October 16, 2020

Mr. Harvey Perlman
Chair, ULC Collection and Use of Personally Identifiable Data Committee
Nebraska College of Law
McCollum Hall (LAW) 263
Lincoln, NE 68583-0902

Dear Mr. Perlman,

Common Sense Media, Consumer Federation of America, Electronic Frontier Foundation, and Privacy Rights Clearinghouse are non-profit groups dedicated to defending individual privacy; we have worked hard to advance meaningful privacy legislation at the state and federal levels. Lawmakers' desire to improve privacy protections is evident by the hundreds of privacy bills and proposals being introduced across the country, and we appreciate the hard work the drafting committee has put into formulating model legislation for the Collection and Use of Personally Identifiable Data Act (CUPIDA).

That stated, our groups have serious concerns with the October discussion draft. While our groups appreciate new legislative approaches to privacy protection, this draft is an attempt to take an unfinished committee draft and incorporate aspects of an entirely different alternative draft. Far from producing a "best of both worlds," the October discussion draft introduces new definitional problems and a confusing set of consumer protections. The ULC is within its rights to develop a new approach to long standing privacy challenges, but we are concerned that the October draft does this in a fashion that will not benefit individuals or ensure adequate privacy protections.

First, we are concerned about a number of new definitions introduced in the proposal. The most important definition in any privacy law is the scope of information that is covered by that law. Three terms — "deidentified data," "pseudonymized data," and "publicly available information" — are overbroad, unique to the ULC proposal, and ultimately undermine individual's privacy. This is compounded by a narrow definition of "personal data" that focuses exclusively on direct identifiers.

The October definition introduces a completely unique definition of "deidentified data" that only creates more confusion about what businesses must do to deidentify data. We do not understand what this definition accomplishes. It is unclear what the language "personal knowledge of the relevant circumstances" intends to do in the context of this definition. We assume this definition means that stripping away direct identifiers (and subjecting this information to some sort of technical control) permits any information to be taken outside the scope of CUPIDA. However, this ignores the relevance and use of indirect identifiers to track

individuals. CUPIDA's definition must be replaced; we recommend using the widely-accepted FTC definition.[1]

We also take issue with the definitions of "pseudonymized data" and "publicly available information" for several reasons. For example, the exclusion of information "observable from a publicly accessible vantagepoint" effectively excludes facial recognition from the scope of this proposal. It also excludes broadcasts of technical information that can be used to monitor, track, and surveil families, which is particularly important in an Internet of Things environment. At minimum, the October definitions are overbroad and not in line with existing frameworks like the California Consumer Privacy Act (CCPA) and EU General Data Protection Regulation (GDPR).

Second, the October discussion draft has incorporated the alternative draft's focus on "compatible data practices." While this shift may be a laudable way to move away from often criticized notice-and-choice approaches, it undermines any privacy-protecting goals in the October discussion draft. "Compatible data practice" largely seems to support the digital status quo and is defined in a manner that favors business interests over individual privacy. Helen Nissenbaum, who formulated the initial idea of respecting context in data flows, has been critical of business-friendly formulations of consumer's reasonable expectations.[2] The October draft makes this mistake, giving entirely too much leeway to companies to determine what constitutes a compatible use. Permitting processing "likely to substantially benefit such individuals" must be stricken. It has no limiting principle. Companies already argue that privacy-invasive practices "benefit" consumers, and without defining what constitutes a benefit, this begs the question of what data practices are not compatible.

The October discussion draft further compounds this problem by including both "development of new products and services" and targeted advertising within the scope of compatible data practices. Product development has no limitation, and concerns over businesses' secondary use of personal information is one of the motivating drivers behind privacy legislation. Businesses should not collect information for one purpose and use it for another, even if it is ostensibly for internal product development. To illustrate how inappropriate such an exception can be, the ULC Committee need only look at the example of the Ever app, which marketed a photo storage app that was ultimately used to develop facial recognition products.[3] The October discussion draft's treatment of targeted advertising is even less appropriate. Commentary to the October discussion draft adopts ad industry talking points when it states that CUPIDA should be designed to allow "common web practices" to permit "other

---

[1] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 21 (2012).
[2] Helen Nissenbaum, Respecting Context to Protect Privacy: Why Meaning Matters, Science and Engineering Ethics 24(4) (2015), doi: 10.1007/s11948-015-9674-9.
[3] Olivia Solon & Cyrus Farivar, *Millions of people uploaded photos to the Ever app. Then the company used them to develop facial recognition tools.*, NBC News (May 9, 2019), https://www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371.

content-producers to command higher prices from advertisers."[4] This suggests that CUPIDA ultimately enshrines the current status quo -- contrary to GDPR, CCPA, and other state proposals like the Washington Privacy Act.

