CompTIA

DATE: April 4, 2019

TO: House Committee on Business and Industry

FROM: Sarah Matz
Director, State Government Affairs
CompTIA

RE: **IT Industry Comments on HB 4390 and HB 4518**

On behalf of CompTIA and the nearly 2000 technology companies we represent, I appreciate the opportunity to share our perspective on HB 4390 and HB 4518, legislation that is modeled after the California Consumer Privacy Act (CCPA) and would establish requirements for businesses that collect consumers' personally identifiable information (PII).

Our member companies have long-understood the importance of protecting their users' privacy and securing the data they collect and store. Consumer trust equates to good business. But we also understand that despite the industry's best efforts, new privacy and data security laws are being considered here in the U.S. and around the world. However, while these laws were often developed with the best of intentions, they are more likely to result in significant compliance costs and stifled innovation than improving consumer protection.

We share the goal of ensuring consumer's privacy and protecting sensitive PII; however, we are concerned with legislation that replicates the CCPA as that law is not settled; was poorly drafted to include numerous ambiguities, definitional, and operational issues; and has the unintended consequence of weakening consumer privacy and increasing security threats. For these reasons, we respectfully suggest that the committee not move forward with the bill but continue with a measured and thoughtful approach by studying the issues with the CCPA and its evolution and continue the dialogue with impacted stakeholders.

Both bills appear to generally track the CCPA, a law that was quickly drafted and enacted in less than a week to avert the certification of a parallel ballot initiative on privacy. The consequence of this process in California, which left no room for meaningful public dialogue and stakeholder input before its swift enactment, is a law that includes provisions which may undermine privacy and data security and makes implementation and compliance needlessly confusing and costly. In fact, there are at least 19 additional privacy bills in the current California legislature that are adding to the confusion and regulatory burden for businesses.

Furthermore, the CCPA is a work in progress and by no means a model to pass in Texas or any other state. CCPA will not take effect until January 2020, is likely to be

amended further, and will be clarified in regulations promulgated by the California Attorney General. The date upon which enforcement can begin is not even set. The Attorney General may only begin enforcement six months after publication of the final rules issued pursuant to the Attorney General rulemaking or July 1, 2020, whichever is sooner. In short, we do not even know – and will not know for some time – what the CCPA will require once 2019 amendments and an Attorney General rulemaking are complete. This is creating both risk and uncertainty for companies that are doing business in California.

We are also concerned with the immense compliance burden for companies without necessarily improving consumer protection. For example, large U.S. companies have spent approximately $7.8 billion to comply with Europe's privacy law[1], the General Data Privacy Regulation (GDPR), while some smaller companies have chosen to cut off EU access to their services rather than spend the money necessary to comply[2]. With CCPA, companies operating in California are now likely to spend millions of dollars on compliance costs as compliance with GDPR does not mean a company is compliant with CCPA. It should be noted that the Texas bills are different enough from CCPA such that businesses would not be able to simply leverage the functionality built for California and apply it to operations involving Texas consumers. If a policy were enacted in Texas this year, we are concerned that some companies may be put in the difficult position to choose between compliance and ceasing operations in Texas, particularly if they're already dedicating resources to protecting data and user privacy.

Thank you for your thoughtful consideration of our concerns. The hugely complex and technical set of issues in California's privacy law, the basis for both Texas bills, need to be studied and refined far more precisely. It is for these reasons that we urge the Committee to not move forward with the bill at this time but to carefully consider if additional privacy requirements are needed.

About CompTIA

The Computing Technology Industry Association (CompTIA) is a leading voice and advocate for the $1.5 trillion U.S. information technology ecosystem and the 11.5 million technology and business professionals who design, implement, manage, market, and safeguard the technology that powers the U.S. economy. Through education, training, certifications, advocacy, philanthropy, and market research,

---

[1] Oliver Smith, The GDPR Racket: Who's Making Money From This $9bn Business Shakedown, Forbes, May 2, 2018, available at https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-fromthis-9bn-business-shakedown/#6c03c1e234a2.

[2] Nate Lanxon, Blocking 500 Million Users Is Easier Than Complying With Europe's New Rules, Forbes, May 25, 2018, available at https://www.bloomberg.com/news/articles/2018-05-25/blocking-500-million-users-is-easier-thancomplying-with-gdpr.

CompTIA is the hub for advancing the tech industry and its workforce. For more information, please visit comptia.org.