December 4, 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 efforts of the Uniform Law Commission's Collection and Use of Personally Identifiable Data Drafting Committee (Committee) to develop uniform model privacy legislation. MSPC remains concerned, however, with the latest draft of the Collection and Use of Personally Identifiable Data Act (CUPIDA)[2] as well as with the discussion of these issues that took place during the October 16, 2020 call.

The current draft of CUPIDA heavily regulates consumer-facing businesses, while exempting other sectors – such as financial institutions, service providers, and data brokers – that use consumers' personal information. Moreover, the Committee indicated during its recent call that data controllers should dictate the privacy practices of data processors via their contracts with these entities. Data controllers – the majority of which are millions of Main Street small and mid-sized businesses – do not have the market power or resources to police the privacy practices of data processors or to enforce the privacy provisions of contracts with them to ensure that data processors comply with CUPIDA's provisions. The approach that the CUPIDA draft currently takes, then, will not be effective in achieving the Committee's goals. Instead, it will leave gaping exceptions that will be exploited, particularly by technology and data broker companies, like Facebook and Equifax, whose practices were a primary driver of public concerns that led to nationwide privacy reforms in the first place.

For data privacy legislation to be both just and effective it must follow a basic principle: entities subject to the law should be responsible only for conduct they can control, and they should not be responsible for conduct they cannot control. If that concept is not followed, the law will not modify behavior to conform with the policy goals that lawmakers seek to achieve. Instead, the law will punish some entities who have no ability to avoid such punishment and may allow disfavored behavior to continue unabated. Unfortunately, as written, CUPIDA fails to follow this basic principle and, unless modified as suggested below, will result in both unjust and ineffective outcomes.

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, gas stations to travel plazas, and self-storage to convenience stores, MSPC member companies interact with consumers day in and day out. Our members' businesses can be found in every town, city and state in our nation, providing jobs, supporting our economy and serving Americans as a vital part of their communities.

[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 (Oct. 12, 2020)(hereinafter "CUPIDA").

Collectively, the industries that MSPC member associations represent directly employ nearly 34 million Americans and constitute over one-fifth of the U.S. economy by contributing $4.5 trillion (or 21.8%) to the U.S. gross domestic product. Our success depends on maintaining trusted relationships with our customers and clients: trust that the goods and services we provide are high quality and offered at competitive prices; and trust that the information customers provide to us is kept secure and used responsibly. 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]

II. COMMENTS ON CUPIDA

A. An individual cannot effectively exercise rights under CUPIDA if a data processor is not obligated to comply with statutory requirements; processors should have equivalent obligations as controllers to honor consumers' rights requests.

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, and data processors are not required to comply. Data processors' exemptions cause the entire privacy regime envisioned by CUPIDA to fail because it prevents a consumer from effectively exercising his or her rights as outlined in Section 4, including: (1) receiving a copy of his or her personal data; (2) correcting an inaccuracy in his or her personal data; (3) reviewing a company's data processing practices; (4) providing consent for a data practice that is not consistent with consumer typical expectations; and (5) protecting his or her personal data from prohibited data practices. A data controller cannot effectuate any of these rights fully without data processors having statutory obligations to comply with the provisions of the law.

For example, Section 5 of CUPIDA requires a data controller to provide a copy of an individual's personal data that the data controller currently maintains. In many cases, once a data controller shares a consumer's personal information with a data processor, the data controller no longer keeps a record of that data. A data controller therefore must depend on the data processor to responsibly and securely maintain the data for the controller, and respond to the individual's rights request with a copy of the personal data so that the data controller can comply with the law. The data processor, however, is not required to do so by the current language of CUPIDA. The absence of statutory language that would require data processors to fulfill individual rights requests where they alone are in the position to do so will allow processors to simply refuse to meet these obligations without any effective remedy for consumers.

Section 5 further requires the data controller to correct inaccuracies a consumer identifies in his or her personal data, but a data processor does not have similar obligations. In order to comply with CUPIDA, the data controller will be required to request that the data processor make the requested corrections to the consumer's personal data in the processor's possession. The data controller, however, cannot force the data processor to correct the data, and therefore has no way to comply with the law or fulfil the consumer's request.

