common sense kids action™

April 23, 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

Mr. William McGeveran
Reporter, ULC Collection and Use of Personally Identifiable Data Committee
Mondale Hall
229 19th Ave., South
Minneapolis, MN 55455

Dear Mr. Perlman and Mr. McGeveran:

Now more than ever privacy protections are essential to kids' safety and well-being, in the home, at school, and in our communities. Common Sense Media, and its policy arm Common Sense Kids Action (together, Common Sense), has been active in advancing kids' and families' privacy rights at the state and federal level over the last two decades from student privacy protections to updates to the federal Children's Online Privacy Protection Act (COPPA), to co-sponsoring the California Consumer Privacy Act (CCPA).

States are currently considering a variety of different privacy and security rules, and 700 different privacy bills were introduced in states across the country this year. As the Uniform Law Commission (ULC) considers formulating model legislation for the Collection and Use of Personally Identifiable Data Act (CUPIDA), **Common Sense cautions the Committee against advancing model legislation that trades away meaningful privacy protections for the sole sake of finding consensus among industry voices.** We recommend that any final product:

1. Include strong and clear definitions of what personal data is covered and how it can be de-identified;
2. Explain how companies collect, use, and share data in terms parents and kids can understand and provide easy mechanisms to access, delete, and move data;
3. Restrict secondary uses of information and mandate data minimization requirements;
4. Limit data disclosures to unknown third parties and business affiliates;
5. Include additional protections to safeguard the personal data of vulnerable children and teens, such as prohibitions on behavioral advertising and third-party disclosure;
6. Ensure any affirmative obligation on families or individuals to opt-out to protect their privacy be easy to effectuate and easily understandable and accessible;
7. Avoid overbroad and unnecessary exceptions for businesses who may be covered, usually only in part, by federal laws like COPPA, GLBA, and HIPAA;

8. Carefully consider what privacy and security requirements, if any, small businesses should be exempt from following;
9. Include reasonable data security provisions; and
10. Provide strong individual redress and enforcement mechanisms when companies violate an individual's privacy.

We appreciate the hard work that has gone into the existing draft proposal, and that both specific provisions and wording are in flux, but we encourage the Committee to seek input and feedback from consumer groups, privacy advocates, and non-corporate stakeholders.

We also write now to offer the following recommendations as the Committee continues its work on CUPIDA.

## I. Definitions of "Personal Data"

Stakeholders have criticized that some definitions in the April draft are confusing or unworkable.[1] While the April draft includes some novel terms, it is likely this criticism stems from the draft's definitions of "personal data" and "deidentified." These terms are key because the protection provided by any privacy framework fundamentally depends upon the definitions of (1) what personal data is covered and (2) what entities have to do to deidentify that information to get out of the law's scope.

There has been some discussion among stakeholders of narrowing the scope of personal data in CUPIDA, but **a broad definition is needed to meaningfully protect privacy and cabin misuse of information.** Historically, companies have taken a narrow view as to what information constitutes personal information -- obvious identifiers like name or Social Security numbers were all that needed to be protected. But when in-store shopping purchases can be used to infer pregnancy status and location to infer religion, and family loyalty club memberships and online browsing history are assessed by colleges before students even apply, more must be protected.[2] CUPIDA's inclusion of "probabilistic inferences" and device identifiers is an important inclusion to capture data that can, on the surface, appear to be seemingly innocuous.

On the flip side, **definitions of "deidentified" data should not be so broad as to undermine a CUPIDA's scope of coverage.** Deidentification has become tremendously contentious. Not only do deidentification techniques fail, but "anonymous" information can also present real risks to

---

[1] *See* Comments of the State Privacy & Security Coalition (Apr. 16, 2020), *available at* https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=e68d42e9-bacc-be67-8ef5-0f5bb6fc8757&forceDialog=0.

