No. 19-783

In the
Supreme Court of the United States

NATHAN VAN BUREN,
Petitioner,

v.

UNITED STATES,
Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Eleventh Circuit

AMICUS CURIAE BRIEF OF THE ASSOCIATION OF MEDICAL DEVICE REPROCESSORS IN SUPPORT OF PETITIONER

JEFFREY L. BERHOLD
JEFFREY L. BERHOLD, P.C.
1230 Peachtree St.
Suite 1050
Atlanta, GA 30309
(404) 872-3800

STEPHEN D. TERMAN
Counsel of Record
J. MASON WEEDA
OLSSON FRANK WEEDA
TERMAN MATZ PC
2000 Pennsylvania Ave., NW
Suite 3000
Washington, D.C. 20006
(202) 789-1212
sterman@ofwlaw.com

Counsel for Amicus Curiae

July 7, 2020

Becker Gallagher · Cincinnati, OH · Washington, D.C. · 800.890.5001

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

REGULATIONS

OTHER AUTHORITIES

INTEREST OF THE *AMICUS CURIAE*[1]

The Association of Medical Device Reprocessors ("AMDR") is a non-profit trade organization representing FDA-regulated firms that collect, clean, repair, disinfect and/or re-sterilize (among other steps) medical devices marketed by the original equipment manufacturer ("OEM") for "single use." AMDR's interest in this case is the reasonable and fair application of the Computer Fraud and Abuse Act ("CFAA") as it may relate to reprocessing of medical device and medical device components.

The single use devices ("SUD") that AMDR members reprocess are diverse and include, without limitation, cardiovascular, general surgery, patient monitoring and compression therapy, and orthopedic medical devices. AMDR members provide hospitals with safe and effective reprocessed devices, which lower healthcare costs, ensure a stable supply chain, help expand patient access to treatments, and reduce the adverse environmental impact of medical waste.

---

[1] No party nor its counsel authored this brief in whole or in part or contributed money to fund preparing or submitting this brief. No person or their counsel, other than the *amicus* party or its members (Innovative Health, Medline ReNewal, Nescientific, REnu, a subsidiary of Arjo, Inc., Stryker Sustainability Solutions, Inc., a wholly-owned subsidiary of Stryker Corporation, Sustainable Technologies, a Cardinal Health business, and Vanguard AG) contributed money intended to fund preparing or submitting the brief. Petitioner, Van Buren, filed a letter of blanket consent to *amici*. Respondent, United States, granted consent to *amicus curiae* AMDR on June 8, 2020 via electronic mail.

Many SUDs can be reprocessed safely pursuant to Food and Drug Administration ("FDA") regulations. Commercial SUD reprocessors are regulated as "manufacturers" and are subject to the same requirements as the OEM, including:

- Registering all reprocessed products
- Obtaining premarket clearance or approval
- Compliance with FDA's quality system regulation
- Submitting adverse event reports
- Tracking devices whose failure could have serious outcomes
- Correcting or removing from the market unsafe devices
- Meeting labeling requirements
- Submitting the reprocessing facilities to regular inspection

Perhaps most significantly, before a reprocessed medical device can be marketed or sold, a reprocessor must demonstrate—and FDA must agree—that the reprocessed device is "substantially equivalent" in terms of safety and efficacy to the device manufactured by the OEM, *i.e.*, the "predicate device." In fact, SUD reprocessors are held to higher premarket requirements than OEMs, as reprocessors must submit additional validation and testing data not required of the original device manufacturer.

At least one study has confirmed that certain OEM devices had a higher defect rate than the reprocessed versions of those same devices,[2] and a number of Government Accountability Office (GAO) reports have generally underscored FDA's own data showing clinical "confidence in reprocessed SUDs, with some participants stating that there were actually fewer performance problems with reprocessed SUDs than with new SUDs."[3]

The savings realized through the use of reprocessed SUDs allows hospitals and healthcare providers to cut costs significantly and redirect those funds, for instance, toward hiring more medical professionals, expanding patient access to procedures, or investing in newer technology, which ultimately enhances and improves patient care. In 2018, AMDR members saved hospitals nearly $500 million.[4] Similar to use of a generic drug, the savings associated with the use of reprocessed SUDs is significant in a world of escalating healthcare costs.

---

[2] Terrence J. Loftus, *A Comparison of the Defect Rate Between Original Equipment Manufacturer and Reprocessed Single-Use Bi-Polar and Ultrasound Diathermy Devices, 9* J. Med. Devices 4 (Dec. 2015).

