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 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-alexas-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.