As defined in Section 8 of CUPIDA, an incompatible data practice is a practice that is not consistent with typical expectations of privacy.[4] Section 8 requires a data controller to obtain consent from an individual before engaging in such an incompatible data practice. A data processor, however, is not similarly required to obtain consent from consumers – directly or indirectly – to engage in an incompatible data practice. A data controller might not request

[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/

[4] *Supra* 2 *at* Page 11.

consent from the consumer because it does not intend for the data to be used in an incompatible way, but the data processor, without consent, could nonetheless engage in incompatible activity. This contradiction in the law will undermine consumers' control over their data and their faith in the law to protect their interests.

Furthermore, section 8(d) of CUPIDA makes a data controller liable for a data processor's activity. The data controller should not be held responsible for the actions of data processors that conflict with the law. Likewise, Section 9 prohibits data controllers and data processors from processing personal data via a prohibited data practice. While we recognize that a data processor is also prohibited from engaging in prohibited practices, a data controller will be liable for the data processor's behavior as outlined in Section 9(c).

Rather than exempting data processors from these requirements and making data controllers liable for processors' actions, data controllers should serve as the conduit for consumers to request their privacy rights and data processors should be required to honor the consumer requests that controllers pass along to them. To do otherwise (as CUPIDA does now) means the law will provide no requirements for processors to help fulfill consumer rights requests, even when they are in a gating position with respect to that fulfillment, while simultaneously punishing controllers for failures to fulfill requests when they, quite literally, cannot control the outcome.[5]

CUPIDA 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's rights request), then they should be held liable for those violations. These proposed modifications to CUPIDA, if made by the Committee, 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 the law.

B. Data processors regularly violate consumers' privacy expectations and will continue these practices under CUPIDA.

There have been many instances of data processors violating consumers' privacy expectations. In fact, consumer privacy legislation has often been spurred by consumer privacy concerns with data broker, technology, and telecommunications industry practices. Any privacy law should make its primary mission ensuring that these privacy-threatening practices by data processors are violations of the law and subject to appropriate penalties.

The most notorious example of a data processor using personal data for its own purposes is that of Cambridge Analytica. Cambridge Analytica was a political consulting firm that acquired the personal data of millions of Facebook's users under the guise of academic research.[6] Cambridge Analytica, which would be classified as a data processor by CUPIDA, then sold the data to political campaigns allowing them to build profiles on potential voters based on their psychographic information that Cambridge Analytica had compiled without the individuals' knowledge these profiles would be sold to political campaigns. Under CUPIDA, Cambridge Analytica would be

[5] The irony here is that the terminology used in the bill obfuscates the reality: controllers are often the small businesses that have no market power to "control" a large, nationwide service provider like an ISP, data cloud provider, or credit reporting agency. These processors, often nationwide businesses and much larger than their clients, affirmatively control the terms of the contract which is often written as a standard form contract and presented to their smaller clients on a take-it-or-leave-it basis. But the processor community continues to support the *fiction* that controllers will control processors through contracts. In the majority of cases, that is not true. It would therefore be better if the legislation used terms like business and service provider so that the loaded language of controller and processor does not obfuscate which entity truly has the market power. Typically, that market power belongs to processors which largely dictate the terms of these business relationships through contracts of adhesion. Those processor businesses should bear responsibility for their own actions.

[6] *See* Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, "How Trump Consultants Exploited the Facebook Data of Millions," New York Times (March 17. 2018) *available at* https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

allowed to sell this sensitive data and would not be required to comply with CUPIDA because it is merely a data processor.

Similarly, data aggregators, which are data processors under CUPIDA, regularly share private information they receive from data controllers, like location data, with other parties without the consent of the data subject. For example, the major wireless carriers frequently share consumer data with data aggregators. In one instance, LocationSmart, the data aggregator, allowed anyone using their service to obtain the location of individuals using these wireless carriers' services without the individuals' consent or even the ability to opt-out of such location disclosures.[7] Additionally, LocationSmart sold consumer location information to 3Cinteractive, a mobile marketing company, which then sold that information to Securus Technology, a correctional facility communications company.[8] With that data, Securus Technology was able to track individuals' locations without their knowledge or consent.

