OAG_FAV_SB201
Uploaded by: Abrams, Hanna
Position: FAV

BRIAN E. FROSH
Attorney General

ELIZABETH F. HARRIS
Chief Deputy Attorney General

CAROLYN QUATTROCKI
Deputy Attorney General

WILLIAM D. GRUHN
Chief

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL

FACSIMILE NO.
(410) 576-6566 (F)

WRITER'S DIRECT DIAL NO.
(410) 576-7296

February 12, 2020

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

FROM: Hanna Abrams, Assistant Attorney General

RE: Senate Bill 201 – Personal Information Protection Act - SUPPORT

The Office of the Attorney General supports Senate Bill 201 ("SB 201"), which provides much-needed protections to Maryland Consumers. The Office of the Attorney General supports the bill's amendments to the Maryland Personal Information Protection Act ("MPIPA").

The Bill Makes Necessary Updates to Keep Pace with Data Collection Practices

It is no longer possible to participate in society without providing personal information to private companies and other third parties that reveal intimate details of one's life, either alone or in combination with other information.

MPIPA has a relatively limited scope. It simply requires companies that collect or store consumers' personal information to: (1) reasonably protect it, and (2) notify consumers, and the Attorney General's Office, if there is a data breach that exposes that information.[1] These baseline protections, however, only apply to data that fits within MPIPA's definition of personally identifiable information ("PII").[2] SB 201 amends MPIPA to update the definition of PII to include

[1] Md. Code. Ann., Com. Law §§ 14-3503; 14-3504 (2013 Repl. Vol. and 2019 Supp.).
[2] Currently, MPIPA defines personal information, in Md. Code Ann., Com Law § 14-3501(e)(1), as:
(i) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable:
1. A Social Security number, an Individual Taxpayer Identification Number, a passport number, or other identification number issued by the federal government;
2. A driver's license number or State identification card number;
3. An account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account;
4. Health information, including information about an individual's mental health;
5. A health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self-insured, that permits access to an individual's health information; or

new types of sensitive personal data that companies are collecting and clarifies the notification requirements following a breach.

SB 201 adds three types of personal information to the information that companies are required to protect using the same data security practices as other similarly sensitive information. The first is activity-tracking data. Wearable devices and mobile apps are collecting very sensitive information about our habits and daily lives. They track our location, our exercise and fitness habits, vital statistics, diet, weight, and even fertility cycles. Marylanders legitimately expect this kind of information to be private, and companies should be required to maintain this information securely.

The second type of personal information that SB 201 aims to protect is genetic information. An increasing number of companies offer consumers the opportunity to learn about their ancestry, genealogy, inherited traits, and health risks for a low cost and a swab of saliva. This presents a very exciting opportunity, but poses serious privacy risks. These companies do not always consider themselves "covered entities" under the Health Insurance Portability and Accountability Act ("HIPAA") and the current statutory definition of "personal information" does not presently include genetic information. Therefore a company that collects this highly personal, sensitive information could suffer a breach that is not covered under the existing law. The privacy risk posed by exposing a person's genetic information is, in many ways, even higher than that posed by financial information. You cannot change your genetic makeup; once genetic information is exposed, there is not a simple fix like being reissued a new credit card. In fact, the risks of exposing sensitive genetic information are so high that in December 2019 the Pentagon advised members of the armed forces not to use home DNA testing kits.

Third, SB 201 protects non-public social media information. Social media companies allow users to restrict the audience that can receive and view information that users posts. Users can also choose to share their information with the general public. SB 201 does not cover information made generally available to the public through social media. But, where social media companies invite users to share private information by creating spaces in which people feel safe sharing nonpublic information, for example sharing information with just your virtual friend, consumers have a legitimate expectation of privacy. This bill requires companies to maintain security practices that protect this non-public information the same way they are required to protect other personal information.

These three categories of information deserve protection. Adding them to MPIPA simply means that companies that collect this information, and frequently profit from it, must reasonably protect it, and let consumers know if it has been stolen.

<u>The Bill Updates How We Are Notified About Breaches</u>

In addition to protecting personal information, MPIPA requires companies to notify consumers and the Attorney General's Office after it has been exposed. This allows consumers to

---

6. Biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account; or

(ii) A user name or e-mail address in combination with a password or security question and answer that permits access to an individual's e-mail account.

take quick action to protect their information, such as changing passwords, freezing credit reports, notifying financial institutions, and monitoring accounts. The Attorney General's Office needs to know about a breach quickly so that we can advise the throngs of consumers that call us asking for guidance on what to do and, when appropriate, take enforcement actions. The current law permits businesses to delay notification in two ways – (1) businesses are permitted an opportunity to first investigate the breach and then (2) they have 45 days from the date of the conclusion of their investigation to issue their notice. This framework allows for too much of a time-lag between the discovery of the breach and the notification deadline. It also does not require companies to provide necessary information that would assist the Attorney General's Office in providing guidance to Marylanders. SB 201 will correct both of these issues.

