July 17, 2020

Rep. Aaron Michlewitz
Chair, House Committee on Ways and Means
24 Beacon St.
Room 136
Boston, MA 02133

Rep. Claire D. Cronin
Chair, Joint Committee on the Judiciary
24 Beacon St.
Room 243
Boston, MA 02133

Re: S. 2820 testimony opposing Section 65 ban on use of facial recognition technology

Dear Representatives Michelewitz and Cronin:

Thank you for the opportunity to provide input on S2820 as your committees consider this important legislation passed by the Senate. SIA is a nonprofit trade association representing businesses providing a wide range of security products and services across the U.S., including more than 23 companies headquartered or with major operations centers in Massachusetts.

We support legislation providing meaningful reforms to policing practices that would result in stronger community engagement, address inequities, and help ensure that the kind of tragic events like we have witnessed the past few months in our nation never happen again. However, we are concerned with inclusion of what should be considered an unrelated provision. Section 65 would ban any government entity in the Commonwealth from virtually any use of facial recognition technology, despite the potential for tremendous benefits when used effectively and responsibly.

Addressing concerns about public sector applications of this technology is a legitimate policy objective, building public trust by ensuring that it is only used for purposes that are lawful, ethical, and non-discriminatory. We support establishing the special commission as called for in the provision, to examine these issues and make policy recommendations. But there is little evidence use of the technology has contributed to racial profiling or the other systematic issues of primary concern in police reform that would justify a blanket ban.

Instead, for over a decade it has been used as a speed and accuracy enhancing tool in many thousands of investigations, to reduce human error and eye-witness misidentification, eliminate innocent persons as potential offenders, recover human trafficking victims and help crack cold cases.[1] In fact, many law enforcement agencies believe that it contributes to fairer and more effective policing, by potentially reducing the impact of human bias, and reducing unnecessary police to civilian contacts in communities impacted historically by a strained relationship with local police.

In any case, it is clear the ban on facial recognition included in S2820 is intended to address the public concerns about facial recognition technology regarding possible government uses that could raise privacy and civil liberties concerns. However, it would also ban many non-controversial public sector uses of the technology that do not raise such concerns. The purpose is often simply to help validate one's identity, with obvious benefits to

[1] https://www.securityindustry.org/2020/07/16/facial-recognition-success-stories-showcase-positive-use-cases-of-the-technology/

the users. Under the ban, hospitals and other health care facilities owned by state and local governments would be prohibited from using the technology, as others have, to reduce the need for frontline health care workers to touch surfaces in order to access to clean rooms and other secure facilities. The bill would also curb potential workplace safety enhancements for public employees and protections for building visitor and occupants, from:

- validating identities noninvasively and accurately when requiring access to secure facilities and systems
- speeding employee entry through security checkpoints, preventing lines where people are clustered in proximity
- protecting the sensitive citizen data often held by government entities, by helping ensure only authorized persons are permitted access
- increased security at checkpoints of buildings such as courthouses, were both workers and visitors face threats
- integration with building controls for HVAC, fire alarm and emergency communications systems that increase occupant safety and achieve other goals like increased energy efficiency

Accordingly, we urge you to amend Section 65 to:

- ***Alternatively, establish conditions or limitations that apply to specific uses of the technology*** to address potential risks, versus a blanket ban that would also eliminate most benefits for citizens in the Commonwealth.
- ***Provide an additional exception for non-controversial uses in building systems.*** The provision already provides an exception from the ban for personal electronic devices. Similar to how it is commonly used to unlock an electronic device, facial recognition enabled access control systems allow an authorized user to unlock a door or to access a secured area.

Lastly, some discussions about banning the technology have centered around the potential for negative impact on women and minorities from “bias” in the technology. It is critically important to use high performing products. Industry is striving to provide technology that is as effective and accurate as possible across all types of uses, deployment settings. The National Institute of Standards and Technology (NIST), the world’s leading authority on this technology, found last year that the highest performing technologies had “undetectable” differences across demographic groups, while most others performed far more consistently than had been widely reported in the media and a number of non-scientific tests.[2]

On behalf of SIA and its members, we urge the Committees to closely reevaluate Section 65, and seek alternative ways to address concerns about facial recognition without unnecessarily limiting the benefits of this critically important technology. Please let us know if we can provide further information or assistance.

Jake Parker
Senior Director, Government Relations
Security Industry Association
301-804-4722
jparker@securityindustry.org

[2] https://www.securityindustry.org/report/what-nist-data-shows-about-facial-recognition-and-demographics/