



**Paul
Roberts**

Founder

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

April 17, 2023

**Honorable Members of the Joint Committee on Innovation,
Development, Economic Advancement and Business
Maine State Legislature
210 State Street
Augusta, ME 04330**

Chairs Curry and Roberts and members of the Joint Committee on Innovation, Development, Economic Advancement and Business:

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 LD 1487/SP 608](#) an “An Act to Ensure That Residents of the State Have the Right to Repair Their Own Electronic Devices.”

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

No Cyber Risk In Repair

As you know, LD 1487/SP 608 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. As such, it does not create any new cyber risk, given that manufacturers are already distributing the required repair and service information.

In arguing against this pro-consumer requirement, opponents are asking for permission to share diagnostic tools, information and parts to their *business partners* (authorized repair providers), but deny them to their customers -the individuals who *own the devices in need of repair*. And they’re doing this in the name of data privacy and security? That argument defies logic.

Repair information not used in cyber attacks on devices.

It is also important to understand that, from the perspective of cyber risk, the kinds of information covered by LD 1487/SP 608 -schematic diagrams, service manuals, diagnostic software, administrative codes, replacement parts- do not contribute to attacks on connected devices. Instead, 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 poor quality of embedded software released by manufacturers and the absence of robust security features that fuels the epidemic of cyber attacks on connected devices, not the availability of schematic diagrams and service manuals.

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.

Independent repair is just as secure as authorized repair

In opposing right to repair laws, 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 doing research ahead of its [2021 Nixing the Fix](#) report to Congress, the FTC explicitly asked manufacturers to provide 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. The Commission concluded 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 a right to repair is a vital tool that will extend the lives of consumer devices and ensure their safety, security and integrity. Modern electronics have many new, wonderful software-based features.. But the price of convenience cannot be manufacturer monopolies on service and repair that deny Maine residents their property rights while imposing considerable costs on families, communities and local economies. LD 1487/SP 608 will greatly improve the quality of life of Maine consumers, families, and communities, while promoting small businesses and reducing e-waste throughout the state. I urge you to pass it.

Sincerely,

A handwritten signature in black ink that reads "Paul Roberts". The signature is stylized, with the first letters of the first and last names being prominent.

Paul Roberts | paul@securepairs.org