Paul Roberts

Founder

—

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

July 14, 2023

Chair Darrell Issa, Ranking Member Hank Johnson, and Honorable Members of the Subcommittee on Courts, Intellectual Property, and the Internet of the Committee on the Judiciary
Congress of the United States
House of Representatives
2138 Rayburn House Office Building
Washington, DC 20515-6216

Chair Issa, Ranking Member Johnson, and members of the Subcommittee on Courts, Intellectual Property, and the Internet:

My name is Paul Roberts and I am the founder of Secure Repairs (securepairs.org), an organization of more than 350 cyber security and information technology professionals who support the right to repair. I am speaking to you today on behalf of our members to make clear that the fair access to repair materials, such as those required under right to repair laws, *does not increase cyber risk*. In fact, it can contribute to healthier and more secure ecosystems of smart, connected devices.

About me: I have covered the cybersecurity space for more than 20 years as a reporter, editor and industry analyst. Since 2012, I have served as the publisher and Editor in Chief of The Security Ledger (securityledger.com), an independent cybersecurity news website that covers the intersection of cybersecurity and the Internet of Things. I am the Cyber Content Lead at ReversingLabs, a provider of cloud-based intelligence on malware and software supply chain risks, and I sit on the board of The Repair Coalition. My writing and reporting on cybersecurity has appeared in publications including Forbes, The Christian Science Monitor, MIT Technology Review, The Economist Intelligence Unit, CIO Magazine, ZDNet and Fortune Small Business. I have appeared on NPR's Marketplace Tech Report, KPCC AirTalk, Fox News Tech Take and Al Jazeera.

Secure Repairs (securepairs.org) includes some of the nation's leading corporate executives, academics, security researchers and information security professionals. We ardently support a robust, open repair ecosystem and wish to dispel myths, propagated by those opposed to this important consumer right, that access to repair information and tools somehow poses a cyber risk. It does not.

No Cyber Risk In Repair

At its core, proposed right to repair legislation considered by this Congress such as the REPAIR Act simply asks manufacturers of devices that already provide repair and maintenance information to their *authorized* repair providers to also provide them at a fair and reasonable price to their *customers* - the owners of the devices - and to third parties those customers may hire to do repair and maintenance for them.

By definition, the information covered by right to repair laws is not sensitive or protected, as evidenced by the fact that manufacturers distribute it widely to hundreds, thousands or tens of thousands of repair professionals working on behalf of their authorized providers. That includes everything from auto mechanics working at dealerships to hourly workers staffing the Geek Squad at Best Buy. To say that we will increase cyber risk by also providing that information and tools to the owners of devices or independent repair professionals defies explanation.

Independent repair is just as secure as authorized repair

In opposing right to repair laws, manufacturers also like to lean on the notion that authorized repair providers are more reliable and cyber secure than independent repair providers. This committee should understand that there is no evidence to support these claims.

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.

Hacked via schematics? Not a thing.

It is also important to understand that, from the perspective of cyber risk, the kinds of information covered by right to repair laws plays no role in fueling cyber attacks on connected devices. The vast majority of attacks on Internet connected devices - from smartphones and tablets to home appliances and automobiles - exploit software vulnerabilities in embedded software produced, managed and released by the manufacturer.

In addition, hackers exploit weak configurations, like default administrative usernames and passwords configured by manufacturers that are common to devices and never changed, or wide-open and insecure communications ports designed to facilitate deployment and remote management of devices, but that give remote hackers access to administrative interfaces and stored data.

Examples of this kind of attack grab headlines almost daily. The recent spate of attacks on the MOVEIt file transfer application are a good example. Those attacks, carried out by the Cl0p ransomware gang, leveraged a remotely exploitable hole in the MOVEIt application software to get access to sensitive data stored on the application. The MOVEIt attacks have affected more than 200 organizations and 17.5 million individuals, according to estimates, including a long list of U.S. colleges and universities, healthcare, financial pharmaceutical and energy firms and more.

And malicious actors have no shortage of potential targets to choose from in the U.S. A recent study of the security of IoT devices by Phosphorus Labs, a cybersecurity company, found that **68% of devices studied contained known, 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.

In short, it is the poor quality of deployed software and the poor state of device security - not the availability of diagnostic and repair tools and information - that fuels cyber attacks on connected devices. As someone who has covered the cybersecurity space for more than two decades, I can say with assurance that hackers are not scrutinizing schematic diagrams, reading through service manuals or using diagnostic software designed to service and repair devices to facilitate their attacks. Shoddy and insecure software and poorly configured devices leave the doors to our home, business and government networks and data wide open. Hackers simply step through those open doors.

A Right to Repair is key to a secure Internet of Things

In fact, properly implemented, right to repair laws will promote a healthier and more secure ecosystem of smart, connected devices, rather than undermine it. As the Internet of Things ages, individuals, businesses and governments will find they have to maintain deployed devices after manufacturers have ended support for them. The problem of "abandonware" is already evident and growing, as the makers of connected devices walk away from the responsibility to support the software that powers their creations, leaving U.S. businesses and consumers in the lurch.

There are many reasons for abandoning support of smart, connected devices - from the typical considerations of resources and profitability to manufacturers going out of business or being acquired. While it may be impossible to force companies to support connected products for the two, three or four decades that are their full, useful life, we can empower the larger economy to pick up where manufacturers leave off. Right to repair laws will foster a diverse ecosystem of small, aftermarket service providers that can step into the role once occupied by OEMs to supply software updates and patches, service and repair deployed devices and so on. Right to repair laws help ensure that devices will have long and productive lives, reducing the total cost of ownership for businesses and consumers and the amount of electronic waste they produce. At the same time, these laws will foster a range of business and employment opportunities up and down the economic ladder.

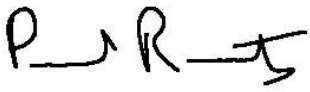
Repair: Pro-Consumer, Pro-Competition, Pro-Environment

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 your constituents property rights they have enjoyed for centuries, while imposing considerable costs on our families, small businesses and communities.

Federal right to repair legislation like the REPAIR Act, the SMART Act and the Fair Repair Act will greatly improve the quality of life for consumers, families, and communities, while promoting small businesses and reducing e-waste throughout

the country. Such legislation is a long overdue corrective to abusive and anti-competitive industry practices. On behalf of our more than 300 members, I strongly urge this committee to support the passage of right to repair legislation.

Sincerely,



Paul Roberts | paul@securepairs.org