Dawn D. Gile
Legislative District 33
Anne Arundel County

Finance Committee

Chair

Anne Arundel County
Senate Delegation

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

Miller Senate Office Building
11 Bladen Street, Suite 3 East
Annapolis, Maryland 21401
410-841-3568 · 301-858-3568
800-492-7122 *Ext.* 3568
Dawn.Gile@senate.state.md.us

Testimony in Support of SB0541 - Maryland Online Data Privacy Act of 2024

Madame Chair, Madame Vice Chair, and Fellow Members of the Senate Finance Committee:

Currently, Maryland lacks a comprehensive online privacy law, presenting a significant issue. Companies operate unchecked, gathering and monetizing personal and sensitive information from our lives without our awareness or consent. When we download seemingly "free" applications, they come at the cost of our personal data, surreptitiously collected by these apps. We unwittingly become both consumers and commodities. Shockingly, over 70% of mobile apps share user data with third parties, and research reveals that 15% of these apps are linked to five or more tracking mechanisms. This data encompasses a wide range of personal information, from mental health and reproductive data to location data, all gathered, aggregated, and traded without our explicit consent or knowledge.

For example, imagine a scenario where someone downloads a fitness tracking app to monitor their daily exercise routine. Unbeknownst to them, the app not only records their workout sessions but also collects data on their sleep patterns, heart rate, and even their location throughout the day. This information, seemingly innocuous on its own, becomes part of a vast network of data points that are bought and sold by third-party companies. Eventually, this individual's personal habits and whereabouts are commodified without their consent, raising serious concerns about privacy infringement and potential misuse of sensitive data.

Consider another recent example wherein it was revealed that Pray.com, a popular religious app, had been sharing comprehensive user data with third-party entities. Users were shocked to learn that their personal information, including intimate details such as mental health struggles, had been shared without their explicit consent. For instance, they found themselves targeted with ads on platforms like Facebook, promoting services like "Better Marriage," "Abundant Finance," and "Releasing Anger." This breach of trust raised profound ethical concerns regarding the handling of sensitive user data by technology firms and underscored the critical need for robust privacy regulations and increased transparency from app developers concerning data collection and sharing practices.

In Europe, comprehensive data privacy laws, exemplified by the General Data Protection Regulation (GDPR), afford extensive safeguards for individuals' personal data, prioritizing transparency and user consent. Conversely, the United States federal government has not yet implemented legislation comparable to the GDPR. In response to this federal inaction, numerous states across the nation have taken proactive measures to protect consumer privacy. Presently, fourteen (14) states have enacted data privacy laws, while several others have similar legislation pending. These laws encompass a range of provisions, including mandatory disclosure of data breaches and granting individuals greater control over the usage of their personal data. This collective endeavor by individual states underscores a dedication to bolstering consumer privacy and fostering trust in digital interactions.

Solution

SB0541 establishes a number of consumer protections, including:

- Data minimization – making sure companies are only collecting and processing the data needed for the transaction at hand;
- Data protection – ensuring companies keep the data they do collect safe;
- Consumer control over personal data – giving consumers the right to know what is collected and who it is shared with, along with the right to correct the data, delete the data, and opt out of targeted ads, sale of data and profiling;
- Extra layers of protection for sensitive data. Sensitive data includes:
    - Biometrics
    - Geolocation
    - Reproductive, mental health, and gender affirming care.
    - Racial or ethnic origin, religious beliefs, sexual orientation, citizenship, or immigration status
    - Personal data that a controller knows or has reason to know is that of a child.

Because this is a lengthy bill, I am submitting with this testimony an overview of the bill for the Committee's convenience.

I respectfully request a favorable report on SB0541.