



Consumer
Technology
Association™

ctia™



NetChoice

INTERNET
COALITION



 **repair done right**

September 27, 2024

Chairman Scott Conklin
Members, Pennsylvania House Commerce Committee

Re: Electronics Manufacturers Opposition to HB 2535

Dear Chairman Conklin and Committee Members:

On behalf of the hundreds of manufacturers and businesses our organizations represent, we respectfully oppose HB 2535, legislation which would mandate original equipment manufacturers (OEMs) of digital electronic equipment sold or used in Pennsylvania to provide independent repair providers with diagnostic and repair information, software, tools, and parts – but without requiring any of the critical consumer protections afforded by authorized repair networks, such as training and competency certification, and putting at risk protections manufacturers have built in for consumer data privacy and security. Without any vetting process for qualified repair facilities, the potential for consumer harm is significant and undermines the innovations manufacturers have developed to protect customers. Additionally, we have concerns that this legislation would assist in establishing a “patchwork” of repair legislation in the states, thus creating a burdensome and contradictory compliance regime for members of industry. Industry has attempted to work with advocates on numerous occasions to develop a national memorandum of understanding, but our efforts have been repeatedly rebuffed. It appears their preference is to relitigate this issue on a state-by-state basis, which will inevitably result in a costly, confusing, and onerous compliance patchwork.

Our organizations represent a broad spectrum of manufacturers of home appliances, consumer electronics, HVACR, security equipment, toys, lithium-ion batteries, and other connected electronic products, as well as companies that rely on the secure operation of these devices. 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. 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 offer and 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.

HB 2535 mandates that OEMs treat any independent repair provider in much the same way as authorized network providers – but without any contractual protections, requirements, or restrictions. In doing so, the bill places consumers and their data at risk, undermines the business of Pennsylvania companies that are part of OEM-authorized networks, and stifles innovation by putting hard-earned intellectual property in the hands of hundreds, if not thousands, of new entities. Further, the bill fails to account for the wide range of repair and refurbishment options currently available to Pennsylvania consumers from both OEM-authorized and independent repair sources. It also does not address advancements in sustainability by electronic product manufacturers.

For these reasons, we urge the committee against moving forward with this legislation without addressing these identified issues.

HB 2535 harms consumer security

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. Computers, tablets, and smartphones are at risk of hacking, and weakening of the privacy and security protections of those products will increase risks to consumers. With access to technical information, criminals can more easily circumvent security protections, harming not only the product owner but also everyone who shares their network. In an era of sophisticated cyberattacks, we should not make it easier for criminals to hack security provisions.

Forcing OEMs to provide unauthorized repair facilities with information on how to bypass consumers' safety locks presents unacceptable risks to consumers' data privacy. [A recent study](#) found that privacy violations already occur when consumers seek computer or phone repairs, with technicians accessing female customers' personal data at a higher rate than males. Without the contractual safeguards created by authorized repair networks that allow OEMs to hold bad actors accountable, HB 2535 will merely create new opportunities for snooping repair technicians to access and copy consumers' personal data.

HB 2535 harms consumer safety

Manufacturers offer authorized repair networks to provide consumers with assurance that their products are serviced by properly trained and vetted repair professionals who have the necessary skills to safely and reliably repair electronic products.

Most consumer technology products are comprised of complex electronics which require specialized training and sophisticated test instruments to repair safely. Some types of repairs can be extremely detailed, complicated, and dangerous to anyone without proper training. It is particularly important that products containing high-energy lithium-ion batteries are repaired only by trained professionals who understand and mitigate the hazards associated with installing, removing or replacing these batteries. In January 2021, the U.S. Consumer Product Safety Commission released a consumer safety warning that rechargeable lithium-ion battery cells, when they are “loose” and not installed in a device or part of an integral battery, are “potentially hazardous to consumers when handled, transported, stored, charged, or used to power devices” and “can overheat and experience thermal runaway, igniting the cell’s internal materials and forcibly expelling burning contents, resulting in fires, explosions, serious injuries and even death.”

Manufacturers want to ensure that their products are serviced by professionals who understand the intricacies of their products and have spent time procuring the knowledge necessary to safely repair them and return them to consumers without compromising those standards or undermining the safety and security of their products. Authorized repair networks not only include training requirements but also have the technical skills and test instruments to verify that repair parts meet all necessary performance and safety specifications. 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 professional 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 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 provides a wide range of consumer choice for repair with varying levels of quality, price, and convenience without mandates imposed by the legislation.

Manufacturers’ authorized networks of repair facilities guarantee that repairs meet OEM performance and safety 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,

manufacturers would not be able to stand behind their work, warranties, technical support, ongoing training, and business support.

HB 2535 mandates the disclosure of protected proprietary information

Manufacturers make significant investments in the development of products and services, and the protection of intellectual property is a legitimate and important aspect of sustaining the health of the vibrant and innovative technology industry. However, HB 2535 puts at risk the intellectual property that manufacturers have developed.

Consumer electronics' on-board software (i.e., firmware) are key to the functioning and operation of the hardware it is embedded in, and firmware helps protect against unauthorized access to other software and applications. That software is subject to copyright under federal law, and Section 1201 of the Digital Millennium Copyright Act, a related federal law, ensures that bad actors cannot tamper with the digital rights management that copyright owners use to protect this software. The problem is that making repairs to hardware components may require the circumvention of digital rights management and leave the software in an unprotected state – harming the copyright owners of the software.

Firmware controls many other product functions, and opening it up for repair purposes exposes other more sensitive functions, such as security features, to potential tampering. 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 the 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, distributors, and repair networks at risk.

HB 2535 fails to account for advancements in sustainability by electronic product manufacturers

The bill is partly based on an inaccurate assumption that the bill will aid in the reduction of electronic waste in the state of Pennsylvania. According to a recent study by Yale and Rochester Institute of Technology researchers, e-waste generation in the U.S. peaked in 2015 and is in a period of extended decline (see "[Electronic Waste on the Decline, New Study Finds](#)"). This trend is corroborated by the most recent data from the U.S. Environmental Protection Agency whose [data](#) shows consumer electronics as the fastest declining part of the municipal solid waste stream.

Electronic product 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 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, 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 the bill.

Conclusion

Thank you for considering 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 safety and security of their electronic products, as well as the sensitive data that they contain. We are committed to working with you to promote digital privacy and security, while resisting unwarranted intervention in the marketplace with one-size-fits-all mandates that compromise consumer safety and protection. Many of the members of our coalition have already taken measures to ensure consumers have numerous options for repairing their devices and appliances. For those reasons, we oppose HB 2535.

Sincerely,

Air Conditioning, Heating and Refrigeration Institute (AHRI)
Consumer Technology Association (CTA)
CTIA – The Wireless Association
Internet Coalition
Medical Imaging & Technology Alliance (MITA)
National Electronic Manufacturers Association (NEMA)
NetChoice
PRBA – The Rechargeable Battery Association
Repair Done Right
TechNet
Telecommunications Industry Association (TIA)