyber fraud can follow. The sale of an internet user's profile or browsing habits can lead to harassment by "lead generators," including predatory for-profit colleges that buy this surreptitiously collected data to target low-income students for high-cost, low-return programs.¹

Beyond these clear and tangible dangers presented by unregulated internet businesses, there is also the simpler issue of consumer privacy. Americans use the internet for just about everything these days – to shop for insurance, communicate with their healthcare providers, purchase day-to-day needs, etc. Children – even very young children – use the internet as well. Many internet firms currently collect data from all these users and resell it to other companies for the purposes of creating targeted ads.

¹https://www.democraticmedia.org/sites/default/files/field/public-files/2015/forprofitcollegeleadgenreport_may2015_uspirgef_cdd_0.pdf



Consumers have few opportunities to consent to have this data collected and sold, and even fewer opportunities to remove their data from websites should they choose to do so. Last year, the Wall Street Journal reported that internet and phone apps collecting very personal data – including fertility tracking information – was being sold directly to Facebook for a profit.² These kinds of actions aren't just disturbing, they're clear violations of internet users' right to privacy – and Maryland has a responsibility to protect our state's individuals, children, and families from companies looking to sell personal information for monetary gain.

These types of concerns, as well as consumer privacy concerns have led other states and countries to implement new laws and regulations to expand data protections for users.

- This January, California's Consumer Privacy Act (CCPA) took effect. This landmark legislation ensures that consumers have the right to know what information companies are collecting about them, why that data is being collected, who their data is being shared with, etc. It also gives internet users the right to tell companies to delete their information, and/or not sell or share it.³ Since it has gone into effect, consumers have been using the protections that have been put in place.
- Also in 2018, Europe's General Data Protection Regulation (GDPR) took effect. This EU-wide regulation created a new framework developed through four years of discussion and negotiation meant to protect consumers on the internet. It provides crucial consumer rights, including a right to be forgotten, a right to demand one's personal information from a website be released to that individual, a need for internet companies to get greater consent from users, etc. This law is being called the world's most comprehensive internet privacy regulation.⁴

Because of the borderless nature of the internet, large companies are already complying with internet privacy legislation in California and in Europe, so they should not have trouble adhering to similar legislation in our state. In fact, it would be less burdensome for large companies to simply modify their privacy protections nationally, as a number of states including Florida, Illinois, New Hampshire, Virginia, and Washington state are introducing privacy measures⁵.

SB 957 is good public policy that updates Maryland's laws to be responsive to the changing technological world and the realities of the current internet climate. It shouldn't take an extensive knowledge of the internet and its inner-workings to protect one's own privacy – it should be an inalienable right for consumers to have control and consent over whether their personal information is bought and sold by faceless online firms. For all of those reasons the Maryland Consumer Rights Coalition supports SB 957 and urges a favorable report.

Best,

Marceline White

² <https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636>

³ <https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html>

⁴ <https://blog.centrifify.com/consumer-privacy-benefits-gdpr/amp/>

⁵ <https://www.natlawreview.com/article/additional-us-states-advance-state-privacy-legislation-trend-2020>



Maryland Consumer Rights Coalition

Executive Director

CommonSenseMedia_FWA_SB957

Uploaded by: Jerome, Joseph

Position: FWA



February 19, 2020

The Honorable Delores G. Kelley, Chair
Senate Finance Committee Members
3 East
Miller Senate Office Building
Annapolis, MD 21401

RE: SB957, the Online Consumer Protection Act—SUPPORT

Dear Chair Kelley and Members of the Committee:

Thank you for considering the Online Consumer Protection Act (SB957).

Common Sense is a national organization representing kids, parents, and educators that is dedicated to helping kids and families thrive online and on social media. Common Sense has over 108 million users, and our educational materials are used in 50% of US schools, including by over 8,000 teachers in Maryland. Common Sense was a sponsor of California's precedent-setting consumer privacy law, the California Consumer Privacy Act (CCPA). We have also sponsored and supported privacy laws across the country and at the federal level.

We support the Online Consumer Protection Act as an important first step towards protecting Maryland's privacy.

The daily drumbeat of data misuse and abuse is adding to a growing distrust of the online and tech world. And concerns are particularly acute for kids: Ninetyeight percent of children under 8 in America have access to a mobile device at home. Half of teens say they feel addicted to their mobile devices, and those teens overall consume an average of nine hours a day of media. It's not hyperbole to say that children today face surveillance unlike any other generation—their every movement online and off can be tracked by potentially dozens of different companies and Organizations.

At Common Sense, it is our goal to help our tens of millions of American members improve the digital wellbeing of their families – and while in many instances that means teaching parents, teachers, and kids good digital hygiene practices and privacy skills, it also means ensuring there are baseline protections in place. Even extremely savvy digital citizens are powerless if they do not know what companies are doing with their information, if they cannot access, delete, or move their information, or if they have no choices with respect to the use and disclosure of their information.



What do families want in such protections? According to our research:

- More than 9 in 10 parents and teens think it's important that websites clearly label what data they collect and how it will be used.
- Those same numbers – more than 9 in 10 – think it is important that sites ask permission before selling or sharing data.

The Maryland Online Consumer Protection Act would offer these protections, and it would ensure that our most vulnerable children – up to age 16 – are protected from having their data shared with data brokers and other companies looking to profile and profit off of them.

This bill recognizes that it is not just health, or financial information, that needs protections. This bill recognizes that Marylanders have privacy rights in all of their information, no matter who holds it. The bill would allow Maryland residents to access the personal information companies collect about them--and port or delete their data if they wish. Adults can tell companies to stop sharing their personal information. Importantly – the most vulnerable get the highest protections – kids under 16 can't have their data shared. Additionally, while the bill does not have specific breach provisions, it still helps protect consumers from breaches: if a company doesn't have your information because you've deleted it or because it wasn't sold to them, they can't lose it. The Attorney General enforces violations, and the bill applies equally to service providers, edge companies, and brick and mortar entities, if they research certain size thresholds.

It brings the rights of Maryland residents into line with those enjoyed in California. Without this legislation, Maryland residents will suffer from a lower-tier of online privacy rights. Common Sense is eager to work with members of this committee to advance SB957, and please do not hesitate to reach out with any questions to 563.940.3296 or via email at jjerome@commonsense.org.

