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 SERVICE ORGANIZATIONS IN SUPPORT OF PETITIONER

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

JOHN G. DILLARD
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
jdillard@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

OTHER AUTHORITIES

INTEREST OF THE *AMICUS CURIAE*[1]

The Association of Medical Device Service Organizations ("AMDSO") is an international trade association organized to represent the interests of organizations that are engaged in the service and repair of reusable medical devices. AMDSO members are independent service organizations ("ISOs") and service and repair reusable medical devices for the healthcare industry across the U.S., ranging from small provider offices to large hospital groups. In order to service and repair medical devices, AMDSO members have quality systems in place that are audited to comply with a medical device quality standard promulgated by the International Organization for Standardization standards.[2] When servicing and repairing certain reusable medical devices, AMDSO

---

[1] No party or 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 (Mobile Instrument, Northfield Medical, Endoscopy Specialist, Inc., EndoMobile, Innovative Endoscopy Components, and Restore Robotics), 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* AMDSO on June 29, 2020 via electronic mail.

[2] U.S. Food and Drug Administration ("FDA") has historically opted to not actively regulate third-party service and repair of medical devices. In order to service and repair medical devices, AMDSO members have quality systems in place that are certified to comply with International Organization for Standardization standards. AMDSO members generally comply with International Organization for Standardization standard 13485 for Medical Device Quality Systems; *see* www.iso.org/iso-13485-medical-devices.html.

members may need to access information in a device's computer system. AMDSO's interest in this case involves the proper application of the Computer Fraud and Abuse Act ("CFAA") as it relates to the service and repair of medical devices.

Every reusable medical device requires service and repair, which can range from cleaning and disinfecting surgical instruments to maintaining and repairing ultrasound imaging systems. AMDSO members service and repair broad categories of medical devices, including endoscopes, imaging systems, drills and saws, and instruments for open, laparoscopic, and robotic surgery. ISOs work with and on behalf of hospitals to ensure reusable medical devices are in proper working condition and are serviced and repaired to ensure safety and effectiveness.

Medical device ISOs are part of a massive repair industry in the United States. The Food and Drug Administration concluded that "[ISOs] provide high quality, safe, and effective servicing of medical devices," and "the continued availability of third-party entities to service and repair medical devices is critical to the functioning of the U.S. healthcare system."[3] Healthcare providers save billions of dollars and eliminate millions of pounds of waste every year through the use of ISOs to keep their devices in working order. Those savings are passed on to patients and private and government insurers.

---

[3] FDA, *FDA Report on the Quality, Safety, and Effectiveness of Servicing of Medical Devices in Accordance with Section 710 of the Food and Drug Administration Reauthorization Act of 2017* (May 2018), *available at* www.fda.gov/media/113431/download.

ISOs play a similar role in a myriad of products from cars and trucks to heavy machinery and industrial robots that are operated or controlled in whole or in part by a "computer" as defined by the CFAA. Moreover, factories, offices and homes are being swept into the "internet of things" – devices that talk to each other and the cloud, *i.e.*, software and services that run over the internet. The internet of things includes everything from industrial robots to household refrigerators. As a result, more and more repairs involve access to a "protected computer" as defined by the CFAA. Altogether, the domestic repair industry overall is hundreds of billions of dollars. As described in more detail below, an overly broad interpretation of "exceeds authorized access" under Section 1030(a)(2) could have massive, unintended consequences for independent service organizations generally and AMDSO members specifically.

AMDSO is providing the court with the perspective of independent service organizations to ensure that its ruling does not have a massive unintended effect on the repair industry. 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.

SUMMARY OF ARGUMENT

The CFAA should be interpreted so not to prevent a device owner's right to repair. The right for owners to repair and maintain their own property, including medical devices, has been engrained in U.S. patent, trademark, and copyright law as well as state analogues. 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 CFAA was passed in 1986 to target serious computer crimes and has been interpreted by certain Circuits to have broader applicability than intended by Congress. As a result, OEMs have attempted to argue that medical devices and other devices and systems that such devices connect to, purportedly fall under the scope of the CFAA (some devices connect directly, or indirectly through an operating system on the generator or console, to the internet).