Notifying Consumers About Breaches Earlier Allows Them to Protect Themselves

The longer a business waits to notify consumers about a breach, the greater the risk of harm and identity theft. This bill updates the timeline for providing notice and brings Maryland in line with the recent developments in this area. The European Union's celebrated General Data Protection Regulation ("GDPR") requires companies to provide notice within seventy-two (72) hours of discovering a breach (Article 33), and so do the New York Department of Financial Services Cybersecurity Regulations (N.Y. Comp. Codes R. Regs. Tit. 23 § 500.17). This bill does not go that far – it requires notification to occur with 30 days of discovery of a breach.

Companies are taking advantage of the current law. Right now, MPIPA requires notice "as soon as reasonably practicable, but not later than 45 days after the business concludes [its] investigation" into the breach. Md. Code Ann., Com. Law § 14-3504(b)(3). There are two problems with the current law. First, the triggering event to start the clock is after a company *concludes* an investigation into whether or not the data is likely to be misused. Companies have been elongating the investigation step and delaying its conclusion in order to postpone providing notice. This bill updates the triggering event for notification to when a business discovers a breach. Numerous other states, including but not limited to Colorado, Florida, New Mexico, Ohio, Tennessee, Vermont Washington, and Wisconsin, use discovery of the breach as the trigger that starts the notification clock.

When a hacker takes information, the likelihood is that the information will be misused. This bill recognizes this reality by shifting the default presumption in evaluating whether notification is necessary: it requires businesses to notify consumers unless they determine that the breach *does not* create a likelihood of misuse. In other words, businesses will have to notify consumers of a breach unless they can conclude there is not going to be harm to consumers.

The second problem with the current law is that companies have been ignoring the operative clause: "as soon as reasonably practicable," and instead focusing only on the "45 days," often waiting right up until 45 days to provide notice. Such needless delay is harmful to consumers, as it provides criminals more time to exploit consumers' data before consumers are alerted that they are at risk. If consumers are informed, they can take steps to protect themselves. That is why the bill requires notifications within 30 days of discovery of a breach. 30 days is fair.[3] It is over ten times longer than the recent developments in this area in Europe (GDPR), and is

[3] The previous proposed bill suggested notification 10 days after discovery of a breach. This was extended to 30 days based on feedback from business representatives.

identical to the notification timeline in Colorado[4] and Florida.[5] Thirty days after discovery may sound like a short period of time, but the bill recognizes that businesses may need time to determine the scope and impact of a breach and provides time to do this. MPIPA Section 14-3504(d)(1)(ii) allows companies to delay notification "to determine the scope of the breach, identify the individuals affected, or restore the integrity of the system." Companies will not have to rush to report a breach before they know what happened. Instead, the law allows time to make a determination. The point is to eliminate the reasons for delaying notification that companies are abusing now, such as business reasons, convenience, and the public relations impact. Breach notifications routinely come on Friday afternoons, which demonstrates that they are not currently coming "as soon as reasonably practicable," rather they are coming when companies hope fewer people will notice.

SB 201 makes other necessary adjustments to the notice timelines to accomplish a quicker exchange of information. The business that owns or licenses the data is responsible for sending a breach notice, and the 30-day timeline discussed above relates to how long that data owner has to notify consumers after it becomes aware of a breach. However, sometimes businesses entrust their data to third parties, and when a breach occurs at that third party, the breach notice still comes from the business that owns or licenses the data. It is important for the data owner to know about the breach as soon as possible. Separate timelines are in place for how long a third party can wait before telling the data owner or licenser. Under the current law, that could *double* the time it takes for a consumer to learn about a breach, just because it occurred at a third party and not a direct owner of the data. That is unjustifiable, and this bill addresses that problem. If the breach of information in the possession of a third party occurs, the bill gives the third party 10 days from its discovery of the breach to notify the data owner, as the breach notice ultimately comes from the data owner. There is no reason to allow the third party to shield the information from the data owner for longer than that.

SB 201 fixes one other timeline loophole. Sometimes the FBI or Secret Service steps in to investigate a breach (often if they suspect it originated from a state actor). MPIPA allows a company to delay providing notice while law enforcement is investigating a breach if it is informed by the investigating agency that a public breach notification will impede its investigation. That makes sense. But what does not make sense is that MPIPA currently allows a company to delay notice for up to 30 days after getting the go-ahead from the FBI or Secret Service to notify the public. That 30 days is on top of the other already-lengthy timelines for notification. While a law enforcement investigation *should* toll the timelines for notice, once law enforcement says that it is alright to notify, there is no reason to delay notification for 30 more days. Preparations to notify can, and must, be occurring in parallel with any FBI or Secret Service investigation. To that end, the bill changes that 30-day period to three days after the law enforcement agency "green light" public breach notification.

Ensuring That Consumers Receive and Absorb Notice of Breach

SB 201 improves the method of notifying consumers so that more people will receive notice and more people will comprehend the information conveyed.

