TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Northeast | Telephone 774.230.6685
One Beacon Street, Suite 16300, Boston, MA 021081
www.technet.org | @TechNetNE

February 3, 2021

The Honorable Senator Delores G. Kelley, Chair
Senate Finance Committee
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

Re: TechNet Opposition to SB 412 – Repair Legislation

Dear Chair Kelley,

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. Our diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over three million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

Thank you for the opportunity to provide feedback on SB 412, legislation which would mandate original equipment manufacturers (OEMs) of digital electronic equipment or a part of the equipment sold in Maryland to provide independent repair providers with comprehensive diagnostic and repair information, software, tools, and parts.

TechNet respectfully opposes this legislation. This is a complex issue that extends far beyond the stated intent of providing access to parts, tools, technical manuals, and software to a broad range of electronic products. TechNet and its members are concerned that this legislation would have the potential for troubling, unintended consequences, including serious cybersecurity, privacy, and safety risks.

Technology companies have every incentive to ensure that their customers have ample opportunity to get their products repaired – in fact, our brands depend on being able to provide superior customer service. Currently in Maryland, consumers in all corners of the state have the opportunity to have their devices repaired in a variety of locations and price points. It is imperative that technology companies be able to manage their repair networks in order to provide safe and effective repairs.

Our member companies maintain extensive networks of authorized repair partners that are well-trained and highly qualified to safely and securely repair or refurbish their products. Any repair shop can apply to become an authorized repair provider at

no cost to the repair person. Repairs and refurbished products from authorized partners ensure that a product is safe, secure, and meets factory specifications, including the most recent software updates and other improvements. This is the quality control and accountability consumers expect and deserve.

Proponents of these bills will level claims that electronic products are not getting recycled. On the contrary, electronic product manufacturers design policies and programs to ensure that they are continuously improving the sustainability of their products and reducing the overall amounts of e-waste generated. In fact, a recent independent study led by a researcher at the Yale School of the Environment's Center for Industrial Ecology, and published recently in the Journal of Industrial Ecology, has found that the total amount of electronic waste generated by Americans has been declining since 2015.

These bills also create significant safety and security concerns. Most consumer electronics use lithium ion batteries, which are small, powerful, and efficient. This enables the design of thinner and lighter portable electronics. Lithium ion batters may pose serious safety risks if they are not designed, manufactured, and installed properly. Enabling untrained and unauthorized third parties to open devices and replace lithium ion batters or other high-risk components, without adequate training, may result in serious and entirely avoidable injuries or destruction of the device. Leased equipment also presents potential financial liabilities. Many consumers choose to rent expensive equipment from service providers as a cost-saving measure, but could be responsible for the full cost of the product if improper repair results in destruction of the device.

Further, individuals keep a wealth of sensitive personal data on their devices. It is essential each repair person is properly trained in how to not only repair the device, but also establishes a relationship with the manufacturer in order to create an accountability link to protect consumers. If a consumer drops their electronic device off at a repair shop, they ought to be granted some level of security and recourse in the unfortunate circumstance that their data is compromised.

Enabling untrained and unauthorized third parties to replace and repair device components can result in the disabling of key hardware security features, and can impede the update of firmware that is important to device security and system integrity. A security breach of one device can potentially compromise the security of a platform or other connected devices in a network. It is essential to protect consumers from the introduction of malware and potential cyber-security risks and tampering concerns that unauthorized repair can lead to.

Right to Repair legislation has been introduced and defeated in over 20 states across the country because it would have allowed unrestricted access to digital keys and proprietary information for thousands of internet-connected products including smart phones, televisions, fire alarms, Wi-fi routers, computers and more. The minimal

benefits of allowing access consumers to this information is greatly outweighed by the privacy and safety risks.

We fear that once a manufacturer loses control of their ability to repair the devices they alone develop and produce, their intellectual property is at enormous risk. A government mandate would force manufacturers to reveal sensitive technical information about their products, including source code, and proprietary parts and tools. This presents a security risk for the use of a product, the network, and other devices connected to the network, and could allow for tampering with firmware controls that protect copyrighted works.

Thank you for your consideration of this testimony. Please do not hesitate to contact me if I can provide any additional information.

Sincerely,

Christopher Gilrein
Executive Director, Massachusetts and the Northeast
TechNet
cgilrein@technet.org