Main Street
PRIVACY COALITION

March 11, 2021

Harvey Perlman, Chairman
Collection and Use of Personally Identifiable Data Drafting Committee
Uniform Law Commission
111 N. Wabash Avenue, Suite 1010
Chicago, IL 60602

Dear Chairman Perlman:

The Main Street Privacy Coalition (MSPC), a coalition of 19 national trade associations representing more than a million American businesses,[1] supports the Uniform Law Commission's (ULC's) Collection and Use of Personally Identifiable Data Drafting Committee (Committee's) efforts to draft uniform model privacy legislation. MSPC believes the updated draft of the Collection and Use of Personally Identifiable Data Act (CUPIDA)[2] is a more workable privacy structure for Main Street businesses than previous drafts have been and appreciates the steps the Committee has taken to address concerns we have raised throughout this process.[3]

MSPC supports the approach that the CUPIDA draft currently takes to distinguish between compatible and incompatible uses of personal data and to differentiate between collecting and third-party controllers, which acknowledges that the collecting controller is not the only entity in the privacy chain of custody that exercises control over consumer data. MSPC, however, remains concerned that a collecting controller is the only entity with a legal obligation to provide a consumer with a copy of the consumer's data and the collecting controller remains liable for incompatible data practices of a third-party controller or a data processor. Additionally, MSPC believes CUPIDA should not exempt financial institutions or entities subject to the Gramm-Leach Bliley-Act (GLBA).

MSPC offers the comments below outlining our concerns that remain with CUPIDA. By closing these loopholes, the consumer protection that CUPIDA would provide will be improved.

---

[1] From retailers to Realtors®, hotels to home builders, grocery stores to restaurants, and gas stations to convenience stores, its member companies interact with consumers day in and day out. Collectively, the industries that MSPC trade groups represent directly employ nearly 34 million Americans and constitute over one-fifth of the U.S. economy by contributing $4.5 trillion to the annual U.S. gross domestic product. *See* https://mainstreetprivacy.com/about/ for a complete list of the members of the Main Street Privacy Coalition.

[2] *See* National Conference of Commissioners on Uniform State Laws, Collection and Use of Personally Identifiable Data Act (March 4, 2021)(hereinafter "CUPIDA").

[3] *See* Letter from MSPC to Chairman Perlman (September 16, 2020). *See also* Letter from MSPC to Chairman Perlman (December 4, 2020).

II. COMMENTS ON CUPIDA

A. Section 2 Definitions

As mentioned above, MSPC appreciates the addition of a definition for "collecting controller" to make the distinction between the controller that initially collects data and a third-party controller of that data. With the addition of this definition, CUPIDA recognizes that third-party controllers can *and do* exercise control over a consumer's personal data. In addition, it clarifies that entities that do not initially collect a consumer's personal data are not assumed to merely be a data processor. Data processors, therefore, can be classified as controllers if they engage in activity that determines the purpose of processing the data they possess.

The "processor" definition in CUPIDA is drafted in such a way that it expects a processor will only receive data from a controller. This definition should be adjusted to recognize a processor can receive data from another processor. For example, processors often use one or more subcontractors in order to complete the processing of data. For those subcontractors, the data is not received from a controller, but it is received from a processor.

MSPC would also like to highlight that the definition of "sensitive data" specifically includes credit card numbers, but does not include debit card numbers. Both should be noted in the definition.

B. Section 3 Scope – CUPIDA Unfairly Exempts Financial Institutions

MSPC remains concerned with the exemptions in CUPIDA for financial institutions and other entities subject to the GLBA who would otherwise be considered collecting controllers under CUPIDA in light of their collection and use of consumers' most sensitive data. It is important for the Committee to recognize and acknowledge that GLBA does not provide for any of the consumer rights established in Section 5 of CUPIDA. Financial institutions and other entities that are data controllers and subject to GLBA would therefore be able to avoid CUPIDA's requirements leaving consumers unprotected, which is underscored by the "or" included in Section 3(b)(4).

Additionally, the current draft's language states that financial institutions and other entities subject to GLBA are not subject to CUPIDA even if they do not treat the data in substantial compliance with GLBA. Merely being covered by the law exempts these entities from CUPIDA's reach regardless of how they handle the data. Furthermore, Section 3(b)(5) indicates personal information subject to GLBA is exempt even if it is "collected, used, processed, or disclosed by an entity ***other than*** a financial institution" *(emphasis added)*. As drafted, CUPIDA would exempt data collected by a financial institution, resulting from a transaction with a financial institution or collected by the financial institution in the course of providing a financial product.[4] A broad exemption such as this would leave consumers' most valuable and sensitive data exposed and unprotected.

