

Paul Roberts

Founder

SecuRepairs
54 Cross Street
Belmont, MA 02478
617 817 0198
paul@securepairs.org

February 1, 2021

The Honorable Members of the Finance Committee
Maryland State Capitol
Senate Office Building
Annapolis, Maryland 21401

Chair Kelley , Vice Chair Feldman and members of the Finance Committee:

My name is Paul Roberts and I am the founder of SecuRepairs.org and Editor in Chief of The Security Ledger, a cyber security news website. I am speaking here today to express **my support for SB 412** an act concerning consumer protection and right to repair.

My organization, SecuRepairs (securepairs.org) is a not for profit group of more than 200 of the country's top information technology and information security experts. Our members include leading executives, academics, security researchers and information security professionals who support a digital right to repair.

The most important thing I want to do today is make you aware of our group. Our members include leading executives, academics, security researchers and information security professionals who support a digital right to repair. We are free at any time to brief you or your staff on the actual security issues affecting connected devices and how digital right to repair laws like Senate Bill 412 will **increase, not reduce the security of consumer electronics.**

I have provided my contact information on this testimony and would be happy to facilitate meetings with our experts.

No Cyber Risk In Repair

At this hearing and others, you will be told by manufacturers and industry lobbyists that digital right to repair bills such as SB 412 creates cyber security risks that will lead to hacks, data theft and other undesirable outcomes. In this and other state houses, these same industry representatives have said that requiring manufacturers to make schematic diagrams and diagnostic tools that they already supply to their authorized repair partners available to a device's owner is a security risk that is not worth taking.

Let me be blunt: these claims *are simply not true.*

Internet of Things Insecurity isn't about Repair

How do I know? Let me state the obvious: because in the United States there is *no digital "right to repair"* today. However, *there is* an epidemic of software vulnerabilities, cyber attacks and compromises of connected

“smart” electronic devices and Internet of Things products.

In recent years, you have likely encountered countless stories [of hacked webcams](#) and [home routers](#) - incidents that took place in the U.S. and abroad. In fact, there are so many of these exposed and hacked “smart” devices, that entire malicious networks of them - so-called “botnets” - are used by cyber criminals to carry out denial of service attacks, spread malicious software and send email spam.

These hacked devices and malicious global networks exist not because of the availability of schematics or diagnostic software for repair, but because of the security weaknesses of already manufactured and deployed electronics. The sad truth is that many home electronics, smart home devices, appliances, even machinery roll off the assembly line with exploitable software vulnerabilities. Many more devices are insecure by design or in how they are deployed in homes and businesses. These hundreds of millions of Internet connected devices contain the digital equivalent of unlocked or unlockable doors that malicious actors can step through.

Manufacturers and their lobbyists want you to believe that security is their top priority. But their actions -and the record - say otherwise. Even today, home broadband routers that bring Internet connectivity to your homes and offices might ship with the same default administrator account and password. Further, that password to access the device may be trivial, or entirely absent.

Finally, many of these devices are deployed in an insecure state. Their software contains known and unpatched security holes that can be exploited. Furthermore, the devices lack features to automatically update or notify owners when updates are available.

Un-needed communications ports on these devices are open and “listening” for anyone on the Internet who wishes to connect. Communications to and from these devices are sent “in the clear” letting others snoop on it and steal sensitive information like passwords and account credentials.

Their arguments before you today do not reflect their desire to protect customer data, but instead their desire to snuff out independent competition for aftermarket parts and repair that will impinge on their own service revenue and extend the life of their products, reducing the frequency of profitable device upgrades. The cost to consumers, the economy and our environment for these de-facto monopolies is very high, indeed.

Some questions to ask repair opponents

What can you do? First: listen to what cyber security experts, rather than industry lobbyists say. My group represents 200 of the country’s top information security experts. As I said, we are free at any time to brief you or your staff on the actual security issues affecting connected devices and how digital right to repair laws like Bill 412 will increase, not

reduce the security of consumer electronics.

Second, I urge you to ask tough questions and push back on the false narrative pushed by industry that owner repairs and independent repair poses a security risk.

- Ask them if they have any empirical evidence to support their assertion that repairs conducted by their authorized repair professionals are in any way superior to repair conducted by owners and independent repair professionals.
- Ask them if they have any empirical evidence that supports their assertion that authorized repair professionals are more trustworthy or less likely to misuse customer data than owners or independent professionals.

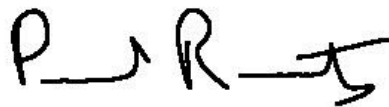
There is plenty of circumstantial evidence that their claims about the integrity of their authorized service ecosystem are inflated. For example, in April 2019, Immigrations and Customs Enforcement raided a Texas-based Samsung Authorized Service provider, CVE Technology Group and detained more than 280 people suspected of being undocumented immigrants hired as cheap labor to do “authorized repair and refurbishing” of Samsung devices.

Repair: Pro-Consumer, Pro-Competition, Pro-Environment

In a world that is increasingly populated by Internet-connected, software powered objects - the so-called “Internet of Things” - a digital right to repair is a vital tool that will extend the life of electronic devices, ensuring their safety, security and integrity. We all want and benefit from new, connected products. But the price of convenience, connectivity and cool features cannot be monopolies on aftermarket service and repair that deny owners their property rights and impose considerable costs on the consumers, the economy and the environment. SB 412 will make homes, businesses, schools, cities and towns across the state of Maryland more secure and less vulnerable to cyber attacks and other malicious behavior.

The digital right to repair law you are considering today is a rare spectacle. It is simultaneously pro-competition, pro-consumer and pro-environment. I urge each of you to vote to pass this bill out of your Committee and that the full legislature have the opportunity to act on it this year.

Sincerely,

A handwritten signature in black ink, appearing to read 'P. Roberts'.

Paul Roberts | paul@securepairs.org