



September 16, 2020

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 model privacy legislation, particularly if it can help provide a uniform approach to data privacy law across the United States. MSPC, however, remains concerned with the current draft of the Collection and Use of Personally Identifiable Data Act (CUPIDA).²

To that end, MSPC offers the comments below so that any draft model legislation formally adopted by the ULC is effectively well-balanced and can provide consumers with necessary privacy protections while ensuring that the burdens of protecting consumer data privacy are not disproportionately borne by any one sector of the economy. In our view, the current draft of CUPIDA fails to achieve that balance. Instead, it regulates consumer-facing businesses the most heavily, while exempting other sectors, such as financial institutions and data brokers, that engage in significant use of consumers' personal information without regulation by this or other federal laws to the same extent. We therefore appreciate the Committee's review and consideration in its forthcoming meetings of MSPC's concerns.

I. ABOUT THE MAIN STREET PRIVACY COALITION

MSPC is comprised of a broad array of national trade associations representing businesses that line America's Main Streets. 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. Our members can be found in every state, city, and town in our nation, providing jobs, supporting our economy and serving Americans as a vital part of their communities.

The foundation of our industries is trust, and the relationships we build with our customers. Our customers trust us with their personal information, and it is on our responsibility to earn that trust. For these reasons, our industries and associations have come together to form the MSPC, dedicated to the enactment of comprehensive and uniform data privacy laws. MSPC believes any strong, equitable and effective data privacy law should follow several key principles, and these principles offer context for MSPC's concerns with CUPIDA.³

¹ 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 (Aug. 19, 2020) (hereinafter "CUPIDA").

³ See Letter from MSPC to Chairman Perlman (June 25, 2020) supporting a model law that promotes transparency for consumers, preserves customer services and benefits, requires responsibility for one's own conduct, includes statutory obligations for all, and contains no exemptions. See also <https://mainstreetprivacy.com/principles/>

II. COMMENTS ON CUPIDA

- A. A “data processor” must have the same or equivalent requirements as a “data controller” in uniform privacy legislation for the privacy law to effectively protect consumers.

Virtually every industry sector – whether consumer-facing or business-to-business – handles significant volumes of consumer information. For that reason, every entity handling consumer data in an information chain of custody should have equivalent statutory obligations to protect that data and honor consumer requests with respect to it. As currently drafted, many protections proposed under CUPIDA only create obligations for a data controller with respect to the consumer’s information. Data processors are exempt from the key provisions that protect consumer data and allow a consumer to exercise his or her rights, including Sections 4, 5, 6 and 7.⁴

Data processors’ exemption makes the entire privacy regime envisioned by CUPIDA fail. The Committee should not advance a model law with loopholes that leave consumers unprotected when their personal data is held by a service provider that argues it is merely a data *processor*. Rather than exempting data processors from these requirements, data controllers should serve as the conduit for consumers to request their privacy rights and data processors should be held to honor those consumer requests too. Sections 4, 5, 6, and 7 should be revised to legally obligate data processors to the same requirements to which data controllers are subject in these sections, and if data processors fail to meet those obligations (e.g., honor a consumer rights request), they should be held liable for those violations. These modifications will ensure a consumer’s rights exercised under CUPIDA are honored by *all* parties handling his or her information, and that the data controllers who complied with CUPIDA are not penalized for failures of data processors to comply with it.

Additionally, Section 7(c) of CUPIDA requires a data controller to be liable for a data processor’s activity. The data controller should not be held responsible for the data processor—especially when the data processor has no equivalent requirements to comply with CUPIDA and the data controller does not have the means or capital to control the behavior of the data processor. For instance, many Main Street businesses do not have the market power to contractually force large technology and telecommunications companies that serve them as “data processors” to comply with certain privacy obligations that protect the Main Street businesses’ customers. Data controllers, however, are dependent on data processors’ taking immediate and complete action to fulfill consumer rights requests in order for the data controller to comply with the law, as currently drafted. CUPIDA therefore should be amended to require *all* parties to comply with its protections and hold each entity separately accountable for failing to protect data and honor consumers’ rights requests. CUPIDA should not rely on smaller Main Street businesses to police larger, multinational corporations serving as data processors. Unless required by U.S. privacy laws, as they are under the EU’s General Data Protection Regulation (GDPR), data processors will not agree to contractual provisions requested by Main Street businesses that would require the data processors to take all necessary actions to fulfill consumer rights requests within their control and not within the data controllers’ control.

