Dr. Richard Forno, Senior Lecturer, UMBC, and Dr. Avi Rubin, Professor, Johns Hopkins University

Testimony for SB0412

Senate Finance Committee, Wednesday, Feb. 3, 2021

Consumer Protection - Right to Repair

POSITION: FAVORABLE

Members of the Senate Finance Committee, it is our honor and pleasure to offer some insights into SB0412 regarding a consumer's ability to repair technology products. The comments expressed in this statement reflect our own views and not necessarily those of UMBC or Johns Hopkins University.

We are writing to express enthusiastic support for SB0412, which requires fair access to parts, tools, service information and repair software. This legislation is a common-sense step that among other things, cuts consumer costs and decreases harmful electronic waste. As recognized experts in cybersecurity, we wish to assure you that the provisions of this bill will not put citizens, businesses or public sector organizations at greater risk of cyber attack. If anything, failing to pass it may place them at greater risks, some of which we describe below.

No Cybersecurity Risk In Third-Party Repair

You have been told by manufacturers and industry lobbyists that digital right to repair bills such as the one you are considering creates cybersecurity risks that will lead to hacks, data theft and other undesirable outcomes. In this and other state houses, these industry representatives continue arguing that asking manufacturers to make available to customers the same schematic diagrams and diagnostic tools that they already supply to their authorized repair partners is a security risk that is not worth taking.

We shall be blunt: these claims *simply are not true.*

How do we know? Let's state the obvious: because we have no digital "right to repair" today. What we do have is an epidemic of cyberattacks and compromises of connected electronic devices and Internet of Things products. Malicious networks composed of hacked home routers, webcams and other devices, can be linked together to form vast, global networks that become platforms to launch a range of malicious activities such as denial of service attacks and stealing confidential personal or business information. And outside of the Internet of Things (IoT) and cybersecurity, devices like mobile phones, computers, televisions, home appliances, and even cars are becoming increasingly more anti-consumer, essentially transformed into proprietary 'black boxes' that *only* the manufacturer can diagnose and fix things in. Sadly, new cyber incidents, vulnerabilities, and exploits in these devices are reported on an almost weekly basis.

In most cases, the manufacturers of these devices have not disclosed technical information or diagnostic codes that allow cyber criminals to cause mischief. No – today's home electronics, from televisions and refrigerators to baby monitors, smart doorbells, speakers, and more come off the assembly line and ship to customers with software vulnerabilities such as a common administrative password that the user is unable to change on their own, or poorly implemented software designs. Meaning, **when products get 'hacked' it most likely happened without the attacker having any proprietary knowledge provided by the vendor.** Unfortunately, at the moment, without such knowledge, customers, users, operators, and drivers are unable to take steps on their own or work with knowledgeable third parties to protect themselves from such attacks when reported and disclosed.

Creating the Digital 'Company Town'

To us, **concerns over 'hacking' and cybersecurity are not the real issue driving industry resistance to the Right to Repair.** Rather, many technology vendors want to create the digital equivalent of the antiquated 'company town' concept where they, *and only they*, provide the goods, services, and support for its citizens. In the modern digital world, that socioeconomic model creates a single point of failure and vulnerability for individuals and business alike. Would you want to tell the Maryland family farmers that the *only* way their tractors and farm equipment can be serviced is by a Deere employee and not the experts employed by a local small business garage? We wouldn't. Would you want to tell these same family farmers that their digitally enabled farm equipment cannot be used indefinitely - even with reduced functionality - and *must* be updated or replaced on the manufacturer's timeline and not theirs, thus forcing customers to spend money needlessly? Again, we wouldn't. As we will describe, such **hypothetical examples represent an anti-consumer, anti-business, anti-environmental situation that puts vendor profits and consumer lock-in above all else.**