[2] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. Times (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html; Audie Cornish, *How Political Campaigns Are Using 'Geofencing' Technology To Target Catholics At Mass*, NPR (Feb. 6, 2020), https://www.npr.org/2020/02/06/803508851/how-political-campaigns-are-using-geofencing-technology-to-target-catholics-at-m; Douglas MacMillan & Nick Anderson, *Student tracking, secret scores: How college admissions offices rank prospects before they apply*, Washington Post (Oct. 14, 2019), https://www.washingtonpost.com/business/2019/10/14/colleges-quietly-rank-prospective-students-based-their-personal-data/.

individuals and communities.[3] While companies reasonably want an escape valve from having to give the same level of protection to all information at all times, businesses can be quick to claim information is sufficiently deidentified or even anonymous when it is not.[4]

**Scoping what information is properly de-identified warrants careful consideration.** At minimum, we recommend CUPIDA adopt a standard more closely based on the Federal Trade Commission's ("FTC") three-pronged test that requires companies to: (1) take "reasonable measures" to deidentify information; (2) make a "public commitment" to process data in a deidentified fashion and not attempt to reidentify data; and (3) contractually prohibit downstream recipients from reidentifying the data.[5]

## II. Defining Sensitive and Non-Sensitive Data

The current draft of CUPIDA distinguishes between sensitive and non-sensitive categories of personal data. If the Committee is going to include a definition of sensitive or special data, which itself comes with some risks, this definition should both capture the full range of sensitive information protected by existing privacy frameworks and include, per the general definition of personal data, any probabilistic inferences about sensitive data.

**At minimum, however, the Committee should look to categories of sensitive information being advanced by bipartisan efforts in Congress and protect this information accordingly.**[6] Unfortunately, some stakeholders appear to be advising the Committee to not even go this far. One stakeholder has already suggested that "notice, deletion, and opt-out right[s] are sufficient for sensitive personal data" and that opt-in and opt-out consent requirements are functionally equivalent, this is contrary to widespread acknowledgement that sensitive data warrants special protections.[7] Further, the Federal Trade Commission's 2012 Privacy Report explicitly states that entities "should obtain consumers' affirmative express consent before collecting sensitive data."[8]

---

[3] Natasha Lomas, *Researchers spotlight the lie of "anonymous" data*, TechCrunch (July 24, 2019), https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/ (The researchers cite data broker Experian selling Alteryx access to a de-identified data set containing 248 attributes per household for 120 million Americans, for example.).

[4] Joseph Jerome, *De-Identification Should Be Relevant to a Privacy Law, But Not an Automatic Get-Out-of-Jail-Free Card* (Apr. 1, 2019), https://cdt.org/insights/de-identification-should-be-relevant-to-a-privacy-law-but-not-an-automatic-get-out-of-jail-free-card/.

[5] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 21 (2012).

[6] *See* Consumer Online Privacy Rights Act (COPRA) of 2019 & the United States Consumer Data Privacy Act of 2019.

[7] *Compare* Comments of RELX-LexisNexis (Apr. 20, 2020), *available at* https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=7d50362c-c61f-2c45-2be5-b90c003be62c&forceDialog=0, *and* Comments of National Association of Mutual Insurance Companies (Apr. 16, 2020), *with, e.g.,* Special Category Data, Article 9 of the EU General Data Protection Regulation.

[8] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 58 (2012).

Though consent requirements are not a panacea, model legislation should not take the position that sensitive information is deserving of fewer protections than is best practice.

**Additionally, we would recommend further thought and consideration be put into the categories of personal information identified as sensitive in CUPIDA.** We would recommend that, first, the data of children under the age of 16 also be deemed sensitive and be subject to consent requirements. This is consistent with the CCPA, which provides an opt-in to the sale of information for consumers less than 16 years of age.[9] It is also consistent with recognition by the FTC and others that young people warrant special consideration.[10] Second, we would also support the inclusion of precise geolocation information, which is acknowledged as sensitive by marketers and was wisely included in a similar list of sensitive data in the recent draft Washington Privacy Act.

## III. Scope

Industry voices continue to push for carve outs for their privacy-invasive protections, often justifying these exceptions on the grounds that they are already regulated by federal privacy laws. These exemptions are often unwarranted.