This issue is further complicated by Section 14’s provisions, which require the use of contracts to enforce CUPIDA. MSPC opposes Section 14 because it allows data controllers to enter into an agreement governing the processing of data with data processors, but it still places the obligations of CUPIDA solely on data controllers. These provisions would create asymmetry in the marketplace and are anti-small business. Instead, data processors should have their own legal obligation to comply with CUPIDA. If not, data controllers would be required to use the judicial system to force data processors to comply when consumers exercise their rights. Because of the associated costs and the market power imbalance, however, data controllers will rarely be able to do this unless they match the market power and have the same level of legal resources as the service providers with whom they are suing. The

⁴ It is also worth noting that Sections 9, 10, 11, and 16 of CUPIDA are drafted to apply to a data controller or a data processor. MSPC believes Sections 9, 10, 11, and 16 should apply to both a data controller and a data processor. In fact, the titles of Sections 9, 10, and 11 indicate those sections were intended to apply to both entities.

CUPIDA regime therefore will fail to fulfill consumers' expectations with respect to comprehensive data privacy protections or provide them with remedies against the businesses that are actually responsible for failing to fulfill their rights requests.

For example, according to data published by the Federal Communications Commission, approximately half of all Main Street businesses have access to only one high speed Internet broadband provider that can handle the volume and speed required for business.⁵ Because there is no alternative provider, those Main Street businesses are forced to sign whatever "standard form" contract is offered to them by the telecommunications company – it is non-negotiable for a small business in need of broadband. The Main Street business has no power to dictate the provisions of the agreement, and therefore cannot require the service provider – in this case one that will claim to be a data processor – to abide by data privacy requirements and to honor the rights requests of the Main Street business's customers. Resorting to contractual requirements as a means for data controllers to police the privacy practices of data processors is therefore not a viable pathway for ensuring the data processor complies with CUPIDA's provisions.

Furthermore, Sections 12 and 13 only apply to data controllers and should be modified to apply to data processors as well. Section 12, especially provision 12(c), will not work if a data processor does not have the same requirements as the data controller. For example, a Main Street business may share customer data with a digital marketing firm to help send promotions to customers, but no longer has control over that data when it is in the custody of the data processor. The digital marketing firm must therefore be under an obligation to provide a way for the consumer to opt-out of targeted advertising.

Section 13 should also clarify that data processors cannot use the personal data from a data controller for a secondary purpose. If a data processor were to use the personal data that the data processor receives from a data controller, then that data processor should be considered a data controller for those purposes and be subject to all of the obligations and requirements of a data controller for that use.

Finally, the definitions of data controller and data processor in Section 2 are drafted in such a way that many entities considered to be data controllers will be able to claim they are exempt from CUPIDA's requirements because they are a data processor – even if they operate in both capacities. We have seen this with regard to other privacy laws. Companies such as Facebook have interpreted the "service provider" exemptions in California's new privacy law to escape the coverage of that law, even though the privacy violations of Facebook were among the primary concerns that led to the law's creation in the first place.⁶ These definitions should be edited to clarify that, in order to remain a data processor, the entity cannot determine the purposes or means of processing, including the use of personal data for a secondary purpose. If an entity does so, the definitions should clearly state it is a data controller for purposes of CUPIDA.

B. CUPIDA should not exempt financial institutions or entities subject to the Gramm Leach Bliley Act because that federal law does not provide equivalent privacy protections.

MSPC is further concerned with the exemptions in CUPIDA for financial institutions and other entities subject to the Gramm Leach Bliley Act (GLBA). GLBA does not provide for any of the consumer rights established in Section 4 of CUPIDA. Therefore, financial institutions and other entities defined as data controllers that are subject to GLBA would be able to avoid CUPIDA's requirements and consumers would not be fully covered by CUPIDA

⁵ See "FCC report finds almost no broadband competition at 100 Mbps speeds," by Jon Brodtkin, *Ars Technica* (Feb. 12, 2018) available at <https://arstechnica.com/information-technology/2018/02/fcc-report-finds-almost-no-broadband-competition-at-100mbps-speeds/>.