Further, the October discussion draft even permits *incompatible uses* so long as "the consumer had a reasonable opportunity to withhold consent to that incompatible use." As we are seeing with the CCPA, companies are going to great lengths to frustrate individuals' ability to even opt-out of data sales.[5]

There are other problems with the October discussion draft, as well, including:

- Section 2's definition of "sensitive information" is narrow and warrants additional discussion. For instance, the inclusion of "real time geolocation information" ignores the privacy interests in historical geolocation data.
- Section 3 includes broad exclusions from CUPIDA's coverage based on different federal laws, including the Children's Online Privacy Protection Act (COPPA), Gramm-Leach-Bliley Act (GLBA), and Health Insurance Portability and Accountability Act (HIPAA). These laws provide weaker privacy rights and protections in some respects, so exempting personal information when it is subject to them would leave individuals in a confusing and disadvantageous position of having different rights and protections for the same types of data, depending on the entities using that data. Since these federal laws do not preempt state laws, CUPIDA should apply to the extent that it provides stronger rights and protections.
- Section 4's recitation of individual rights removes any right to delete personal information, replacing deletion rights with a "redress" right for incompatible or prohibited practices. This is not consistent with either the GDPR or CCPA, which include deletion rights.
- Section 5 makes clear that the protection from being treated differently or waiving one's rights only applies to access and correction rights, not to CUPIDA as a whole. Section 5 also does very little to ensure "reasonable procedures" are not burdensome on consumers. As we are seeing with the CCPA, companies are making it difficult for individuals to exercise their right to access personal information collected about them. (This is similarly the case under HIPAA, which is seeing ongoing federal enforcement over access problems.) The October draft should specify how an individual can exercise their rights, and we would recommend pulling from the California AG's CCPA implementing regulations, which provide mechanisms for how to exercise rights and detail how companies must communicate about them.

---

[4] For a discussion of the problematic adoption of advertising industry talking points, see Consumer, Privacy, and Civil Liberties Organizations Disappointed in FTC Staff Stance on Targeted Advertising (Nov. 26, 2018), https://consumerfed.org/testimonial/consumer-privacy-and-civil-liberties-organizations-rebuke-ftcs-stance-on-targeted-advertising/.

[5] Maureen Mahoney, California Consumer Privacy Act: Are Consumers' Digital Rights Protected?, Consumer Reports Digital Lab (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf.

- Section 6 includes commentary that controllers may disclose information to law enforcement without disclosing this. This is a controversial statement. At minimum, this highlights that deferring to companies to determine what are “compatible” and “incompatible” data practices is problematic.
- Section 9 both enumerates various harms triggers, rather than saying violations of CUPIDA are per se harms, and creates a high bar to any enforcement, including requiring companies to “recklessly and knowingly” fail to secure data or “willfully” disclose data in violation of the proposal.
- We continue to be skeptical of CUPIDA’s implementation of voluntary consensus standards and other privacy frameworks. At minimum, however, Section 13, subsection (g) allows state AGs to recognize compliance with a "substantially similar privacy framework" like GDPR and CCPA as a way to comply with CUPIDA. It should be made clear that controllers must extend those framework's rights to state residents. Plenty of companies are already "complying" with the GDPR or CCPA, but that does not ensure protections and rights for residents in other jurisdictions.

Strong privacy legislation requires data minimization and privacy-by-default. The October discussion draft moves further away from this premise towards enshrining an unacceptable status quo. We strongly encourage the committee to reconsider its commitment to adopting language from the alternative draft absent considerably more discussion and debate.

Sincerely,

Common Sense Media
Consumer Federation of America
Electronic Frontier Foundation
Privacy Rights Clearinghouse