April 9, 2019

The Honorable Ed Chau, Chair
Assembly Privacy and Consumer Protection Committee
State Capitol Building, Room 5016
Sacramento, CA 95814

Re: AB 1163 (Eggman) - Electronic Products Manufacturers Opposition

Dear Chairman Chau:

On behalf of the hundreds of manufacturers and businesses our organizations represent, we respectfully oppose AB 1163 by Assembly Member Eggman, legislation which would mandate original equipment manufacturers (OEMs) of digital electronic equipment or a part for the equipment sold in California to provide independent repair providers with diagnostic and repair information, software, tools, and parts.

Our organizations represent a broad spectrum of manufacturers of consumer electronics, home appliances, HVACR, security equipment, medical devices, toys, lithium ion batteries, and other connected electronic products as well as companies that rely on the secure operation of these devices such as entertainment software publishers. All of these companies stand behind the quality of their products. Our members develop products and services for a wide range of commercial, government, and consumer users that are often highly regulated. Their customers depend on these products to operate safely, securely, and accurately, whether they are being used to support banking and commercial transactions, transmit and store sensitive personal data, support industrial operations, medical applications, or securely deliver entertainment and other services. As businesses, government agencies, and consumers continue to increase their reliance on connected devices to help deliver efficiency, convenience, and services, it is important to remain vigilant and focused on mitigating the risks associated with the safe and secure operation of those products.

AB 1163 mandates that OEMs provision any independent repair provider in much the same way as authorized network providers, but without any contractual protections, requirements, or restrictions, and in doing so, places consumers and their data at risk, undermines the business of California companies that are part of OEM-authorized networks, and stifles innovation by putting valuable intellectual property in the hands of hundreds if not thousands of new entities. Further, the bills fail to account for the wide range of repair and refurbishment options currently available to California consumers from both OEM-authorized and independent repair sources as well as advancements in

sustainability by electronic product manufacturers. For these reasons, we urge the Assembly against moving forward with this legislation.

AB 1163 threatens consumer security and safety

One of our chief concerns with this legislation is its potential to weaken the privacy and security features of various electronic products. The security of user information on these products is of the utmost importance to consumers that rely on them. Industrial equipment, home appliances, smartphones, computers, servers, consumer electronics, medical devices, and other software-enabled connected devices are at risk of hacking, and weakening of the consumer privacy and security protections of those products. With access to proprietary guides and tools, hackers can more easily circumvent security protections, harming not only the product owner but also everyone who shares their network. We are concerned that mandating disclosure of sensitive proprietary tools and information may make device manufacturers an enticing target for malicious behavior. Bad actors could seek to exploit compliance requirements for illegal purposes, such as circumventing digital locks protecting copyrighted content and/or making unauthorized modifications. This problem would be compounded if those bad actors share details on how to exploit this proprietary information (such as posting on the internet), which could be replicated by others.

Consumers, businesses of all sizes, public schools, hospitals, banks, and industrial manufacturers all need reasonable assurance that those they trust to repair their connected products will do so safely, securely, and correctly. State law should not mandate that all manufacturers must provide a "how to" manual for any product and provide it to anyone who asks.

Manufacturers offer authorized repair networks to provide consumers with assurance that their products are serviced by properly trained and vetted repair professionals that have the necessary skills to safely and reliably fix software-enabled products. Some types of repairs can be extremely detailed,, because of the integrated network of software programs found in modern devices. It is particularly important that products containing high-energy lithium ion batteries are repaired only by trained professionals who understand the hazards associated with these batteries.

Manufacturers want to ensure that their products are serviced by professionals who understand the software that operates their products and heave spent time procuring the knowledge necessary to safely repair and return it to the consumer without compromising those standards or undermining critical safety and security features (such as technological protection measures). Authorized repair networks not only include training requirements, but also ensure that only the correct parts and procedures will be used. Consumers can be protected by warranties or other means of recourse. The legislation provides no such protections for consumers, repair shops or manufacturers.

When an electronic product breaks, consumers have a variety of repair options, including using an OEM's authorized repair network, which often include local repair service providers as well as mail-in, and even in-house repair options for some categories of products. Consumers may also choose to use one of many independent repair service providers; although they do so without the quality assurance provided by using a manufacturer's authorized network provider. The point is that the free market economy already provides a wide range of repair choices without the mandates imposed by this legislation.

Manufacturer authorized networks of repair facilities guarantee that repairs meet OEM standards. If an OEM's brand and warranty are to stand behind repair work and assume product liability, it is only

reasonable that the repair facility demonstrates competency and reliability. Without the training and other quality assurance requirements of authorized service providers – implemented through enforceable legal contracts that ensure compliance and accountability that protect consumers – manufacturers would not be able to stand behind their work, warranties, technical support, ongoing training, and business support.

AB 1163 mandates the disclosure of protected proprietary information

Manufacturers make significant investments in the development of software, products and services, and the protection of intellectual property is a critically important aspect of sustaining the health of the vibrant and innovative technology industry. However, AB 1163 puts at risk the intellectual property that manufacturers have developed.

