UNITED STATES COPYRIGHT OFFICE

Long Comment Regarding a Proposed Exemption Under 17 U.S.C. § 1201

This is a Word document that allows users to type into the spaces below. The comment may be single-spaced but should be in at least 12-point type. The italicized instructions on this template may be deleted.

Please submit a separate comment for each proposed class.

NOTE: This form must be used in all three rounds of comments by all commenters not submitting short-form comments directly through Regulations.gov, whether the commenter is supporting, opposing, or merely providing pertinent information about a proposed exemption.

When commenting on a proposed expansion to an existing exemption, you should focus your comments only on those issues relevant to the proposed expansion.

[ ] Check here if multimedia evidence is being provided in connection with this comment.

ITEM A. COMMENTER INFORMATION

Meredith Rose, *Senior Policy Counsel*
mrose@publicknowledge.org

Public Knowledge
1818 N St NW, Ste 410
Washington, DC 20036

Kyle Weins, *CEO*
kyle@ifixit.com
Elizabeth Chamberlain, *Dir. of Sustainability*
elizabeth@ifixit.com
iFixit
1330 Monterey St.
San Luis Obispo, CA 93401

ITEM B. PROPOSED CLASS ADDRESSED

Class 5: Computer Programs--Repair

ITEM C. OVERVIEW

We seek to expand the existing exemption for repair of consumer devices to include industrial and commercial equipment. While numerous policy rationales for this expansion exist, "as a threshold matter, the Register considers whether proponents have established a record that supports defining the class of works broadly by demonstrating that sufficient commonalities exist for the proposed uses."[1] The Register has previously held that a class is appropriate in scope "where the record establishes that users of such works are similarly affected by the prohibition on circumvention, and where . . . the class is further narrowed by reference to particular types of uses"[2] and commonality among different device types.[3] In short, a class must show that (1) users are similarly situated regarding the need for circumvention; (2) the uses covered by the proposal are similar; and (3) the devices themselves share sufficient commonalities.

Previous recommendations have specifically cited an insufficient record on the first (similarly situated users) and third (commonalities among devices) elements as a primary reason for rejecting an expanded exemption.[4] We seek to correct that here by explaining how users are similarly situated, and providing appropriately "illustrative examples of a wide variety of devices" within the proposed category.[5] To do this, we have selected four "index" examples that illustrate the necessity of the proposed exemption, as well as the universality and scope of adverse effects: commercial food preparation, construction equipment, programmable logic controllers (PLCs), and enterprise IT. All devices are designed for ongoing commercial and industrial use. All devices are outfitted with operation-critical software whose diagnosis, maintenance, and repair functions are locked behind a TPM. And in all cases, the lack of an

[1] U.S. COPYRIGHT OFFICE, SECTION 1201 RULEMAKING: SEVENTH TRIENNIAL PROCEEDING TO DETERMINE EXEMPTIONS TO THE PROHIBITION ON CIRCUMVENTION, RECOMMENDATION OF THE REGISTER OF COPYRIGHTS 194 (2021) ("2021 Recommendation").

[2] 2021 Recommendation at 197.

[3] 2021 Recommendation at 194.

[4] 2021 Recommendation at 202, citing U.S. COPYRIGHT OFFICE, SECTION 1201 RULEMAKING: SIXTH TRIENNIAL PROCEEDING TO DETERMINE EXEMPTIONS TO THE PROHIBITION ON CIRCUMVENTION, RECOMMENDATION OF THE REGISTER OF COPYRIGHTS 191-94, 202-05 (2018) ("2018 Recommendation").

[5] 2021 Recommendation at 202.

exemption--and the resulting downtime caused by the user's inability to perform the most basic diagnosis and repair--results in significant, quantifiable financial harm.

ITEM D. TECHNOLOGICAL PROTECTION MEASURE(S) AND METHOD(S) OF CIRCUMVENTION

Commercial Soft Serve Machines

The Taylor Company manufactures a wide range of commercial food preparation equipment, including grills, frozen drink machines, and batch freezers. Most well-known is their soft serve machine. Thanks to a six-decade partnership with McDonald's, Taylor machines are found in more than 13,000 franchise locations worldwide.[6] It was not until 2017 that McDonald's began to allow franchisees to purchase machines from another source.[7] The physical components are relatively simple; its functionality is primarily controlled by its onboard computer.[8]

When a Taylor soft serve machine breaks, it displays an error code. These codes--such as "(L/R) BRL>41°F (5°C) AFTER PF"--are unintuitive and require interpretive aid. While error codes are listed in the Owner's Manual, others require access to a service manual only made available to authorized technicians, or accessible via a TPM-locked on-device service menu. This menu can be accessed either by use of a Taylor-approved diagnostic tool, or via an extended, undocumented combination of key presses.[9] Codes are also regularly updated and re-assigned via firmware updates, meaning that a code translation from June may no longer be accurate in

[6] Andy Greenberg, *They Hacked McDonald's Ice Cream Machines--and Started a Cold War,* WIRED (Apr. 28, 2021), https://www.wired.com/story/they-hacked-mcdonalds-ice-cream-makers-started-cold-war/.