Let's put this in a context we all can relate to: In 2020, Covid-19 shut down stores around the country. If you owned a Google Pixel phone and you break the phone's screen or camera, the only way you're able to get the device serviced without voiding the warranty is to send it back to Google or drop it off at a location operated by Google's sole authorized service partner.[1] Customers can't simply bring their phone to a local electronics store to diagnose or fix serious problems themselves or obtain replacement parts without risking voiding their warranty.[2] Making this more problematic is that many modern electronics vendors often intentionally design their products in ways that require proprietary tools and software to access and/or repair - and in some cases, consider any 'non-genuine' replacement parts to be faulty, substandard, or otherwise problematic, even if they're not. Companies across industry sectors, from electronics to farm machinery, take similar anti-consumer, anti-competitive approaches in designing products that lock customers and third-party experts out as well. Moreover, situations like Covid-19 may close vendor stores or authorized repair centers, further leaving customers in a precarious situation if they need immediate assistance with diagnosing or servicing a product. **This set-up directly impacts the independence and resiliency of Marylanders by restricting their ability to fix critical products used in their lives and businesses in a timely manner – and potentially at a better price.**

Mobile phones are but one example. Think about how difficult it is to repair or service automobiles, televisions, home appliances, farm equipment, and other devices these days without the vendor's direct assistance. Increasingly, these devices and vehicles are *only* serviceable by the vendor or vendor authorized entities, of which there may be few if any, such as a company's own store or dealership. Unfortunately, to use these products, customers often 'agree' to this dependency by accepting the terms of service licensing agreements -- which are lengthy, densely worded documents that few if any actually take the time to read, let alone understand.[3] **Forcing such a fragile dependency on customers has *nothing* to do with enhancing cybersecurity but everything to do with reinforcing a vendor's ability to create greater customer lock-in and revenue-generating dependence** on them for servicing these devices - while simultaneously limiting a customer's ability to challenge this one-sided situation.

Even worse, consumers are particularly vulnerable when vendors decide to no longer support a given product and force consumers to upgrade. And then *those* upgrades may require other upgrades in their information ecosystem, too. Consider when you upgrade your Microsoft Windows operating system -- oftentimes you must also upgrade most, if not all, of the other software, and even attached items like printers, used on that computer to ensure compatibility. The same can happen with items ranging from IoT devices to automobiles, appliances, or farm equipment, because there are technical dependencies everywhere. Consequently, **consumers become the victims**, trapped in a perpetual cycle that needlessly costs them time, money, productivity, independence – and resiliency.

Of course, industry will argue that the opposite is true: that the security of the software that runs their devices and the integrity of their customers' data is their 'top priority'. Yet based on their actions, there

simply is not any evidence that these industry claims are true. If anything, **industry's opposition to the Right to Repair is a matter of ensuring consumer dependence on them as the sole source of support for those products.**

So what to do? In exploring this issue, we encourage you to listen closely to what cybersecurity experts, academics, independent researchers, end-users, and customers say, rather than just what industry lobbyists claim. Groups like the Electronic Frontier Foundation, SecuRepairs, and the Maryland Public Interest Research Group are three examples of nonprofit organizations offering objective insights and analysis on why the Right to Repair is essential today.

Speaking as cybersecurity practitioners and lifelong 'geeks' we reject the false narrative being pushed by vendors that owners and independent repair entities pose a security risk if granted access to, information about, and the right to repair their products. Vendors claim security is their top concern. *Make them prove it!* For example, SecuRepairs wisely recommends legislators not blindly accept industry claims but challenge them to substantiate their claims over cybersecurity concerns related to the Right to Repair by asking the following questions:

- Ask if they can provide objective evidence to support their claim that repairs conducted by 'authorized' repair professionals are in *any* way superior to repairs conducted by owners and independent third-party repair professionals if given the same tools and knowledge.
- Ask if they can provide objective evidence to support their claim that vendor repair professionals are more trustworthy and/or less likely to misuse customer data than owners or independent repair professionals.
- For technology companies, ask how many open software security vulnerabilities (CVEs) exist for their products and what the average length of time it takes to issue patches for those is. In our view, cybersecurity vulnerabilities that remain open for more than 60-90 days strongly suggests that a vendor apparently is unwilling or unable to address them, preferring to keep their customers at-risk to cybersecurity problems.
- Ask product vendors to confirm that the user data stored on their devices and sent to/from them is secured with strong, unbreakable encryption. By 'user data' we refer to things the average user doesn't have access to, such as diagnostic information, internal configurations, and other generally hidden metadata generated by the product, such as when or how long it was used.

