Harvey S. Perlman
Professor of Law

Memo

To: CUPID Drafting Committee

From: Harvey Perlman, Chair

Re: CUPID or PDPISS

For our discussion next week on August 13 (1:30 CDT), I have tried below to outline my understanding of where we are and the more central issues that need to be resolved, at least tentatively, so we can move forward. (I make no comment on the unfortunate acronyms).

My takeaway from the call yesterday is that both drafts contain some attractive and innovative features. CUPID is more comprehensive and more prescriptive and thus has more challenges in terms of achieving consensus on all issues. At the same time, it follows the form of recent privacy legislation, has some consumer support, and compliance would be comfortable for major data players who have already adjusted to the California and European models. PDPISS is narrower and seeks to address privacy interests arising out of consumer transactions for a set of core personal data characteristics. It would significantly reduce compliance costs of smaller entities and thus may be acceptable to a broader swath of data collectors. It most likely would not satisfy the more adamant privacy advocates.

We face, it seems to me, three very general options as to how to proceed: (1) we stay the course with CUPID's comprehensive approach of privacy regulation, making such refinements as we can to address the costs of compliance and enforcement; (2) we shift to PDPISS, reconceptualizing our project as one more tailored and less intrusive in scope; or (3) we make an effort to blend the two approaches in yet undefined ways.

Even if we were to prefer elements of each draft, the initial decision must be whether we are willing to continue to pursue a more comprehensive data privacy act or whether we will be content with the narrower approach. I outline below some of the consequences of that decision:

1. PDPISS is largely limited to the procedural elements of fair information practices, i.e., access, opportunity to correct, and opportunity to delete. CUPID is broader and deals with constraints on use of personal data.
2. PDPISS is limited, for privacy purposes, to personal data which is data that clearly identifies an individual, such as name, social security number, IP address. CUPID attempts to address a broader range of data that may not directly identify a person but may be used in combination with other data to do so.

University of Nebraska Lincoln
College of Law
1875 N. 42nd St ¦ Lincoln, NE 68583-0902 ¦ 402-472-8118 ¦ hperlman1@unl.edu

3. PDPISS is limited to regulating the relationship between consumers and consumer-facing entities and does not address data brokers who obtain consumer data and use it for other purposes.
4. PDPISS incorporates a "compatible use" concept to permit uses for which it can reasonably said consumers impliedly consent. CUPID reduces reliance on consent but places more obligations to provide notice.
5. CUPID imposes some obligations on data controllers and brokers to manage the privacy elements of their data collections such as incorporating audits and assessments. PDPISS requires assessments only for security and not for privacy purposes.
6. PDPISS largely defers to other sector privacy regimes not inconsistent with its regime. CUPID tends to specify some of the regimes that are exempt but otherwise is more comprehensive in its scope. Integration with other privacy regimes will be a difficult issue regardless of which framework we choose to follow.
7. CUPID alludes to voluntary consensus standards. PDPISS develops in much greater detail and accords more weight to them in the enforcement regime.

The decision between a comprehensive or tailored data privacy act will drive which draft to pursue even as we consider incorporating elements of the other.

Some personal thoughts

With your indulgence I want to let you know my own views, though none are so firmly held that I could not be persuaded to the contrary. My instinct is that we should end up somewhere in the middle between these two drafts and I've been struggling with what that might mean. I am attracted to PDPISS because it would be much easier to refine it to a workable proposal. The integration of whatever we do with the multiple privacy regimes already in place is somewhat daunting. And, of course, the less prescriptive our approach, the less controversy we create.

On the other hand, I am concerned that the narrower version would place us outside the mainstream of data privacy efforts and thus make us largely irrelevant. There is already considerable compliance infrastructure in place in response to CCPA and GDPR and I suspect the larger tech companies, having made this investment, will not easily abandon it even if they might have preferred a narrower approach at the outset. Indeed, they could not abandon it because they will still have to comply with GDPR.

So I keep wondering what the middle ground might look like. The idea of "compatible uses" and the limitations on obligation of notice and consent in PDPISS seem sensible to me. And I am attracted to its formulation of the enforcement regime, including flushing out the language on voluntary consent standards. On the other hand, I support CUPID's recognition that privacy is at risk beyond a narrow definition of personal data and imposing some burdens on data controllers and brokers to monitor their own privacy policies seems appropriate.

Because of the compliance costs of CCPA and GDPR, they are made applicable to companies that are significantly invested in data processing, exempting companies that fall below thresholds of revenue from data use, number of data subjects, etc. I wonder whether we don't possibly have an opportunity to establish some low compliance costs standards for all companies collecting personal data (exempting compatible uses if property defined) and to retain the more prescriptive regime for the big data controllers and brokers. This may be impractical or fanciful thinking on my part.

I look forward to our discussion next Thursday.