Sincerely,
Joseph Jerome
Multistate Policy Director

Consumer Reports_FWA_SB 957

Uploaded by: McInnis, Katie

Position: FWA

Testimony of Katie McInnis for the Maryland Senate Hearing on the Maryland Online Consumer Protection Act

Before the Senate Finance Committee

February 19, 2020

SB 0957 and HB 0784—SUPPORT WITH AMENDMENTS

Katie McInnis, Policy Counsel, Consumer Reports, Inc.

Thank you Chair Senator Delores G. Kelley and Vice Chair Senator Brian J. Feldman for this opportunity to speak with you today about the SB 0957—the Maryland Online Consumer Protection Act. My name is Katie McInnis and I serve as a policy counsel for the advocacy division of Consumer Reports.

Consumer Reports is an independent, nonprofit member organization. We use our rigorous research, consumer insights, journalism, and policy expertise to inform purchase decisions, improve the products and services that businesses deliver, and drive regulatory and fair competitive practices. We work to support and protect Americans' fundamental right to privacy; and this bill takes important steps to protect this critical liberty.

Unfortunately, the United States lacks comprehensive privacy protections to safeguard consumers' personal information, even as data collection and sharing practices have become more and more prolific and aggressive. And this bill could advance consumer protections in several important ways. For instance, it will give people access to the information that companies have about them, extends the right to control the sale of your data, and will allow consumers to request companies delete the private information they have about them. Importantly, the bill would prevent companies from retaliating against consumers for exercising their rights under this Act.

Consumers have repeatedly made it clear that they want more, not fewer, protections, and this legislation is a step in the right direction. For example, a recent Consumer Reports' survey found that 92 percent of Americans think companies should get permission before sharing or selling users' online data and that 70 percent of Americans lack confidence that their personal information is private and secure.¹

Consumers clearly desire the ability to limit data collection, detrimental uses, and unnecessary retention and sharing, but lack the ability to easily and efficiently exercise those preferences. Your

¹ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), <https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/>.

bill could help change this dynamic for the better and give consumers more control over their personal data.

However, there are ways that the law should be improved to be more protective of consumers.

Most importantly, identity verification is not necessary for a consumer to opt-out of the sale of their personal information. Much of the data used for tracking consumers cannot be tied to an individual consumer. Accordingly, the California Consumer Privacy Act, one of the strongest state privacy bills, does not require verified opt-outs. Companies who send fraudulent opt-out requests could invite liability under existing law, but we could support a provision that prohibits companies from sending opt-out requests unless at a consumer's direction.

Second, a bill that relies upon consumers taking advantage of opt-out rights needs some sort of mechanism to let consumers opt out of whole categories of data sharing all at once—otherwise, the opt-out rights are not scalable and workable. In California, many companies are sending consumers to multiple sites in order to exercise their preferences.² For this reason, the California Attorney General has issued regulations requiring companies to treat universal signals like browser headers to be binding opt-out requests.³

Third, the business purpose exemption should be narrowed, limited to a set of specific operational purposes—otherwise, companies will try to use the data for unrelated purposes that consumers cannot control. Relatedly, we suggest putting more limits on what service providers can do pursuant to their contracts. Already, we are seeing companies try to get around the California Consumer Privacy Act through the service provider exemption.

Strong enforcement is essential. We urge the Committee to consider adding more resources for the Attorney General, and private enforcement of rights. Without effective enforcement, consumers will have no protection against companies who seek to violate their privacy.

Finally, lawmakers should resist efforts to water down or weaken the law. This legislation will give consumers needed protections and will not affect the existing profit model for online businesses.

We appreciate the leadership of Senators Lee, Benson, and Lam and Delegates Carey and Watson for introducing and sponsoring a bill to help protect Marylanders' personal information. And we look forward to working with you to advance critical privacy and security protections for all Maryland residents.

² See @jasonkint, TWITTER (Jan. 1, 2020), https://twitter.com/jason_kint/status/1212431443772788737.

³ See Proposed Regulations, California Consumer Privacy Act at § 999.315(c), CAL. DEP'T OF JUSTICE (Oct. 11, 2019), <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf>.

MDDCCUA_FWA_SB957

Uploaded by: Murray, Rory

Position: FWA

Chairwoman Delores Kelley
3 East
Miller Senate Office Building
Annapolis, MD 21040

SB957: Maryland Online Consumer Protection Act
Testimony on Behalf of MD|DC Credit Union Association
Position: Oppose

Chairwoman Kelley, Vice-Chair Feldman and Members of the Committee,

On behalf of the MD| DC Credit Union Association and the 84 Credit Unions and their 1.9 million members that we represent in the State of Maryland, we appreciate the opportunity to testify on this legislation. Credit Unions are member-owned, not-for-profit financial cooperatives whose mission is to promote thrift and provide access to credit for provident and productive purposes for our members. **Without our requested amendment, we cannot support this bill.**

1. We request the following amendment:

A business that is subject to and in compliance with § 501(b) of the federal Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, § 216 of the federal Fair and Accurate Credit Transactions Act, 15 U.S.C. § 1681w, the federal Interagency Guidelines Establishing Information Security Standards, and the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, and any revisions, additions, or substitutions, shall be deemed to be in compliance with this subtitle.

An affiliate that complies with § 501(b) of the federal Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, § 216 of the federal Fair and Accurate Credit Transactions Act, 15 U.S.C. § 1681w, the federal Interagency Guidelines Establishing Information Security Standards, and the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, and any revisions, additions, or substitutions, shall be deemed to be in compliance with this subtitle.

2. The federal Gramm-Leach-Bliley Act already establishes several safeguards for consumers

First and foremost, the safety and needs of our members come first. However, this bill is drafted in a way that will make it duplicative and overly burdensome to comply since we already comply with Gramm-Leach-Bliley. Credit unions, like all financial institutions, have to comply with the Gramm-Leach-Bliley Act, which implements many safeguards to protect a consumer's non-public information (NPI). We request a Gramm-Leach-Bliley exemption to this law, as is the case with most, if not all, other Maryland consumer protection statutes that apply to financial institutions.

(A) Under Gramm-Leach-Bliley, financial institutions must give the following notification:

- give their customers - and in some cases, their consumers - a "clear and conspicuous" written notice describing their privacy policies and practices.