Medical device service and repair is lawful under the CFAA based upon the intrusion theory of liability (as adopted in the Second, Fourth, and Ninth Circuits), and is arguably unlawful under the misappropriation theory. As discussed in more detail below, third party repair and service companies may need to access information from the devices which have been acquired from healthcare providers. There is no malicious hacking, *i.e.*, breach of security, on someone else's device, because the ISO has permission from the device owner. In enacting and amending the statute, Congress showed no intent to adversely affect owners' rights to repair and maintain their property.

A broad interpretation of "exceeds authorized access" under the misappropriation theory may put the right to repair and service in peril. The misappropriation theory of liability opens the door for OEMs to impose "terms of use" on the device preventing downstream device owners and their agents (*i.e.*, ISOs) to access information on the device and system connected to it. These reusable devices are owned by the healthcare provider, yet the OEM would be able to restrain the right to repair.

Under the misappropriation theory, the CFAA could reach most modern-day products - medical devices, smart phones, household appliances, and motor vehicles. Extending control of servicing and repair to the manufacturer, would restrict the owners' rights thereby having a massive adverse impact on an industry that is critical to healthcare and ultimately increasing healthcare costs for the consumer as well as medical waste. AMDSO requests that this Court interpret "exceeds authorized access" under the intrusion theory of liability to preserve the longstanding right to repair.

ARGUMENT

I. MOST MODERN-DAY DEVICES, INCLUDING REUSABLE MEDICAL DEVICES, ARE "PROTECTED COMPUTERS" UNDER THE CFAA.

Section 1030(a)(2) prohibits anyone from exceeding "authorized access" of a "computer" and obtaining information from a "protected computer." 18 U.S.C. § 1030(a)(2)(C). The CFAA defines the terms "computer" and "protected computer." Computer is defined as "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). Household thermostats and microwave ovens are computers under this definition. So are MRI and CT imaging systems. *See*, *e.g.*, *Philips Med. Sys. Puerto Rico Inc. v. GIS Partners Corp.*, 203 F. Supp. 3d 221, 231 (D.P.R. 2016) (determining that MRI machine is a computer).

They are also "protected computers" because they "affect interstate commerce." 18 U.S.C. § 1030(e)(2)(B). The typical industrial or consumer device is sold in a nationwide or worldwide market and affects interstate commerce. Moreover, a "protected computer" effectively includes all "computers with Internet access." *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012). The typical device – from an endoscope to a refrigerator – is now connected to the internet.

As part of their quality systems, an ISO may need to "access" information stored on the device to ensure that the device is functioning properly and communicating with any connected devices. OEMs may impose "terms of use" that purport to govern "access" to information on the device or connected devices or systems and may limit such access. Although the ISO is not a party to such "terms of use," it is in possession of the device. Under such circumstances, the question is whether Congress intended the CFAA to allow OEMs to impose "terms of use" to limit the longstanding right to repair medical devices (and most modern devices that are "connected computers") by amending its "terms of use" language delineating when the user "exceeds authorized access."

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

The right to repair is recognized in patent, copyright, and trademark common law. "The 'first sale' doctrine is a common-law doctrine with an impeccable historic pedigree." *Kirtsaeng v. John Wiley & Sons, Inc.*, 133 S. Ct. 1351, 1363 (2013). After first sale, 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. *Impression Prod., Inc. v. Lexmark Int'l, Inc.*, 137 S. Ct. 1523, 1531–32 (2017). Similarly, repair of a product that has a trademark or a copywritten software product does not form the basis for liability under trademark or copyright law. *See Champion Spark Plug Co. v. Sanders*, 67 S. Ct. 1136 (1947), *Prestonettes, Inc., v. Coty*, 44 S. Ct. 350, 351

(1924); *Universal Instruments Corp. v. Micro Sys. Eng'g, Inc.*, 924 F.3d 32, 46 (2d Cir. 2019) (citing 17 U.S.C. § 117(a)).

Congress did not intend for the CFAA to infringe upon owners' right to repair. Instead, Congress intended the CFAA to apply to instances of hacking. *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1000 (9th Cir. 2019)("The CFAA was enacted to prevent intentional intrusion onto someone else's computer—specifically, computer hacking"). Put simply, the CFAA is intended to prevent accessing a computer without authorization, *i.e.*, accessing another person's device without permission.