Consumer electronics now contain a sophisticated integrated package of software that make the product perform thousands of tasks based on the manufacturers' intent. Virtually all modern electronics contain an operating system, middleware (software that lies between an operating system and the applications running on it), firmware (software programs permanently etched into the device's hardware), and digital rights management software (the DRM, aka, "digital locks" that control the use, modification, and distribution of copyrighted works such as software and multimedia content). Software programs are copyrightable subject matter under federal law, and Section 1201 of the Digital Millennium Copyright Act ensures that bad actors cannot tamper with the digital rights management that copyright owners use to protect this software. Granting independent repair shops (i.e., those not authorized by the manufacturer) the tools and know-how to modify the various software programs to restore functionality may expose the devices' security features to potential tampering, including disabling or removal of the digital locks.. This action may well be in violation of federal law if done without the permission of the copyright owner (subject, of course, to the rules and regulations of the US Copyright Office and the Library of Congress).

Importantly, however, firmware controls many other product functions, and opening it up for repair purposes exposes to potential tampering other, more sensitive functions, such as security features. Given the scope of products covered and what must be provided under the legislation – including diagnostics, tools, parts, and updates to software – it is highly likely some of that information would be proprietary. Providing unauthorized repair facilities and individuals with access to proprietary information without the contractual safeguards currently in place between OEMs and authorized service providers places OEMs, suppliers, distributor and repair networks at risk on many levels.

AB 1163 fails to account for advancements in sustainability by electronic products manufacturers

AB 1163 is based on an inaccurate assumption, specifically that there is a "growing quantity of e-waste" in California. However, CalRecycle data on implementation of the *Electronic Waste Recycling Act of 2003* show California e-waste not growing but rather declining since 2012[1]. According to the Rochester Institute of Technology Golisano Institute of Sustainability, in the U.S. e-waste generation

[1] CalRecycle (February 2017). *Update on California's Covered Electronic Waste Recycling Program Implementation of the Electronic Waste Recycling Act of 2003*. Accessed at: http://www.calrecycle.ca.gov/electronics/CEW/ProgramStats.pdf

peaked in 2013-2014 and is in a period of extended decline[2]. This trend is corroborated by the most recent data from U.S. EPA[3].

Electronic products manufacturers have developed robust policies and programs to ensure that they are continuously improving the sustainability of their products for their whole lifecycle, from design, to material sourcing, product performance, reuse, and responsible end of life management. This has led to continued innovation and the use of new technologies which provide consumers improved devices while simultaneously reducing the overall amount of e-waste generated – all under the existing product repair environment. And with new technologies like OLED and additional light-weighting across the electronics industry, additional declines in e-waste generation are expected to continue during the coming decades.

Repair and reuse are important elements of electronics manufacturers sustainability efforts. Not only is repair and reuse in the OEM's best interest so that consumers can continue to use and enjoy their products, but many OEMs are returning still-useful electronic products to active service to get the maximum benefits out of the resources used to make them. Additionally, under revised "green" procurement standards set to go into effect this year, federal agencies and other purchasers will be required to purchase computers that meet certain environmental performance criteria under the Electronic Product Environmental Assessment Tool (EPEAT) rating system. These existing policies and programs promote repair and reuse without the consumer safety, security, or business concerns raised by AB 1163.

Conclusion

Thank you for your consideration of our perspective on this complicated issue. Our members bear a significant responsibility to the businesses, governments, and individual consumers that depend on us to protect the integrity of their electronic products, as well as the proprietary software they contain. We are committed to working with you to promote digital privacy and security, while resisting unwarranted state intervention in the marketplace with one-size-fits-all mandates that compromise consumer safety and protection. For these reasons, we oppose Assembly Bill 1163.

Sincerely,

Air Conditioning, Heating and Refrigeration Institute (AHRI)
Association of Home Appliance Manufacturers (AHAM)
Bay Area Council
California Chamber of Commerce (CalChamber)
California Technology & Manufacturers Association (CMTA)
Computing Technology Industry Association (CompTIA)
Consumer Technology Association (CTA)
CTIA – The Wireless Association

[2] Rochester Institute of Technology Golisano Institute of Sustainability (July 2017). *Sustainable Materials Management for the Evolving Consumer Technology Ecosystem*. Accessed at: https://www.rit.edu/gis/ssil/docs/Sustainable%20Materials%20Management%20for%20the%20Evolving%20Consumer%20Technology%20Ecosystem.pdf

[3] Office of Resource Conservation Recovery, U.S. Environmental Protection Agency (December 2016). *Electronic Products Generation and Recycling in the United States, 2013 and 2014*. Accessed at https://www.epa.gov/sites/production/files/2016-12/documents/electronic_products_generation_and_recycling_2013_2014_11282016_508.pdf

Entertainment Software Association (ESA)
Information Technology Industry Council (ITI)
Internet Coalition
National Electrical Manufacturers Association (NEMA)
NetChoice
PRBA – The Rechargeable Battery Association
Security Industry Association (SIA)
State Privacy and Security Coalition, Inc.
Silicon Valley Leadership Group (SVLG)
TechNet
Telecommunications Industry Association (TIA)
The Toy Association

CC: Members, Assembly Privacy and Consumer Protections Committee
The Honorable Susan Talamantes Eggman
Nichole Rapier Rocha, Consultant, Assembly Privacy and Consumer Protection Committee
Jared Yoshiki, Assembly Republican Caucus Consultant