There are two types of notice in MPIPA: (1) direct notice, which means sending mail directly to each affected consumer (or directly notifying by phone or possibly by email if certain

[4] C.R.S. § 6-1-716.
[5] Fla. Stat. § 501.171(3)(a).

requirements are met); and (2) substitute notice, which typically just means posting notice on the company's website and notifying statewide media.

Direct notice is better and more effective than substitute notice for a number of reasons. Substitute notice is an ineffective means of notifying people without internet access, people who do not watch the news, and the many people that simply do not think general reports apply to them until they are notified directly. This was highlighted in the Equifax breach. Equifax first reported that 143.5 million SSNs had been breached. Equifax provided substitute notice. Later, Equifax discovered that an additional 2.5 million people were impacted. It decided to send the subsequent class direct notice by mail. The Attorney General's Identity Theft Unit received at least as many calls from consumers following the direct notice to 2.5 million people as we received after the substitute notice to the initial 143.5 million people.

When there are major breaches, big companies choose the ineffective substitute notice in order to save money, but it comes at the expense of consumers actually learning about the breaches that put them at risk. Under MPIPA, small companies already have to provide direct notice to each consumer. Big companies that put more people at risk should be held to the same standard, so this bill removes the option of either direct notice or substitute notice, and instead requires both.[6]

And finally, the bill addresses the content of breach notices to the Attorney General. MPIPA already requires a company to notify the Attorney General prior to notifying consumers, but gives no details on what the notice must contain.[7] As a result, we do not always receive the information that we need to properly respond to consumers who call us for help. This bill clarifies what information should be included in the notice to the Attorney General. This makes it easier on companies by taking out the guesswork as to what they should include in their notice and provides our office with the information that we need to assist consumers, including the number of affected Marylanders, the cause of the breach, steps the company has taken to address the breach, and a sample of the notice letters that will be sent to consumers. This information is readily available to companies at the time they provide notice.

For these reasons, we urge a favorable report.

Cc: Members, Finance Committee
The Honorable Susan C. Lee

[6] Currently, under MPIPA, a company can use substitute notice if direct notice would cost more than $100,000 or there are more than 175,000 affected consumers. Md. Code Ann., Com. Law § 14-3504(e).
[7] Md. Code. Ann., Com. Law. § 14-3504(h).

PGCEX_FAV_SB201
Uploaded by: Alsobrooks, Angela
Position: FAV

THE PRINCE GEORGE'S COUNTY GOVERNMENT

OFFICE OF THE COUNTY EXECUTIVE

BILL:	**Senate Bill 201 - Commercial Law - Personal Information Protection Act - Revisions**
SPONSOR:	**Senator Lee**
HEARING DATE:	**February 12, 2020**
COMMITTEE:	**Finance**
CONTACT:	**Intergovernmental Affairs Office, 301-780-8411**
POSITION:	**SUPPORT**

The Office of the Prince George's County Executive **SUPPORTS Senate Bill 201 - Commercial Law - Personal Information Protection Act - Revisions**, which expands the Maryland Personal Information Act to include an individual's genetic information, activity tracking data, and nonpublic social media information and to cover businesses that maintain personal information. The bill also reduces the time a business must notify affected individuals of a personal data breach from 45 to 30 days if the business owns the data and to 10 days if the business does not own or licenses the data. In addition, the bill outlines the information to be included in such notifications.

With cybercrime on the rise, the data trading (which includes selling of personal information) has topped $160 billion worldwide.[1] Juniper Research's Cybercrime & the Internet of Threats 2018 report estimates cybercriminals will steal 33 billion records annually by 2023.

This legislation provides more aggressive reporting requirements and timing that will assist consumers by having more immediate knowledge that their identity information was compromised in conducting commercial and/or financial electronic transactions. More expedient knowledge will prompt consumers to take actions to mitigate potential use of their personally identifiable information and put available protective measures in place.

[1] McGuire, Michael. *Into the Web of Profit*, Bromium Inc., April 2018, pg. 23, Accessed on Feb. 11, 2020, at https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf

For the reasons stated above, the Office of the Prince George's County Executive **SUPPORTS Senate Bill 201** and asks for a **FAVORABLE** report.

MDDCCUA_FAV_SB201
Uploaded by: Murray, Rory
Position: FAV

MD|DC
Credit Union Association

Chairwoman Delores Kelley
3 East
Miller Senate Office Building
Annapolis, MD 21401

SB201: Commercial Law – Personal Information Protection Act – Revisions
Testimony on Behalf of MD|DC Credit Union Association
Position: Support

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. The MD|DC Credit Union Association is in support of modifying the current security breach notification requirements.

