April 20, 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 6858

Mr. William McGeveran
Reporter, ULC Collection and Use of Personally Identifiable Data Committee
Mondale Hall
229 19th Ave., South
Minneapolis, MN 55455

Re: Further Reforms to Draft Data-Privacy Legislation

Dear Mr. Perlman and Mr. McGeveran:

Thank you both for the hard work you've put into the Committee's development of the Collection and Use of Personally Identifiable Data Act (CUPID). From organizing this week's teleconference to drafting the proposed bill, you both have kept the ball moving on a critical piece of legislation. And although there is much good in the proposed bill, I fear that without further edits, the bill will not successfully guard consumers' data privacy while preserving companies' innovation.

Below, I have listed NetChoice's concerns and proposed alternatives that we believe will strengthen the bill, and ensure the bill becomes a workable piece of legislation.

1. Remove the Private Right of Action

State attorneys general must be the only enforcers of state privacy laws. Although well intentioned, the private right of action provision will do extensive harm, undermine the credibility of the Act, and upend enactability. First, consider a related example: Illinois's Biometric Information Privacy Act (BIPA). Under BIPA, private parties can sue companies for technical violations of the act—no harm required. Even the original sponsor of the law stated that he never intended the law to be used as it has to profit the plaintiffs bar at the expense of Illinois residents' access to technology.

As a result, plaintiffs have brought hundreds of lawsuits against companies big and small. Even companies that have tried in good faith to comply with the law have opted to settle, because they fear that mere technical violations can add up to many more times than they can afford.

Faced with such liability, companies have become more cautious than is necessary. For privacy advocates, this may appear to be a cause for celebration. But in reality, this is an unintended consequence that does little to promote privacy and does much to undermine innovation. What's more, start-ups and small businesses lack the resources to defend themselves against lawsuits, even lawsuits that are meritless. Thus, laws that rely on reasonable practices but that allows for private rights of action—which the proposed bill does—stifle competition and enshrine the market's dominant players. That's bad for consumers and it's bad for innovation.

Experience under federal privacy laws also shows that a private right of action is not necessary to effectuate a bill's purpose. The Graham-Leach-Blilely Act, for example, imposes data-protection obligations on financial institutions and tasks federal agencies like the Consumer Financial Protection Bureau and Federal Trade Commission with enforcement. The law does not have a private right of action. By giving exclusive enforcement power to these agencies, the law allows the government to pursue a range of remedies that relate to those agencies' authorizing statutes. This gives the agencies flexibility in crafting remedies that not only respond to a specific company's violations but also signal best practices to others in the industry.

Likewise, the Health Insurance Portability and Accountability Act does not contain a private right of action. Instead, the Department of Justice has criminal enforcement authority and may seek fines or imprisonment against those who violate the law. This enforcement regime has proved effective: covered entities take seriously their obligations under the law and compliance rates are high.

Should the private right of action remain, the bill will split enforcement authority between a state's attorney general and the courts. This duel-enforcement regime will introduce *even more* uncertainty into calculations that businesses must make. Indeed, it is likely that some courts will disagree with a state's attorney general on what constitutes a violation and the extent of harm. In turn, businesses—especially small ones—will struggle to adopt policies and practices that balance a consumer's privacy with the company's legitimate need for data use and collection.

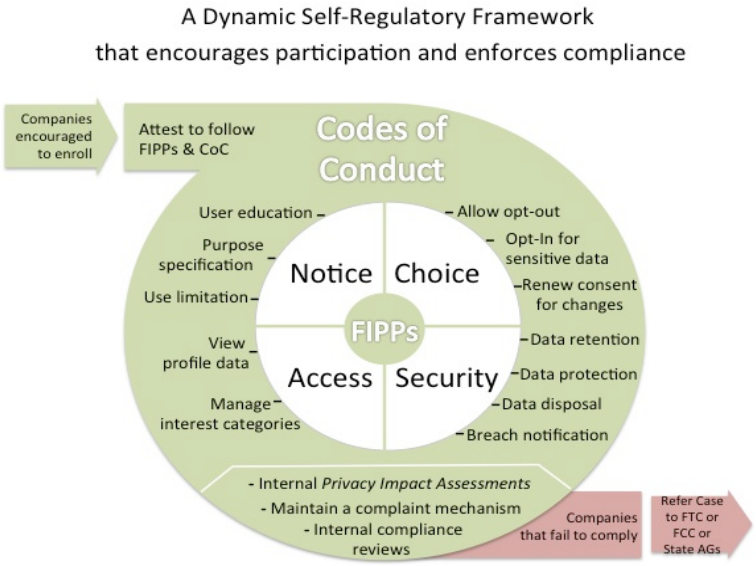
By centralizing enforcement in one person—a state's AG—we can ensure that a state speaks with one voice on data-privacy protection. Given the hodge-podge of laws we have now, uniformity and consistency must be the proposed bill's target. If not, we'll be no better off than we are now. Even worse, states may be hemmed in by court decisions that freeze in place what some judges consider reasonable. As you know, technology develops rapidly; new ideas spring up seemingly overnight; new challenges arise daily. States, like the federal agencies charged with enforcing federal privacy laws, will benefit from flexibility. So, too, will businesses and consumers, who can work with state agencies to implement and enforce the statute in a fair, consistent manner—and one that balances all interests.