**The Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Financial Modernization Act ("GLBA"), and the Children's Online Privacy Protection Act (COPPA) each allow states to provide stronger protections for health, financial and children's information that go beyond federal protections.** Further, the federal laws often only apply in limited circumstances or have exceptions that have become loopholes that swallow the rule. HIPAA, for example, only applies to information collected by "covered entities," which does not cover the complete universe of health information that can be collected by apps and services online. COPPA applies to a limited set of operators of sites and services, and does not apply to "general audience" sites and services, telecommunications carriers. or solely brick and mortar companies.

**Model legislation must not include carve outs without careful consideration and debate, and exceptions should be tailored to specific concerns, not provide a blanket exemption from legal privacy protections.**

## IV. Enforcement and Safe Harbors

[9] Cal. Civ. Code § 1798.120(c).

[10] FEDERAL TRADE COMMISSION, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 55 (May 2014) (noting that principles underlying the Children's Online Privacy Protection Act may apply equally in offline contexts, and that teens often fail to appreciate long-term consequences of posting data online); *see also* Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values, 25-26 (May 2014) (noting young people "need appropriate freedoms to explore and experiment safely and without the specter of being haunted by mistakes in the future").

A privacy law is only as strong as how it is enforced. We appreciate the effort the Committee has taken to include a tailored private right of action in CUPIDA. **Private rights of action can be an effective tool for individuals to obtain redress and combat bad practices for the benefit of all.**[11]

**Existing criticism about private rights of action ignores that the Committee can scope a private right of action to avoid any alleged excessive litigation.** For instance, a private right of action could minimize statutory damages and emphasize injunctive relief. Injunctive relief forces companies to stop practices that violate the law. This is a good potential middle ground, and has precedent in federal law. For example, Title III of the Americans with Disabilities Act prohibits discrimination on the basis of disability in places of public accommodation, but private plaintiffs are only allowed to seek equitable relief like removals of barriers or obstacles rather than any financial awards.[12] Another option modeled after the Fair Credit Reporting Act[13] is to specify exactly which provisions in a privacy law could be subject to private litigation. The CCPA, for example, permits a private right of action for certain data breaches.

We also would caution against the inclusion of any sort of broad Safe Harbor provision. We echo the recent assessment of the UK Information Commissioner's Office that "the time for self-regulation is over."[14] The COPPA Safe Harbor frameworks lead to enforcement entities that can suffer from a lack of transparency and could be beholden to the companies they monitor, creating a conflict of interest.

--

Again, we appreciate the work the Committee has put into the current draft of CUPIDA, and we would encourage the Committee to improve the existing draft and ensure that any model legislation provide strong privacy protections and place meaningful restrictions on how entities have collected, used, and misused our personal information.

Please do not hesitate to reach out with any questions via email to jjerome@commonsense.org.

Sincerely,
Joseph Jerome
Multistate Policy Director

---

[11] *E.g.*, Joseph Jerome, *Private right of action shouldn't be a yes-no proposition in federal US privacy legislation*, IAPP Privacy Perspectives (Oct. 3, 2019), https://iapp.org/news/a/private-right-of-action-shouldnt-be-a-yes-no-proposition-in-federal-privacy-legislation/.

[12] Arlene Haas, *Essential Guide to ADA Title III Enforcement: Private Party Lawsuits* (Jan. 10, 2017), https://www.burnhamnationwide.com/final-review-blog/essential-guide-to-ada-title-iii-enforcement-private-party-lawsuits.

[13] *See, e.g.*, Alexandra Everhart Sickler, *The (Un)Fair Credit Reporting Act,* 28 Loy. Consumer L. Rev. 238 (2015-2016).

[14] Jessica Haworth, *The time for self-regulation is over, UK information commissioner tells tech firms*, Daily Swig (Nov. 6, 2018), https://portswigger.net/daily-swig/the-time-for-self-regulation-is-over-uk-information-commissioner-tells-tech-firms.