August 17, 2020

To: Uniform Law Commission

From: Harvey Perlman, Chair Drafting Committee

Re: Collection and Use of Personally Identifiable Data Act

Introduction

The Collection and Use of Personally Identifiable Data Act (CUPID) regulates commercial enterprises that collect and use personal data from their consumers. The increasing capacity of information technology along with the growing sophistication of data analytics permits personal data to be used for a wide variety of purposes. Most fundamentally, personal data is critical to many business transactions. Financial transactions, for example, require the collection of background credit information. Loyalty programs require the collection and retention of purchasing histories. Online purchases of goods and services require personal data to authenticate the purchaser and permit delivery. Social media outlets enable us to share our news and photos with friends and associates. And, increasingly, the connection of devices to the internet, from our cell phones and virtual assistants to our automobiles and kitchen appliances, provides the opportunity for the collection of significant amounts of information about all our everyday activities.

Beyond the mere collection of our personal information, various data points can be analyzed together using sophisticated algorithms to produce a profile of our activities and to predict our preferences, our health, our attitudes and our lifestyles. For example, it is reported that on-line sellers, using profile data, can set an individualized price for each buyer close to the maximum they would pay for the product. The personal data collected for a particular transaction, when accumulated from all transactions, becomes a valuable business asset that can be sold for use for other purposes. Some business models provide goods or services for free or for less cost by relying on the sale of personal data as a primary revenue stream.

The objective of the drafting committee is to produce a uniform act to regulate the collection, retention, and use of personal data in order to recognize people's interests in the personal data collected and used by companies. In the European Union, the General Data Protection Regulation came into effect in 2018 and provides significant rights for data subjects, including the right to know what data about them was being collected and the purpose for the collection, the right to approve or disapprove of the use of their data, the right to correct inaccurate data, and the right to have the data deleted when no longer necessary for the purpose for which it was originally provided. The GDPR sparked interest in such legislation in the United States, both to benefit consumers and to establish more uniform global rules for handling personal data. California has adopted a comprehensive regulatory regime known as the California Consumer Privacy Act (CCPA) which came into effect in January 2020. An

initiative measure is on the California ballot in November that would expand the regulatory structure over use of personal data. Other states have considered similar proposals. No comprehensive statute has been adopted although some specific privacy related measures have been enacted. For example, Illinois has a statute regulating biometric data and Vermont has a statute requiring registration of data brokers. While several proposals have been introduced in Congress, it does not appear that they will be adopted anytime soon.

There are several major sector specific federal data privacy regimes in place, including the Graham-Leach-Bliley Act (financial data), HIPPA (medical data), the Fair Credit Reporting Act, the Federal Family Educational Rights and Privacy Act (student data) and several others. Similarly, in some states there are more limited privacy regimes applicable to specific industries or activities.

The Committee Process

The project has attracted over 200 observers from a wide variety of technology and other industries interested in data collection as well as from consumer groups. The Committee was able to have one pre-COVID-19 in-person meeting in February which was attended by over 50 observers. Since then we have had several Zoom sessions with active observer participation. We have received numerous thoughtful and detailed position papers from our observers.

An initial framework draft was refined based on the February discussion and was considered at two meetings conducted remotely. On April 14th, the committee held a 90 minute video meeting, with the primary goal of soliciting observer comments on the revised draft. A day long video meeting was then scheduled for April 24th with the primary objective to obtain committee adoption of a first reading draft for submission to the Conference. Between April 14th and April 23rd we received numerous detailed comments, suggestions, and concerns from a variety of stakeholders. Fortunately, most of these came as specific suggestions for revision of the text of the Act but some urged us to reconsider our basic approach. **The current Committee draft is found on the website under the "2020 August 19 Informal Session" tab.**

In April two members of the drafting committee and a small number of observers presented an alternative draft to the Committee. This alternative draft departed in significant ways from the then committee draft. This draft was much less prescriptive, narrowed the scope of the regulatory footprint both in terms of who was regulated and what data was protected, recognized compliance with other similar privacy regimes as sufficient, and incorporated a voluntary consensus process to develop other permissible compliance regimes. It presented a very different framework and philosophy for addressing personal data privacy. **The alternative draft is found on the website under the "2020 August 6 Web Conference" tab.**

The Committee held two meetings in August 2020 to consider which of the competing drafts it was willing to pursue. The first meeting was with observers. While some were attracted to the alternative, others were opposed and preferred the committee draft. A second meeting, with only the committee present, convened a week later. Most thought there were

attractive elements of both drafts and that some middle ground seemed appropriate. Obviously, we have not had the opportunity to develop these thoughts at this point.