⁶ See Patience Haggin, "Facebook won't change web tracking in response to California privacy law," *Wall Street Journal* (Dec. 12, 2019) at <https://www.wsj.com/articles/facebook-wont-change-web-tracking-in-response-to-california-privacy-law-11576175345>.

privacy protections. Furthermore, other businesses that interact with such exempt entities may not be able to fully comply with their obligations under CUPIDA as well.

For example, many Main Street businesses exchange consumer information with financial institutions millions of times per day. Not only does this include payment card information but it may also include credit information (e.g., for store credit deals that are often administered by banks). If a consumer requests of a Main Street business offering point-of-sale credit that the business delete that personal data, it cannot fulfill that request without participation from the GLBA-covered entity that is exempt from CUPIDA. Additionally, if the financial institution refuses to help fulfill that request because they are not subject to CUPIDA's requirements, the Main Street business could face enforcement actions, including private litigation, for failing to comply with the consumer's request.

Parties seeking exemptions for financial entities often argue that Main Street businesses can secure such cooperation in the contracts they have with financial institutions. As described above, this ignores the reality that Main Street businesses often lack the bargaining power to negotiate such terms with financial institutions. Many of these businesses are small or medium-sized enterprises. For instance, approximately 95 percent of all retailers are single-store operators with less than 50 employees. These small businesses can neither negotiate privacy requirements for financial institutions nor afford to sue them to enforce the law. Moreover, many Main Street businesses will not sue financial institutions to enforce contracts because they cannot afford to upset the financial institutions that process their transactions or serve as their creditors.

Simply put, CUPIDA should not exempt any entity, such as those subject to GLBA, that do not have equivalent privacy requirements under federal law. Additionally, CUPIDA should require all data processors to honor consumer requests that are received by data controllers when the data processor is in custody of the personal information and must act in order for the consumer's rights to be exercised. MSPC urges the committee to make these critical modifications to CUPIDA before adopting it as a model law.

C. CUPIDA's definitions should be narrowly scoped to ensure consumer protections without obstructing the ability of businesses to better serve their customers and clients.

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. If CUPIDA is too prescriptive in its approach to data uses, businesses will be unable to use data in beneficial ways consumers expect and appreciate. Furthermore, businesses under an overly prescriptive data regulatory scheme may be unable to innovate and provide customers and clients with the benefits to which they are accustomed. The Committee should modify CUPIDA's definitions in certain respects to ensure they are narrowly scoped to provide consumer protections without unintentionally impeding businesses' ability to serve their customers and clients as they want and expect to be served.

To this end, the Committee should modify CUPIDA's definition of "personal data," which currently prohibits a "probabilistic inference about the individual." This definition is overly broad as it will pull into its scope business proprietary information that was not personal information provided by the customer. Many businesses, for instance, 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 publicly available data. Given the competitive nature of operating a Main Street business, the most successful businesses get to know their customers and meet their needs – this is often celebrated as excellent customer service and leads to greater patronage of the businesses by its customers. Inferring a customers' preference is a legitimate business practice that has been employed for centuries; it is not a breach of their privacy and should not be prohibited under CUPIDA by having it included in an overly broad definition of personal data. MSPC therefore strongly recommends deletion of the sentences in the definition of "personal data" and "profiling" that reference probabilistic inferences.

- D. CUPIDA should permit data controllers the flexibility to determine the most secure and appropriate means to receive consumer rights requests.

Section 7 of CUPIDA permits consumers to request the exercise of their rights by “any reasonable means,” which has the potential to create a system that is insecure and unworkable by design. Data controllers and data processors must have the flexibility to design and implement a secure system through which consumers can exercise their rights that will protect the consumers’ information and not unnecessarily inhibit the company’s business model. For example, a consumer might think it is “reasonable” to tell the convenience store clerk that she or he wants a copy of personal data the convenience store maintains. The convenience store clerk, however, likely has no access to the consumer’s data because of the business’s privacy policy. The process by which a consumer exercises its rights must therefore be secure and streamlined to protect the very data the consumer is trying to access, and businesses should be able to designate the means through which these requests may be made in order to ensure their secure and timely fulfillment.

