State Privacy and Security Coalition, Inc.

January 22, 2018

The Honorable Gregory D. Habeeb
Chair, Subcommittee #2
Virginia House Commerce and Labor Committee
Pocahontas Building, Room E302
900 East Main Street
Richmond, Virginia 23219

Subject: HB 20 – Electronic Products Manufacturers Opposition

Dear Chair Habeeb,

On behalf of the hundreds of manufacturers and businesses our organizations represent, we appreciate the opportunity to share our perspective on HB 20, legislation that would mandate original equipment manufacturers (OEMs) of digital electronic products sold in Virginia to make available those products' diagnostic and repair information, software, tools, and parts to independent repair facilities and product owners.

Our organizations represent a broad spectrum of consumer electronics and home appliance manufacturers that 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 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.

We believe that, if enacted, this legislation would lead to grave unintended consequences to the operation, security and safety of those products. Agreements between OEMs and authorized repair networks, which include businesses of all sizes, would be undermined and provide no protection or quality assurance for consumers. Further, such legislation mandates the disclosure of proprietary information that may violate federal copyright protection and state trade secrets laws. Finally, numerous options are already available to consumers to repair their products, and thus the legislation is unwarranted. For these reasons, we urge the General Assembly against moving forward with this legislation.

The legislation 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 connected devices 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 cyber attacks, we should not make it easier for criminals to hack security provisions.

Consumers, small businesses, large businesses, public schools, hospitals, banks, and industrial manufacturers all need reasonable assurance that those they trust to repair their connected devices 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 repair electronic products. Some types of repairs can be extremely detailed, complicated, performed in someone's home, and, in some cases, dangerous to perform for those without proper training. 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 the product and return it to the consumer without compromising those standards or undermining the safety and security of their products. Authorized repair networks not only include training requirements, but also ensure that only the correct parts and procedures will be used. Consumers are 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 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 consumer choice for repair with varying levels of quality, price and convenience 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.

This legislation 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, this legislation puts at risk the intellectual property that manufacturers have developed.

Consumer electronics use on-board software (i.e., firmware) to help control the product. That firmware 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 necessitate modifying the firmware so that the product will work again.

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.

Conclusion

Thank you for your consideration of our perspective on this issue. We 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 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.

Sincerely,

Northern Virginia Technology Council (NVTC)
Virginia Chamber of Commerce
Virginia Manufacturers Association
Air Conditioning, Heating and Refrigeration Institute (AHRI)
Association of Home Appliance Manufacturers (AHAM)
Computing Technology Industry Association (CompTIA)
Consumer Technology Association (CTA)
CTIA – The Wireless Association
Entertainment Software Association (ESA)
Information Technology Industry Council (ITI)
Internet Coalition
National Electrical Manufacturers Association (NEMA)
NetChoice
Security Industry Association (SIA)
State Privacy and Security Coalition, Inc.
TechNet
Telecommunications Industry Association (TIA)
The Toy Association