- This notice must include:
 - Categories of information collected.
 - Categories of information disclosed.
 - Categories of affiliates and nonaffiliated third parties to whom you disclose the information.
 - Categories of information disclosed and to whom under the joint marketing/ service provider exception in section 313.13 of the Privacy Rule.
 - If you are disclosing NPI to nonaffiliated third parties, and that disclosure does not fall within any of the exceptions in sections 313.14 and 313.15, an explanation of consumers' and customers' right to opt-out of these disclosures.
 - Any disclosures required by the Fair Credit Reporting Act and
 - Policies and practices with respect to protecting the confidentiality and security of NPI

(B) And, protect the information under the Safeguards Rule, which requires:

- Companies must develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.
 - As part of its plan, each company must:
 - **Designate** one or more employees to coordinate its information security program;
 - Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
 - **Design** and implement a safeguards program, and regularly monitor and test it;
 - **Select** service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and
 - **Evaluate** and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

(C) Also, specific to Credit Unions, NCUA Part 748, we are required to:

- § 748.0 Security program.
 - (a) Each federally insured credit union will develop a written security program within 90 days of the effective date of insurance.
 - (b) The security program will be designed to:
 - ...(2) **Ensure** the security and confidentiality of member records, protect against the anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member;
 - (3) **Respond** to incidents of unauthorized access to or use of member information that could result in substantial harm or serious inconvenience to a member;
 - (4) **Assist** in the identification of persons who commit or attempt such actions and crimes, and

- (5) **Prevent** the destruction of vital records, as defined in 12 CFR part 749.
- (c) Each federal credit union, as part of its information security program, must properly dispose of any consumer information the Federal credit union maintains or otherwise possesses, as required under § 717.83 of this chapter.

(D) Finally, Gramm-Leach-Bliley also already has an opt-out provision:

- Section 502 of the Gramm-Leach-Bliley Act (15 U.S.C. § 6802) forbids any financial institution from sharing "nonpublic personal information" with a "nonaffiliated third party" unless the relevant consumer is given notice and an opportunity to opt-out of the sharing.
- (b) Opt-out
 - (1) In general, A financial institution may not disclose nonpublic personal information to a non-affiliated third party unless—
 - (A) such financial institution clearly and conspicuously discloses to the consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 6804 of this title, that such information may be disclosed to such third party;
 - (B) the consumer is given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party; and
 - (C) the consumer is given an explanation of how the consumer can exercise that nondisclosure option.

Without this amendment, we cannot support this bill. Please do not hesitate to contact me at 443-325-0774 or jbratsakis@mddccua.org, or our VP of Advocacy, Rory Murray at rmurray@mddccua.org should you have any questions. Thank you for your consideration.

Sincerely,



John Bratsakis
President/CEO
MD|DC Credit Union Association

TechNet_UNF_SB957

Uploaded by: Fisher, Christina

Position: UNF



TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Northeast | Telephone 508.397.4358
One Beacon Street, Suite 16300, Boston, MA 02108
www.technet.org | @TechNetNE

February 19, 2020

Sen. Delores Kelley, Chair
Senate Committee on Finance
Maryland General Assembly
Miller Senate Office Building, 3 East
Annapolis, MD 21401

Re: SB 957- Maryland Online Consumer Protection Act

Dear Sen. Kelley and member of the Committee:

TechNet is the national, bipartisan network of over 80 technology companies 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 more than three million employees in the fields of information technology, e-commerce, clean energy, gig and sharing economy, venture capital, and finance. TechNet is committed to advancing the public policies and private sector initiatives that make the U.S. the most innovative country in the world.

TechNet respectfully submits these comments in opposition to SB 957 (Lee) pertaining to the collection of personal information by businesses. We appreciate the desire of the Sponsor to address consumer privacy protections. However, we urge Maryland to support federal efforts to create a comprehensive privacy law instead of contributing to a growing patchwork of state legislation.

As you are likely aware, on June 28, 2018, California enacted California Consumer Privacy Act (CCPA), a well-intentioned, but materially flawed new law, that seeks to protect the data privacy of technology users and others by imposing new rules on companies that gather, use, and share personal data. Unfortunately, CCPA was rushed through the California legislative process to avoid a potential ballot fight. Due to a hard deadline to withdraw the initiative, there was little time for substantive policy negotiations about a law that has a tremendous impact on businesses not only in California but across the nation. This has resulted in a law that was enacted just 18 months ago being amended via eight different legislative vehicles. And it is still not final.

While California has worked to address some of problematic provision included in the initial version of CCPA, many challenges remain. One example of a problematic provision is the CCPA's

reference to households and devices in the definition of personal information. This reference run counter to the CCPA's privacy protective goals and should be removed. As drafted, one member of a household – whether they are an abusive spouse or a roommate – has the ability to request access to all of the specific pieces of personal information – including credit card account information, precise geolocation data, or even shopping records – about another member of their household. This has anti-privacy consequences for mundane, everyday behavior, such as requesting information from a grocery delivery store which could inadvertently expose a household member's purchase of birth control or a pregnancy test. As another example, if one household member makes a request to delete all data associated with a household, another household member would be subsequently unable to access their household information. This is just one example of many.

An additional problem with the legislation as drafted is that SB 957 is nearly identical to the original version of CCPA which passed the Legislature in 2018. As such, the bill does not conform to the most recent version of CCPA today, which is likely to significantly change at least twice between now and November of 2020. In addition to amendments that passed the legislature last year, the Attorney General has engaged in a rulemaking procedure which may reinterpret key provisions of the law and add new obligations. Further complicating matters, this fall the sponsor of the 2018 ballot initiative has filed a new privacy ballot initiative, to correct perceived errors in the law and impose new obligations on businesses. This suggests that the privacy debate will continue to change over the next several years, and the true impact of the CCPA will not be known for some time. It is clear that California is not a workable model for other states to pass at this time.

TechNet is also concerned with a patchwork approach that imposes different privacy and security obligations in different states. Privacy laws can be difficult and costly for some of the largest businesses to comply but it's even worse for small businesses and start-ups. If you also factor in multiple states with multiple different laws, the end result can be crippling. The California Attorney General's office estimated that initial, direct compliance costs for CCPA to be \$55 billion, with up to another \$16 billion over the next decade (2020-30), depending on the number of California businesses coming into compliance, and with smaller firms likely facing a disproportionately higher share of compliance costs relative to larger enterprises. These numbers should be a warning to lawmakers as they consider any data privacy legislation.