Moreover, the “any reasonable means” provision in Section 7 conflicts with Section 8 of CUPIDA, which has specific requirements for creating a procedure to respond to a consumer’s request to exercise their rights and file that procedure with the Attorney General. To that end, MSPC suggests that Section 7(a) be modified to strike the “any reasonable means” language and simply refer to the procedures in Section 8, which in turn should be modified to provide the flexibility that both data controllers and data processors need to implement a system that works best for their business models.

- E. CUPIDA’s nondiscrimination provisions are highly problematic and would invalidate customer loyalty programs preferred by consumers.

As noted above and in previous letters to the Committee as one of our principles, MSPC believes that any privacy legislation should preserve the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships, including through the use of rewards and loyalty programs. As drafted, Section 17 would prohibit consumers who choose to participate in a customer loyalty program from receiving discounted prices or better service than consumers who choose not to participate through the exercise of a privacy right. This would effectively prohibit the provision of loyalty programs altogether.

For example, most grocery stores provide discounted pricing for consumers that participate in their customer loyalty program. Grocery store customers are not required to participate in the loyalty program—it is voluntary, and they must opt in to participate. But, if a customer does not want purchasing data collected, they cannot participate in the grocery store’s loyalty program because it requires such collection to determine the level of customer engagement. The exercise of that customer’s preferences should not inhibit the store from providing discounts or improved services to loyalty plan customers who voluntarily sign up for the program. CUPIDA, however, would prohibit a business from charging a lower price or providing better service to their loyal customers who voluntarily allow their data to be collected, thereby making it impossible to provide loyalty plan benefits to its customers.

MSPC believes that CUIPDA should be amended to strike this highly problematic pricing regulation provision that counters consumer expectations and does not provide any measure of privacy protection.

- F. CUPIDA should not include a private cause of action.

In line with the rest of the business community, MSPC is also concerned with the inclusion of the private cause of action provisions in Section 20 and 21. Allowing for private causes of action creates opportunities for meritless lawsuits often directed at the smallest businesses on Main Street. This has happened in many other areas of law – patent trolls, ADA trolls, etc. – and could be particularly pernicious with respect to privacy litigation given the

complexity of privacy compliance regimes, the evolving nature of technologies used to comply with privacy laws, and the subjective nature of assessing a business's privacy practices.

Furthermore, the costs of fighting class action lawsuits over privacy practices would be substantial and many Main Street businesses would not have the resources to do so, which plaintiffs' lawyers also know. Because it is significantly less expensive to settle than to fight an unsubstantiated accusation, many businesses will be forced to settle despite not being in violation of the law, and the law could therefore create a whole new cottage industry of "privacy trolls" that prey on businesses that lack the legal expertise and resources to do anything other than settle the claims.

As drafted, CUPIDA will create incentives for plaintiffs' lawyers to send hundreds of thousands of demand letters and potentially file lawsuits with questionable merit simply to extract quick, easy settlements from unsuspecting Main Street businesses as many other troll campaigns have done. For these reasons, MSPC urges the Committee to strike the private causes of action sections from CUPIDA.

G. CUPIDA's data privacy report filings create unnecessary administrative burdens.

The provisions in Section 8 of CUPIDA create an inordinate administrative burden for some entities and MSPC believes these should be removed. As described above, the approximately 95% of retailers are small, single-location operators with less than 50 employees. For these 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 road-side convenience stores, 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 data controllers despite the scoping provisions of Section 3.

It is overly burdensome to ask these businesses to file the type of privacy report required by Section 8 with the Attorney General, and arguably it will be a little value to the office itself. As the Section 8 drafting comment indicates, provisions like this are difficult to apply because of the variety of businesses and industries subject to the law's requirements. Filing a report risks becoming a compliance "gotcha" game that small businesses cannot win even if they implement appropriate privacy protections for their customers. Compliance with the substantive provision of the law should be sufficient without adding burdensome filing requirements that prioritize the ability to file paperwork over compliance with the law. We therefore urge the Committee to drop these reporting requirements from CUPIDA as an unnecessary administrative burden.

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 meet and deliberate over the draft text of CUPIDA. We stand ready to provide the Committee with additional information on any of the concerns outlined here.

Very truly yours,



Doug Kantor
Steptoe & Johnson LLP

On behalf of the Main Street Privacy Coalition
<https://mainstreetprivacy.com>