The current law allows a business to conduct an internal investigation **prior** to 45-day window to notify consumers about a data breach begins. This standard is far too unpredictable because companies can take as long as they would like to conduct an internal investigation. The ambiguity in the current law is harmful to consumers. Removing the provision which allows the internal investigation to be conducted prior to the notification window beginning, will ensure, unless law enforcement directs the business to delay notification, that consumers are aware that their data may have been compromised within 30 days that the business discovers or is notified of the breach. Consumers should have knowledge of a potential compromise of their information as early as possible, and this bill will help accomplish the goal.

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
8975 Guildford Rd., Suite 190
Columbia, MD 21046

Lee_FAV_SB201
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.

THE SENATE OF MARYLAND
Annapolis, Maryland 21401

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

February 12, 2020

Senate Finance Committee

Senate Bill 201 – Commercial Law – Personal Information Protection Act – Revisions

Senate Bill 201 strengthens the Maryland Personal Information Protection Act (MPIPA) in response to changes in the type of data being collected about consumers and the seemingly constant slew of data breaches. When our data is used for services we seek, the misuse of that data must compel service providers to notify us as soon as possible, or they are doing all consumers a disservice. Privacy is of critical importance in the 21st century and personally identifiable data that can be used to steal and take over an identity is of the highest importance. This bill is outlining simply the process to notify a potential victim of identity theft to be on guard from a service they likely paid, only to have their trust abused.

SB201 recognizes the dramatic changes in the data collection landscape since the previous update of MPIPA and, accordingly, expands the definition of personal information in the statute to include activity tracking data, including behavioral data and geo-location data, as well as genetic information and non-public social media data. Your DNA, your minute-by-minute location and your private communications and connections with friends and family are among the most personal and sensitive pieces of information that companies can collect about you. These categories of information should clearly be included under the definition of personal information.

SB201 strives to streamline the industry response to data breaches and empower consumers by expediting the notification process. The way many businesses store and protect their data is through a third party, essentially a company that maintains data. Under current law, if a company that maintains data discovers or is notified of a breach, they have, at maximum, 45 days to notify the owner/licensee of that data; our bill changes that cap to 10 days. This is reasonable because

there is not much the maintainers of the data are required to do at this point but tell the licensee of the data. The investigation into whether there was harm would come later.

Once a data owner or licensee discovers of receives notice that there has been a data breach, they currently have 45 days to notify consumers. Our bill changes that cap to 30 days. Under current law, the company is not required to notify consumers that a breach has occurred unless they make an affirmative determination that harm is likely to result from that breach. This bill switches that standard so that a company is required to notify consumers that a breach has occurred unless that make an affirmative determination that harm is unlikely to result from the breach.

Prior to consumer notification, the licensee or owner of data must report to the Office of the Attorney General a description of the breach and how it occurred, the scope of the breach and the number of Marylanders effected, and a draft of the notification that the company plans to share with affected consumers. Any sensitive information would be shielded from PIA requests.

The process of consumer notification is also changed under this bill. Data owners and licensees are now required to notify consumers by written notice, electronic mail or hard mail; licensees are no longer able to provide only substitute notice (i.e. setting up a webpage where consumers to check if their information was compromised). Imagine being a consumer whose personal information, from your credit history to your social security number, was compromised in the Equifax breach. Would you feel comfortable re-entering all of your personal information on a website set up by the company that had just compromised that information? Direct notification to consumers that harm has been is necessary and is not an undue burden on industry.

The bill also adds a requirement that a business that *maintains* the personal information of a Maryland resident implement reasonable security procedures that are appropriate given the nature and size of the business collecting that information. This requirement already exists for data owners and licenses; adding the requirement for maintenance of data is simply a clarification.

For all of these reasons, I respectfully request a favorable report on SB201.

Nancy Egan_UNF_SB201
Uploaded by: Egan, Nancy
Position: UNF

American Property Casualty Insurance Association
INSURING AMERICA apci.org

Testimony of
American Property Casualty Insurance Association (APCIA)
before the
Senate Finance Committee
SENATE BILL 201- Commercial Law – Personal Information Protection Act - Revisions

February 12, 2020

Letter of Opposition

The American Property Casualty Insurance Association (APCIA) is a national trade organization representing nearly 60 percent of the U.S. property casualty insurance market. APCIA appreciates the opportunity to provide written comments in opposition of Senate Bill 201. APCIA strongly opposes Senate Bill 201, which proposes amendments to the breach notification requirements of the Maryland Personal Information Protection Act. These amendments are inflexible and have the potential to erode existing consumer protections.

State breach notification laws must strike the appropriate balance between providing meaningful notice guidelines that inform consumers when there is a risk of harm while avoiding the potential to desensitize consumers. As drafted, SB 201 would expand the definition of "Personal Information" to include data elements such as "Activity-Tracking Data" and "Nonpublic Social Media Information." These data elements are extremely broad and could include information that poses no risk of harm to a consumer. For example, if there is a device capable of recording a consumer's vehicle speed, how would a breach of that data cause consumer harm or require swift consumer action? In addition, we are unaware of any state that includes these data elements in their breach notification law. These deviations further perpetuate the current patchwork of state laws.

