August 21, 2020

VIA EMAIL

Representative Giovanni Capriglione
Senator Jane Nelson
Cochairs
Texas Privacy Protection Advisory Council

Re: Texas Privacy Protection Advisory Council Public Survey

Dear Representative Capriglione and Senator Nelson:

The U.S. Chamber Institute for Legal Reform ("ILR")[1] appreciates the opportunity to comment on the Texas Privacy Protection Advisory Council ("TPPAC") Public Survey ("RFI"). ILR commends TPPAC for soliciting public input in fulfilling its statutory mandate to evaluate existing state privacy approaches and provide a recommended approach for the State of Texas.[2] ILR urges the TPPAC to take this opportunity to promote sensible legal principles that support innovation in data use and technology, and that avoid inviting abusive lawsuits that are unrelated to consumer harm. This letter offers concrete policy suggestions for the TPPAC to consider and recommend going forward.

A. Texas Can Protect Privacy and Promote Innovation with Smart Policies that Reject Lawsuit Abuse and Promote a Predictable Regulatory Environment, as Reflected in the ILR's Privacy Toolkit.

The best approach to data privacy policy is a unified federal law. A comprehensive and preemptive federal privacy law—like the model that the U.S. Chamber of Commerce has proposed[3]—would ensure that all Americans, no matter their state, can rest assured that their data is safe, while also reaping the distinct benefits of data-driven innovation. This approach would also avoid the pitfalls of a state-by-

---

[1] ILR is the country's most influential and successful advocate for civil justice reform, both in the U.S. and abroad. ILR's mission is to champion a fair legal system that promotes economic growth and opportunity.

[2] *See* Tex. Business & Commerce Code Ann. § 521.053, sec. 2(g).

[3] *See, e.g.*, U.S. Chamber of Commerce, Model Privacy Legislation (updated June 18, 2019), https://www.uschamber.com/sites/default/files/uscc_dataprivacymodellegislation.pdf.

state patchwork approach, including consumer confusion, inconsistent treatment of data, and a challenging compliance environment for businesses.[4]

In the absence of a comprehensive federal privacy law, states understandably may want to review their laws to ensure consumers are protected. Texas is no exception. In contrast to some states that rush to legislate but fail to provide a predictable regulatory environment, Texas laudably has taken a thoughtful approach to considering what policies are right for its citizens. To support states' consideration of privacy law and policy, ILR has released a toolkit for state policymakers ("ILR Toolkit").[5] The ILR Toolkit does not take a position on the substantive aspects of state privacy laws. Rather, it offers commonsense approaches to liability designed to avoid the pitfalls of other states and avoid generating a flood of unnecessary and opportunistic litigation.[6] The most relevant recommendations from the Toolkit are included in this letter, and the full ILR Toolkit is attached for further reference and guidance, as TPPAC does its important work.

The principles recommended in the ILR Toolkit are critically important because they promote a predictable and fair regulatory environment that will lead to better outcomes for consumers.

The plaintiffs' bar has worked tirelessly to exploit and expand privacy laws to manufacture ***thousands*** of high stakes class action privacy lawsuits that target companies operating in good faith and pressure them into settling.[7] These lawsuits are often brought when ***no consumer has been harmed***,[8] by lawyers who brag about large settlements with only "intangible privacy harms" and "without having to show any

---

[4] *See, e.g.*, *Consumers and Businesses "Will Pay a Price" For State-by-State Data Regulations*, Chamber ILR (October 15, 2019), https://www.instituteforlegalreform.com/resource/consumers-and-businesses-will-pay-a-price-for-state-by-state-data-regulations; Chamber ILR, A Perilous Patchwork: Data Privacy and Civil Liability in the Era of the Data Breach (October 2015), https://www.instituteforlegalreform.com/uploads/sites/1/APerilousPatchwork_Web.pdf.

[5] ILR, Mapping a Privacy Path: Liability and Enforcement Recommendations for States (Dec. 2019), https://www.instituteforlegalreform.com/uploads/sites/1/Privacy_Policymaking_Report_Liability_and_Enforcement_Recommendations_for_States.pdf ("*ILR Toolkit*").