TechNet ask you to consider holding SB 957 as California continues to implement CCPA. It is important to wait and learn of any unintended consequences that California will likely face as the first state to pass consumer data privacy legislation. Additionally, Maryland should avoid creating a separate and conflicting privacy law that would only increase compliance costs on businesses and start-ups.

Thank you for the opportunity to weigh in on SB 957 and as the Committee deliberates, please consider our organizations and our member companies a resource. Thank you in advance for your consideration on these matters. Please do not hesitate to reach out with any questions.

Sincerely,



Christina Fisher
Executive Director, Northeast
TechNet
cfisher@technet.org
508-397-4358

MDChamber_Griffin_UNFAV_SB957

Uploaded by: Griffin, Andrew

Position: UNF



LEGISLATIVE POSITION

Unfavorable

Senate Bill 957

Maryland Online Consumer Protection Act

Senate Finance Committee

Wednesday, February 19, 2020

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 4,500 members and federated partners, and we work to develop and promote strong public policy that ensures sustained economic growth for Maryland businesses, employees and families. Through our work, we seek to maintain a balance in the relationship between employers and employees within the state through the establishment of policies that promote fairness and ease restrictive burdens.

Senate Bill 957 creates numerous personal information privacy rights for consumers in the state. Specifically, the bill gives consumers the right to (1) know whether (and what) personal information is collected or disclosed by a business; (2) access (and obtain a copy of) personal information collected by a business; (3) have personal information deleted by a business; (4) stop a business from disclosing information to third parties; and (5) equal service and pricing, regardless of whether the consumer has exercised his or her rights under the bill.

State law does not generally regulate Internet privacy. However, businesses are required under the Maryland Personal Information Protection Act to take precautions to secure the personal information of customers and to provide notice of information of breaches.

SB 957 establishes numerous requirements for businesses that handle the personal information of consumers, and our member businesses are concerned with the significant costs they will incur as a result of the additional burdens of compliance outlined in this legislation.

This legislation, as introduced, will have a significant negative impact on Maryland's business community. Specifically, the bill establishes a maximum civil penalty of \$2,500 on a per-violation basis. In the event of theft or unlawful access, even a small to medium-sized business could become exposed to fines in the hundreds of millions.

For these reasons, the Maryland Chamber of Commerce respectfully requests an **Unfavorable Report** on Senate Bill 957.

NealKarkhanis_UNF_SB957

Uploaded by: Karkhanis, Neal

Position: UNF



Leah J. Walters
Vice President & Chief Deputy, State Relations

February 19, 2020

The Honorable Senator Delores G. Kelley, Chair
The Honorable Brian J. Feldman, Vice-Chair
Senate Finance Committee
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

RE: ACLI Opposes Senate Bill 957 - Maryland Online Consumer Protection Act

Dear Chairwoman Kelley and Vice-Chair Feldman:

Thank you for the opportunity to comment on Senate Bill 957 (S. 957) on behalf of the American Council of Life Insurers. The American Council of Life Insurers (ACLI) is the leading trade association driving public policy and advocacy on behalf of the life insurance industry. 90 million American families rely on the life insurance industry for financial protection and retirement security. ACLI's member companies are dedicated to protecting consumers' financial wellbeing through life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, and dental, vision and other supplemental benefits. ACLI's 280 member companies represent 94 percent of industry assets in the United States. Specifically, in Maryland, 235 companies account for 94% of all life insurance premiums.

The insurance industry is a consumer privacy leader in support of clear obligations in the appropriate collection, use and sharing of sensitive personal information. The financial services sector has and continues to respect consumer privacy. Insurers have ably managed consumers' sensitive medical and financial data for well over a century. Insurers must collect and use personal information to perform essential business functions – for example, to underwrite applications for new insurance policies, to pay claims submitted under these policies, and to provide longevity protection through retirement products. 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 financial services industry would be **uniquely** affected by the establishment of new general privacy requirements at the individual state level. Senate Bill 957 would add to the mix of existing privacy laws for insurers—resulting in additional complexities and expenses of implementation and will inevitably result in conflicting scopes, definitions, notice requirements and consumer rights.

As currently drafted, ACLI opposes S. 957 and suggests several amendments if it were to pass. The insurance industry is already subject to multiple layers of privacy regulation in the form of the Gramm-Leach-Bliley Act (“GLBA”), the Privacy of Consumer Financial and Health Regulation, the Financial

The Honorable Senator Delores G. Kelley
The Honorable Brian J. Feldman
February 19, 2020
Page 2

Information Protection Act, the Insurance Information and Privacy Protection Act, the Fair Credit Reporting Act (FCRA) and Health Insurance Portability and Accountability Act (“HIPAA”). Senate Bill 957 does not recognize these laws or Maryland’s comprehensive insurance privacy laws and should be amended to provide an exclusion for insurers who are already complying with such laws.

Senate Bill 957 includes many provisions from the California Consumer Privacy Act of 2018 (CCPA), a comprehensive data privacy law which grants consumers sweeping new rights to govern use of their personal information. The California law was passed in four days, behind the scenes, with no public input. It was rushed and the result is evident. Some of the purported consumer protection disclosure requirements render consumers’ personal information even more vulnerable. The severe impact to entities forced to completely overhaul their business practices in order to comply with the law was not given much, if any, thought. As a result, there were nearly 40 bills proposed in California last session by various interest groups to attempt to fix the law. CCPA was amended during the final hours of the California legislative session last September. Still, both legislators and the consumer advocate proponents of the legislation are seeking additional significant changes both by a comprehensive ballot initiative as well as legislation in 2020.

Senate Bill 957 would create a new opt-in/opt out structure that is ambiguous and would have unintended results absent modification. As such, it should be amended so that it reflects the well-established and perfected approaches already in place under the GLBA, HIPAA and FCRA to create a straightforward list of circumstances in which opt-out is required. Even the new CCPA framework recognizes the value of incorporating these well-established structures.

Senate Bill 957 does not include any of the business to business personal information exemptions that California passed in September of 2019. While the legislation contains an employment exemption for personal information a business collects during the employment process, it is extremely limited and may inadvertently impair the offering of employee benefit programs, among other impacts. It also does not include any of the California Privacy Rights Act of 2020 amendments which are critical to improving the bill.