SB 201 would also amend the Personal Information Protection Act to reduce the timeframe within which a business must notify consumers from 45-days following an investigation to 30-days following discovery or notification of a breach. Following a breach, businesses must assess the situation, prevent any potential damage, and perform a diligent investigation to understand the impact and whether any consumers will be affected. Without meaningful time to investigate, a business will be forced to over notify, which could inundate consumers with notices. As such, consumers will likely become desensitized and may ignore significant notices that require consumer action.

Additionally, the method for providing notice in the event of a breach should be flexible. The existing delivery framework in the Personal Information Protection Act achieves this necessary flexibility; however, SB 201 would require e-mail notices, website posting, and notification to major media outlets. As a practical matter, if just one Maryland consumer is impacted by a breach that triggers a notification obligation, the business would be required to post the breach notice on its website and notify major statewide media. This requirement could unnecessarily create consumer confusion and concern. For the reasons stated above, APCIA opposes SB 201 and urges an unfavorable vote.

Nancy J. Egan, State Government Relations Counsel, DE, MD, VA, WV Nancy.egan@APCIA.org Cell: 443-841-4174

2020 MBIA Priority Issues

Uploaded by: graf, lori

Position: UNF

MARYLAND BUILDING INDUSTRY ASSOCIATION

marylandbuilders.org

The Ripple Effect of Home Building

ECONOMIC IMPACT OF RESIDENTIAL HOME BUILDING IN MARYLAND PER YEAR

Industries Involved

$1.23 BILLION

The jobs, wages and local taxes (including utility connection and impact fees) generated by development, construction and the sale of a home.

Ripple Effect of Wages

$649 MILLION

The wages and profits for local residents earned during the construction period are spent on other locally produced goods and services.

Ongoing, Annual Effect

$420 MILLION

The local jobs, incomes and taxes generated as a result of the home being occupied.

MBIA 2020 PRIORITY ISSUES

Housing Affordability

Safe, decent, housing that is affordable provide fundamental benefits that are essential to the well-being of families and communities. However, owning or renting a suitable home is increasingly out of financial reach of many households. The cost of housing is determined by many factors, including labor and material prices; interest rates and financing costs; federal, state and local regulations; and supply and demand. In today's market, a limited supply of land, a shortage of skilled labor, and rising fees are contributing to higher prices.

Workforce Development

A skilled and capable workforce that is adequate to meet our housing demand is vital to home builders. Despite competitive pay, the home building industry continues to experience labor shortages. This translates into higher housing costs, increased home prices, difficulty completing projects on time, and lower economic growth

Inclusionary Zoning

While the policy offers a solution for the growing need for affordable housing across the state, we must ensure there are appropriate offsets and incentives to compensate for the economic impact to builders and developers.

Transportation/ infrastructure

Traffic congestion in the state is among the worst in the nation. We need to find practical solutions to this problem to get people to their jobs and housing in safe, timely manner.

Adequate Public Facilities Ordinances

APFOs have emerged as a popular planning technique however local jurisdictions' attempts to reduce APF capacities artificially constrain development and negatively impacts jobs growth and economic development.

Forest Conservation

The Forest Conservation Act should be used as one of many tools to maintain Maryland's 40% forest canopy coverage. Currently, Maryland's coverage exceeds the 40% threshold. This is a result of enforcement of the existing FCA and other policies throughout the state. This provides evidence that Maryland's tree canopy policies are working as intended and do not need to change at this time.

Business Climate

Maryland must look for opportunities to assist businesses in navigating regulatory compliance and coordinating the complicated development approval process.

#mbiaworkingforyou

MBIA SB 201 Testimony

Uploaded by: graf, lori

Position: UNF

MARYLAND BUILDING INDUSTRY ASSOCIATION
11825 West Market Place | Fulton, MD 20759 | 301-776-6242

February 12, 2020

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

RE: Opposition to Senate Bill 201 (Commercial Law - Personal Information Protection Act - Revisions)

Dear Chairwoman Kelley:

The Maryland Building Industry Association, representing 100,000 employees of the building industry across the State of Maryland, opposes Senate Bill 201 (Commercial Law - Personal Information Protection Act - Revisions).

This measure requires businesses that maintain personal information of clients, customers, and other individuals to maintain extensive security procedures, with strict new requirements for how the business must notify the public. If the business has reason to believe there has been a breach, the business must conduct an investigation and notify the consumer of the potential breach.

While we appreciate the intent to protect sensitive private information and ensure consumer protection, the specific requirements regarding notification and investigation are concerning. As drafted, this bill removes the requirement for an investigation to conclude before the clock starts ticking for the business to provide notice to consumers. Notification is understandable but if notice must be provided before the investigation is concluded, the communication to consumers will be incomplete.

For these reasons, MBIA respectfully requests the Committee give this measure an unfavorable report. Thank you for your consideration.