[6] *Id.* at 1.

[7] *See generally* ILR, Ill-Suited: Private Rights of Action and Privacy Claims (July 2019), https://www.instituteforlegalreform.com/uploads/sites/1/Ill-Suited_-_Private_Rights_of_Action_and_Privacy_Claims_Report.pdf ("*Ill-Suited*").

[8] *See generally* ILR, Engineered Liability: The Plaintiffs' Bar's Campaign to Expand Data Privacy and Security Litigation (Apr. 2017), https://www.instituteforlegalreform.com/uploads/sites/1/Engineered_Liability_The_Plaintiffs_Bars_Campaign_to_Expand_Data_Privacy_and_Security_Litigation.pdf.

direct loss."[9] Companies of all types and sizes have been sued. For example, the United States Court of Appeals for the Seventh Circuit recently allowed a lawsuit under Illinois law to proceed against a manufacturer, where employees complained under state law that they were not given proper disclosures related to their use of a vending machine, even though the alleged violations did not result in any "tangible consequences."[10] In another case, the Ninth Circuit allowed a lawsuit to go forward against a social media company based on the same state law over a website's function that the lead plaintiff described as a "nice feature" and which resulted in no harm.[11] The company in that case settled this year for ***more than half-a-billion dollars***.[12] In 2018, a Texas district court allowed a plaintiff to sue an oil and gas company for thousands of dollars under a statute with a private right of action for seven unwanted telephone calls.[13] At the time, the plaintiff had "asserted between 50-150" similar claims and even "taught classes showing others how to sue" under the statute.[14] In sum, well-intentioned—but misguided—privacy laws across the country are spawning a slew of unnecessary and counterproductive litigation against legitimate businesses. Worse still, ILR research has shown that these privacy laws are "***inefficient and ineffective*** for addressing privacy concerns[.]"[15]

In light of these cautionary tales, Texas is presented with a valuable opportunity. The Lone Star State can provide the nation with a roadmap for successful privacy legislation that effectively protects consumers *and* ensures that "Texas continues to flourish as a hub of innovation, technological advancement, and economic prosperity."[16]

---

[9] *Inside the Firm: Privacy and Technology*, Edelson, https://edelson.com/inside-the-firm/privacy-and-technology/ (last visited Aug. 20, 2020).

[10] *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 624 (7th Cir. 2020), *as amended on denial of reh'g and reh'g en banc* (June 30, 2020).

[11] *See generally Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937, 205 L. Ed. 2d 524 (2020). The "nice feature" language comes a deposition, quoted in the Appellant's Brief.

[12] *See BIPA Settlement Should Keep Companies Up At Night, Lawyer Says*, ILR (Feb. 6, 2020), https://www.instituteforlegalreform.com/resource/bipa-settlement-should-keep-companies-up-at-night-lawyer-says.

[13] *Morris v. Hornet Corp.*, No. 4:17-CV-00350, 2018 WL 4781273, at *5 (E.D. Tex. Sept. 14, 2018), *report and recommendation adopted*, No. 4:17-CV-00350, 2018 WL 4773547 (E.D. Tex. Oct. 3, 2018).

[14] *Id.*

[15] *Ill-Suited*, at 1 (emphasis added).

[16] *Governor Abbott Delivers Remarks At Groundbreaking Of New Uber Hub In Dallas*, Office of the Texas Governor (Nov. 1, 2019), https://gov.texas.gov/news/post/governor-abbott-delivers-remarks-at-grand-opening-of-new-uber-hub-in-dallas (internal quotations omitted).

B. Texas Should Consider Key Procedural Protections to Ensure That Any Private-Sector Focused Privacy or Security Legislation Does Not Chill Innovation.