It's also worth noting that no state has enacted comprehensive privacy legislation that includes a private right of action. In fact, bills that include it have failed time and again. From Washington to New Jersey—even Illinois—private causes of action have doomed such legislation. Because we want the proposed bill to be adopted and to be adopted by as many states as possible, the Committee must remove this red flag.

2. Include a Safe-Harbor Provision

As written, the proposed bill is a top-down regulatory scheme that sets covered entities up for failure. Even those that seek to comply with the bill cannot be assured total compliance all the time. Coupled with the bill's private right of action for technical violations, this guarantees that businesses will be harmed unnecessarily.

To remedy this, the bill must include a safe-harbor provision that encourages the development of industry-wide codes of conduct to create privacy and security standards. Rather than relying on governmental enforcement and constant oversight, we suggest an industry self-regulatory approach. The state can certify industry self-regulatory approaches. Compliance with the self-regulatory body constitutes compliance with the privacy regime. This further eliminates the need for protracted rulemakings and instead allows regulation at the speed of innovation. This



approach has succeeded in protecting privacy via laws like Children's Online Privacy Protection Act (COPPA) by providing flexibility and accountability.

These standards can then be used to evaluate businesses' actions. Those that stray far from the standards, or those who do so with malicious intent, can be held accountable. On the other

hand, businesses that act ethically can proceed knowing that they won't face nearly unlimited liability for technical deviations that result in no harm.

This framework is not new in American law, either. Even negligence law gives individuals discretion and generally holds them accountable only when they act unreasonably. This same reasonable-behavior framework also guides the FTC, for example, which uses standards and safe harbors to enforce data-security laws and has done so to great success. Without some measure of discretion—like that afforded by a safe harbor—the bill will impose strict liability on companies. Again, although that may appeal to some privacy advocates, it'll conflict with federal frameworks, hurt innovation, and group good businesses with unethical ones.

3. Limit the Proposed Bill's Scope

NetChoice agrees fully with the Consumer Data Industry Association's comment that the proposed bill should not apply to business-to-business transactions.[1] Businesses share data for legitimate reasons, and unreasonably limiting their ability to do so will harm the very consumers the proposed bill is meant to protect. Sometimes, sharing consumer data is even required by law. The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, for example, requires certain businesses to disclose a senders' physical address to alert recipients. Although federal law is supreme and would be unaffected by the bill, the proposed bill should not discourage businesses *not* covered by federal law from engaging in data-sharing practices that seek to protect consumers in similar ways.

4. Better Define Terms

Laws must give covered entities notice of what's acceptable behavior and what's not. With clear standards and definitions, laws can be enforced consistently and fairly. Without them, laws become prone to abuse and unfair application. Here, the bill's comprehensive in scope, but vague on details. The definitions for "data custodian" and "sensitive data" are confusing and don't give covered businesses adequate notice of what's required of them. Other definitions, like those for "household data," "de-identified data," and "device," are unworkable. Left unchanged, these definitions will ensure the bill does more harm than good.

Moreover, this Act should address *all* data collectors much in the way that the EU General Data Protection Regulation does. Under GDPR, it does not matter if a collector is a 501(c)(3), (c)(6), or any other designation. All are covered. We have seen data breaches at non-profit organizations.

Take for example the data breaches at the University of Maryland and Yale University. Since 2005, educational institutions have had an average of over 66 breaches a year. Other non-profits have

[1] Letter from Eric J. Ellman, Sr. VP, Consumer Data Industry Association, to William McGeveran, Reporter, ULC Collection and Use of Personally Identifiable Data Committee, 4 (Apr. 14, 2020).

also had an average of over 9 data breaches since 2005. That is almost one breach per month, yet none of these breaches are subject to most data breach notification laws.

As the AGs and FTC's consumer protection authority is limited to commercial businesses, expended oversight would require allowing the AGs enforcement power over non-profits who can already take actions against non-commercial entities.

5. Promote Consistency and Predictability

The Uniform Law Commission has long promoted legislation that aims to give the public consistent application of laws, leading to predictable results. Yet this proposed bill does just the opposite. By failing to preempt local laws, the proposed bill leaves covered entities vulnerable to conflicting obligations in the very same jurisdictions.

And because the bill encourages each state AG to promulgate her own rules, the bill will lead to inconsistent standards across the country. This is made even worse by Section 8(c) of the bill, which gives AGs a vague power to decide what constitutes "unfair or deceptive" practices. The provision is not helped by limiting the power to when businesses "do not provide reasonable protection for a data subject's privacy." What does this mean? How protective must they be? Surely different states will interpret this differently. And, again, that would serve businesses no better than the existing patchwork of state privacy laws.

Thank you for the opportunity to share NetChoice's concerns. We appreciate that crafting a workable data-privacy bill is no easy work, and we hope our comments help improve the bill so that it balances all stakeholders' interests and succeeds. Please let me know if you have any questions or would like to talk further.

Sincerely,

Carl Szabo
General Counsel & Vice President, NetChoice

Chris Marchese
Policy Counsel, NetChoice