Memorandum of Issues

Uniform Personal Data Protection Act
formerly,
Collection and Use of Personally Identifiable Data Act (CUPID)

To: Uniform Law Commissioners

From: Harvey Perlman, Chair
Jane Bambauer, Reporter

Date: July 1, 2021

The Prefatory Note to the draft for final reading places this Act in context and outlines the significant issues and approaches taken in the draft. We will not repeat those points here. This memorandum explains how the proposal has evolved from the draft on first reading in September 2020. That evolution has been significant.

The drafting committee was charged with producing a comprehensive personal data privacy law. In 2018 the European Union had adopted the General Data Privacy Regulation which imposed significant restraints on companies collecting and processing personal data. California subsequently adopted an act, largely modeled after the European version, with a delayed implementation date. Several proposals surfaced in Congress, but little progress was made. Several state proposals were similarly unsuccessful. Almost all commercial companies collect some form of personal data from their customers and with a modern global economy, uniformity with regard to the collection and use of that data seems appropriate. The challenge, of course, is to balance the benefits of data practices with the consumer's interest in how their personal data is employed.

Developing a comprehensive personal data privacy law faces several complexities. The collection of personal data is essential to completing many types of transactions. For example, every credit card transaction must collect a credit card number that identifies the account owner. The type of transaction often determines the data to be collected and its subsequent use. Purchasing insurance requires considerably more personal data than the purchase of groceries. For a variety of reasons, personal data may be required to be maintained by commercial entities after completion of a transaction, from internal and external oversight, to responding to consumer complaints, requests for returns, or fraud prevention. In addition, there are both large and small companies, from those like Facebook and Google to small independent stores with loyalty programs, that provide content, discounts, and other benefits to its users in return for the collection and retention of personal data.

Regulating the collection and use of personal data across such a diverse set of data practices can require considerable regulatory detail, either imposed in the legislation or delegated to an enforcement agency. The result is high costs of compliance by firms and high

costs of enforcement by the agency. The European and California models follow this path, but in return apply their privacy regimes only to larger data users that realistically can afford the compliance costs. Personal data collected by smaller firms goes largely unregulated.

When the act, then the Collection and Use of Personally Identifiable Data Act (CUPID), was presented to the Conference for its first reading, the drafting committee faced an inflection point. Over the course of the first drafting year, the committee worked with a draft that largely reflected the European and California approach. This approach was premised on the need of firms to obtain consent from consumers for collection and use of personal data. In some contexts, explicit consent was required, in others consent was achieved by providing an opportunity to withhold consent. Obtaining consent often required prior personal notice of the nature of the collection and use. The draft also included a right to data deletion under certain conditions.

Shortly before the first reading presentation, a small group of drafting committee members and observers proposed an alternative draft – one that made elaborate provision for consent unnecessary anytime the use of data was within the normal expectations of consumers and proposed an optional process for consumers and business entities to develop voluntary consensus standards regarding appropriate use of personal data in particular industries. At the first reading, the commissioners were made aware of the alternative draft, but the focus remained on the committee draft. The alternative draft was available on the ULC website.

Over the course of the next year, the drafting committee decided to focus on the alternative draft and, with the help of many engaged observers, refined it by reincorporating some of the access and correction rights from the original draft. It is this approach that we present for final reading. It establishes the right of a data subject to seek access to personal data and to have it corrected when necessary. It provides for transparency for the use of personal data. It provides incentives for firms to pseudonymize or deidentify personal data—thus enhancing consumer privacy and security. It authorizes compatible uses of data, uses that ordinary consumers have come to expect, without requiring individual consent. And it provides that uses that go beyond consumer expectations must be based on consent unless they are in the clear and direct interest of the data subject. The act outlines certain uses of data that are prohibited in all circumstances. It encourages firms to conduct confidential assessments related to the privacy and security protections it provides to data it collects. It authorizes stakeholders within industries, both consumers and firms, to collaborate and develop voluntary consensus standards that can govern data practices. And it authorizes the State Attorney General or private individuals to enforce the act within the framework of existing state consumer protection statutes.

The Act also applies to all firms that collect or use personal data regardless of size. Smaller firms can avoid most of the regulatory requirements if they only collect and use personal data for compatible uses.

The drafting committee also acknowledges that several industry specific privacy regimes are already in place, particularly at the federal level. The committee chose to exempt data processing subject to these federal regimes from this act.

Finally, Commissioners should be aware that the First Amendment plays some role in determining how far personal data may be protected. The United States Supreme Court has held that personal data collected by private firms is "speech" and thus can be regulated only for important governmental interests. Clearly, information that is already public can be regulated in only very limited circumstances. The Act exempts public information from its regulations. The Act also avoids clash with the First Amendment in other ways. For example, unlike other models, the Act does not provide the consumer with the option to require their data to be deleted. There are a variety of reasons why data retention is appropriate, even if the data subject objects, and it is not clear that First Amendment considerations would permit a compulsory obligation to delete data in most instances.

We believe the Act, as proposed, represents a balanced, workable, and efficient structure for protecting personal data from uses that place consumer interests at significant risk. At the same time, it reduces the high compliance costs on the private sector and the significant enforcement costs on state governments that would make the Act difficult to enact.