The RFI asks two questions with regard to the private sector. *First*, "[w]hat key components of privacy and protection of information that is linked to a specific individual, technological device, or household should be considered by the Texas Privacy Protection Advisory Council?" *Second*, "[a]re there laws in Texas, other states, or relevant jurisdictions which govern the private sector in the privacy and protection of information which should be considered by the Texas Privacy Protection Advisory Council?" Below, ILR draws on its Toolkit to address each of these questions by (i) recommending several important procedural components, and (ii) highlighting laws that rightly incorporate these protections, as well as flagging cautionary tales where these protections are not in place.

1. Texas should preclude private rights of action.

Texas should eschew private rights of action in any privacy legislation for three reasons. *First*, private rights of action vest enforcement authority with plaintiffs' attorneys—parties that are not well-equipped to uphold the public interest. Private attorneys' goal is typically to secure the largest payout possible, *not* to promulgate an effective and coherent enforcement regime.[17] For this reason, attorneys afforded a private right of action—through statutes like the Telephone Consumer Protection Act ("TCPA")—typically target legitimate companies with deep pockets, not the true bad-faith actors that harm consumers.[18] In addition, plaintiffs' attorneys lack the expertise and public accountability to enforce complicated privacy statutes that often turn on ambiguous terms and novel technologies.[19]

Second, private rights of action impose disproportionate costs and deter innovation. For example, Illinois' Biometric Information Privacy Law ("BIPA") establishes a private right of action and provides for thousands of dollars in liquidated damages per violation—even for technical violations that are easy to fix and that have

---

[17] *Chamber ILR Toolkit*, at 3–4.

[18] *Id.* ("Plaintiffs' lawyers' infamous use of the Telephone Consumer Protection Act (TCPA) provides a great example of this: a comprehensive study of litigation brought under the TCPA's private right of action found that 'it is not the unscrupulous scam telemarketers that are targeted by TCPA litigation, but rather legitimate domestic businesses' that have resources to pay 'lucrative settlements or verdicts.'" (citations omitted)).

[19] *Id.* at 4.

not harmed consumers.[20] This regime has caused plaintiffs' attorneys to file hundreds of BIPA-related suits in recent years that threaten to put legitimate companies out of business.[21] Companies will be hesitant to deploy innovative new products and services—even if they do so in an eminently safe and compliant manner—if they are all-but-guaranteed to face a massive class-action lawsuit as a result.[22]

Third, proposed private rights of action—due to their numerous problems—often impede legislative consensus. Washington's attempt to pass a comprehensive privacy law provides a cautionary tale. Washington State Senator Reuven Carlyle—the key Senate sponsor of the Washington Privacy Act—released a statement after that bill collapsed, announcing that after two years of bipartisan cooperation, the legislature was not "able to reach consensus."[23] Senator Carlyle explained:

> The impasse remains a question of enforcement. As a tech entrepreneur who has worked in multiple startup companies, and in the absence of any compelling data suggesting otherwise, I continue to believe that strong attorney general enforcement to identify patterns of abuse among companies and industries is the most responsible policy and a more effective model than the House proposal to allow direct individual legal action against companies.[24]

Thus, were it not for the State House's insistence on a private right of action, Washington could very well have been the second state in the country to pass a comprehensive consumer privacy law.

Fortunately, Texas has an easy option to prevent this myriad of issues: precluding private rights of action. Texas has rightly taken this approach with its biometric privacy law by vesting enforcement with the Texas attorney general, rather than with private attorneys.[25] Many federal statutes—including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Children's Online

---

[20] *Id.* at 4.

[21] *See id.* at 4.

[22] *Id.* Related to this point, in the event Texas does impose a private right of action—and, to reiterate, it should not—it should limit attorney's fees. *See id.* at 22–25.

[23] *Carlyle issues statement on Washington Privacy Act*, Sen. Reuven Carlyle (Mar. 12, 2020), http://sdc.wastateleg.org/carlyle/2020/03/12/carlyle-issues-statement-on-washington-privacy-act/.

[24] *Id.*

[25] Tex. Bus. & Com. Code Ann. § 503.001(d) ("A person who violates this section is subject to a civil penalty of not more than $25,000 for each violation. The attorney general may bring an action to recover the civil penalty.").