[7] Julie Jargon, *McDonald's Customers Scream, and Get New Ice Cream Machines,* WALL ST. J., (Mar. 2, 2017), https://www.wsj.com/articles/mcdonalds-customers-scream-and-get-new-ice-cream-machines-1488476862.

[8] Petitioner iFixIt conducted a detailed "teardown" video of a Taylor C709 ice cream machine, discussing both its physical components and the error codes they encountered in the process, which the Office may find useful for its review. iFixIt, *Why McDonald's Ice Cream Machines Are Always Broken and How To Fix Them*, YouTube (Aug. 29, 2023), https://www.youtube.com/watch?v=2uCpY3tFTIA.

[9] Greenberg, supra n 6. Importantly, it is unclear whether the 16-press key sequence documented in 2021 still works, or has been changed in subsequent firmware updates.

December.[10] And although Taylor includes an Owner's Manual with its new machines, these manuals are incomplete, laid out in a way that is confusing to would-be repairers, and often already out of date by the time they ship.

Construction Equipment: Proprietary Diagnostic Kits

Sennebogen, Liebherr, and Caterpillar are heavy equipment manufacturers. Sennebogen primarily produces cranes and material handlers;[11] Liebherr and Caterpillar manufacture a wide variety of construction equipment including cranes, earth movers, excavators, and concrete equipment.[12] These machines utilized networked sensors that connect to a central computerized diagnostic system.

For all three companies' products, critical diagnostic and error information is locked behind TPMs that can only be bypassed by using authorized, licensed, and branded tools. Sennebogen requires a proprietary control system, known as a SenCon, which it regularly refuses to sell or provide to large dealers.[13] Liebherr machines depend on two separate kits: LiDIA (for hydraulics systems) and SCULi (for engines), which are only available by private sale to authorized technicians.[14] Caterpillar uses the CAT ET system, which is only available with full functionality

[10] Notably, Taylor technicians regularly deploy firmware updates as part of repair visits--at times without informing the franchise owners.

[11] *Products*, Sennebogen https://www.sennebogen.com/en/products (retrieved Dec. 20, 2023).

[12] *Construction Machines*, Liebherr, https://www.liebherr.com/en/usa/products/construction-machines/construction-machines.html (retrieved Dec. 20, 2023); *Equipment*, Caterpillar, https://www.cat.com/en_US/products/new/equipment.html (retrieved Dec. 20, 2023).

[13] We spoke with two companies who deal with this equipment regularly: Process Equipment, a large materials handling equipment company based in Florida; and Kuhn EQ, a dealer of heavy equipment for the recycling industry that is an authorized dealer for Lefort, but not Sennebogen, Liebherr, or Caterpillar. Process Equipment reported challenges acquiring necessary diagnostic tooling. Kuhn EQ Sales said they're facing exactly the same issues, and added that every heavy equipment company has its own proprietary diagnostics software. Kuhn Sales Manager Mike Schulz notd that when he entered the business 15 years ago, he knew a repair tech who could troubleshoot any engine by the way it sounded; now, all repairs require a laptop, and most require they defer to a dealer or authorized technician.

[14] *Digital products and services for combustion engines: Minimize your downtime.*, Liebherr https://www.liebherr.com/en/usa/products/components/combustion-engines/digital-products/digital-products.html (last retrieved Dec. 20, 2023). The LiDIA system also comes in two "flavors": "Technician Servicer," and a more limited "Technician Light" license which provides a narrower slice of functionality. *LiDIA Diagnostics Tool*, Liebherr, https://www.

to dealers and authorized technicians.[15] Many repairs involving the electronic control module (ECM) in a CAT machine--such as restoring "working hours" settings after rebuilding an engine--require a CAT ET license only available to dealers.