According to the Federal Communications Commission, the wireless carriers "relied heavily on contract-based assurances" that Securus Technology would obtain consent from the wireless carriers' customers before accessing their location information—a practice that obviously did not work.[9] Moreover, Zumigo, a data broker that receives its location data from T-Mobile, shares its data with MicroBilt, a credit reporting company.[10] According to reports, MicroBilt shared that location data with a bounty hunter.[11] And, Copley Advertising contracted with a religious pregnancy counseling and adoption agency to use location data to send anti-abortion advertisements to women.[12]

As another example, Turn, Inc., a digital advertising company, was given access to certain personal data of Verizon Wireless' customers. Verizon Wireless, however, had created a system for tracking its own consumers when they search the internet using their wireless phones by creating a tracking cookie that hid an undeletable number in the browsing results of its customers.[13] Turn, Inc. figured out the tracking system and was able to reconstruct Verizon customers' private data without the permission of the consumer or Verizon. Of separate concern, Verizon Wireless'

---

[7] *See* Zack Whittaker, "A bug in cell phone tracking firm's website leaked millions of Americans' real-time locations," ZDNET (May 17, 2018 https://www.zdnet.com/article/cell-phone-tracking-firm-exposed-millions-of-americans-real-time-locations/

[8] *See* Jennifer Valentino-DeVries, "Service Meant to Monitor Inmates' Calls Could Track You, Too," New York Times (May 10, 2018) *available at* https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html.

[9] *See* Federal Communications Commission, "FCC Proposes Over $200 Million In Fines Against Four Largest Wireless Carriers For Apparently Failing To Adequately Protect Consumer Location Data," (Feb. 28., 2020) *available at* https://docs.fcc.gov/public/attachments/DOC-362754A1.pdf.

[10] *See* Joseph Cox, "I Gave a Bounty Hunter $300. Then He Located Our Phone," Vice (Jan. 8, 2019) *available at* https://www.vice.com/en/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.

[11] *Id.*

[12] *See* Nate Raymond, "Firm settles Massachusetts probe over anti-abortion ads sent to phones," Reuters (Apr. 4, 2017) *available at* https://www.reuters.com/article/us-massachusetts-abortion/firm-settles-massachusetts-probe-over-anti-abortion-ads-sent-to-phones-idUSKBN1761PX.

[13] *See* Julia Angwin, Mike Tigas, "Zombie Cookie: The Tracking Cookie That You Can't Kill," ProPublica (Jan. 14, 2015) *available at* https://www.propublica.org/article/zombie-cookie-the-tracking-cookie-that-you-cant-kill. *See also* Federal Trade Commission, "Federal Trade Commission vs. Turn, Inc." *available at* https://www.ftc.gov/system/files/documents/cases/turn_inc_final_complaint.pdf.

virtual private network (VPN) allows McAfee to collect data and target ads to consumers.[14] In fact, the majority of free VPN services are selling consumer data to third-party companies.[15]

The prevalence of this secondary market for consumer data demonstrates why data processors must have direct statutory obligations to comply with any privacy law for it to actually be effective in dissuading such lucrative and privacy-threatening practices. As currently drafted, however, all of these data aggregators and third-party companies would be exempt from key aspects of CUPIDA because they are defined as data processors, which are exempt from the obligations that apply only to controllers. By only requiring only data controllers to comply with CUPIDA, the Committee is allowing data processors' nefarious practices to continue despite its stated intention that CUPIDA is trying to protect consumers from such practices.

C. A data controller cannot force a data processor to comply with CUPIDA's requirements via their contracts.

During the Committee's October 16, 2020 conference call, Ms. Bambauer indicated data controllers can require data processors to comply with CUPIDA's requirements through more robust contracts. That does not reflect reality. CUPIDA cannot rely on smaller Main Street businesses to police larger, multinational corporations serving as data processors.

Many Main Street businesses are small or medium-sized enterprises—approximately 95 percent of all retailers are single-store operators with less than 50 employees. These small businesses cannot negotiate privacy requirements for large multinational corporations, monitor whether those corporations comply with such requirements, or afford to sue them to enforce the law.

In many cases, the data processors are so dominant (especially in particular geographic markets) that data controllers cannot even risk the possibility that those processors would no longer do business with them. For example, only one ISP may provide broadband services to every business on Main Street; in that case, not doing business with that ISP means a business cannot have an online presence and compete with the other businesses on Main Street. So standard-form contracts of adhesion presented by processors must be signed by these Main Street businesses in order to compete in the marketplace, despite the fact that they are not writing the terms and are not controlling the processors.

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 data processors comply with CUPIDA's provisions. Taking this approach will make CUPIDA ineffectual and a tool by which processors will shift privacy obligations and liability onto the small businesses they serve, who have no ability to negotiate contracts with equivalent bargaining power and protect their interests vis-a-vis processors.

D. CUPIDA should not exempt financial institutions or entities subject to the Gramm Leach Bliley Act because these institutions have no equivalent privacy obligations under federal law.