[3] *See* U.S. Government Accountability Office, GAO-08-147, *Reprocessed Single-Use Medical Devices: FDA Oversight Has Increased, and Available Information Does Not Indicate That Use Presents an Elevated Health Risk*, 21 (Jan. 2008).

[4] *See* Jessica Kim Cohen, Modern Healthcare, *Medical Device Reprocessing Saved Providers $470 million last year*, (July 29, 2019).

Reprocessing also builds resiliency into the healthcare supply chain. The COVID-19 pandemic financially devastated U.S. hospitals and exposed weaknesses in the supply chain, which failed to ensure adequate personal protective equipment ("PPE") and other desperately needed medical devices, some of which can be reprocessed. Hospital use of existing medical device and supply assets lessens the need to acquire more new devices from a global supply chain. With greater attention now placed on ensuring an affordable, secure, and reliable supply chain of medical devices and equipment, reprocessing is, now more than ever, critically important for U.S. hospitals.

The reprocessing services offered by AMDR members also have a positive effect on the environment. AMDR members helped hospitals divert more than 15 million pounds of waste from landfills in 2018 alone. On average, medical device reprocessing can divert over 50,000 pounds of medical waste from a single hospital each year—the equivalent weight of more than five elephants. Hospitals spend anywhere from $44 to $68 per ton on waste disposal, which one study equates to $259 to $401 million spent by hospitals on waste on an annual basis.[5]

As a result of the safety profile, strengthened supply chain and cost and waste savings, reprocessed devices

[5] *See* Scott Unger and Amy Landis, Journal of Cleaner Production, *Assessing the Environmental, Human Health, and Economic Impacts of Reprocessed Medical Devices in a Phoenix Hospital's Supply Chain,* (January 20, 2016).

are purchased by all "top hospitals" as listed by U.S. News & World Report[6] and are used in all 50 states.

In some instances, and as described in more detail below, such reprocessed devices may be subject to the Computer Fraud and Abuse Act ("CFAA" or "Act"), creating potential civil and/or criminal liability for reprocessors. While AMDR does not take this view, some OEMs have attempted to assert that repair or servicing of medical devices can implicate the CFAA. Medical technology has advanced significantly since passage of the CFAA and many medical devices, including reprocessed medical devices, and their accompanying generators or consoles, arguably constitute "computers" or "protected computers" and contain "information" under the Act.

AMDR is therefore providing the court with the perspective of medical device reprocessors to ensure that its ruling does not have an unintended effect on medical device reprocessors or healthcare delivery organizations. We request that any civil or criminal liability for exceeding unauthorized access, as defined by the Act, be limited to the intrusion theory of liability.

---

[6] *See* "U.S. News Best Hospitals by Specialty 2019-2020, National Rankings " (Aug, 14, 2018), available at https://health.usnews.com/best-hospitals/rankings.

SUMMARY OF ARGUMENT

The right to repair and reprocess has been part of our common law for centuries. The owner of a device has never lost the right to operate, repair, and maintain their device throughout developments in patent, trademark, and copyright law. In that spirit, FDA has created a regulatory process for specialized companies to reprocess medical devices for healthcare providers.

The CFAA was passed in 1986 to target serious computer crimes and has been interpreted to have broader applicability than intended by Congress.[7] Not surprisingly, many single-use medical devices (devices), along with the systems powering and controlling them (generators and consoles), purportedly fall under the scope of the CFAA. AMDR members reprocess many such single-use devices, *e.g.*, laparoscopic electrosurgical devices including ultrasonic scalpels, diagnostic electrophysiologic and ultrasound cardiac catheters, and pulse oximeter sensors. Such devices may connect directly, or indirectly through an operating system on the generator or console, to the internet.

This case presents a question of great importance to the repair industry generally and medical device reprocessors specifically. Medical device reprocessing is entirely lawful under the intrusion theory of liability evolving in the Second, Fourth, and Ninth Circuits. The reprocessor is accessing information from devices

---

[7] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act,* 94 Minn. L. Rev. 1561, 1564 (2010).

acquired from healthcare providers. There is no malicious hacking, *i.e.*, breach of security, on someone else's device. In enacting and amending the statute, Congress showed no intent to reach more broadly to encroach on the right to repair.

On the other hand, a broad interpretation of "exceeds authorized access" may put the right to repair and reprocess in jeopardy. The misappropriation theory of liability would allow the OEM to impose terms of use on the device preventing downstream device owners from repairing or reprocessing the device. AMDR would not presume to be able to imagine all of the ways in which OEMs would set out language in customer contracts, product labels, and onscreen warnings, among other means, that would constrain the ability of the medical device reprocessor to access information on the device and system connected to it. Again, these devices are owned by the healthcare provider or medical device reprocessor. Yet, the OEM would be able to restrain the right to repair.