Privacy Protection Act ("COPPA")—take a similar tack.[26] In addition, Nevada's recently-enacted online privacy law contains explicit language barring private rights of action.[27] Texas should maintain this proven approach in any privacy legislation it considers to avoid unintentionally shuttering Texas businesses and chilling innovation.

2. Texas should include notice and cure periods.

Businesses should be afforded an opportunity to fix a problem before they are subjected to liability.[28] Providing parties with notice and an opportunity to cure privacy violations before subjecting them to enforcement is a commonsense and good policy for several reasons. *First*, it incentivizes industry to cooperate and respond to concerns about their privacy practices, rather than taking a defensive, litigation-oriented mindset.[29] *Second*, it frees up limited resources by allowing businesses to easily remedy technical violations, reserving the state's valuable enforcement resources for serious violations or issues that parties are unwilling to fix.[30] *Third*, it creates a predictable and collaborative business environment, allowing businesses to come into compliance without fear of unnecessary and overly-punitive litigation.[31]

Given the numerous benefits of notice and cure periods, they are unsurprisingly commonplace. While far from perfect, the California Consumer Privacy Act ("CCPA") requires giving organizations notice and an opportunity to cure before its enforcement provisions kick in.[32] The Minnesota Human Rights Act precludes suits by would-be plaintiffs unless they notify establishments of alleged accessibility violations and give them time to cure those violations.[33] At the federal level, the Federal Trade Commission ("FTC") Act provides a cure period for certain warranty claims.[34] Texas should adopt this sound policy in any privacy law it may consider.

---

[26] *Chamber ILR Toolkit*, at 5.

[27] *See* Nev. Rev. Stat. Ann. tit. 52, § 603A.360(3) (2019) (providing that the privacy law does "not establish a private right of action against an operator.").

[28] *ILR Toolkit*, at 7.

[29] *Id.* at 7–8.

[30] *Id.* at 8.

[31] *Id.*

[32] Cal. Civ. Code §§ 1798.150(b), 1798.155(b).

[33] Minn. Stat. § 363A.331(2).

[34] 15 U.S.C. § 2310(e).

3. Texas should offer safe harbors.

Good privacy legislation will guide covered businesses to best practices and approaches, giving legitimate companies a clear path to compliance and allowing enforcers to focus on true bad actors.[35] Safe harbors—legislative provisions that specify certain actions an organization may choose to take or standards that it could meet that will preclude liability—are good policy for several reasons. *First*, safe harbors give businesses a clear path to compliance, which benefits both industry (in the form of greater certainty) and consumers (in the form of greater compliance).[36] *Second*, safe harbors preserve scarce enforcement resources. Legitimate businesses will take advantage of safe harbors by following their delineated compliance path, allowing enforcers to better allocate their resources to go after true bad-faith actors.[37]

Safe harbors are a regular feature in privacy and cybersecurity laws. For example, Ohio's cybersecurity law allows organizations to take advantage of a statutory affirmative defense if they "[c]reate, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information and that reasonably conforms to an industry recognized cybersecurity framework[.]"[38] COPPA also provides safe harbors, allowing organizations to remain complaint with that statute "by following a set of self-regulatory guidelines, issued by representatives of the marketing or online industries, or by other persons," subject to the approval of the FTC.[39] Texas should take a similar approach in any privacy law it considers, providing organizations with a clear path to compliance with reasonable, flexible safe harbors.

4. Texas should include civil penalty caps.

Civil penalty caps allow for enforcers to provide incentives for compliance with state law without the threat of disrupting entire industries.[40] Civil penalty caps are good policy for several reasons. *First*, organizations already have strong incentives to protect consumers. Privacy and cybersecurity incidents carry significant adverse consequences for businesses, including loss in share value, lost goodwill, and significant out-of-pocket

---

[35] *ILR Toolkit*, at 10.

[36] *Id.* at 10–11.

[37] *Id.* at 11.

[38] Ohio Rev. Code Ann. tit. 13, § 1354.02(A) (2018).

