**BRIAN E. FROSH**
*Attorney General*

**ELIZABETH F. HARRIS**
*Chief Deputy Attorney General*

**CAROLYN QUATTROCKI**
*Deputy Attorney General*

**WILLIAM D. GRUHN**
*Chief*
Consumer Protection Division

**STATE OF MARYLAND**
**OFFICE OF THE ATTORNEY GENERAL**
**CONSUMER PROTECTION DIVISION**

January 26, 2022

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

FROM: Hanna Abrams, Assistant Attorney General

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

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

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

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

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

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

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

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

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

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

The tech industry exploits and sells this sensitive information about our private lives. Companies are collecting information that gives strangers personal information about us including gender, religious beliefs, sexual preferences, and even our precise locations. The adtech industry regularly collects, shares, sells, and processes consumer data. At least 70% of mobile apps share data with third parties, and 15% of the apps reviewed were connected to *five or more* trackers.[4] The extraction of personal information, particularly because it is done frequently without consumer knowledge, poses a significant threat to both our privacy and our safety.

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

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

---

[4] Lee Matthews, *70% Of Mobile Apps Share Your Data with Third Parties*, Forbes, (June 13, 2017), https://www.forbes.com/sites/leemathews/2017/06/13/70-percent-of-mobile-apps-share-your-data-with-third-parties/#562270ce1569.

[5] Molly Omstead, *A Prominent Priest Was Outed for Using Grindr. Experts Say It's a Warning Sign*, Slate (July 21, 2020), https://slate.com/technology/2021/07/catholic-priest-grindr-data-privacy.html.

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

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

[8] Julia Angwin et al., *Facebook Job Ads Raise Concerns About Age Discrimination*, N.Y. Times (Dec. 20, 2017), https://www.nytimes.com/2017/12/20/business/facebook-job-ads.html.

[9] Julia Angwin et al., *Facebook (Still) Letting Housing Advertisers Exclude Users By Race*, ProPublica (Nov. 21, 2017), https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin.

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

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

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

We urge a favorable report.

Cc: Members, Finance Committee
The Honorable Susan Lee

[10] *See* Technology Safety, Data Privacy Day 2019: Location Data & Survivor Safety (Jan. 28, 2019), https://www.techsafety.org/blog/2019/1/30/data-privacy-day-2019-location-data-amp-survivor-safety.

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

## APPENDIX A

## CONSUMER RIGHTS UNDER SB 11

**The Right of Transparency**

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

**The Right to Know**

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

**The Right to Delete**

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

**The Right to Opt Out of Sale/Third Party Disclosure**

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

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

**The Right of Non-Discrimination**

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

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

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

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

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

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

**Definition of Consumer**

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

**Exemptions**

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

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

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

[27] Cal. Civ. Code §§ 1798.100-199.