Service and repair of reusable medical devices is lawful and does not constitute "unauthorized access" under the intrusion theory of liability. An ISO is not breaking into another person's computer; it is servicing and repairing the device on behalf of the owner (*e.g.*, a hospital, or health care provider) to ensure the device functions as intended. Under these circumstances, the reprocessor is not "breaking and entering" anyone else's computer. *U.S. v. Valle*, 807 F.3d 508, 525 (2d Cir. 2015).

Many reusable medical devices are connected to other devices and computer systems or equipment. An ISO may need to access information on such connected devices to ensure the reusable device functions as intended. For example, an ISO may have to obtain information from the device to reset it. An ISO's quality system procedures may require testing and verification and validation activities to ensure proper function.

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 scope of "computer" and "protected computer" is broad, but that does not change the fact that a device owner may repair his or her own device.

In the absence of evidence that Congress intended the CFAA to limit the right to repair, the Court must presume that Congress intended to retain the right under common law. *Kirtsaeng*, 133 S. Ct. at 1363. The right to repair has continued through the development of the law of patent, copyright, and trademark and such right should not be defeated by the CFAA.

III. THE MISAPPROPRIATION THEORY OF LIABILITY UNDER THE CFAA WOULD PUT THE RIGHT TO REPAIR AT RISK.

Under the misappropriation theory of liability, the OEM would define what is authorized access to a device. OEMs have tremendous incentive to restrict third-party repairs in the fine print of the terms of use. ISOs create competition in the repair aftermarket – reducing overall prices and taking market share from the OEMs. They also reduce the ability of the OEM to steer the consumer away from repairing the existing device to purchasing a new one. The ISO has no say in the terms of use dictated by the OEM to the consumer.

OEMs already include "terms of use" on most reusable medical devices that restrict the owner and end user of the product – this may be included on the label, as part of the contract, or as part of "clickwrap" for devices that have a software interface. Those terms of use can include broad restrictions, *e.g.*, only the OEM may service the device, or more specific restrictions, *e.g.*, accessing firmware on the device. The OEM could argue under the misappropriation theory that the device owner is violating the CFAA by violating access restrictions in its own terms of use. This would essentially prohibit the device owner or the ISO of its choosing from doing the necessary inspection, repair, and of the device.

Importantly, the CFAA imposes both criminal and civil liability, including injunctive relief, and the interpretation of "exceeds authorized access" here will apply equally to civil liability under the CFAA. *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012). Accordingly, relying on prosecutorial discretion would not save the right to repair, *i.e.*, ISOs would still be subject to civil liability for exceeding authorized access under the CFAA, even if the Department of Justice decided not to prosecute such cases criminally. Civil liability includes compensatory damages and equitable relief for any person who suffers damages or loss. 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). Would the OEM be able to restrict the use of "data, a program, a system, or information" on your device? Loss includes the cost of "responding to an offense" or "conducting a damage assessment."

18 U.S.C. § 1030(e)(11). Would loss include the cost of preparing and bringing a civil action?

In theory, the OEM would be able to create liability for the ISO simply by promulgating restrictive terms of use and "responding" to violations of those terms of use. The OEM could turn something perfectly legal – the repair of your device – into something that may be subject to criminal sanction and civil injunction. It would overturn centuries of jurisprudence on the right to repair. It would upend repair markets totaling hundreds of billions of dollars. There is no evidence that Congress intended the CFAA to reach this far.

Based on the foregoing, an overly broad interpretation of "exceeds authorized access" would allow the OEM to dictate when and how the CFAA applies and restrict the right to repair, having a massive impact on the healthcare industry. The result would be a significant increase in healthcare costs and medical waste. Ultimately, it would be the consumer paying the price, as these increases in healthcare costs will trickle down to the patient, employer, and taxpayer. AMDSO members are instrumental to the delivery of life saving medical technologies, while keeping costs down. AMDSO strongly believes that downstream entities should not be blocked from the right to repair by OEMs one-sided and self-serving terms of use.

CONCLUSION

For all the foregoing reasons, AMDSO 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,

JOHN G. DILLARD
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
jdillard@ofwlaw.com

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

Counsel for Amicus Curiae,
Association of Medical Device
Service Organizations

July 7, 2020