Accordingly, the committee draft is what is before you for this informal session. However, in this memorandum, I have tried to set out the major issues faced by the drafting committee—many of them highlighted by the competing drafts.

The Current Draft

The current "first reading" draft is still very much a work in progress. The Drafting Committee has voted to submit this to the Conference for your comments but no committee vote has been taken to approve any section or the work as a whole. This draft, like most first reading drafts, is designed to solicit comments from other Commissioners and, importantly, keep this project on schedule for a final reading in the summer of 2021.

The following are some of the significant issues, by no means in order of their importance, which the committee will be considering during the coming year. All comments are welcome.

a. *The Framework: Contractual, Standards-based, and Rights-Based Models*. Most current U.S. privacy law presumes that personal data may be freely collected and processed in the absence of any specific law forbidding it, and most such laws are limited to particular narrow industries or types of information (health, financial services, students, etc.). Commercial privacy generally has been governed by a "notice and choice" model under which the treatment of a consumer's personal data is often disclosed in terms of service or privacy policies which the consumer seldom reads. That treatment can include subsequent disclosures to or uses by third parties for unrelated purposes. In theory, the consumer may "opt out" of these practices by choosing not to use a product or service, thus exercising a weak form of consent when they use services that collect data. This model has come under increasingly strong criticism for failing to offer sufficient protection. European law, seen most recently in the GDPR, begins with the opposite presumption, that individuals have inherent rights in their personal data and it may be collected and processed only when specifically allowed by law. One of those legally authorized methods is obtaining "opt-in" affirmative consent from a consumer, but this is largely limited to uses connected with the particular purposes for which the personal data was collected in the first place. There have been criticisms of the European model for inflexibility that does not adequately reflect the realities of the marketplace, and in some cases it may be inconsistent with the First Amendment. Recent proposals in state legislatures and Congress try to chart a middle course between these extremes of contractual consent or personal rights, and the committee will continue to deliberate about the optimal balance.

Even though they begin with opposite presumptions, both of these models end up relying heavily on a form of individual consent. That traditional reliance on consent, particularly but not exclusively in the online world, generally provides little protection for data subjects and little guidance for business enterprises in processing personal data. A third approach might be to focus rather on general standards that should be met when data collectors utilize personal data. Given the diversity of enterprises that collect and process personal data, a standards-based approach might announce some floor of regulatory expectations but require particular industries to adopt codes of conduct or voluntary consensus standards and then to hold them accountable for compliance with those standards. These requirements would apply independently from individual consumers' consent.

The current committee draft moves toward less focus on notice and consent as the basis for privacy protection. The alternative draft provides an even more dramatic departure, emphasizing that uses of data consistent with the expectations of consumers when making the disclosure are impliedly consensual without specific notice where as other, non-compatible uses, must be fully disclosed.

It is likely that any act addressing these issues will blend all of these perspectives. The committee welcomes your views on this fundamental question. It will be central to the Committee's deliberations in the year ahead.

b. *Scope.* The scope section exempts both small businesses and specific data activities that are already subject to data privacy regulation. Also exempt are some uses where the public interest in use and retention of data justifies some limitation on data subject rights. Whether the right exemptions are included and the scope of the exemptions are matters that remain before the committee. To highlight some particular issues:

i. Blending this Act with other regulatory regimes that also have privacy objectives. Of particular note is the federal Graham-Leach-Bliley Act which regulates financial data collected by financial and other institutions. The current draft exempts personal data already regulated by GLB or any other data activity if the financial institution voluntarily complies with GLB. The alternative draft would have a broadly worded exemption for covered entities that comply with not inconsistent regulatory regimes.

ii. Employment data. The current draft exempts data collected by an employer about an employee in the context of the employment relationship. It has been argued this is too narrow and should extend to

other forms of agency relationships. The alternative draft would apply only to transactions between consumers and the consumer-facing entities and would thus not apply to data derived from non-consumer transactions.