For more information about this position, please contact Lori Graf at 410-800-7327 or lgraf@marylandbuilders.org.

cc: Senate Finance Committee Members

MDChamber-Griffin_UNF_SB201
Uploaded by: Griffin, Andrew
Position: UNF

MARYLAND
Chamber of Commerce

LEGISLATIVE POSITION:
Unfavorable
Senate Bill 201
Commercial Law – Personal Information Protection Act – Revisions
Senate Finance Committee

Wednesday, February 12, 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.

The purpose of the state's data breach law is to require that state residents be notified when there has been an unauthorized acquisition of certain types of unencrypted, computerized personal information (PI) that could lead to a risk of financial harm or identity theft. SB 201 seeks to change this law in a manner that causes concerns to the broader business community.

Some of the primary concerns with SB 201 include:

- Proposals to add to the list of data elements that can trigger a breach notification. For example, a breach could now occur if the data involves a name in combination with "activity-tracking data" and any information or data derived from it. No other state's data breach law includes this data point.
- There are several changes in the bill with respect to specified time periods in providing notices of a data breach. It is typical that state data breach laws allow for a delay in providing notices when requested by law enforcement – this bill does not include any such language.
- As is the case with all other states, Maryland's current law allows for "substitute notice" of a data breach that may be given, if certain conditions are met, in lieu of notice by postal or electronic mail or telephone. This bill proposes mandated public notice by posting on websites and the notification of media. This has the potential to cause extreme confusion and worry for individuals who may not be impacted by the breach. This radically changes the structure of "substitute notice," which is not in line with any other state.
- The provision requiring a notice to the Maryland Attorney General for "any vulnerabilities that were exploited," which would then be posted to the AG's website, provides a roadmap for criminals to find and exploit weaknesses in other systems.

The Maryland Chamber of Commerce strongly urges cooperation with the stakeholders impacted by the outcomes of SB 201 to find a solution that meets the intent of this legislation in an effective and sensible manner without undue burden.

For these reasons, the Maryland Chamber of Commerce respectfully requests an **unfavorable report** on **SB 201**.

Exelon_UNF_SB201
Uploaded by: Lanzarotto, Katie
Position: UNF

An Exelon Company

An Exelon Company

February 12, 2020

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

OPPOSE - Senate Bill 201
Commercial Law – Personal Information Protection Act – Revisions

Senate Bill 201 requires that Maryland businesses that collect customer information implement and maintain certain data breach notification procedures and practices. Customer information includes account information, social security numbers, driver license numbers and forms of tracking data, which could include electricity consumption data collected by Pepco and Delmarva for billing purposes.

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

We look forward to working with 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

MDRetailers_UNF_SB201
Uploaded by: Locklair, Cailey
Position: UNF

SB 201
Commercial Law - Personal Information Protection Act – Revisions

Senate Finance Committee
OPPOSE

SB 201 re data security amendments has numerous issues we would like to draw the committee's attention to.

In Section 7 regarding activity – tracking data: this section is too broad. It should apply only to when a business is tracking data by following wherever a shopper visits across the web. Currently this definition would also include what we track on our own website, which should be our data.

(1) Under "personal information," there are some additions that would set a new precedent for what is, or is not, "personal information".
a. Page 3, line 4 – there is no language in the country that states, "*data collected through an app or electronic device capable of tracking individual activity, behavior, or location; and any information derived from this data"* as part of a "personal information" definition within a breach notification law.
b. Page 3, line 24 – has the same issue and states "*(IV) nonpublic social media information about an individual, including communications, postings, pictures, videos, connections between individuals, connections between accounts, and actions."* This is also found no where else in the country as part of a "personal information" definition.

In section 14-3504(b)(3), we are fine with 30 days if the deleted language "concludes the investigation…" is restored. From date of discovery of the breach is not workable. If it is date of discovery, then we need at least 45 days.

14-3504(f) was previously about substitute notice and now requires additional notices. We are unclear if that the intent as the section was meant to address substitute notice.

(3) Regarding Attorney General Notice – On page 7, line 19 – The requirement to provide notice to the AG *prior* to giving notice to impacted consumers does not make sense. We believe the goal should be investigating the security incident and determining who is impacted. We shouldn't be taking valuable time/resources to prepare a separate notice to the Attorney General, especially before we give notice to consumers. We would ask what the point of giving prior notice to the Attorney General would accomplish. At the very least, the requirement should be to provide notice *contemporaneously* with notice to consumers.

We thank the committee for their time and look forward to working with you all on this legislation. For the above reasons, we remain in opposition to this legislation.

BOMA_UNF_SB201
Uploaded by: Popham, Bryson
Position: UNF

BOMA BALTIMORE

Phone 410.752.3318
Fax 410.752.8295
720 Light Street
Baltimore, MD 21230
info@bomabaltimore.org
www.bomabaltimore.org

February 12, 2020

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

RE: Senate Bill 201 - Commercial Law - Personal Information Protection Act – Revisions - OPPOSED

Dear Senator Kelley,

I am writing in my capacity as both the Legislative Chairman of the Building Owners and Managers Association of Greater Baltimore (BOMA), and as a member of its Board of Directors, to express BOMA's concerns regarding the referenced legislation.

