April 21, 2020

Mr. Harvey Perlman
Harvey and Susan Perlman Alumni Professor of Law
University of Nebraska-Lincoln
Nebraska College of Law
McCollum Hall (LAW) 263
Lincoln, NE 68583-0902

Dear Harvey,

Thank you for your thoughtful response to our comments, and for your openness in finding the right solution to these difficult problems. The numbered points below are taken from your responses in the same order.

1. "I understand your concern about the top down structure, but it seems to me that it is a matter of taste as to whether a particular provision is a 'broad principle' or a 'command'."

Our apologies for not being clearer in our initial comments. We were trying to draw the distinction between a "bight line rule," and a "flexible standard." While the current draft seeks to implement the broad principles of fair information practices (notice, compatible secondary uses, express consent for incompatible uses, access, amendment, security and accountability), it does this using bright-line rules. This is very difficult to do. The social norms of privacy are inherently context specific, making any attempt to draft a universal bright-line rule either over-inclusive or under-inclusive. Inevitably, a bright-line rule will either unduly burden covered entities or fail to provide consumers appropriate levels of protection. Either way, a proposed statute using bright line rules will find it very hard to secure a political consensus. It is much easier to capture the context specific social norms of privacy with a statute expressing the principles as flexible standards, for when these norms are expressed at a high level of generality, it is much easier for diverse stakeholders to agree to them. There is no doubt legislatively enacted flexible standards are

"commands" in the sense that they create legal obligations that did not exist before, but they provide organizations with the flexibility to implement the general statutory requirements in a manner appropriate to the particular circumstances of their industry and sector, allowing for a kind of "bottom up" process, which can be seen in our discussion of voluntary consensus standards" in #4 below. The great success of the UCC is directly attributable to the fact that Llewelyn made liberal use of flexible standards, avoiding bright line rules wherever possible. We invite you to consider the same strategy.

2. "We will definitely be considering a two-tiered definition of personal data which makes a lot of sense to me personally."

We are pleased that you have found the "two-tiered" definition of personal data to be helpful.

3. "You are correct to observe that we have not fully integrated this into the baby FTC Acts although we have started that integration with use of "unfair and deceptive" practices. The problem of course is that the enactments of the baby FTC Acts among the states has been done with great variation. The language used, the procedures available, the power to adopt regulations or not, are all areas where there is wide differences among the states. Integration is neither simple nor fully possible."

So long as every state has a UDAP consumer protection law linked to Section 5 of the FTC Act, which prohibits unfair and deceptive acts and practices, the differences these statutes may have in terms of scope, remedies, agency regulations, and procedure, are not differences that make a difference. For the past 20 years, the FTC, partnering with state attorneys general, has used Section 5's unfair and deceptive act and practices jurisprudence to require businesses with notices of privacy practices to "do what they say they do." This has resulted in a common-law process allowing the courts to "fill in the gaps" of the existing sectoral privacy regime. Recognizing this, a Model Act needs to be integrated into the existing FTC jurisprudence. This can be done by requiring all covered entities to appropriately and reasonably implement in their notices of privacy practices, the principles of fair information practices (notice, compatible secondary uses, express consent for incompatible uses, access, amendment, security and accountability). By aligning the Model Act with the consumer protection framework, it also becomes possible to avoid conflicts with the hundreds of existing federal and state sectoral privacy statutes. Attempting to directly regulate personal data puts the Model Act in tension with these sectoral privacy laws, with each one requiring its own special drafting solution. Few state legislatures would have the patience to attempt such a lengthy and complicated task. The second draft's attempt to delegate the task to state attorneys general is not only constitutionally problematic but presents a task few Attorney Generals would be willing to undertake. The CCPA ignores the problem entirely, making a sub-rosa delegation of the task to the courts, who will no doubt be busy for some time. If we are correct that none of these solutions are viable, the only alternative is to build on the existing framework of

consumer protection. Rejecting this approach because of the diversity in state UDAP laws, makes the perfect the enemy of the good.

4. "We have a start toward voluntary consensus standards in the "privacy commitment" in section 8 which permits each business to adopt its own method of complying with the general principles of the act. I am interested in pursuing a more formal adoption of the VCS standards but it will not get done by April 24th."

