March 6, 2019

The Honorable Delores G. Kelley, Chair
Members of the Senate Finance Committee
3 East
Miller Senate Office Building
Annapolis, MD 21401

RE: SB 0613 -- Maryland Online Consumer Protection Act -- Neutral

Dear Chair Kelley:

The Center for Democracy & Technology is a non-profit, non-partisan technology advocacy organization based in Washington, D.C., that works to promote democratic values by shaping technology policy and architecture, with a focus on the rights of the individual. CDT supports laws, corporate policies, and technological tools that protect privacy and security online. We write today to encourage the Maryland General Assembly to enact a meaningful privacy law that will protect the interests of all Marylanders.

The Maryland Online Consumer Protection Act (SB 0613) is a good first step, echoing protections established by the California Consumer Privacy Act (CCPA), but stronger privacy protections are warranted. Below, we offer several suggested improvements for the current proposal.

Meaningful Privacy Laws Should Address How Companies Collect, Use and Share Data

In 2019, privacy laws must not double down on the notice-and-consent model by focusing solely on user controls and privacy self-management. The existing proposal ultimately places a burden onto individuals to protect their privacy when the ideal is to place obligations onto companies to cease unfair and surprising practices involving our data. To be meaningful, privacy laws must address corporate behaviors and thereby redistribute some of the privacy burden back on to entities that are in the business of collecting, using, and sharing data.

Our preference is for lawmakers to create prohibitions and restrictions on certain data practices. As a practical matter, strong rules that limit collection and repurpose can address privacy problems that emerge through data analytics, sharing, and exploitation.[1] For example, in CDT's model privacy legislation,[2] we include provisions to make it unlawful to engage in

[1] Prepared Testimony and Statement for the Record of Woodrow Hartzog, Hearing on "Policy Principles for a Federal Data Privacy Framework in the United States" Before the Senate Commerce Committee 10 (Feb. 27, 2019), https://www.commerce.senate.gov/public/_cache/files/8b9adfcc-89e6-4df3-9471-5fd287051b53/3F23C463B1B622BAE22C47019C913FF8.hartzog-testimony-senate-privacy-principles-final.pdf.

[2] Center for Democracy & Tech., Federal Privacy Legislation, https://cdt.org/campaign/federal-privacy-legislation/ (last visited Mar. 1, 2019).

certain data processing practices. Specifically, we target activities involving biometric, location, and health information, among others, where the use, sharing, or even collection of this data is not required either to provide or add to the functionality of a product, service, or specific feature requested by an individual. SB 0613 could be improved by limiting secondary uses or unnecessary collection outside of carefully considered business purposes (like product fulfillment) or for limited security and fraud prevention activities. Companies have shown that they should not have unlimited discretion to define what constitutes a business purpose.

To the extent SB 0613/HB 0901 allows users to opt-out of sharing personal information with third parties, it is undercut by non-standard definitions of "service providers" and "third parties." Service providers are usually defined as entities that process data solely to facilitate the primarily relationship between the covered entity and the user. To that end, privacy laws exempt them from third party processing bans because they are needed to deliver the service requested by the user. In this bill, service providers are defined as any company that processes personal information for a "business purpose" in accordance with a written contract, without further definition of what an allowable "business purpose" is. By allowing companies to evade the third party ban by simply entering into a contract with the original covered entity, this opt-out right may have little practical effect. We would recommend that the definition of service provider be amended, and other restrictions be placed on service providers, including prohibitions on any further licensing or resale of information, as well as require businesses to take reasonable efforts to monitor their service providers.

De-Identification Safe Harbors Should Be Clarified or Removed

While SB 0613 includes a broad definition of covered "personal information," it provides exceptions for the use of so-called "de-identified," "aggregate," and "pseudonymized" information.[3] Determining when information is unable to "reasonably be linked" either directly or indirectly to a person or device is a complicated technical as well as legal question. In general, CDT would caution against the inclusion of these concepts absent a much more comprehensive legislative framework or regulatory guidance.