MSPC has very strong concerns regarding the exemptions for financial institutions subject to the Gramm-Leach-Bliley Act (GLBA) that are outlined in Section 3 of CUPIDA. GLBA does not provide for any of the consumer rights established in Section 4 of CUPIDA. Specifically, **GLBA does not require financial institutions**, who

[14] *See* Karl Bode, "Verizon Didn't Bother to Write a Privacy Policy for its 'Privacy Protecting' VPN," Vice (Aug. 6, 2018) *available at* https://www.vice.com/en/article/a3q4gz/verizon-didnt-bother-to-write-a-privacy-policy-for-safe-wi-fi-privacy-protecting-vpn.

[15] *See* Nathan Resnick, "Be cautious, free VPNs are selling your data to 3rd parties," The Next Web (May 28, 2018) *available at* https://thenextweb.com/contributors/2018/05/28/be-cautious-free-vpns-are-selling-your-data-to-3rd-parties/.

would be defined as controllers under CUPIDA to: (1) provide a copy of an individual's personal data; (2) correct an inaccuracy in an individual's personal data upon reasonable request; (3) provide notice and transparency about their data processing practices; (4) obtain consent for any processing that would constitute an incompatible data practice; (5) abstain from processing personal data using prohibited data practices; or (6) conduct routine data privacy assessments.

Rather, GLBA merely includes a marketing opt-out, in which financial institutions must mail an annual notice informing consumers they have the right to opt out of the sharing of sensitive financial information with unaffiliated third parties. That's the sum total of financial institutions' statutory privacy requirements under GLBA.

Financial institutions that are subject to GLBA would be able to avoid CUPIDA's requirements and consumers would not be fully covered by CUPIDA's privacy protections, even among data controllers. For example, many businesses exchange consumer information with financial institutions (some are data processors and some are not) millions of times per day. Often, only the financial institution, not the data controller, has information that is subject to a consumer rights request under Section 4 of CUPIDA. As outlined with regard to data processors above, then, a data controller will not be able to fulfill some consumers' requests to exercise their Section 4 rights without participation from the GLBA-covered entity.

It is also worth noting that credit card companies and other financial institutions regularly collect and sell their customers' data to advertisers and marketers or other data aggregators.[16] Banks share consumer data with credit card companies like Mastercard and Visa (who act as data processors) millions of times each day in order to complete transactions. Those banks deal directly with consumers and would be considered data controllers except that CUPIDA exempts them from controller requirements merely because they are subject to GLBA.

A recipient of data from CUPIDA-exempt banks, Mastercard, advertises its ability to share the consumer data it collects as a service for other businesses.[17] In this scenario, neither the financial institution nor the data processor has any obligation under CUPIDA to protect a consumer's privacy with regard to the information it tracks and subsequently sells or uses. A consumer, therefore, does not have any recourse to exercise his or her privacy rights as outlined in Section 4 of CUPIDA. Exempting financial institutions from CUPIDA leaves consumers exposed and their privacy unprotected. It is further evidence of a broken model that claims to protect consumers but leaves them exposed and subject to privacy abuses by exempted processors and exempted financial institution controllers.

CUPIDA should not include carveouts for any industry, such as those subject to GLBA, unless the industry has equivalent privacy requirements under federal law. MSPC urges the committee to require financial institutions subject to GLBA to comply with CUPIDA, just like it requires other controllers with much less sensitive customer financial information to comply with the Act despite their much less risky data uses.

III. CONCLUSION

MSPC appreciates the Committee's diligent work on model privacy legislation and its consideration of the concerns raised above as it continues drafting the next version of CUPIDA. We hope the Committee will consider these

[16] *See* Peter Cohan, "Mastercard, AmEx And Envestnet Profit From $400M Business Of Selling Transaction Data," Forbes (Jul. 22, 2018) *available at* https://www.forbes.com/sites/petercohan/2018/07/22/mastercard-amex-and-envestnet-profit-from-400m-business-of-selling-transaction-data/. *See also* Kate Kaye, "Mastercard, Amex Quietly Feed Data To Advertisers," AdAg (Apr. 16, 2013) *available at* https://adage.com/article/dataworks/mastercard-amex-feed-data-marketers/240800.

[17] *See* Mastercard, Data and Services, *available at* https://www.mastercardservices.com/en/solutions.

issues and require all entities to comply with its privacy requirements so that CUPIDA can effectively protect consumer privacy across industry, which is what consumers also expect our privacy laws to do.

Sincerely,

Main Street Privacy Coalition
https://mainstreetprivacy.com