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

March 9, 2020

TO: The Honorable Dereck E. Davis, Chair
Economic Matters Committee

FROM: Hanna Abrams, Assistant Attorney General

RE: House Bill 784 – Maryland Online Consumer Protection Act (SUPPORT)

The Office of the Attorney General supports House Bill 784 ("HB 784"), which returns to Marylanders the right to control 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] House Bill 784 provides consumers with three basic rights that address these concerns: (1) the right to know what information companies collect, (2) the right to delete that information, and (3) the right to tell companies not to sell that information.

Right now, companies are collecting and selling increasing amounts of sensitive information about our lives without our knowledge or consent. This information draws an intimate picture about our personal lives: our gender, religious beliefs, sexual preferences, and even our precise location. At least 70% of mobile apps share data with third parties, and 15% of the apps reviewed were connected to *five or more* trackers.[3] That means that when you open a weather app to check the temperature, your data may be shared with multiple businesses you have never heard of, and it continues to be shared even after you have closed the app. Because of the specificity and scope of the information that is collected, and the absence of knowledge and consent, this practice 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*.
[3] 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.

The tools that we currently have in place come into play only 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.[4] But this bill provides something more – it is preventative. It gives consumers the ability to protect themselves by limiting the amount of consumers' personal information available for hackers to find.

A constant stream of discoveries shows how data is being monetized without consumer consent:

- A New York Times investigation found that many of the apps that collect location information for localized news, weather, and other location services share that information with third parties for advertising and other purposes.[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]

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

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

psychologists or doctors. Instead, these apps frequently share data for advertising or analytics to Facebook or Google without even disclosing this to users.[9]

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:

- Using the personal information consumers are unwillingly sharing, employers have consciously targeted advertisements at younger men to keep older workers and females from learning of certain job opportunities,[10] and landlords have prevented racial minorities from seeing certain housing advertisements.[11]
- 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.[12]

Consumers do not want their personal data being used for purposes beyond providing the service they signed up for. HB 784 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.

CONSUMER RIGHTS UNDER HB 784

The Right of Transparency

Transparency is the first critical step – it allows consumers to make informed decisions. HB 784 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).[13] Businesses will also include the same information in their online privacy policies.[14]

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

[9] 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.
[10] 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.
[11] 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.
[12] *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.
[13] Section 14-4202.
[14] Section 14-4204(d).

source of the information; (3) with whom the business shared the consumer's data; and (4) why it shared the data.[15] Businesses must provide accessible methods of making requests for this information.[16]

The Right to Delete

HB 784 would require businesses to honor consumer requests to delete personal information the business collected about them.[17] It makes ample exceptions, to allow businesses to keep information for research purposes, and where required by law.[18]

The Right to Opt Out of Sale/Third Party Disclosure

In some cases consumers may elect to receive services from a business that collects their information, but they can still elect not to have their data sold. Exercising this right means that the business that collected a consumer's information can maintain it, but cannot share it with third parties.[19] Consumers will be able to exercise this right via a clear and conspicuous link on the business' website.[20]

The bill provides further protection to minors, barring businesses from disclosing their information to third parties.[21]

The Right of Non-Discrimination

HB 784 bans discrimination against anyone who exercises one of the above-described rights.[22] 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.

SCOPE OF HB 784

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.[23] This bill does not impede the ability of businesses to use personal information for research purposes for the public good. It allows a business to ignore a consumer's request to delete information if keeping the information is necessary to engage in public or peer-reviewed scientific, historical, or statistical research in the public interest.[24]

---

[15] Section 14-4203.
[16] Section 14-4204.
[17] Section 14-4205.
[18] Section 14-4205(d).
[19] Section 14-4206.
[20] Section 14-4206(d).
[21] Section 14-4206(b).
[22] Section 14-4207.
[23] *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).
[24] Section 14-4205(d)(5); *see also* Section 14-4209 (requiring privacy and security protections for personal information used for research purposes).