This Court has always presumed that Congress did not intend to limit the common-law right to repair in the absence of evidence to the contrary. It has been true of patent and trademark law alike. The stakes are just as high in interpreting the CFAA. The statute now reaches many modern-day medical devices, as well as billons of smart phones, household appliances, and motor vehicles. The right to repair lowers costs, preserves quality, and reduces waste. It is an essential part of the American free enterprise system and its "can-do" attitude. AMDR respectfully requests that this Court interpret "exceeds authorized access" under

the intrusion theory of liability to preserve the longstanding right to repair or reprocess medical devices – and any other "protected computer" – under the CFAA.

ARGUMENT

I. MEDICAL DEVICE REPROCESSING IS PART OF A LONG HISTORY IN THE LAW OF THE RIGHT TO REPAIR

The courts and legislatures of this country have long recognized that the ownership of property includes the right to repair that property. In fact, the common law has frowned upon restraints on the alienation of chattels for centuries. *Impression Prod., Inc. v. Lexmark Int'l, Inc.*, 137 S. Ct. 1523, 1531–32 (2017). That common-law right to repair is recognized in the law of patent, copyright, and trademark. For example, the doctrine of patent exhaustion recognizes that the first sale terminates the patent rights in those goods. *Id.* at 1532. A repair shop is free to restore and sell used cars without fear of infringing a patent in the car or any existing or replacement parts. *Id.*

Nor does a repair of a trademarked product form the basis for liability under trademark law. *Champion Spark Plug Co. v. Sanders*, 67 S. Ct. 1136, 1139 (1947), *Prestonettes, Inc., v. Coty*, 264 U.S. 359, 368 (1924). Furthermore, copyright law expressly provides for the modifications of the software on a device that are essential for the continued use of the device.[8]

[8] Nor would a repair shop violate the anticircumvention provision of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a), by circumventing encryption on a device to gain access to information

Universal Instruments Corp. v. Micro Sys. Eng'g, Inc., 924 F.3d 32, 46 (2d Cir. 2019) (citing 17 U.S.C. § 117(a)).

The FDA has taken the same view toward the right to repair and reprocess medical devices specifically. Healthcare providers have always had the right to repair and reprocess their own medical devices, subject to FDA or other requirements. With advances in technology, however, they must depend more and more on third parties specializing in repair and reprocessing of complex medical devices. As discussed above, FDA regulates medical device reprocessors as medical device manufacturers, and requires reprocessors to obtain a premarket clearance prior to reprocessing a SUD. The FDA clearance process is designed to determine whether the reprocessor has established, through testing and validation, that the SUD maintains its safety and effectiveness after reprocessing. 21 C.F.R. § 820.30. Since regulation of SUD reprocessing began twenty years ago, healthcare providers have been increasingly exercising their right to repair and reprocess SUDs through regulated, commercial medical device reprocessing firms to reduce costs, improve service, and prevent waste.

---

on the device solely for purposes of maintenance and repair. *Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc.*, 421 F.3d 1307, 1318 (Fed. Cir. 2005).

II. MANY MODERN-DAY MEDICAL DEVICES ARE "PROTECTED COMPUTERS" UNDER THE CFAA

Under the CFAA, you may not "exceed authorized access" of a "computer" and thereby obtain information from a "protected computer." 18 U.S.C. § 1030(a)(2)(C). Computer "means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device…" 18 U.S.C. § 1030(e)(1). Not surprisingly, many medical devices fit the statutory definition of computer – including biometric sensors, inhalers and pumps, and CT and MRI scanners. *See*, *e.g.*, *Philips Med. Sys. Puerto Rico Inc. v. GIS Partners Corp.*, 203 F. Supp. 3d 221, 231 (D.P.R. 2016) (reasoning that a computer controls the operation of MRI machines). The SUDs reprocessed by AMDR members are arguably electronic devices "performing logical, arithmetic, or storage functions." 18 U.S.C. § 1030(e)(1). Moreover, as the medical device industry quickly evolves, AMDR expects to see more and more devices that perform such functions.