De-identification is not foolproof and, thus, legislation requires very clear definitions and legal consequences for using de-identified data. SB 0613 does not achieve this. While the bill has a detailed multi-pronged definition of what constitutes de-identified data, this definition does not match the Federal Trade Commission's existing "three-part" test for de-identifying information. We support the deployment of technical safeguards as a core component of de-identification, but the proposal could provide further specificity as to what sort of "business processes" beyond contractual limits are appropriate. Further, privacy advocates already have acknowledged in California that additional clarity as to what this entails is needed, so Maryland lawmakers must not incorporate a de-identification safe harbor without additional scrutiny.[4]

[3] These terms and their definitions are lifted from the CCPA, which borrows these concepts from the EU General Data Protection Regulation.

[4] Consumer and Privacy Group Letter to CCPA Authors 3 (Aug. 13, 2018), *available at* https://regmedia.co.uk/2018/08/21/ca-privacy-act-advocates.pdf.

CENTER FOR DEMOCRACY & TECHNOLOGY

At present, the interrelationship between "de-identified," "aggregate," and "pseudonymized" data is unclear.[5] This creates a situation that is unfair to businesses and may not protect individual's privacy.[6] If these terms are not further clarified, CDT would recommend that Maryland lawmakers remove the definitions of "pseudonymized" and "aggregate," and clarify that businesses that make use of de-identified data are required to describe their methods for de-identifying personal information to provide meaningful external accountability. Specifying that contractual agreements are required for sharing of de-identified information is also useful. This should go beyond existing practices however, and require reasonable and affirmative efforts to oversee how third parties and other partners use de-identified information.

Meaningful Privacy Laws Require Effective Enforcement

Robust enforcement is often an under appreciated requirement for a privacy law to be meaningful. Too frequently, laws assume that a state Attorney General or consumer protection regulator is positioned to adequately enforce data protection requirements, but this is far from clear.

Like the CCPA, SB 0613 places its primary enforcement burden on the Maryland Attorney General (AG). In California, for example, the AG has already had to request additional resources and personnel simply to prepare to enforce the law. More recently, the California AG has proposed that the CCPA be amended to include a private right of action to bring suit for privacy violations.[7] A separate legislative proposal allocated $700,000 and five staff positions to aid in the development of the AG-led regulatory process envisioned by the CCPA and echoed in SB 0613. Comparable federal proposals would authorize the FTC to hire 175 new lawyers and technical experts to assist in enforcement.

If Maryland intends to enact a similarly wide-ranging privacy law, lawmakers must consider whether the Maryland Attorney General has either the existing resources or expertise necessary to enforce the law. The current proposal would require at least five separate rulemaking exercises. Section 14-4211 would require the Maryland AG to solicit broad public participation and adopt regulations to:

1. Address the definition of personal information;

[5] For example, the law's treatment of pseudonymized information is exclusively in the context of business research, though this is not the only place where companies currently make use of such data. Marketers, for instance, claim to use pseudonymous data for online advertising.

[6] Mitchell Noordyke, *CCPA offers minimal advantages for deidentification, pseudonymization, and aggregation*, IAPP (Jan. 17, 2019), https://iapp.org/news/a/ccpa-offers-minimal-advantages-for-deidentification-pseudonymization-and-aggregation/ .

[7] As AG Becerra has stated, the CCPA's general "lack of a private right of action, which would provide a critical adjunct to governmental enforcement, will substantially increase the AGO's need for new enforcement resources." Letter of Attorney General Becerra to CCPA Authors (Aug. 22, 2018), *available at* https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2018/08/ag-becerras-letter-re-california-consumer-privacy-act.pdf.

2. Process consumer access requests;
3. Develop a uniform opt-out logo or button;
4. Ensure notices can be easily accessible and understood; and
5. Address financial incentive offerings.[8]

These are no easy tasks. In order for the law to be effective, SB 0613 must provide additional support for the Maryland AG.

--

Thank you for the opportunity to comment on SB 0613. We hope these comments will be useful as Maryland lawmakers work to protect the privacy of Marylanders, and CDT looks forward to engaging further on these issues. Please do not hesitate to reach out with any questions to 202.407.8812 or via email at jjerome@cdt.org.

Sincerely,
Joseph Jerome
Policy Counsel, Privacy & Data Project
Center for Democracy & Technology

[8] The appropriateness of financial incentives really varies based upon whether a service or business is essential or the information is sensitive. For example, CDT has previously suggested permitting financial inducements in the limited context of internet service providers when conditioned by the following:

- consumers are provided clear information about the program/exchange;
- consumers can opt-out;
- companies comply with all notice requirements; and
- companies commit to not design programs that are unconscionable or coercive.