[4] 16 CFR 313.3

The MSPC appreciates the Committee's attempt to include a small business exception for compatible data practices in Section 3 of CUPIDA, but the bracketed numbers are not reflective of the number of transactions a small business conducts in a calendar year. For example, a single, "mom-and-pop" convenience store averages more than 494,000 individual transactions per year. Many small businesses therefore will be subject to CUPIDA even if they only process data using compatible data practices such as through accepting credit and debit card payments.

C. Section 4 – Collecting Controllers Should Not Be Liable for Violations by Data Processor or Third-Party Controller

MSPC appreciates that CUPIDA has been updated to include requirements that a processor must comply with a consumer request. MSPC, however, remains concerned that CUPIDA requires a data controller to be liable for a data processor's activity. For example, Section 4(a)(7) requires controllers to provide redress for incompatible or prohibited data practices. If an incompatible practice is performed by a different controller or a processor, an innocent controller that fully complied with the law should not be liable. Likewise, Section 4(b) does not exempt the collecting controller from liability if the third-party controller or processor fails to comply with their requirements. The collecting controller should not be held responsible for the third-party controller or processor. The notion that one "controller" actually controls the activities engaged in by another "controller" is a fiction that should not be advanced by CUPIDA and certainly should not result in liability for the "controller" that did not commit or have control over a violation of CUPIDA committed by another entity.

D. Section 5 – Extend Right to Copy and Correct Personal Data to All Entities, Except Where a Fraudulent Request is Made

Consistent with consumers' expectations of privacy, all entities handling consumers' data should have statutory obligations to protect consumer data and honor consumer rights requests. Despite the advances the Committee has made to extend CUPIDA's requirements to all entities in the privacy chain of control, the collecting controller remains the only entity with an obligation to provide a consumer with a copy of his/her data. In many cases, once a collecting controller shares a consumer's personal data with a processor or third-party controller, the collecting controller no longer keeps a record of some or all of that data. A collecting controller will be forced to depend on the third-party controller or processor to respond with a copy of the personal data so that the collecting controller can comply with the law. Third-party controllers and processors, however, are not required to do so by the current language of CUPIDA. The absence of such a requirement will allow third-party controllers and processors to only provide partial data or simply refuse to provide data without any effective remedy for consumers and with unmerited liability for collecting controllers. This not only hurts consumers – because their rights requests will be ineffective – but it also unfairly shifts the burden and liability for such failures onto the collecting controller.

Additionally, there should be an exception to Section 5(b)(1) so that an entity is not required to provide a copy of personal data in the event of a fraudulent request.

E. Section 6 – Impractical to Present Privacy Policy at Time of Transaction for Millions of Small Business Storefronts

The provisions in Section 6 of CUPIDA create an inordinate administrative burden for millions of small business storefronts. As described above, approximately 95% of retailers are small, single-location operators with less than 50 employees. For these and other Main Street businesses, the owners also frequently manage the checkout counter as well as oversee the accounting and any other job that is needed in the store. Many of these retailers, such as local coffee shops, may have hundreds of thousands of customers making small-dollar transactions per year, and these businesses will therefore remain within the scope of the bill as controllers despite the scoping provisions of Section 3.

Provisions like this are difficult to apply because of the variety of businesses and industries subject to the law's requirements. With that in mind, businesses that only engage in compatible data practices such as doing nothing more than receiving payment information in order to complete transactions should not be required to provide a privacy policy at the time of those transactions. Such a requirement would not advance privacy interests but could slow transactions and burden small businesses, such as on-the-go convenience stores where customers make small-dollar transactions in short visits while commuting or traveling.

F. Section 7 – CUPIDA Should Include Protections for a Customer Loyalty Program as a Compatible Data Practice

Section 7 of CUPIDA should include a clear exemption for loyalty programs. A Main Street business's success depends on the relationship it has with its customers and clients. Consumers will choose businesses that they trust will use their information securely and responsibly. As such, MSPC supports privacy legislation that preserves the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships, including rewards and loyalty programs, as seen in the recent privacy law enacted by Virginia.[5] The current draft of CUPIDA, however, indicates data used for "targeted decisional treatment, including setting a price" is not a compatible data practice.

