A Critique of the Uniform Law Commission's Uniform Personal Data Protection Act

In 2021, the Uniform Law Commission (ULC) finalized its Uniform Personal Data Protection Act (UPDPA), a model law intended to be a guide to states seeking to enact broad privacy laws. Unfortunately, the ULC's law is beyond disappointing. Quite frankly, the UPDPA is quite terrible. No state should adopt it in whole or in part. It is hard to find anything to salvage in the UPDPA. It's a law as clunky as its acronym. I find it shocking that the ULC could propose such a awful law. It is, sad to say, quite shameful.

The UPDPA is quite spare and loose. The heart of the law is basically as follows: (1) companies can use personal data without people's consent as long as there is a "compatible data practice" and (2) if the event of an "incompatible" data practice, companies only need to provide a chance to opt out.

The ULC has cooked up a broth that is so insubstantial, so thin and fetid, that it is hardly any different from bilge water. One might think I'm exaggerating for dramatic effect, but if you look at the law, you'll see that my comments are far from rhetorical flourishes but are quite restrained.

More specifically, Section 7(a) provides:

> A controller or processor may engage in a compatible data practice without the data subject's consent. A controller or processor engages in a compatible data practice if the processing is consistent with the ordinary expectations of data subjects or is likely to benefit data subjects substantially.

This provision is so vague that it permits companies to do

nearly anything. Even data practices that are not expected by people are fine if a company deems them "likely to benefit data subjects substantially." Every company thinks that what it does provides a benefit and makes the world a better place. It's hard to imagine how anyone could fail to cook up a rationale for nearly any data use that wouldn't somehow constitute a "compatible" practice.

This is quite bad, but the UPDPA gets even worse. Section 8(b) provides:

> A controller may process personal data that does not include sensitive data using an incompatible data practice if at the time personal data is collected about a data subject, the controller provides the data subject with notice and information sufficient to allow the data subject to understand the nature of the incompatible data processing and a reasonable opportunity to withhold consent to the practice.

When companies use personal data for incompatible purposes, the UPDPA just requires an opportunity to opt out. This is the much maligned notice-and-choice approach, which has been savagely criticized for decades. Modern laws have been moving away from the notice-and-choice approach, and even those that adopt it at least make some attempt to reign it in or otherwise make it less noxious.

The law is essentially allowing the fox to guard the henhouse and telling the fox to eat only chickens when compatible with its appetite.

The UPDPA provides the barest of rights (mainly access and correction). Although I have been critical of rights as insufficient to protect privacy, the solution isn't to omit most rights that other laws provide.

When it comes to obligations on data controllers, the UPDPA

also barely requires anything – just a risk assessment that remains confidential. This is paperwork that nobody will see, with no standards, and with no consequences. Most laws impose quite a few duties on data controllers, but the UPDPA asks hardly anything from data controllers. The law is not really a privacy protection law but a pathetic attempt to legitimize nearly unfettered collection and use of personal data with hardly any responsibilities and zero accountability.

In retro fashion, the law adopts an antiquated definition of personal data, Section 2(10): "'Personal data' means a record that identifies or describes a data subject by a direct identifier or is pseudonymized data."

The modern way to define personal data is based on the EU's General Data Protection Regulation (GDPR) – as identified or *identifiable* information. But the UPDPA only focuses on data that directly identifies individuals even when so much data can readily be linked to a person. The vast majority of the approximately 150 comprehensive privacy laws worldwide adopt definitions akin to the GDPR, as do recent US state privacy laws.

Of course it's no big surprise that the UPDPA lacks a private right of action and has minimal enforcement. But it doesn't matter, as there's hardly anything in this law to enforce.

The UPDPA doesn't push the law forward. It is hard to find anything in the law to advance the ball even an inch. This law does more to hurt privacy than to help it. The law basically tells business to do whatever they want with hardly any restrictions. And, if businesses are somehow so ridiculously out of line that they contravene the law, there are hardly any consequences.

The UPDPA is not an attempt at compromise between industry and consumer protection advocates. It's not even a good attempt to pander to industry because many companies have proposed laws

far more privacy protective than the UPDPA. Perhaps the UPDPA is an attempt to pander to a very small and shrinking segment of industry that wants to imagine a world 50 years ago and forget about the GDPR, the explosion of privacy laws worldwide, and the emerging new privacy laws in the U.S. states. The UPDPA is an exercise in denialism.

I struggle to see what the purpose of the UPDPA is. It certainly won't gain any respect among any commentators beyond the most stalwart pro-industry types. It won't gain respect from the EU, as it doubles down on so many things that are derided about the US approach to privacy. It won't gain the respect of other countries. It is weaker than the state laws being passed now and weaker than most other privacy laws on the books. It won't help consumers or address the concerns animating the wave of privacy legislation right now. Doing nothing is better than enacting the UPDPA. I thus wonder what the point of the UPDPA really is.

In contrast to the ULC effort, the American Law Institute (ALI) engaged in a similar effort to guide privacy legislation – the *Principles of the Law, Data Privacy*. I was a reporter on the project along with Professor Paul Schwartz (Berkeley Law). Our process was an extensive seven-year effort involving a diverse group of thought leaders: academics, in house counsel, law firm attorney, and judges. Industry perspectives were well represented, as were academic ones from a variety of viewpoints. We reached a reasonable consensus. There are many aspects of our ALI project that I personally might have written differently were I king, but our goal was to forge a good compromise. We proposed approaches that aimed to push the law forward and that a wide range of stakeholders could live with. For more background on the ALI Data Privacy Principles project, I wrote a short essay with Paul about it here.

Unfortunately, the ULC effort seems not to have attempted to reach any kind of compromise and appears to have excluded a diverse range of viewpoints.

Hopefully state legislatures will see the flaws of the UPDPA and ignore it. There's a clear call from the public for meaningful privacy protections. Passing a hollow law might placate people for a few years until they realize they've been had, and then the call for stronger privacy laws will continue.

The UPDPA is obsolete on arrival, not only using antiquated approaches, but also even watering them down. The ULC should scrap the UPDPA and start over from scratch. State legislatures should avoid the UPDPA in its totality.

* * * *

This post was authored by Professor Daniel J. Solove, who through TeachPrivacy develops computer-based privacy and data security training. He also posts at his blog at LinkedIn, which has more than 1 million followers.

Professor Solove is the organizer, along with Paul Schwartz, of the Privacy + Security Forum an annual event designed for seasoned professionals.