Businesses Currently Offer Many of These Protections, But Only to Select Consumers

At least 19 companies have implemented the privacy protections required under the California Consumer Privacy Act ("CCPA") for all Americans,[25] including Marylanders: Amazon, Apple, DoorDash, Facebook, Google, Lutron, Microsoft, Netflix, PayPal, Ring, Roku, Starbucks, Strava, Toyota, Twitter, Uber, UPS, Wiland, and Zillow.[26]

However, many nationwide companies are restricting consumer access rights and deletion rights to California residents alone.[27] These businesses include: Acxiom, Airbnb, Alaska Airlines, Altria, AMC, Amobee, Aristotle, AT&T, Best Buy, BevMo, Chipotle, Civis, Comcast Xfinity, CVS, Disney, Deep Root Analytics, Dominos, eBay, Eero, Epsilon, Equifax, Equinox, Experian, ExxonMobil, Face App, Fitbit, Ford, General Motors, Grindr, Honda, Hulu, i360, JetBlue, Kayak, L2, Live Nation, LiveRamp, Lyft, Macy's, Marriott, Mastercard, Nissan, OpenTable, Orangetheory Fitness, Pinterest, Quora, Redfin, Resy, Samsung, SiriusXM, Snap, Southwest Airlines, Spotify, Staples, Target, TargetSmart, Ticketmaster, Tinder, TransUnion, TrueData, Uber, Unilever, Verizon, Verizon Media, Visa, Volkswagen, Walmart, Washington Post, Whitepages, Whole Foods, and Yelp.[28]

This list demonstrates that despite business protestations, compliance is possible. There is no reason that Marylanders should be offered fewer privacy protections than citizens of other states.

The Impact Is Limited to Larger Businesses

HB 784 is drafted to limit its impact to larger businesses that are collecting data indiscriminately. To do so, it has revenue and population thresholds. Only businesses that have (a) an annual gross revenue of over $25 million; (b) annually buy, receive, or share the personal information of 100,000 or more consumers; or (c) derive at least half of their annual revenue from selling consumer personal information are required to comply with HB 784.[29] This language, while similar to that in the CCPA, doubles the consumer threshold established in the CCPA.[30]

Additionally, the bill will only impact a business that "buys, receives for the business's *commercial purposes*, sells, or shares *for commercial purposes*, alone or in combination, the personal information of 100,000 or more consumers, household, or devices."[31] In order to fall under the umbrella of HB 784, the "receiving" or "sharing" transactions must be for "commercial purposes" rather than "business purposes." A company's "business purpose" is when the business

---

[25] 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 HB 784 and the CCPA.

[26] Geoffrey Fowler, *Don't sell my data! We finally have a law for that*, WASH. POST (Feb. 6, 2020) https://www.washingtonpost.com/technology/2020/02/06/ccpa-faq/?arc404=true (including direct links to the companies CCPA info as well as access and deletion requests).

[27] A more complete list can be found: https://caprivacy.github.io/caprivacy/full/.

[28] *Id*.

[29] Section 14-4201(d).

[30] Under Cal. Civ. Code Sec. 1798.140(c)(1)(B) must "alone or in combination" sell/buy or shares/receive for "commercial purposes" more than 50,000 records of 'consumers" "household, or devices" a year to meet the 'number of records sold/bought'' threshold. SB 957 doubles this eligibility threshold. In fact, the current California ballot initiative referenced by many of those testifying in opposition to SB 957 proposes raising the business eligibility threshold under the CCPA to 100,000. *See* The California Privacy Rights Act of 2020.

[31] Section 14-4201(d)(2) (emphasis added).

"uses personal information . . . in a manner reasonably necessary to achieve the operational purpose for which the information was collected."[32] This is distinct from its "commercial purpose." The text and context of HB 784 make clear that not all consumer transactions qualify to meet this threshold. For example, the bill would **not** affect businesses that conduct 100,000 simple consumer transactions per year or the equivalent of 275 transactions per day such as selling 275 cups of coffee a day. Rather, this threshold, as well as the businesses that derive at least half their annual revenue from selling personal information, targets the practices of data brokers and other businesses that profit from receiving, or sharing personal information. Thus, even if a coffee shop sold 100,000 cups of coffee in a single day, these sales would not trigger HB 784's eligibility threshold.[33]

Definition of Consumer

HB 784 defines "consumer" as "an individual who resides in the state."[34] 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

HB 784 incorporates several exemptions, including for personal information collected pursuant to the federal Gramm-Leach-Bliley Act ("GLBA") and implementing regulations.[35] 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, HB 784 does not alter those regulations. Financial institutions have the same obligation to protect personal information under the California Consumer Privacy Act.[36]

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. HB 784 provides these protections to Marylanders.

---

[32] Section 14-4201(e).
[33] 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.
[34] Section 14-4201(g).
[35] Section 14-4208(b)(8).
[36] Cal. Civ. Code §§ 1798.100-199.

We urge a favorable report.

Cc: Members, Economic Matters Committee
The Honorable Ned Carey