STATE PRIVACY & SECURITY COALITION

ULC CUPIDA 4/14 High-Level Issues

A. Serious High-Level Issues

1. The COVID-19 crisis has delivered a severe shock to the economy and it does make sense to adopt different privacy requirements at this point. All states have pushed back state legislative timelines for considering privacy legislation. It makes sense for the ULC either to push back its timeline for finalizing this model legislation, or to proceed very cautiously in light of the fact that there are only 2 states that have passed omnibus privacy legislation thus far.

2. Private Right of Action –

   The Committee should take up removing the private right of action at the 4/24 meeting.

   No state has enacted omnibus privacy legislation with a private right of action and this issue has already doomed passage of bills in Washington, New Jersey and Illinois.

   This issue has a critical effect on what requirements are in the law because obligations are intensely operational and well-meaning companies cannot be assured of being in full compliance all the time.

   This right of action would create statutory damages without any proof of harm, and is particularly susceptible to abuse.

   Invites abusive gotcha lawsuits for technical non-compliance with difficult requirements.

   The inclusion of a private right of action would make it very difficult to engage the business community in a meaningful way.

3. This is very far from a Uniform State Law in a highly operational area that requires uniformity –

   Each State AG would do its own rulemaking.

   Absence of preemption of local laws is a major problem.

   AG authority in § 8(c) giving the AG vague power to deem commitments "unfair or deceptive" if "they do not provide reasonable protection for a data subject's privacy" is utterly boundless and extremely vague, and would lead to conflicting interpretations in different states. It must be deleted.

A uniform state law should require or strongly encourage AG coordination in pursuing cases.

4. Unworkable definitions (device, household data, de-identified data) or are confusing (data custodian, sensitive data)

5. Absence of B2B Exemption

6. Overbroad Risk Assessment –

   Should be required only for sensitive data [or uses of personal data that are sensitive]

   Should be conducted once for each use case, not every two years for all processing

   Criteria should be general ones, not specifically including profiling, and non-measurable risks like general anxiety that are very difficult to anticipate or operationalize

7. Excessive Regulation of Processor Activities –

   Requiring specific notice of processor sharing (when CCPA does not)

   Barring any use of data by processor when CCPA contains exceptions

   Requiring consent for use of sub-processors

   Class action exposure if don't have a contract in place

8. Wasteful Regulatory requirements –

   Requiring filing of regulatory commitments with each State AG when need to post the same info on the entity's website

   These commitments cover operational methods of compliance, not outcomes, which would result in huge regulatory filing requirements every time a regulated entity changed their compliance procedures. These sorts of commitments are both confusing and far too rigid

   Requiring a toll-free number, even when entity does not communicate with residents by phone

   Requiring appointment of a DPO (an issue for smaller entities, for which 50,000 pieces of PI collected is a very low threshold to be subject to the law)

9. Needs a safe harbor

10. Children's privacy requirements need to be consistent with COPPA (it preempts inconsistent state laws)