In addition, these devices routinely fall under the definition of "protected computers" as they are "affecting interstate commerce." 18 U.S.C. § 1030(e)(2)(B). New and reprocessed medical devices are sold and shipped across state lines in nationwide and worldwide markets. Moreover, the reprocessed medical device may be considered part of a larger "protected computer." Many reprocessed medical

devices are physically connected to a larger interface, a generator or console, on site to power and control the device. Since FDA requires both the OEM and the reprocessor to verify and validate that the design of the device works as it is intended, *see* 21 C.F.R. § 820.30(f)-(g), the reprocessor may need to access information stored on the device to ensure that the device is functioning properly and communicating with the ancillary generator or console interface. By way of example, an OEM may design an SUD to cease working after a single use when subsequently connected to a generator or console. Under these circumstances, a reprocessor would need to access a console to ensure the SUD communicates properly allowing an additional use. Furthermore, such systems are sometimes connected to the internet. The broad definition of "protected computer" – "affecting interstate commerce" – effectively includes all "computers with Internet access." *U.S. v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012). OEMs routinely update software on the generators or consoles, sometimes via interstate wires.

OEMs often impose "terms of use" that purport to govern access and operation of their products, including single-use medical devices and the generator or console that may power or control the instrument. The OEM may attempt to limit access to, or information on, the device specifically, or the system generally, to hinder the ability of the hospital to repair or reprocess its medical devices. The commercial reprocessor is not a party to any such contractual restrictions. Under such circumstances, the question is whether Congress intended to allow OEMs to impose "terms of use" to limit the longstanding right to repair for modern-day

medical devices – or smart phones, household appliances, or motor vehicles – by amending its terms of use language delineating when the user "exceeds authorized access."

III. THE INTRUSION THEORY OF LIABILITY PRESERVES THE COMMON-LAW RIGHT TO REPAIR.

AMDR agrees with the Second, Fourth, and Ninth Circuits that Congress intended the CFAA to apply to instances of hacking, rather than misappropriation. *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1000 (9th Cir. 2019), *United States v. Valle*, 807 F.3d 508, 525 (2d Cir. 2015), *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 203 (4th Cir. 2012). "The CFAA was enacted to prevent intentional intrusion onto someone else's computer—specifically, computer hacking." *hiQ Labs*, 938 F.3d at 1000. Congress enacted the relevant sections of the statute to protect the "privacy" of "computer information" by outlawing its "theft" from "private computers." S. Rep. 104-357, 7 (1996) (Jud. Comm. Rep.). Put simply, the CFAA is intended to prevent accessing a computer without authorization, *i.e.*, accessing another person's device without permission. Most important for purposes of this brief, someone "exceeds authorized access" by breaching a layer of security on someone else's computer. Under those circumstances, the hacker is not "entitled" to be there. 18 U.S.C. § 1030(e)(6).

Medical device reprocessing is lawful and does not constitute unauthorized access under the intrusion theory of liability. The reprocessor is not breaking into another person's computer. The device owner (*e.g.*, a

hospital, or health care provider) explicitly provides used SUDs to the reprocessor to be reprocessed, which includes ensuring that the device works with the larger system. In addition, the medical device reprocessor takes title to the device, assumes legal responsibility for it, and markets it as its own SUD, pursuant to FDA requirements. Under these circumstances, the reprocessor is not "breaking and entering" anyone else's computer. *Valle*, 807 F.3d at 525.

Many of these reprocessed SUDs must "talk" with ancillary equipment, such as generators or consoles. Such ancillary equipment is not intended for single use and therefore is not reprocessed. To meet FDA's requirements, however, the reprocessor may need to access information from the generator or console connected to the SUD to ensure operability of the SUD for an additional use. The reprocessor will acquire such equipment for that purpose.

Moreover, the intrusion theory of liability serves the goals of Congress in enacting the statute – to prevent danger to life and property arising from malicious hacking. Clearly, the CFAA makes it a crime to break into someone else's device or breach the security of someone else's data storage facility. However, it is not illegal to access any information on your own device, or data in a storage facility connected to your device to operate and maintain your device. Under those circumstances, the information has not been kept private. As discussed above, the term "computer" is broad and now includes biometric sensors, surgical instruments, and delivery devices – as well as handheld phones, household appliances, and farm

tractors. Although the scope of the definition of "computer" is broad, the balance remains the same – an individual may repair a device that he/she owns but may not hack into a device owned by someone else.

In enacting and amending the CFAA, Congress gave no indication that it intended to limit the right to repair one's own property. In the absence of evidence of such intent, the Court must presume that Congress intended to retain the right to repair and reprocess under the common law. *Kirtsaeng v. John Wiley & Sons, Inc.*, 133 S. Ct. 1351, 1363 (2013). "The 'first sale' doctrine is a common-law doctrine with an impeccable historic pedigree." *Id.* The right to repair and reprocess has continued through the development of the law of patent, copyright, and trademark, not to mention the law and regulation of medical devices. The right to repair and reprocess should survive the CFAA as well.

