FAVORABLE

TESTIMONY PRESENTED TO THE
HOUSE COMMITTEE ON ECONOMIC MATTERS

HB 807
CONSUMER PROTECTION – ONLINE AND BIOMETRIC DATA PRIVACY

DR. GREG VON LEHMEN
STAFF, MARYLAND CYBERSECURITY COUNCIL

POSITION: SUPPORT
FEBRUARY 22, 2023

Chairman Wilson, Vice Chairman Crosby, and members of the committee, thank you for the opportunity to provide testimony. I am Dr. Greg von Lehmen, staff to the Maryland Cybersecurity Council, a statutory body that is chaired by the Attorney General. Last summer, the Council formed an ad hoc subcommittee on consumer and child privacy. I staffed the subcommittee and produced the final subcommittee report. I have been approved by OAG in my staff role to urge favorable consideration of the bill due to my familiarity with the work of the subcommittee and the research that I conducted for the report.

Let me say by way of additional background that the subcommittee convened five times between July and December of last year. It received comments from more than ten interested parties, including public policy advocacy groups, an industry representative, privacy law attorneys, and the Attorney General of California, among others. The subcommittee adopted the report in December to help inform privacy legislation for Maryland.

I would make three broad points in connection with the bill.

First, the problem the bill addresses is the enhanced exposure to harm that consumers face as a result of the expansive, commercial collection of sensitive personal information. There is a vast data ecology that is focused on developing as detailed a profile of each consumer as possible. These profiles include where we go on the internet and in our cars, who we co-locate with, where we live, where we have lived, what we buy, our health conditions, our gender orientation, musical and TV viewership tastes, political leanings, and hundreds of other data points. These data are not pinned to a device; they are pinned to a known person.

There are various types of risk that such detailed profiles pose. A significant risk is the exposure to data breaches. Data from PrivacyRights.org indicates that 10 billion US consumer records have been compromised between 2004 and 2019. Data published for Maryland suggests that the in recent years the average number of separately reported residents impacted per year by a breach is about 600,000.[1] With data breaches can come a variety of harms: identity theft, extortion, sextortion, and reputational damage, among others. The US Department of Justice reported that losses in 2018 due to identify theft, including personal account take-overs, exceeded $15 billion.

The consumer's exposure is becoming more severe as commercial interest grows in using biometric data for a variety of purposes, such as authentication of credit cards at checkout. The problem is that once biometric data held by a company is breached and spilled into the criminal market, countermeasures become very difficult. Biometric data cannot be changed like a password.

Second, considering these risks, the question becomes what tools can be given to consumers to help them manage their exposure. The bill answers this question by incorporating widely accepted privacy principles. These principles include:

- *Transparency*. Consumers have a right to easily understandable information about data collection, use, and sharing practices.
- *Respect for context*. Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- *Data minimization*. Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- *Access, accuracy, and control*. Consumers have a right to access and correct personal data in usable formats as well as to delete personal information entirely.
- *Security*. Consumers have a right to secure and responsible handling of personal data
- *Accountability*. There should be mechanisms to enforce these principles.

These principles are not arbitrary but have developed over time out of a sense of concern about data accumulation and its impacts. The federal government first

[1] Note that the total likely does not consist of unique cases, since separately reported breaches may affect the same residents. The number of unique residents affected is likely lower See Office of the Maryland Attorney General, data breach snap shots for 2020, 2018, and 2016, respectively, at https://www.umgc.edu/content/dam/umgc/documents/upload/data-breaches-fy-2020-snapshot-pdf.pdf, https://www.umgc.edu/content/dam/umgc/documents/upload/data-breaches-fy-2018-snapshot.pdf, and https://www.umgc.edu/content/dam/umgc/documents/upload/data-breaches-fy-2016-snapshot.pdf

formulated and implemented most of the principles just mentioned starting in the 1970s because of the troves of personal data that it holds. These are known as the Fair Information Principles Practices (FIPPS).[2] With the growth in commercial data collection, the Obama Administration in 2012 called for the application of those principles in an expanded form to the commercial sector. This was the Administration's Consumer Bill of Rights.[3] Similar concerns prompted the EU's General Data Protection Regulation (GDPR) in 2014.[4] Today five US states have implemented the foregoing principles in some measure for millions of Americans: California, Colorado, Connecticut, Virginia, and Utah. These statutes have created a track record. The risk of unintended consequences can be known and minimized. There is no reason that I can see for not implementing the foregoing principles in Maryland law as the bill would do.

Finally, parents need help in managing the risk to their children. The federal Children's Online Privacy Protection Act (COPPA) has not kept pace with the explosion of mobile devices that allow children to access apps not just at home but wherever they are.

- Children mispresent their age in violation of terms of use and participate on general audience platforms: Facebook, TikTok, Snapchat, among others—at scale.
- The risks that children face on these platforms are well documented—grooming is one—but it also includes targeted advertising. Repeated reports of the American Psychological Association, the Journal of Pediatrics, and others have shown that targeted advertising affects children's self-image, how they compare themselves to others, and results in harmful behaviors.
- Hundreds of thousands of child-directed applications—children's games—do collect what COPPA defines as personal information on children, including information on their device and browsing that is then linked to them. Moreover, they do it without any meaningful mechanism for first obtaining verifiable parental consent as COPPA requires. Here, too, the data is used to shape advertising that is targeted at them.

The bill takes some remedial steps in connection with these problems. The ad hoc subcommittee report goes further, including recommendations such as a different knowledge standard for companies operating general audience platforms.

[2] See Fair Information Principles Practices (FIPPS) at https://www.fpc.gov/resources/fipps/
[3] The White House (2012). Consumer Privacy in a Networked World. https://nsarchive.gwu.edu/document/16084-white-house-consumer-data-privacy
[4] General Data Protection Regulation at https://gdpr-info.eu/

Consequently, I support the language at the end of the bill that would establish a Task Force to examine COPPA-related issues and consider appropriate recommendations.

To conclude, I urge a favorable consideration of the bill. Thank you for the opportunity to testify. I would be happy to answer any questions.