BOMA, through its nearly 300 members, represents owners and managers of all types of commercial property, comprising 143 million square feet of office space in Baltimore and Central Maryland. Our members' facilities support over 19,000 jobs and contribute $2.5 billion to the Maryland economy each year.

Our specific concern with Senate Bill 201 may be found in new language on page 3, lines 4-9. This language is broadly drafted, and significantly expands the definition of "personal information" under current Maryland law. The additional language could be construed to include data which has long been considered to be both confidential and proprietary to an employer. In effect, it could transform the property of the employer into property of the employee, in the form of "personal information." We do not believe this result is intended under SB 201.

As an example, "activity-tracking data" under the bill could include an employer's email system, internet services or other computer programs (either on employer-provided computers or employer-provided phones or tablets). Such a result would conflict with the legal recognition granted by Federal and State courts to the principle that an employee has no privacy interest in data transmitted or received on such employer-provided devices. Many companies, including BOMA members, have employee policies which so state, and these policies are acknowledged by the employee at time of employment or when an employee begins to use these devices. While the intent of the bill may be to address a broader issue (e.g. search engine privacy), the language as drafted, if SB 201 is enacted, may create a credible claim by an employee that an employer may not review an employee's use of an employer-provided hardware or networks.

BOMA believes that such consequences, even if unintended, are potentially damaging to the business model of BOMA members. As an example, an employee could divulge with impunity information that is considered confidential and proprietary to the employer, and the statute could be used improperly as a shield against an employer who seeks to discover such disclosure.

While there are other concerns as well, many of which would affect businesses generally, we hope this example illustrates both the problems that could be caused by this legislation and the need to be precise in determining the scope of personal information that, as a matter of public policy, requires legislative protection.

For these reasons, BOMA respectfully requests an unfavorable report on Senate Bill 201.

Sincerely,

Kevin J. Bauer

MAMIC_UNF_SB201
Uploaded by: Popham, Bryson
Position: UNF

MAMIC
Maryland Association of
Mutual Insurance Companies

191 Main Street, Suite 200 – Annapolis MD 21401 – 410-268-6871

February 12, 2020

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

RE: Senate Bill 201 - Commercial Law - Personal Information Protection Act – Revisions - OPPOSED

Dear Senator Kelley,

On behalf of the Maryland Association of Mutual Insurance Companies (MAMIC), I respectfully request an unfavorable report on Senate Bill 201.

MAMIC is comprised of eleven mutual insurance companies that are headquartered in Maryland and neighboring states. Approximately one-half of our members are domiciled in Maryland and are key contributors and employers in our local communities. Together, MAMIC members offer a wide variety of insurance products and services and provide coverage for thousands of Maryland citizens. As mutual insurers, MAMIC members are owned entirely by our policyholders, and any profits earned are either retained by the company or returned to policyholders in the form of dividends. By contrast, stock insurers are owned by shareholders. Profits generated by a stock insurer are distributed to investors who may or may not have a policy of insurance with the company.

We have a number of concerns about this legislation, which affect MAMIC members both as insurers and small businesses in Maryland. First, the language in Section 14-3504 referencing breach and notification is highly problematic. Reducing the notification period to 30 days after discovery of the breach would impose a significant burden on the small businesses that constitute MAMIC membership. Similarly, with respect to information not owned by one of our members, the notification period is even shorter – 10 days.

Furthermore, the language concerning "activity-tracking data" on page 3, lines 4-9, is overly broad. It could, for example, apply to an employee's use of a company email system, which is traditionally considered to be the exclusive property of an employer. That same broadening of personal information could apply to standard activities conducted by non-employees of insurers, such as data collected by an insurance appraiser while assessing damage to someone's home or automobile.

MAMIC notes that SB 201 is intended to apply to businesses generally, and not solely to insurers. Because of the unique structure of insurance companies and their need to handle the personal information of many different insureds, we respectfully suggest that any such privacy legislation be drafted and enacted by the legislature in consultation with the Maryland Insurance Administration.

For the reasons listed above, we respectfully request an unfavorable report on Senate Bill 201.

Thank you,

Jill Showalter
President

LATE - ACLI_UNF_SB201
Uploaded by: Ryan, Vince
Position: UNF

Financial Security...for Life.

Vincent Ryan
Legislative Director

February 12, 2020

The Honorable Delores G. Kelley
Chair, Senate Finance Committee
Miller Senate Office Building
11 Bladen St
Annapolis, MD 21401

RE: Senate Bill 201 – Personal Information Protection Act Revisions

Dear Senator Kelley:

The American Council of Life Insurers (the "ACLI") appreciates the opportunity to present our concerns with Senate Bill 201 ("S. 201") as it relates to consumer data breach protocols. Specifically, ACLI has concerns with § 14-3501 and § 14-3504 and recommends that the Committee submit an unfavorable report on S. 201. We have outlined our concerns with each section below.

