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

March 30, 2022

TO: The Honorable C.T. Wilson, Chair
Economic Matters Committee

FROM: Hanna Abrams, Assistant Attorney General

RE: Senate Bill 11 – Workgroup on Online Consumer Personal Information Privacy – SUPPORT

The Consumer Protection Division of the Office of the Attorney General supports the creation of the Online Consumer Personal Information Privacy Workgroup as outlined in Senate Bill 11 as amended.

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. For the past four years, the Consumer Protection Division has supported legislation that protects these rights; however, this legislation has been stymied by concerns over unintentional consequences or business concerns that have not been clearly articulated. Developing a comprehensive privacy framework that considers consumer interests as well as any impacts on access to technology and downstream repercussions requires in-depth discussions that are not generally feasible during the busy General Assembly session. A workgroup provides this opportunity and demonstrates the commitment of the legislature to protect consumer privacy rights.

A workgroup would consider consumers' rights to privacy that impact how they are able to control what information companies collect and how businesses are able to use their information, such as the:

- Right to Transparency
- Right to Know
- Right to Delete
- Right to Opt-out of Sale/Third Party Disclosure
- Right to Non-Discrimination[2]

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

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 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.[3] 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.[4]
- Social media profiles and internet usage may be used to determine creditworthiness.[5] 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.[6] 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,[7] and landlords have prevented racial minorities from seeing certain housing advertisements.[8]
- The secondary use and sharing of location data creates a serious safety risk, particularly for survivors of intimate partner violence, sexual assault, and gender-

---

[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.

[4] 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.

[5] 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/.

[6] 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.

[7] 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.

[8] 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.

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.[9]

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.[10]

Maryland was on the forefront of consumer privacy when it enacted its data security protections and this workgroup would continue in that tradition. Although the Division would prefer that the General Assembly enact a substantive bill to address consumers' rights to protect their personal information online, we believe that Senate Bill 11 presents the best opportunity of achieving that goal next year.

We urge the Economic Matters Committee to issue a favorable report on Senate Bill 11.

cc: Members, Economic Matters Committee
The Honorable Susan Lee

[9] *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.

[10]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.