Finally, S. 957 includes a private cause of action for violation of its provisions. We recommend eliminating this provision as a private right of action undermines agency enforcement, results in disparate outcomes for consumers and hinders innovation and consumer choice. [Additional amendments include effective date, contents of the notice itself, consumer requests and enforcement.]

Maryland may want to consider taking action similar to a recently proposed resolution in Arizona, [Resolution 2013](#), which advocates for a single, comprehensive federal standard for consumer data privacy regulation.

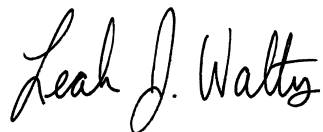
Consumers and companies need privacy requirements that are consistent and equivalent across state borders, provide equal protections to all consumers regardless of where they are located, support growth and innovation, and which provide legal transparency. Differing privacy standards will lead to consumer confusion, differing consumer rights and protections, obstruct the flow of information, and impede interstate commerce. Differing state privacy approaches are confusing and frustrating to consumers, who will now face different rights to control their personal information based upon where they live or with whom they are doing business. These conflicts must be taken into consideration as you work to develop comprehensive obligations regarding the use of personal information which applies equally and uniformly to all industries.

For these reasons, ACLI and its member companies oppose Senate Bill 957 and urge an unfavorable vote.

The Honorable Senator Delores G. Kelley
The Honorable Brian J. Feldman
February 19, 2020
Page 3

ACLI and its member companies are committed to working with this committee on trying to solve some of these complexities, to find solutions that protect consumer privacy and, at the same time, enable innovation and business growth and opportunities for the State of Maryland.

Sincerely,

A handwritten signature in black ink that reads "Leah J. Walters". The signature is written in a cursive style with a large, stylized initial "L".

Leah J. Walters

SPSC_UNF_SB957

Uploaded by: Kingman, Andrew

Position: UNF

STATE PRIVACY AND SECURITY COALITION

February 19, 2020

Senator Delores G. Kelley
Chair, Senate Finance Committee
3 East
Miller Senate Office Building
Annapolis, MD 21401

Re: SB 957 (Oppose)

Dear Chairwoman Kelley, Vice Chair Feldman, and Members of the Committee,

On behalf of the State Privacy and Security Coalition, a coalition of 30 leading technology, retail, communications, online security, payment card, and automobile companies, as well as eight trade associations, I appear today in opposition to SB 957.

Let me be clear: Our coalition believes that the federal government is the most appropriate venue for uniform privacy legislation. We understand, however, that state legislatures may be unwilling to wait for a federal solution. We are always willing to engage in a stakeholder process that would result in fair and meaningful privacy protections for consumers. We evaluate privacy legislation on whether it appropriately balances consumer control and transparency, operational workability, and cybersecurity (because as more information is provided to consumers, cybersecurity risks for all parties increases).

Unfortunately, this bill – based on the problematic California Consumer Privacy Act (CCPA) – does not meet these tests. In fact, it not only replicates problems that stem from the CCPA, it also creates new ones with the ways in which it strays from the CCPA. We discuss some of the most significant issues below.

The CCPA is Not a Viable Model

It does not make sense to enact legislation in Maryland based on unfinished and confusing legislation like the CCPA.

Although part of the statute went into effect January 1, there are still significant changes likely to be implemented. First, the Attorney General's regulations are scheduled to be released sometime in the second quarter of 2020, with implementation beginning July 1, 2020. The initial draft was twenty-five pages of additional substantive requirements. The latest draft – released just last Friday – modified those requirements further, adding new requirements and deleting others.

Second, the original drafter of the 2017 CCPA ballot initiative has decided that he was unsatisfied with the ultimate outcome of CCPA, and consequently is gathering signatures to put forth another ballot initiative for 2020. This will significantly overhaul the current text of the statute, and create new, additional requirements.

STATE PRIVACY AND SECURITY COALITION

Since its passage in June 2018, and including the two vehicles referenced above, the CCPA will have been amended *eight times* in just over two years. This is not the kind of sustainable, long-term vision that a state should apply to privacy law that governs cutting edge technology.

The CCPA's core aims – to provide consumers more transparency and control – can be accomplished with much simpler, much more comprehensible language that increases consumer benefit while reducing implementation costs.

SB 957 Will Cost Millions of Dollars for Maryland's Small Businesses

We recognize that SB 957 defines a “Business” with higher thresholds than the CCPA. Still, this would sweep in many small businesses in the state, saddling them with extreme compliance costs (particularly since SB 957 does not reflect the CCPA's amended definition of “Business” that removes reference to “devices”). A business that “collects” 100,000 pieces of personal information need only 274 transactions a day to be affected by CCPA – 274 unique visits to a website, or 274 credit card transactions for a merchant – and that business is within this legislation's scope.

The CCPA is incredibly and needlessly costly to the business community. The Attorney General's own study estimated that the cost of *initial* compliance costs for implementation would total \$55 billion. For businesses with 20 or fewer employees, costs are estimated at \$50,000. For businesses with fewer than 50 employees, costs are estimated at \$100,000.

SB 957 Would Eliminate Loyalty Programs for Maryland Consumers

Unlike the CCPA, which contains some relief for businesses that offer loyalty and customer rewards programs, SB 957 would eliminate their use in the state, because the legislation would prohibit charging different prices or rates for goods or services, or providing a different level or quality of goods or services to the consumer. This is the core of many loyalty or frequent purchase programs, and would immediately mark Maryland as a stay-away for businesses that offer these types of programs.

SB 957's Outlier Opt-Out Requirement Is Unworkable

SB 957 goes far beyond the CCPA's already broad opt-out requirement for the “sale” of information. Even under the CCPA, the opt-out right is so far-reaching that it covers transactions like a business-to-business's website using a free analytics tool to understand the web traffic it is receiving. SB 957 goes much farther than this, purporting to benefit consumers by allowing an opt-out to any “disclosure” of information to a third party. In practice, this provision will be the subject of endless litigation and fails to recognize the realities of the online ecosystem.