<u>Right To Repair: Pro-Consumer, Pro-Competition, Pro-Environment</u>

The ability of individuals to service, repair and maintain their property is a core right of ownership that has been recognized in U.S. law and common law for centuries -- and onerous terms of service and/or controversial licensing agreements should not preclude that. SB0412 will update those basic individual rights and consumer protections for a digital age as manufacturers seek to turn hundreds of millions of owners into locked-in tenants of their own technology in a new approach to the outdated 'company town' concept. I**n this time of increasing wealth inequality and concentrations of market power by large technology firms, a digital right to repair ensures that the promises, potentials, and capabilities of modern technology products are distributed <u>equally</u> to consumers, communities and small businesses alike.**

A digital right to repair is a vital pro-consumer, pro-small business policy tool that will extend the life of electronic devices, ensure their safety, security and integrity. Enhanced product knowledge and localized ability to service and repair digital devices in timely manners will make homes, businesses, schools, cities and towns across Maryland less vulnerable to the effects of cyber attacks and other types of malicious behavior. Moreover, endorsing the Right to Repair will reduce the potential for needless electronic waste ("e-waste") and unnecessary technology upgrades, thus providing tangible environmental and economic benefits to the State, businesses, and individual consumers as well.

For years, Maryland has been an informed leader in how it's approached technology matters, especially when it comes to cybersecurity. The digital right to repair law you are considering today is a rare

opportunity. The proposed legislation is simultaneously pro-competition, pro-consumer, pro-environment, and helps ensure that Marylanders can remain resilient and competitive in the networked society and business landscapes of the future. We urge you to continue thinking innovatively about technology and pass SB0412 during this legislative session.

[1] https://support.google.com/store/answer/7182296

[2] https://support.google.com/store/answer/7169154

[3] https://www.nytimes.com/2021/01/23/opinion/sunday/online-terms-of-service.html

# # # #

Witness Bio:

Dr. Richard Forno is a Senior Lecturer in the UMBC Department of Computer Science and Electrical Engineering, where he directs the UMBC Graduate Cybersecurity Program and serves as the Assistant Director of UMBC's Center for Cybersecurity. His twenty-five year career includes helping build a formal cybersecurity program for the United States House of Representatives, serving as the first Chief Security Officer at Network Solutions (then, the global center of the internet Domain Name System) and consulting for the Department of Defense and Fortune 500 companies. He has worked with all levels of management on technical and non-technical projects pertaining to cybersecurity, incident response, cyber defense, information operations, and critical infrastructure protection. Richard is an affiliate of the Stanford Center for Internet and Society (CIS) and from 2005-12 was a Visiting Scientist at the Software Engineering Institute at Carnegie Mellon University, serving as an instructor for the CERT Coordination Center (CERT/CC). He is co-author of the forthcoming book "Cybersecurity for Local Governments." (Wiley)

Contact: E-mail: rforno@umbc.edu

Dr. Aviel (Avi) D. Rubin is Professor of Computer Science and Technical Director of the Information Security Institute at Johns Hopkins University. He is also the Director of the JHU Health and Medical Security Lab. Prior to joining Hopkins, Rubin was a research scientist at AT&T Labs. He is also the founder of Harbor Labs, a CyberSecurity company. Rubin testified about information security before the U.S. House and Senate on multiple occasions, and he is the author of several books about computer security. Rubin is a frequent keynote speaker at industry and academic conferences, and he delivered a widely viewed TED talk in 2011 and another TED talk in September, 2015. He also testified in federal court as an expert witness on numerous occasions in matters relating to high tech litigation. Rubin served as Associate Editor of IEEE Transactions on Information Forensics and Security, Associate Editor of Communications of the ACM (CACM), and an Advisory Board member of Springer's Information Security and Cryptography Book Series. In 2010-2011 Rubin was a Fulbright Scholar at Tel Aviv University. In January, 2004 Baltimore Magazine named Rubin a Baltimorean of the Year for his work in safeguarding the integrity of our election process, and he is also the recipient of the 2004 Electronic Frontiers Foundation Pioneer Award. Rubin has a B.S, ('89), M.S.E ('91), and Ph.D. ('94) from the University of Michigan.

Contact: E-mail: rubin@jhu.edu