



DATE: February 23, 2016

TO: Joint Committee on General Law

FROM: Kevin Callahan
Director, State Government Affairs
CompTIA

RE: **IT Industry Comments in Opposition to Raised HB 5326**

Chairman Leone, Chairman Baram and members of the General Law Committee, my name is Kevin Callahan, and I respectfully submit this testimony on behalf of the Computing Technology Industry Association ("CompTIA").

CompTIA is a non-profit trade association representing the information technology industry. With more than 2000 member technology companies of all sizes, 3000 academic and training partners, and more than two million IT certifications issued, CompTIA is dedicated to advancing industry growth through educational programs, market research, networking events, professional certifications and public policy advocacy.

This legislation would broadly prohibit the capture and use of an individual's biometric identifier – specifically, a record of face geometry – by a business for "commercial purposes" unless the business has received the individual's consent. While intended to address privacy concerns, this bill raises some very complex questions about the collection of biometric identifiers by businesses and the ultimate use of this information. While CompTIA and our members share concerns about these issues, we are fearful that Raised HB 5326 is overly broad and impractical, and would result in the unintended consequence of slowing progress in bringing emerging technologies to consumers. We therefore must oppose this bill.

Companies collect biometric data to provide efficient and effective services to consumers to make their lives better and easier. Biometric data is commonly used by businesses for purposes such as authentication, which allows users to securely access and manage their online accounts, and identification, which makes it easier for a user to identify themselves or their friends in photographs posted online. Further, many features powered by facial recognition technology allow people to see when others have uploaded photographs of them online, and thus enhance user privacy by giving them an opportunity to contact the original uploader of the content, or the Internet service provider, if they wish to have the photo deleted from the Internet. As such, biometric data, and specifically facial recognition technology, can be invaluable in combatting human trafficking, child abductions, and improving online security.

While biometrics and facial recognition technology have changed the way we live, a misconception that is rooted in Raised HB 5326 is that notice and consent for the collection of biometric data can be achieved in all instances. This is often not the case, and there are many contexts in which it is impossible to provide clear and conspicuous notice to consumers. This

CompTIA

IT Industry Comments in Opposition to Raised HB 5326

February 23, 2016

Page | 2

may include newsgathering, security, or fraud prevention. For example, facial recognition technology used by a high security facility to verify the identity of a specific individual or when a casino uses facial recognition to identify a card-counter when they walk in the front door. While the facial recognition systems used at these locations may be different than those used by an online website or a retail establishment, these security providers, like websites and retailers, are using facial recognition for a "commercial purpose."

We believe that biometric regulation should balance the benefits of the technology with privacy concerns, and focus on real harm to consumers. Unfortunately, Raised HB 5326 fails to strike this balance. Instead of covering "commercial purposes," legislation should attempt to cover authentication purposes more specifically. The intent should be to assure that individuals are protected from harm in cases where biometric data is used for authentication. The confidentiality of someone's account authentication details is absolutely critical, and is deserving of strong protections, because the sale, sharing or breach of that data could bring great harm to the individual. We should be wary of regulating biometric data that only adds value to an individual's experience.

CompTIA is also concerned that stringent notice and consent requirements will hinder the innovation of other devices because the most promising biometrics technologies cannot incorporate a notice and consent interface. Many of the most promising online technologies currently in development – for example, technologies that make up the so-called "Internet of Things" – often do not have, and could not reasonably be expected to have, an interface to enable consumers to receive notice or provide consent. We believe it is crucial that any biometric regulation allow companies the flexibility in how they choose to notify consumers or enable control over consumers' biometric information.

While we oppose Raised HB 5326, it is important to note that efforts are being undertaken to ensure that consumers' have control, transparency, and security of their biometric data. Most notably, the Future of Privacy Forum, an influential Washington think tank that leads many national policy efforts on digital consumer rights, is already working to address privacy issues associated with facial recognition technology, and are actively convening key policymakers and other stakeholders to develop an industry code of conduct at the national level for companies that use facial recognition technology. Additionally, the Biometrics Institute, an international, independent non-profit organization, recently released updated guidance for how companies in a wide array of industries ranging from retail to banking should go about collecting and safeguarding increasingly prevalent biometric data. Recognizing the fast pace of innovation, the Biometrics Institute plans to update this guidance again in two years.

Thank you for the opportunity to share our perspective on this legislation. The commercial use of biometric identifiers inherently raises some type of privacy implications, but the appropriate approach to protecting consumer privacy is extremely case specific, and should be tied to harm. The type of consent sought by this legislation is impractical, and creates additional and unnecessary burdens that would impede the deployment of new and innovative technologies in Connecticut. For these reasons, CompTIA urges against moving forward with Raised HB 5326.