May 3, 2017

The Honorable Hannah-Beth Jackson
California State Senate
State Capitol, Room 2032
Sacramento, CA 95814

SUBJECT: **SB 327 (Jackson) Information Privacy: Connected Devices**
OPPOSE – AS AMENDED March 20, 2017

Dear Senator Jackson,

On behalf of the Security Industry Association (SIA), we must respectfully oppose CA SB 327, *The Teddy Bear and Toaster Act,* which imposes heavy burdens on manufacturers and sellers of devices, sensors, and equipment capable of connecting to the internet. SIA is an international non-profit trade associations representing approximately 800 companies that manufacture and integrate electronic equipment used in security, life safety and many other applications. We are concerned that the enactment of SB 327 would result in overly broad applications of ill-defined mandates related to data security and notification to manufacturers and sellers of devices, sensors, and equipment capable of internet connectivity.

Based upon the bill's title, *The Teddy Bear and Toaster Act,* SB 327 appears to be geared towards household consumer items and toys. However, the bill's requirements as written would apply to a nearly limitless array of devices that can connect directly or indirectly to the internet, including components of commercial and industrial systems. Connected devices allow systems and equipment to perform better, smarter and in a more coordinated fashion, which benefit Californians in many ways, especially by making security and life safety systems more effective. Networked sensors are already improving the effectiveness of such systems in the consumer, commercial and government arenas by providing real-time connectivity and data collection.

SB 327 outlines notification requirements which mandates manufacturers to design connected devices with visual, auditory, or other indicators to show once the devices are "collecting personal information." This provision could present burdensome implications for internet of things (IoT) technologies utilized in Smart Home, Smart City, and Smart Building applications. For example, a growing amount of life safety equipment – i.e. thermostats; fire sprinkler and suppression systems; emergency lighting; video cameras; carbon monoxide, smoke and fire detectors; access control portals; and residential security systems – are interconnected either directly or indirectly through the internet. If subjected to continuous notification requirements, the core functions of these systems could be disrupted and additionally, it could threaten interoperability between connected devices.

SB 327 also imposes misplaced point of sale requirements on retailers selling connected devices to California consumers. Sales representatives would be required to apprise potential consumers of connected devices' information collection capabilities, applicable privacy policies, and security

patches and features associated with the device. In the event of any miscommunication between the manufacturer and seller, along with legal action authorized against "person(s)" not complying with the point of sale requirements, the bill increases liability risks against/between connected device manufacturers and sellers – the possibility of which inevitably increases barriers to innovation.

The prescriptive requirements in the bill could preclude the ability of our member companies to find innovative ways to address security and privacy considerations throughout the life cycle of connected devices under principles of "security by design" and "privacy by design" and development of industry best practices. Inevitably, given the pace of technology development, setting such prescriptive requirements in statute means both principles will eventually become obsolete and perhaps even counterproductive to their original purpose.

Failures to protect privacy or ensure security can be addressed under existing California law, Civil Code Sec. 1798.81.5(b), which requires businesses that own, license or maintain personal information about California residents to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." If enacted, SB 327 creates a duplicative section of law that would not only generate confusion within our member companies conducting business in California, but also increase risk of frivolous lawsuits.

SB 327 regulatory requirements directly conflicts with the objectives cited in the U.S. Department of Commerce Green Paper entitled, *Fostering the Advancement of the Internet of Things*. Prior to the Green Paper's publication, the U.S. Department of Commerce requested public comment on what steps the U.S. government must take to enable IoT growth, such as convening private-public working groups, creating the necessary infrastructure that creates a robust IoT ecosystem, and promulgate industry-supported policies – not regulations. As noted in the Green Paper, due to the nascent stage of IoT technologies, legislation that creates premature regulations will undoubtedly hinder IoT growth and consequently stifle innovation.

For these reasons, we must respectfully oppose SB 327. Please let us know if SIA or its members can provide information or any other further assistance to you and your colleagues in the legislature as you consider these important issues.

Sincerely,

Don Erickson
CEO
Security Industry Association

cc: Members, Senate Judiciary Committee