securepairs.org
security professionals for a fixable future

Paul Roberts

Founder

—

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

March 1, 2021

The Honorable Members of Committee on Business and Labor
Oregon State Capitol
Salem, Oregon 97301

Chairman Holvey , Vice Chairs Bynum and Barreto and members of the Committee on Business and Labor:

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 a cybersecurity reporter and industry analyst with close to two decades experience in the information security field. I am speaking today to express **my support for HB 2698** an act relating to promoting consumer protection and the 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 membership includes 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 House Bill 2698 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.

Internet of Things Insecurity isn't about Repair

At this hearing and others, you will be told by manufacturers and industry lobbyists that digital right to repair bills such as HB 2698 creates cyber security- and privacy risks that will lead to hacks, data theft and other undesirable outcomes. Let me be blunt: these claims *are simply not true.*

How do I know? Because in the United States right now there is no digital "right to repair." However, *there is* an epidemic of cyber attacks and compromises of connected "smart" electronic devices and Internet of Things products.

Some recent examples; consumers recently banned together to file a class action lawsuit against Ring, a company that makes connected doorbells, after a string of security lapses including one that saw an unknown, remote assailant hijack a Ring camera in an 8 year old girl's room, claim to be Santa Claus and taunt her through the device.

Or consider the recent discovery online of more than 3 Terabytes of video data lifted from Internet connected home webcams, many showing explicit images of owners in the privacy of their homes. These stories go alongside countless stories of hacked home routers, smart TVs and other consumer electronics.

In fact, there are so many exposed and hackable "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.

No Security in Obscurity

Let's be clear: these devices are not being hacked because of the availability of device schematics to replace a failed capacitor or because hackers got their hands on diagnostic software needed to read and interpret a software error code. The truth is that hackers find these smart devices easy prey. Many have rolled off the assembly line with serious, remotely exploitable software holes or laughable security that - once the device is connected to the Internet - will be trivial to bypass.

Many smart home devices, connected appliances and even industrial machinery are insecure by design, insecure by default and insecure in how they are deployed. These 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 the record - as outlined above - says otherwise.

Their arguments before you today should be greeted with deep skepticism. They do not reflect a sincere desire to protect customer data. Rather, they reflect a desire by device manufacturers to snuff out competition for aftermarket parts and repair from owners and independent repair shops. Giving their customers access to\ the same tools and information that they give to their authorized repair shops won't make the Internet any less secure. But it will reduce the profits they make from service revenue and extend the useful life of what they produce, 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 2698 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.

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 Enforcmenent 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. HB 2698 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,

Paul Roberts | paul@securepairs.org