Programmable Logic Controllers

Programmable logic controllers (PLCs) are computers that have been adapted specifically to control and coordinate manufacturing processes at scale. There are many manufacturers making PLCs, from Siemens to Honeywell. Some PLCs control access to safety functions such as detecting equipment failures[16] or unsafe conditions within the manufacturing process.[17] Although PLCs by themselves cost several hundred dollars, the complex manufacturing systems they control (and into which they are integrated) can cost multiple millions.[18]

Many PLCs are purchased as part of an integrated system package; in such cases, system integrators write custom code to control a machine, and sell it as a package to the customer. That code is protected behind the password. Different integrators have different perspectives on whether this code should be locked for security purposes, and if so, at whose discretion (i.e. by

liebherr.com/shared/media/components/documents/einspritzsysteme/liebherr-lidia-diagnostics-tool-short-description.pdf (last retrieved Dec. 20, 2023).

[15] Adept Ape, *How to use Cat ET. Cat Electronic Technician.*, YouTube (Feb. 4, 2021), https://www.youtube.com/watch?v=QsMgZcT_LCw; Comment of user shovelDr, *Need CAT Electronic Technician Software*, Reddit, https://www.reddit.com/r/caterpillar/comments/ti0z3m/comment/i1bdq0a/?utm_source=share&utm_medium=web3x&utm_name=web3xcss&utm_term=1&utm_content=share_button (last retrieved Dec. 20, 2023)

[16] Tanner Grieve, *What Are Safety PLCs?*, Huffman Engineering Inc (Jul. 18, 2017), https://huffmaneng.com/what-are-safety-plcs/.

[17] Ted Mortenson, *What is a Safety PLC?*, Realpars.com (Jul. 6, 2020), https://www.realpars.com/blog/safety-plc.

[18] Comment of user MagnaVoxx, *Supplier wont supply safety password*, Reddit (2023), https://www.reddit.com/r/PLC/comments/16gjjrw/comment/k08l3ci/?utm_source=share&utm_medium=web3x&utm_name=web3xcss&utm_term=1&utm_content=share_button ("This is a matter of ownership first for us, secondly it's a matter of uptime. If we paid 20M+ EUR for a machine we pay for the whole machine, not for a 3rd party (that may not even exist 5-10 years from now) holding the keys to it").

the manufacturer, integrator, vendor, or end user).[19] Servicing the machine requires access to the code, even to change tiny things like timing of functions or system operating hours.

PLC manufacturers take varying approaches to security; however, the most common structure is that access to the PLC's underlying software--including diagnostic and maintenance information--is password protected by default. These passwords may be set by the user during initial setup, or by the PLC's vendor. Vendors often refuse to share these passwords with purchasers. For some models, such as the Siemens Simatic Step 7/S7,[20] lost passwords cannot be reset or recovered.[21] The PLC is rendered unusable; the only solution is to buy a replacement PLC.

Enterprise IT

Dell EMC is a manufacturer of enterprise IT equipment. Its clients include the federal government.[22] It has developed, then abandoned support for, multiple lines of digital storage products, including the DMX, VmaxE, and Vmax2 lines.

These digital storage products contain multiple known points of failure, including failures of storage drives, main boards, and midplane controllers.[23] To access diagnostics, perform

---

[19] User rnav24, *Locking out your code*, Reddit (2018), https://www.reddit.com/r/PLC/comments/bh1itd/locking_out_your_code/ (last retrieved Dec. 20, 2023).

[20] Simatic S7-1200, Siemens, https://www.siemens.com/global/en/products/automation/systems/industrial/plc/s7-1200.html (last retrieved Dec. 20, 2023)

[21] Post by user StamGuy, *Accessing a PLC that is locked with a password*, Siemens Industry Online Support (Jul. 17, 2017), https://support.industry.siemens.com/forum/WW/en/posts/accessing-a-plc-that-is-locked-with-password/171245 ; Post by user ABD2008, *what can i do with CPU S7-313C protected by password ?*, Siemens Industry Online Support (Jan. 26, 2009), https://support.industry.siemens.com/forum/WW/en/posts/what-can-i-do-with-cpu-s7-313c-protected-by-password/25933/?page=0&pageSize=10 ; see also SIMATIC Process Control System PCS 7 Compendium Part F - Industrial Security (V8.2), https://cache.industry.siemens.com/dl/files/220/109742220/att_898787/v1/pcs7_compendium_part_f_en-US_en-US.pdf (last retrieved Dec. 20, 2023)

[22] *Federal Government IT*, Dell, https://www.dell.com/en-us/lp/industry-federal-government-it (last retrieved Dec. 20, 2023).