The bill would create huge uncertainty over service provider and multi-party “ecosystem” arrangements by creating opt-out rights unless these disclosures were “necessary to the performance of a business purpose.” Plaintiffs' lawyers and the AG's Office could challenge virtually any of these arrangements on the ground that it was not “necessary,” even if it was

STATE PRIVACY AND SECURITY COALITION

economically efficient and personal information was not used for any other purpose. This would be hugely disruptive with minimal if any benefit to consumers' privacy. Again, this goes far beyond the CCPA and it would make Maryland a more difficult state to do business in than any other state in a very important respect.

SB 957 Does Not Reflect Many CCPA Amendments

Even if SB 957 was enacted today, it would be out-of-date, because the CCPA has been amended in ways that do not accord with SB 957's current language. For example, critical definitions like "Business" were amended in October 2019 and are not reflected here.

Additionally, the CCPA added a minimal, but sensible and necessary, exemption for business-to-business data. Given that both CCPA and SB 957 purport to protect consumers and regulate consumer data, imposing additional requirements for business-to-business data seems illogical.

SB 957 Creates Significant Cybersecurity Risks for Consumers and Businesses

Like CCPA, SB 957 does not sufficiently allow businesses to take the possibility of fraud, and the maintenance of their cybersecurity infrastructure, into account when responding to consumer requests. Under this bill, a business would have to disclose the name of every cybersecurity vendor it uses, allowing hackers to use this law as a way of creating data maps to detect vulnerabilities. This alone is a multi-billion dollar risk for consumers' personal information.

Additionally, it applies a fraud exemption only to the Right to Delete. This means that if a fraudster impersonates a consumer (made easier by the lack of workable verification requirements in the bill), he or she can request *every piece of information* a business has on a consumer.

SB 957's Enforcement Provisions Incentivize Litigation Over Pro-Privacy Practices

The private right of action in this bill would eviscerate any progress that a privacy bill would accomplish. It has not been accepted in a single state that has seriously considered this type of legislation, including in the privacy laws recently passed in California and Nevada.

There are good reasons to reject class action enforcement. According to a study prepared by Hogan Lovells for the U.S. Chamber Institute for Legal Reform, plaintiffs rarely recover from lawsuits brought in privacy-related cases. Instead, this litigation "often leads to a major payday for plaintiffs' attorneys, even where class members experienced no concrete harm . . . even where class members may have suffered a concrete injury, the data indicates that they are unlikely to receive material compensatory or injunctive relief through private litigation."¹

¹ Mark Brennan et al., Ill-Suited: Private Rights of Action and Privacy Claims, U.S. Chamber Institute for Legal Reform at 5 (July 2019), available at: https://www.instituteforlegalreform.com/uploads/sites/1/Ill-Suited_-_Private_Rights_of_Action_and_Privacy_Claims_Report.pdf

STATE PRIVACY AND SECURITY COALITION

Private rights of action also open the door to class action lawsuits, which impose significant costs and do not result in meaningful benefits for consumers. One study² has shown that in over 150 federal class action lawsuits litigated in federal court: a) *not a single case* ended in a final judgment on the merits for the plaintiffs; b) 31% were dismissed by the courts on the merits; c) only 33% of the cases settled. When cases do settle, another study found that “the aggregate amount that class members typically receive comprises a small fraction of the nominal or stated settlement amount. Since courts base attorneys’ fees on [this amount]...attorneys’ fees often equate to 300%-400% of the actual aggregate class recovery.”³

In conclusion, our coalition opposes SB 957. We would be more than willing to share our experiences as other states grapple with how best to protect consumers. In particular, we are part of the Oregon Attorney General’s Privacy Task Force, and believe that process has been a productive method to bring various stakeholders to the table, and to systematically work through privacy issues at a granular level.

The issues involved here are technical and complex, with serious ramifications for both Maryland consumers and the business community. Accordingly, we ask that this committee not advance SB 957.

Respectfully submitted,



Andrew A. Kingman
General Counsel
State Privacy and Security Coalition

² *Do Class Actions Benefit Class Members? An Empirical Analysis of Class Actions* (2013), available at: <https://www.mayerbrown.com/files/uploads/Documents/PDFs/2013/December/DoClassActionsBenefitClassMembers.pdf>

³ High Cost, Little Compensation, No harm to Deter: New Evidence on Class Actions Under Federal Consumer Protection Statutes, *Columbia Business Law Review* (2017).

Alliance_Auto_Innovation_UNF_SB 957

Uploaded by: Kress, Bill

Position: UNF



February 19, 2020

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

RE: SB 957 - MARYLAND ONLINE CONSUMER PROTECTION ACT - OPPOSE

Dear Senator Kelley:

The Alliance for Automotive Innovation¹ (Auto Innovators) is writing to inform you of **our opposition to SB 957**, which is modeled on the California Consumer Privacy Act (CCPA). The CCPA is a sweeping privacy law that applies to businesses of all sizes across almost every industry, not just technology companies. It was rushed through the legislative process without the benefit of input from numerous crucial stakeholders. As a result, the law is deeply flawed. Many of the CCPA's provisions are simply unworkable in practice or will result in numerous unintended consequences. SB 957 shares many of the same problems as the CCPA.

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.² 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 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

¹ Formed in 2020, 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 the manufacturers producing nearly 99 percent of cars and light trucks sold in the U.S. The newly established organization, a combination of the Association of Global Automakers and the Alliance of Automobile Manufacturers, is directly involved in regulatory and policy matters impacting the light-duty vehicle market across the country. Members include motor vehicle manufacturers, original equipment suppliers, technology and other automotive-related companies and trade associations. The Alliance for Automotive Innovation is headquartered in Washington, DC, with offices in Detroit, MI and Sacramento, CA. For more information, visit our website <http://www.autosinnovate.org>.

² https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf

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. **Therefore, automakers should be excluded from the onerous provisions of SB 957.**

Practical Concerns

With this in mind, we have significant concerns with the proposed legislation. SB 957 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, similar to CCPA, 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 957 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 957 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 from 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 law 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

Given that the state of California has an open rulemaking to further amend and clarify the original law it passed, other states should refrain from enacting laws that will either conflict or impose more burdensome requirements.

Thank you for your consideration of the Auto Innovators' position. Please do not hesitate to contact me at jfisher@autosinnovate.org or 202-326-5562, should I be able to provide any additional information.