§14-3501 – Definition of "Genetic Test" and "Genetic Information"

Section 14-3501 would add new definitions of "genetic test" and "genetic information" to the list of "personal information," which would trigger a data breach notice if the security system was breached. ACLI has concerns with these definitions as they conflict with current definitions of "genetic test" and "genetic information" under §18-120 (a)-(b) of the Maryland Insurance Code.[1][2] Such consistency in the law helps to ensure carrier compliance between the Commercial and Insurance Codes in Maryland, while also enhancing consumer protection.

§14-3504 – Timeframe for Notice to Consumer & Attorney General

Section 14-3504 would significantly amend Maryland's breach of security laws and completely change how and when a business notifies a consumer and the Attorney General of a data breach. The provisions contained in § 14-3504 are so significant we worry that there may be overreporting and consumer confusion. For example, § 14-3504 (b)(2) appears to change the "harm trigger" from "after the

[1] § 18-120 (a): "'Genetic information' means information derived from a genetic test: 1. about chromosomes, genes, gene products, or inherited characteristics that may derive from an individual or a family member; 2. not obtained for diagnostic and therapeutic purposes; and 3. obtained at a time when the individual to whom the information relates is asymptomatic for the disease, disorder, illness, or impairment to which the information relates."

[2] § 18-120 (b)"'Genetic test' means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites that detects genotypes, mutations, or chromosomal changes.

American Council of Life Insurers
101 Constitution Avenue, NW, Washington, DC 20001-2133
(202) 624-2452 t vincentryan@acli.com
www.acli.com

investigation is concluded" to "reasonably determines that the breach does not create a likelihood that the information will be misused." Is an investigation still permitted? Is the investigation allowed to conclude or must the decision be made during an investigation?

In addition, the breach of security notice time frame is significantly altered under this section. Notice of a breach would have to be sent not later than thirty (30) days (as opposed to current law of 45) after the entity discovers or is notified of the breach of the security of a system. Is such notice to be given after the business determines that there is not a likelihood that the information will be misused, or every time a business discovers or is notified of the breach of the security of a system? If there is no likelihood of harm, is a notice required?

Insurers, and particularly life insurers, have been on the forefront of protecting consumers' data and information for well over 100 years. All states have laws in place that require businesses, including insurers, to notify consumers in the event of a data breach involving non-public information. Most of the states adopted laws similar to the approach California adopted many years ago, including Maryland. For the most part, these data breach laws are fairly uniform across the country. Consumers benefit from this uniform approach as they understand the importance of receiving a notice involving the breach of their data.

Adoption of § 14-3504 could cause adverse consequences for Maryland consumers. Laws that lower the thresholds for reporting and shorten the timeframe within which breach notification must occur could be alarming and confusing to Maryland consumers. More notification of "possible" breaches may make consumers immune to such notices and cause consumers not to take such notifications seriously.

Lastly, information to be added to the notice to the Attorney General pursuant to § 14-3504 (h)(2) under condensed timeframes is unreasonable and unduly burdensome. In addition, this specific type of information contained in the above-referenced section may not be available until a complete and thorough investigation is over. Timely and reasonable notice to consumers is our immediate concern.

Conclusion

For the aforementioned reasons, ACLI respectfully requests that the Committee submit an unfavorable report on S. 201.

Thank you in advance for your consideration. I am available at your convenience to address any questions.

Respectfully submitted,

VINCENT J. RYAN

MTC_Richard Tabuteau_UNF_SB0201

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 12, 2020

RE: **OPPOSE** – Senate Bill 201 – *Commercial Law – Personal Information Protection Act – Revisions*

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 201.

Senate Bill 201 expands the Maryland Personal Information Protection Act (MPIPA) by covering additional types of personal information to include genetic information and nonpublic social media information. It also expands the types of businesses that are required to implement and maintain reasonable security procedures and practices to protect personal information from unauthorized use; shortens the period within which businesses must provide required notifications to consumers after a data breach; and requires additional information to be provided to the Office of the Attorney General after a breach has occurred. Violation of the bill is an unfair, abusive, or deceptive trade practice under the Maryland Consumer Protection Act.

Though MTC recognizes the importance of timely, accurate notification to consumers of data breaches there remains major concerns with some of the definitions in Senate Bill 201, as introduced. The proposed requirements in the bill would vastly exceed requirements imposed by other states. Additionally, some of the timeframes are unreasonably short for consistent compliance. We understand that the tech industry is working with the sponsors on amendments and are hopeful that consensus can be reached. However, as currently drafted, MTC urges an unfavorable report for Senate Bill 201.

For more information call:
Richard A. Tabuteau
Pamela Metz Kasemeyer
J. Steven Wise
Danna L. Kauffman
410-244-7000