[39] 15 U.S.C. § 6503(a); *see also COPPA Safe Harbor Program*, FTC, https://www.ftc.gov/safe-harbor-program (last visited Aug. 19, 2020) (providing "[l]ist of currently approved Safe Harbor organizations").

[40] *ILR Toolkit*, at 14–17.

costs.[41] *Second*, laws with unlimited liability—such as the TCPA—have not proven effective in protecting consumer privacy.[42] *Third*, uncapped penalties can deter businesses from innovating, as many organizations will rationally conclude that unveiling a new product or service is not worth the risk of potentially bankrupting their company.[43]

Given the downsides of unlimited liability, civil penalty caps are common. For example, HIPAA limits penalties under a tiered system based on the seriousness of the violation.[44] For low-level offenses, HIPAA caps penalties at "$100 for each such violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $25,000."[45] Texas should adopt civil penalty caps in any privacy law it considers.[46]

5. Texas should specify exclusive attorney general enforcement.

The Texas attorney general is in a better position to enforce any Texas privacy law than other stakeholders for several reasons. *First*, the Texas attorney general is already an expert enforcer of consumer protection issues—including consumer privacy.[47] The Texas attorney general is thus equipped with the expertise to ensure effective application of a statewide privacy law. *Second*, providing for exclusive enforcement authority will create a more stable and predictable enforcement environment by preventing a patchwork of private plaintiff and municipal enforcement policies.[48] A harmonized statewide enforcement policy will better allow businesses to

---

[41] *Id.* at 14.

[42] *Id.* at 15; *see also Ill-Suited.*

[43] *ILR Toolkit*, at 15.

[44] 42 U.S.C. § 1320d-5(a).

[45] Id. § 1320d-5(a)(3)(A).

[46] Texas already caps civil penalties for violations of its biometric law, Tex. Bus. & Com. Code Ann. § 503.001(d) (capping penalties at "$25,000 for each violation"), and for reidentifying certain confidential information, *id.* § 506.006(a) (capping civil penalties at "an amount of not less than $25 or more than $500 for each violation, not to exceed a total amount of $150,000."). WhileILR applauds the imposition of civil penalty caps, these particular caps are likely too high for minor or technical missteps in a state privacy law.

[47] *See, e.g.*, *Consumer Protection*, Attorney General of Texas, https://www.texasattorneygeneral.gov/consumer-protection (last visited Aug. 19, 2020) ("We protect Texas consumers by accepting complaints, filing civil cases in the public interest and educating Texans on how to spot and avoid possible scams."); *Data Breach Reporting*, Attorney General of Texas, https://www.texasattorneygeneral.gov/consumer-protection/data-breach-reporting (last visited Aug. 19, 2020); *Identity Theft*, Attorney General of Texas, https://www.texasattorneygeneral.gov/consumer-protection/identity-theft (last visited Aug. 19, 2020).

[48] *Chamber ILR Toolkit*, at 20.

assess the actions they need to take to comply with the law, improving compliance outcomes.[49]

If Texas is considering providing the attorney general with rulemaking authority, it should carefully consider the scope of such authority.[50] Rulemaking authority can help fill in genuinely ambiguous gaps in statutory language and provide greater certainty in some instances.[51] However, without limits, rulemaking can *reduce* certainty by giving the attorney general a blank slate to rewrite the state's privacy law at will.[52] In addition, *carte blanche* rulemaking authority and ambiguously-worded statutes can lead to administrative delays, poorly-drafted regulations, and economic loss—a situation thathas unfolded with the promulgation of California's CCPA regulations. As the U.S. Chamber explained during California's rulemaking process, the California attorney general's implementing regulations for that law are poised to "cost up to $55 billion in compliance costs for California companies alone" due to, *inter alia*, "many ambiguities and requirements exceeding the authority of the CCPA."[53]

As with the other procedural protections that ILR is recommending, vesting exclusive enforcement of state privacy legislation with a state attorney general is common because it is good policy. Indeed, both Texas and Washington vest exclusive enforcement of their biometric privacy laws with their respective attorney general.[54] Nevada's online privacy law likewise provides that "[t]he Attorney General shall enforce the provisions" of that law and makes clear that the law "do[es] not establish a private right of action[.]"[55] Texas should employ this commonsense approach to any privacy law it considers.