Loyalty programs typically use customer purchase histories in order to provide discounts to repeat customers. Those programs are very popular, benefit consumers, and should not be made illegal by privacy law. In a 2017 study, Forrester found that more than 70 percent of Americans participate in customer loyalty programs and adults, on average, participate in nine programs.[6]

In addition, many businesses make assumptions about which products or services their customers would like to purchase based on a variety of information they have from the existing business-customer relationship and their own sales or publicly available data. For example, it is a common and longstanding retail practice for a sales clerk in a store to ask whether a customer might want a

[5] Consumer Data Protection Act, 2021, ch. 36, 2021 Va. Laws 59.1-571, https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+CHAP0036 (codified at Va. Stat. Ann. § 59.1-571 et seq.).

[6] *See* Forrester Research; *How Consumers Really Feel about Loyalty Programs* (May 8, 2017) *available at* http://www.oracle.com/us/solutions/consumers-loyalty-programs-3738548.pdf.

scarf or tie that matches an outfit the customer is purchasing . Simply performing the analogous service for an online customer by having a website generate similar suggestions for customers should not face legal hurdles.

G. Sections 8 and 9 – Collecting Controllers Should Not Be Liable for Processors' or Third Parties' Incompatible Data Practices or Prohibited Data Practices

As explained above, MSPC remains concerned that CUPIDA requires a collecting controller to be liable for a third-party controller and/or processor's activity if they "knew or should have known" about the incompatible and/or prohibited data practices. That should not be the case.

Frankly, if collecting controllers are liable for another controller's conduct, then third-party controllers (and processors) should similarly be liable for the collecting controller's conduct. Of course, none of these vicarious liability models make sense in a privacy law. The idea that the business that first touches data actually "controls" it is most often a legal fiction. Large service providers have power in the market that allows them to dictate contract terms and structure data uses the way that they think best. Most collecting controllers are very small Main Street businesses – where "controller" is a misnomer – that do not have the wherewithal to change that power dynamic.

Rather than making collecting controllers liable for a third-party controller's or processor's actions, collecting controllers should serve as the conduit for consumers to request their privacy rights. Moreover, if third-party controllers or processors fail to meet those obligations (e.g., honor a consumer rights request), they should be held liable for those violations. The liability provisions in Sections 8 and 9 should be limited such that each business in the chain is responsible for its own incompatible and/or prohibited data practices. These modifications will ensure that the collecting controllers who complied with CUPIDA are not penalized for failures of third-party controllers and processors to comply with it.

The framework established in the latest CUPIDA draft obligates the smallest entities serving customers and holds them liable for failures by processors and third parties. This not only is an unfair shifting of liability onto businesses least capable of absorbing it, but the structure of the proposed law itself fails to set sufficient incentives to protect customer data for the nations' largest businesses who process the greatest amount of consumer data in serving millions of smaller businesses.

H. Section 10 – Data Privacy and Security Assessment Thresholds Inadequate

As with Section 6, the provisions in Section 10 of CUPIDA create an administrative burden for some entities. For the purposes of requiring privacy and security assessments, CUPIDA should set a higher threshold of volume of data and/or sensitivity of data than those that apply for compliance with the rest of the legislation. By having higher thresholds here, the bill could still require the largest, most sophisticated businesses and those with the most sensitive data to undertake assessments but spare small and mid-size businesses – particularly those that do not engage in data processing beyond compatible practices like handling payments – from this expensive and burdensome requirement. Many small and mid-sized operators would be overwhelmed by the requirements of this section.

I. Section 17 – Private Causes of Action Permit Meritless Lawsuits and Privacy Troll Campaigns Aimed at Small Businesses

Allowing for private causes of action creates opportunities for meritless lawsuits. Privacy regimes involve a level of complexity that makes private rights of action inappropriate. Many other areas of law – including patents and the Americans with Disabilities Act – have created burgeoning industries predicated on high volumes of demand letters and meritless lawsuits. Many lawyers have learned that the cost of defending such fact-intensive cases is more than sufficient to justify defendants settling claims for thousands of dollars even when they have no merit. The process of proving that all data was found in response to a consumer request or that no data handling was done that might cause a legal problem would make litigation very cumbersome.

This law should not be an opportunity to spawn a host of privacy trolls that indiscriminately threaten and file privacy suits, especially against small businesses that lack in-house counsel or the capital to defend against such meritless legal actions. MSPC urges the Committee to accept Alternative B with regard to Section 17 and ensure there are no private causes of action permitted under CUPIDA.

III. CONCLUSION

MSPC appreciates the Committee's diligent work on model privacy legislation and its consideration of the concerns raised above as it continues to deliberate the draft text of CUPIDA. We welcome the opportunity to provide the Committee with additional information on any of the concerns outlined here.

Very truly yours,

Main Street Privacy Coalition
https://mainstreetprivacy.com