Sincerely,

A handwritten signature in black ink that reads "Josh Fisher". The signature is written in a cursive style with a prominent "J" and "F".

Josh Fisher
Director, State Affairs

PHI_UNF_SB957

Uploaded by: Lanier, Ivan

Position: UNF



An Exelon Company



An Exelon Company

February 19, 2020

112 West Street
Annapolis, MD 21401
410-269-7115

OPPOSE - Senate Bill Maryland Online Consumer Protection Act

Senate Bill 957 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 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 and security risks to the electric system while protecting the electric utility's ability to service the needs of its customers.

We have provided attached hereto an amendment that addresses our concerns around the sensitive information to which Pepco and Delmarva are privy in order to safely and efficiently operate the distribution system. 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:

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

Ivan K. Lanier
State Affairs Manager
410-269-7115
Ivan.Lanier@pepco.com

Amendment

On page 14, line 24 at the beginning of the line, insert “(2) personally identifiable information collected by an investor-owned gas company, electric company or combination gas and electric company tied to critical electric infrastructure information.”

CTIA_UNF_SB957

Uploaded by: MCCABE, LISA

Position: UNF



**Testimony of
LISA MCCABE
CTIA**

In Opposition to Senate Bill 957

February 19, 2020

**Before the
Maryland Senate Committee on Finance**

Chairman Kelley, Vice Chairman Feldman, and members of the committee, on behalf of CTIA, the trade association for the wireless communications industry, thank you for the opportunity to testify in opposition to Senate Bill 957, which would establish state regulations to address an inherently national and global issue: the protection of personal data. A law that sweeps too broadly, as SB 957 does, will create security risks and presents serious compliance challenges for businesses.

State legislation that sweeps too broadly could have a negative effect. SB 957 is based on a California law that was hastily passed in 2018, without sufficient consultation with impacted stakeholders, and that contains many ambiguities. California legislators enacted certain amendments last year – some with one-year sunsets to continue work in 2020 and 2021 – and may seek additional amendments to the law this year. The California Attorney General is also engaged in a rulemaking process to interpret its provisions. In addition, the sponsor of the original law is now proposing a ballot initiative to add further provisions to the law and change other provisions. As such, the California law is a moving target, and attempts to follow California means that we will have the beginning of a patchwork of state laws that will confuse consumers and burden businesses. Maryland should not rush to follow California.



SB 957 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 requesting consumers in one location, and/or maintain customer data in personally identifiable form, all to be able to comply with customer requests. These practices inherently carry risks, such as making the data a more attractive target to identity thieves and cybercriminals. They can also be burdensome. 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 California and in Maryland if the state enacts SB 957.

It is also unclear how requirements to have consumers delete their data will turn out in practice. These requirements may undermine important fraud prevention activities by allowing bad actors to suppress information. Additionally, there is a concern that bad actors could request deletion of data that would flag them as wrongdoers. Businesses may also have to delete data that will 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

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



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 as 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

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).



Any new state privacy law will contribute to a patchwork of regulation that will confuse consumers and burden businesses that operate in more than one state. Should the data of consumers who live in border cities and towns such as Ocean City or Chevy Chase 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.⁴ 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.⁵

In addition, the study found that any business that collects personal information from more than 137 consumers or devices a day would meet the law's thresholds, while between 50 to 75% that earn less than \$25 million in revenues will have to comply with the law.⁶ It also found that "[s]mall firms are likely to face a disproportionately higher share of compliance costs relative to larger enterprises.⁷ 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

⁴ See Standardized Regulatory impact Assessment: California Consumer Privacy Act of 2018 Regulations, Berkeley Economic Advising and Research, LLC (August 2019).

⁵ *Id* at 11.

⁶ *Id* at 11 and 20.

⁷ *Id* at 31.



large technology firms ... however evidence from the EU suggests that the opposite may be true."⁸ The study found that many smaller firms have struggled to meet compliance costs. The EU regulation of privacy 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.

The scope of the law will likely impact smaller companies and firms. For example, a company or firm that may not meet the applicable thresholds may still be required to comply with the law if the company processes data for an entity that must comply. In that instance, an IT processing firm that processes consumer data for a larger business must be capable of responding to access and data deletion requests.

Consumer privacy is an important issue. 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. The stakes involved in consumer privacy legislation are high. Taking the wrong approach could have serious consequences for consumers, innovation, and competition. 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 S957.

⁸ *Id* at 31.



As mentioned, the only state to enact a comprehensive privacy law is California. This law took effect at the beginning of this year, and it is still a moving target: the legislature recently passed amendments, the Attorney General has yet to promulgate final regulations, and a new ballot initiative would make further substantive changes to the law. It is simply not clear that we have found a good formula for regulating privacy. Accordingly, we caution Maryland and any state from rushing to follow California down this unproven, untested, and unknown path. As such, CTIA opposed SB 957 and would urge the committee not to move this bill. Thank you for the opportunity to testify today.

IA_UNF_SB 957

Uploaded by: Olsen, John

Position: UNF



February 19, 2020

The Honorable Dolores Kelley, Chair
Senate Finance Committee
East Miller Senate Building, Room 3
Annapolis, MD 21401

RE: Opposition to Senate Bill 957

Dear Chairwoman Kelley:

Internet Association (IA)'s mission is to foster innovation, promote economic growth, and empower people through the free and open Internet. The Internet creates unprecedented benefits for society, and as the voice of the world's leading Internet companies, we ensure stakeholders understand these benefits. Nowhere is that understanding as critical to the functionality and vitality of our companies than in consumer trust - trust in the services our companies provide and trust in the handling of the data our users generate.

It is IA's belief that consumers have a right to meaningful transparency and full control over the data they provide with respect to the collection, use, and sharing of that data. Consumers should have the ability to access, correct, delete, and transfer their data from one service to another.

IA appreciates the opportunity to comment on the proposed legislation **SB 957** "the Maryland Online Consumer Protection Act" and to provide insight from efforts in other states as well as at the federal level regarding consumer privacy and the impacts it has on businesses in general, not just Internet-based businesses. IA respectfully requests that the bill be held for further examination of the impact privacy laws have on businesses and consumer experience in both Maryland and the country as a whole.