The "privacy commitment" contained in Section 8 of the second draft, has no relationship to the concept of a "voluntary consensus standard." A "voluntary consensus standard" is a term of art, referring to the result of a private multi-stakeholder process where a general legal requirement such as the duty of "reasonable care" in tort law, is turned a specific internal control (a "bright line rule") for companies to apply to a particular situation or context. For example, manufacturers of mats for public building entranceways, must design their mats to be reasonably safe for the intended purpose. To this end, the American National Standards Institute, working with the National Floor Safety Institute, after a multi-stakeholder process, has issued a voluntary consensus standard for safety in the design of a mat for Commercial Entrance Matting in Reducing Slips, Trips and Falls.

https://www.iccsafe.org/wp-content/uploads/asc_a117/supporting_doc_3-3-1_ANSI_NFSI_B101_6-2012.pdf

This ANSI standard contains extremely specific sets of requirements for mats. There is no requirement, of course, that all manufacturers of mats choose this ANSI voluntary consensus standard (it is in this sense that voluntary consensus standards are voluntary). There may be other industry standards available to choose from, that may have been developed without using the ANSI multi-stakeholder process. There may be some manufacturers who simply decide their mats are reasonably safe for the intended purpose, even though they don't comply with any existing industry standard. And they are free to try to convince a judge of this fact, when someone injured by tripping on their mat files suit against them. However, as a practical matter, nearly all manufacturers today produce their mats in compliance with this ANSI standard. It is not just that conforming to the ANSI standard gets them summary judgment on the issue of reasonable care, but because the ANSI voluntary consensus standard for a safety mat is so widely accepted as the gold standard, the ANSI standard has in effect codified the duty of reasonable care for safety mats in public entranceways. And as the ANSI standard for mats is periodically updated, the updated standard carries with it the standard of care for a safety mat. This is why the Consumer Product Safety Act authorizes the Commission to incorporate "voluntary industry standards" into their regulations for the safety of consumer goods. It is why OMB A-119 provides that federal agencies wishing to incorporate an industry standard (instead of doing the work themselves), may only incorporate "voluntary consensus standards" meeting the ANSI essential due process requirements. One can see how this process works in a privacy statute, by looking at the safe harbor provisions for FTC approved guidelines in

the Children's Online Privacy Protection Act. We would invite you to use the COPPA's safe harbor structure in the Model Act.

5. "I am sensitive to the flaws of trying to adopt a consent framework to regulate consumer interests. I think we moved in your direction. Section 3 totally exempts from the act the collection or retention of data necessary for the transaction initiated by the consumer. This would seem to me to be close to your "implied consent for compatible use" idea. I would value your comment on this and how one might define "compatible" to be broader than transactional, or whether we should."

We are pleased that you are willing to consider giving the term "compatible" a broad definition. As you know, the concept of compatibility figures prominently in the General Data Protection Regulation of the European Union ("GDPR"), where Article 6(4) provides that processing of personal data is not based on the data subject's consent if it is not "compatible with the purpose for which the personal data have been collected." The close tie between consent and the concept of compatibility in Article 6 of the GDPR makes it clear that whether a use or disclosure of personal data is or is not compatible, is just the question of whether that use or disclosure is one for which an individual's consent could reasonably be implied.

For an elegant model of how consent is tied to compatibility in a U.S. privacy law, we would invite you to look at Section 552a(b) of the Privacy Act, which prohibits any use or disclosure of a [personal] record "except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record [would be pursuant to a routine use]." Section 552a(a)(7) of the Act then defines "routine use" as "the use of a record for a purpose which is ***compatible*** with the purpose for which it was collected" (emphasis added). For purposes of the Model Act, the intermediate term "routine use," could be replaced with the term "compatible use." The term "compatible" could then be defined using five general categories of compatible uses or disclosures:

> (A) effectuat[ing] a transaction with a consumer with the consumer's knowledge or participation;
> (B) complying with legal obligations of the covered entity;
> (C) meeting the operational needs and other legitimate interests of the covered entity;
> (D) permitting appropriate internal oversight of the covered entity, or external oversight by an agency; or
> (E) otherwise protecting health, welfare, public safety, national security, or other legitimate public interests that are recognized by law.[1]

[1] This list is drawn from Section 5(I) of the American Law Institute's Principles of Law, Data Protection (listing types of uses and disclosures for which consent is not required).

Because of the high level of generality with which these five principles of compatibility are expressed, it may be easier to obtain agreement to them. At the same time, in the world of concrete particulars, opinions about compatibility will not only diverge, they are likely to be fiercely contested. This is the reason that covered entities should be required to make transparent their compatible uses. While transparency is not a panacea, compatible uses must be identified before disagreements can surface. The Act should not attempt to resolve these inevitable disagreements, but should simply provide for a reasonably fair set of procedures to allow the disagreements to be discussed and debated publicly, first through the process of establishing a safe harbor for approved voluntary consensus standards for compatible uses, and failing that, the enforcement authority of the Attorney General. This approach avoids the discredited "opt-in" "opt-out" consent model for sensitive and non-sensitive data and reinstates a meaningful and robust consent requirement—express written consent for any disclosure that is not compatible.

Thank you for your attention and dialogue.

Sincerely,

Roslyn Layton, PhD*
Visiting Scholar
American Enterprise Institute
1789 Massachusetts Avenue
NW Washington, DC 20036

Ashley Baker
Director of Public Policy
Committee for Justice
1629 K St. NW
Suite #300
Washington, DC 20006

*Views expressed reflect the scholars; American Enterprise Institute takes not policy positions.