IV. THE MISAPPROPRIATION THEORY OF LIABILITY EXPOSES A SIGNIFICANT AND GROWING SHARE OF MEDICAL DEVICE REPROCESSING ACTIVITY TO POTENTIAL CRIMINAL AND CIVIL LIABILITY.

The misappropriation theory of liability puts the right to repair in jeopardy. Some OEMs are hostile to the right to repair as they see it as a threat to sales of new replacement devices. Yet the misappropriation theory would put the OEM in the position of drawing the line on what constitutes a violation of the statute. The OEM, rather than the owner, would decide what "exceeds authorized access" through terms of use. The OEM would be the proverbial fox in the henhouse. The

repair shop would no longer be able to restore a used car without looking over its shoulder.

The medical device reprocessor would face the issue as much as any other independent service organization. Indeed, terms of use are ubiquitous in the medical device industry, including various restrictions on the owner and/or end user. At the time of sale, the OEM typically requires the hospital or provider to agree to "terms of use." The "terms of use" can be imposed as part of the contract, the device label, or be stored on the device or operating system itself. Those terms of use could include broad restrictions, *e.g.*, where the device owner is not to reprocess the device or not resell the device to a reprocessor. The "terms of use" may also include more specific restrictions, whereby the device owner could be restricted from accessing the device's programming or code.

The Eleventh Circuit's misappropriation theory allows the OEM to argue that the reprocessor is exceeding access because it is not complying with the OEM's "terms of use." Under such theory, a reprocessor could exceed authorized access simply by doing what is required by FDA regulations to ensure that the reprocessed medical device is safe and effective. The reprocessor may have to obtain information from the device to test or reset it for an additional use. Yet restrictive terms of use could lead to liability under the CFAA when a reprocessor simply verifies and validates that the device performs as intended.

Moreover, prosecutorial discretion would not save reprocessors and other independent service

organizations from civil liability for exceeding authorized access under the CFAA. The interpretation of "exceeds authorized access" here will apply equally to civil liability under the CFAA. *See*, *e.g.*, *Clark v. Martinez*, 125 S. Ct. 716, 722 (2005). The statute includes a private right of action for compensatory damages and equitable relief for any person who suffers damages or loss by reason of a violation of the statute. 18 U.S.C. § 1030(g). Damages mean "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Loss includes the cost of "responding to an offense" or "conducting a damage assessment." Once an OEM is able to argue that a reprocessor "exceeds authorized access" by violating the terms of use, an OEM could simply point to its own efforts to investigate any attempt to reprocess its devices as a basis for bringing an action against the medical device reprocessor.

Therefore, an overly broad interpretation of "exceeds authorized access" is no small matter to the medical device reprocessing industry and to healthcare providers. To the extent the door is open for OEMs to use or even attempt to use the CFAA against reprocessors, the ultimate result would be a decrease in all of the benefits of reprocessed devices, including cost savings, a more robust supply chain, and waste reduction. Such benefits would further decrease as reprocessors are deterred from innovating and offering new services. In the era of COVID-19, hospitals are struggling financially and limiting access to reprocessed devices will only escalate their costs, and potentially reduce device availability. And, ultimately,

it would be the consumer paying the price, as these increases in healthcare costs will trickle down to the patient, employer and taxpayer.

Medical technology in the healthcare industry is highly regulated and complex, and safety and innovation are paramount. As with other industries, the services provided by aftermarket or downstream servicers, repair and reprocessors are instrumental to the delivery of life saving medical technologies, while keeping costs down. AMDR strongly believes that medical device manufacturers (whether an OEM or reprocessor) should not be blocked or deterred from developing life-saving technologies; nor does AMDR believe that Congress intended for the CFAA to be used as an instrument to allow manufacturers to restrict downstream reprocessors from extending the life of medical equipment so long as it's consistent with FDA requirements.

CONCLUSION

For all the foregoing reasons, AMDR respectfully requests that this Court interpret "exceeds authorized access" as narrowly as possible under the intrusion theory of liability to preserve the longstanding right to repair your medical device – and any other "protected computer" – under the CFAA.

Respectfully Submitted,

STEPHEN D. TERMAN
Counsel of Record
J. MASON WEEDA
OLSSON FRANK WEEDA TERMAN MATZ PC
2000 Pennsylvania Ave., NW
Suite 3000
Washington, D.C. 20006
(202) 789-1212
sterman@ofwlaw.com

JEFFREY L. BERHOLD
JEFFREY L. BERHOLD, P.C.
1230 Peachtree St., Suite 1050
Atlanta, GA 30309
(404) 872-3800

C*ounsel for Amicus Curiae,*
Association of Medical Device
Reprocessors

July 7, 2020