securepairs.org
security professionals for a fixable future

Paul Roberts

Founder

—

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

Feb 9, 2023

Honorable Members of the Committee on Energy and Environment
Oregon State Senate
Oregon State Capitol
900 Court St NE, Salem, OR 97301

Chair Sollman , Vice Chair Findley and members of the Committee on Energy and Environment:

My name is Paul Roberts and I am the founder of SecuRepairs.org, an organization of more than 300 cyber security and information technology professionals who support the right to repair. I am speaking today on behalf of our members to **express our support for SB 542** an act "Relating to a right to repair consumer electronic equipment."

My organization, SecuRepairs (securepairs.org) includes some of the nation's leading corporate executives, academics, security researchers and information security professionals who ardently support a digital right to repair and wish to dispel myths, propagated by industry lobbyists opposed to this important legislation, that repair somehow poses a cyber risk. It does not.

No Cyber Risk In Repair

As you know, SB 542 simply asks electronic device makers that *already* provide repair and maintenance information to their *authorized* repair providers to also provide them at a reasonable price to their *customers*, and to third parties they may hire to do repair and maintenance for them.

In short: opponents of this law are asking for permission to give diagnostic tools, information and parts to their *business partners*, but deny them to the individuals who *own the devices in need of repair* - all in the name of data privacy and security. That argument defies logic.

Hacked via schematics? No.

It is also important to understand that, from the perspective of cyber risk, the kinds of information covered by SB 542 (schematic diagrams, service manuals, diagnostic software, administrative codes, replacement parts) play little to no role in attacks on connected devices.

The vast majority of attacks on Internet connected devices like home routers, DVRs, webcams, and home appliances exploit software vulnerabilities in embedded software released by the manufacturer. Alternatively, hackers exploit weak configurations, like default administrative usernames and passwords that are common to devices and never changed, or wide-open and insecure communications ports that give remote hackers access to devices.

It is the horrendous state of device security - not the availability of diagnostic and repair tools and information - that fuels cyber attacks on connected devices. This is no secret within the cybersecurity industry. A recent study of the security of IoT devices by Phosphorus Labs, a cybersecurity company, found that **68% of devices studied contained high-risk or critical software vulnerabilities**. That's consistent with a 2020 study by Palo Alto Networks that found that 57% of IoT devices are vulnerable to medium- or high-severity attacks while 98% of all IoT device traffic is unencrypted, exposing personal and confidential data and allowing attackers the ability to listen to unencrypted network traffic and collect personal or confidential information.

These glaring security lapses aren't oversights. The same firms paying millions of dollars to lobby against and defeat the right to repair bills in Oregon and other states design, sell and deploy products without consideration of security. And manufacturers - to date - pay little or no penalty for such lax business practices.

Independent repair is just as secure as authorized repair

Finally, in opposing such requirements, manufacturers lean on the idea that their authorized repair providers are more reliable and cyber secure than independent repair providers. But there is no evidence to support these claims. In fact, in doing research ahead of its 2021 Nixing the Fix report to Congress, the FTC explicitly asked manufacturers to provide empirical evidence that authorized repairs were of higher quality or employed superior cybersecurity than independent repair. Manufacturers were unable to provide any such evidence to the FTC. Accordingly, the Commission concluded in its report that there was *no empirical data* that supports manufacturers' claims that authorized repair is safer or of higher quality than independent repair.

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 right to repair is a vital tool that will extend the lives of consumer devices and ensure their safety, security and integrity. Yes, modern electronics have many new, wonderful software-based features. We all want and benefit from the conveniences offered by such "smart," connected products. But the price of convenience, connectivity and cool features cannot be manufacturer monopolies on service and repair. These deny Oregonians the property rights they have enjoyed for centuries, while imposing considerable costs on Oregon families and communities.

SB 542 will greatly improve the quality of life of Oregon consumers, families, and communities, while promoting small businesses and reducing e-waste throughout the state. I urge you to pass it.

Sincerely,

Paul Roberts | paul@securepairs.org