iii. *Business-to-business data*. It has been urged upon us to exempt all business-to business data from the act. The question is whether a broad exemption may incorporate transactions that contain personal data. We will consider whether a narrower exemption makes sense in this setting. The alternative draft would incorporate this exemption.

iv. Publicly available data. The current draft exempts publicly available data which is broadly defined. It is argued that not to do so would raise serious First Amendment objections. However, data algorithms can take widely diverse and sometimes non- personally identifiable public data to profile an individual on matters that otherwise would be private.

c. *Household or device*. Some data collected does not identify a particular individual but rather a household or device. The IP address on a home computer identifies a household. A GPS tracking on an automobile identifies where the automobile has been but not necessarily who is in the automobile. Both narrow the range of possibilities and if analyzed with other data may identify a particular person. How we handle this data is not fully resolved.

d. *Definition of personal data.* The current draft contains a single and relatively broad definition of personal data. It has been suggested that we should consider a two-tiered approach where the broad definition might be subject to some regulation and a narrower definition might be appropriate for other purposes. This may be particularly so where the draft provides data subjects with specific rights that may create burdens for data collectors if they are applicable to a large amount of information. This question will be considered in further drafting. The alternative draft is limited to data that clearly identifies an individual, such as name, address, social security number, etc., and would not encompass for privacy purposes broader forms of data that can be processed to provide individual identification.

e. *Industry-specific standards*. One of the challenges of drafting a broad statute is that the nature of data collection and use, as well as retention, varies from industry to industry. The committee has attempted to define with some specificity the rights data subjects should have with respect to their own personal data but to leave flexibility for companies in how they respond to the assertion of these rights. It has been suggested that we incorporate best practices or voluntary consensus standards as a safe harbor of compliance.

There are some tentative steps in this direction in Section 8 of the current draft but the issue remains under consideration. The alternative draft brings greater focus to voluntary standards and makes them a central mechanism for obtaining compliance.

f. *Data processor obligations*. The obligations of controllers and processors necessarily differ, because processors typically do not have the same direct relationship with data subjects as controllers do. The committee has received many comments on this point and will be exploring ways to ensure both that processors have manageable duties and that data subjects are properly protected. The alternative draft at this point applies only to those who collect data and not to those who process it or who serve as data brokers. There seems to be committee consensus that any draft must incorporate processors and brokers within its regulatory regime.

g. *Enforcement*. The enactment of a workable and meaningful enforcement mechanism to ensure compliance is the most difficult and contentious issue. The current draft provides for both public and private enforcement. Both provisions will be carefully reconsidered before a final draft is presented.

    i. In many states, public enforcement for consumer protection has traditionally been part of the portfolio of the State Attorney General's office. Most states have adopted what are known as "little FTC" acts which often prohibit "unfair, deceptive, or abusive" acts or practices and authorize the state attorney general to enforce its provisions. However, these acts vary widely among the states, both in law and in practice. Some states have aggressive consumer protection units within the AG office and have been given broad powers to issue rules and regulations, hold hearings, and impose administrative remedies. In other states, the authority is considerably more restricted. It has been suggested that we better and more explicitly integrate our enforcement provisions with the "little FTC" acts. This draft is a start in that direction but more work remains to be done.

    ii. Private enforcement, through the authorization of a private cause of action for data subjects injured by violation of their rights, presents difficult issues. Because often the injury for a misuse of personal data is hard to monetize, most proposals authorize modest statutory damages. However, the use of class actions makes even a small presumed damage award a significant financial risk to companies, particularly when their obligation, by necessity, is crafted in general terms such as "reasonable protection." However, consumers observe that to leave their rights exclusively to the priorities and available resources of public agencies

offers uneven and sometimes inadequate protection. The current draft preserves a private cause of action but attempts to narrow its scope to violations of clear directives. It also attempts to provide safe harbors. Whether the current draft is appropriate remains a significant issue for the committee.

The alternative draft substantially relies on the current consumer protection authority of the State Attorney General but contains a narrow private right of action.

h. *Other matters*. This list of issues is not exhaustive, and omission of an item from the list does not suggest that any issue is closed at this preliminary first reading stage. We have received numerous other suggestions for refining some of the current provisions but have not had the opportunity to consider them or to incorporate them into the draft. Each suggestion will be considered as we move toward a final product.