---

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] *See* Letter from Tim Day, Senior Vice President, Chamber Technology Engagement Center, and Harold Kim, Chief Operating Officer, Chamber ILR, to California Attorney General Xavier Becerra (Dec. 6, 2019), https://www.instituteforlegalreform.com/uploads/sites/1/ILR_and_US_Chamber_Comment_to_California_AG_on_CCPA_Regulations.pdf (emphasis omitted).

[54] *See* Tex. Bus. & Com. Code Ann. § 503.001(d) ("The attorney general may bring an action to recover the civil penalty."); 19 Wash. Rev. Code 375.030(2) ("This chapter may be enforced solely by the attorney general under the consumer protection act[.]").

[55] 52 NV Stat. § 603A.360(1), (3).

6. Texas should curtail municipality litigation.

Texas should preclude municipalities from bringing enforcement actions pursuant to a statewide privacy law. There are several reasons for adopting this policy. *First*, municipality enforcement can upset a carefully thought-out statewide enforcement scheme pursued by the state attorney general.[56] *Second*, and relatedly, a patchwork of different enforcement policies within a state can make compliance for businesses more difficult, deterring innovation and economic growth.[57] *Third*, municipalities' incentives may not be aligned with state priorities. For example, municipalities may wish to pursue large settlements to make up for local budget constraints—an incentive that runs counter to evenhanded enforcement of privacy laws.[58]

Texas should preclude municipal enforcement, vesting exclusive enforcement authority with the Texas attorney general. As noted above, this approach is common in state privacy laws—including Texas's own biometric privacy law. Texas was also on the forefront of curbing municipality litigation generally when it passed HB 2826 in 2019. This law now requires any contingency fee arrangement between a private lawyer and a municipal government to be reviewed by the attorney general, who may refuse to approve an agreement that concerns a matter already being addressed by the state.[59] Unified privacy enforcement will similarly benefit consumers and businesses alike with a coherent and stable compliance regime.[60]

C. Texas Should Ensure That Privacy and Security Obligations for The Public Sector Do Not Stifle Data-Driven Innovation.

The RFI asks: "Are there laws in Texas, other states, or relevant jurisdictions which govern the public sector in the privacy and protection of information which should be considered by the Texas Privacy Protection Advisory Council?" While laws governing the public sector are less concerning than those broadly applied to the private sector, Texas should refrain from imposing laws that indirectly stifle innovation or undermine state competitiveness. For example, laws that unduly limit or hamper

---

[56] *Chamber ILR Toolkit*, at 28 ("Municipal enforcement creates a patchwork within a patchwork. Privacy law is already in danger of balkanization at the state level. Municipal approaches would splinter that even further.").

[57] *Id.*

[58] *Id.* at 27.

[59] Tex. Gov't Code Ann. § 2254.1038(a), (b)(3)(A) (requiring Attorney General approval for municipal contingency fee contracts for legal services and empowering Attorney General to refuse to approve such contracts if, *inter alia*, "the legal matter that is the subject of the contract presents one or more questions of law or fact that are in common with a matter the state has already addressed or is pursuing").

[60] *Id.* at 29.

specific technologies or services may place Texas—as a State or through its businesses—at a disadvantage.

D. Conclusion

If Texas decides to pursue a state privacy law, ILR encourages the legislature keep innovation front and center, and be guided by proven approaches and cautionary tales from other states. In particular, Texas should (i) preclude private rights of action, (ii) include notice and cure periods, (iii) offer safe harbors for compliance, (iv) cap civil penalties, (v) vest exclusive enforcement authority with the Texas attorney general, and (vi) curtail municipality litigation.

Respectfully Submitted,

Harold Kim
President
U.S. Chamber Institute for Legal Reform

Attachment: ILR, Mapping a Privacy Path: Liability and Enforcement Recommendations for States (Dec. 2019)