SB 957 appears to borrow from the California Consumer Privacy Act (CCPA), and IA has observed efforts to comply with the enacted legislation costing California businesses millions of dollars in site redesigns, compliance attorneys, lawsuits, and in some cases, monetary penalties. As CCPA has now been in effect for nearly two months, new efforts to augment and worsen the law are underway in that state. In other states, similar efforts to pass comprehensive privacy legislation have been met with varying degrees of success. A new data disclosure law was recently passed in Nevada. Several states, including Washington and Illinois have attempted to pass GDPR-like legislation that is inconsistent with California's law. In the Northeast, privacy



legislation is being considered as close by as New York and New Jersey. While lawmakers in other states recognize a need for consumer privacy, the challenges with enacting legislation at a state level are evident.

There has never been a clearer indication that a federal privacy law is necessary before more states are successful in passing legislation that would create a patchwork of laws that American businesses would be forced to navigate. IA recognizes today's hearing is meant to examine data privacy through the lens of state enforcement, but we respectfully request any legislation that would be advanced adhere to principles that could be adopted at a federal level. Maryland should be in no rush to follow in California's troubled footsteps.

All Americans deserve a modernized U.S. privacy framework that provides people meaningful control over the data they provide to companies online and offline. That includes the ability to access, correct, delete, and download their data. Privacy protections should be consistent, proportional, flexible, and should incentivize businesses to act as good stewards of the personal information provided to them by individuals.

Thank you for your consideration on this important issue and I welcome any questions you may have regarding IA's position on this bill and others before the Maryland Senate. I can be reached at olsen@internetassociation.org or 518-242-7828.

Very truly yours,

A handwritten signature in black ink, appearing to read 'John Olsen', with a long horizontal flourish extending to the right.

John Olsen

Director, SGA Northeast Region

CC: Senate Finance Committee Members

MDDC UNFAV SB957

Uploaded by: Snyder, Rebecca

Position: UNF



Maryland | Delaware | DC Press Association

P.O. Box 26214 | Baltimore, MD 21210

443-768-3281 | rsnyder@mddcpres.com

www.mddcpres.com

To: Finance Committee

From: Rebecca Snyder, Executive Director, MDDC Press Association

Date: February 19, 2020

Re: **SB 957 - Oppose**

The Maryland-Delaware-District of Columbia Press Association represents a diverse membership of media organizations, from large metro dailies such as the Washington Post and the Baltimore Sun, to publications such as The Daily Record and online only outlets such as Maryland Matters and Baltimore Brew.

Our members oppose SB 957, which would create Maryland's version of the California Consumer Privacy Act, which took effect January 1, 2020. This bill would affect our local news outlets, as many consumers read news online and it is likely that our members would hit the 100,000 compliance threshold. Digital audiences are growing for news products as print audiences remain stable or decrease.

It is still too early to ascertain the effects of the CCPA in California and it should not be adopted in Maryland. It is difficult for our members to comply with a patchwork of regulation, when it would make the most sense for Congress to take the lead in creating a privacy act that works for all Americans.

Our members' ability to comply with the provisions of this bill assumes that all the information specified in the bill is held in one place. That is very often not the case and centralizing all of that information represents a large burden for our members in terms of data manipulation and storage. Centralizing this information will also create a single target for hackers.

We agree that more discussion is needed on this issue to create a solution that works across the country. We ask for an unfavorable report.



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

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

Richard Tabuteau_UNF_SB0957

Uploaded by: Tabuteau, Richard

Position: UNF



MARYLAND TECH COUNCIL

TO: The Honorable Delores G. Kelley, Chair
Members, Senate Finance Committee
The Honorable Susan C. Lee

FROM: Richard A. Tabuteau
Pamela Metz Kasemeyer
J. Steven Wise
Danna L. Kauffman

DATE: February 19, 2020

RE: **OPPOSE** – Senate Bill 443 – *Consumer Protection – Security Features for Connected Devices*
OPPOSE – Senate Bill 957 – *Maryland Online Consumer Protection Act*

The Maryland Tech Council (MTC) is a collaborative community, actively engaged in building stronger life science and technology companies by supporting the efforts of our individual members who are saving and improving lives through innovation. We support our member companies who are driving innovation through advocacy, education, workforce development, cost savings programs, and connecting entrepreneurial minds. The valuable resources we provide to our members help them reach their full potential making Maryland a global leader in the life sciences and technology industries. On behalf of MTC, we submit this letter of **opposition** for Senate Bill 443 and Senate Bill 957.

Senate Bill 443 requires a manufacturer of a “connected device” to equip the device with a reasonable “security feature”. A connected device is considered to have a reasonable security feature if it is equipped with a means for authentication outside of a local area network that includes either a preprogrammed password that is unique to each connected device or a process that requires the user to generate a new means of authentication before the user is granted access for the first time. Senate Bill 957 requires businesses that collect a consumer's personal information to provide clear and conspicuous notices to the consumer at or before the point of collection. It requires a business to comply with a request for information within 45 days after receiving a verifiable consumer request.

Though MTC recognizes the importance of protecting online consumer data and providing certain security features for connected devices, the matters that Senate Bill 443 and Senate Bill 957 address should and must be resolved on the federal level. Meaningful consistent compliance by industry would be more reliably satisfied with a uniform nationwide solution. This bill would have the effect of imposing millions of dollars of compliance costs on tech businesses and would harm the State’s economy more than it would protect consumer privacy. We understand that the tech industry is working with the Sponsor on amendments and are hopeful that consensus can be reached. However, as currently drafted, MTC urges an unfavorable report for Senate Bill 443 and Senate Bill 957.

For more information call:

Richard A. Tabuteau
Pamela Metz Kasemeyer
J. Steven Wise
Danna L. Kauffman
410-244-7000

BGE_UNF_SB957

Uploaded by: Washington, Charles

Position: UNF



An Exelon Company

Position Statement

OPPOSE

Finance Committee

2/19/2020

SB 957: Maryland Online Consumer Protection Act

Baltimore Gas and Electric Company (BGE) opposes *Senate Bill 957: Maryland Online Consumer Protection Act*, unless it is amended to address concerns that are specific to Maryland's utilities.

SB 957 is a comprehensive bill that includes various requirements for businesses that collect customer information and how that information can be disclosed or be prohibited from being disclosed at a customer's request. Customer information 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.

BGE understands the concerns about data privacy and appreciates a customer's desire to access personal information, 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.

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