[23] *See, e.g.*, *ECS: Overview and Architecture: Failure Tolerance*, Dell, https://infohub.delltechnologies.com/l/ecs-overview-and-architecture/failure-tolerance-3/ (last retrieved Dec. 20, 2023); *Dell EMC VMAX All Flash Product Guide*, https://www.delltechnologies.com/asset/it-it/products/storage/technical-support/docu67503.pdf (last retrieved Dec. 20, 2023).

maintenance, or replace parts on the machine, the user must input a cryptographic key (specifically, an RSA rotating encrypted passcode). Dell EMC will not supply these passcodes under any circumstances to individuals other than their own technicians.

IBM's Power line of servers similarly require access to a key to perform an array of basic diagnosis, maintenance, and repair functions. Firmware updates require a user to input an Upgrade Access Key (UAK). UAKs are only available to users under maintenance agreements, and IBM has sole discretion to determine which firmware upgrades can be loaded freely, and which require a UAK.

IBM mainframes also require the use of proprietary software tools to replace components such as processors.[24] Maintenance functions must be authorized by passwords which are only made available to IBM employees. For example, a failed CPU can only be replaced by an IBM technician--and for older models for which IBM no longer provides maintenance, there is no possible way to replace the CPU without circumvention. Other maintenance failures, such as "pinned data," cannot be fixed without special keys held exclusively by IBM technicians.

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

Due to the unusually broad nature of the proposed class, we will proceed in three stages. First, we will discuss the viability of "industrial and commercial equipment" as a proposed class, with reference to the Office's previously articulated standards on appropriate class scope. Second, we will conduct a brief fair use analysis, again relying on the Office's previous work in this area. Finally, we will proceed to the adverse effects analysis, focusing primarily on the lack of available and realistic alternatives to circumvention in each of the index examples.

Scope of the Class

As noted above, a class's scope is appropriate when "users of such works are similarly affected by the prohibition on circumvention, and where . . . the class is further narrowed by

[24] For a demonstration of IBM's proprietary software and its use, see Francesco F, *Servicing a million dollar computer - IBM System z10 Mainframe - Replacing a faulty MDA*, YouTube (Nov. 19, 2022), https://www.youtube.com/watch?v=WJLxuUej_JA .

reference to particular types of uses"[25] and the record is sufficiently developed to establish "commonalities … among different device types."[26] In short, a class must show that (1) users are similarly situated regarding the need for circumvention; (2) the uses covered by the proposal are similar; and (3) the devices themselves share sufficient commonalities to be considered as a class.

Users are similarly situated regarding the need for circumvention.

Users, in all cases, are engaged in commercial or industrial activities (or equivalent activities for non-profit or charitable purposes). Lack of third party or self-help repair options results invariably in significant, quantifiable financial harm due to equipment downtime. Each of these devices is used for an ultimately commercial purpose, be it manufacturing, food service, data storage, or construction, and are designed to provide return on their users' substantial up-front investment. Downtime due to a broken industrial or commercial device represents a direct and often irreversible loss of revenue. The cost of downtime varies by device and industry, but ranges from hundreds[27] to millions of dollars per day.[28]

Uses covered by the proposed exemption are similar.

In all cases, the uses are limited to diagnosis, maintenance, and repair necessary to restore affected equipment to pre-error levels of functionality.

[25] 2021 Recommendation at 197.

[26] Id. at 196.

[27] Melissa McMillen, *How Equipment Downtime Affects Your Bottom Line (and What to Do About It)*, QSRSoft (Sep. 7, 2022), https://www.qsrsoft.com/blog/how-equipment-downtime-affects-your-bottom-line-and-what-to-do-about-it/.

[28] Sundeep Ravande, *Unplanned Downtime Costs More Than You Think*, Forbes (Feb. 22, 2022), https://www.forbes.com/sites/forbestechcouncil/2022/02/22/unplanned-downtime-costs-more-than-you-think/?sh=29a2177036f7.

The devices themselves share sufficient commonalities to constitute a cohesive class.

The proposed class consists of physical devices, controlled by copyrighted software, that are designed for use in commercial or industrial settings.[29] Devices designed or marketed for medical, scientific, or consumer use should remain outside the scope of this class. The proposed class covers equipment that is designed for, marketed at, sold to, and utilized by commercial actors.[30] Additionally, devices within the class employ computerized diagnosis and error-identification functions which are locked behind TPMs.

Fair Use

The Register has repeatedly held that "diagnosis, maintenance, and repair of software-enabled consumer devices are likely to be fair uses where the purpose is to restore device functionality."[31] When "properly applied, the fair use factors—together with the existing case law—should ensure that consumers, repair technicians, and other interested parties will be able to engage in most traditional repair . . . activities without fear of copyright infringement liability."[32] However, in order to ensure a thorough record, we will revisit the four factors briefly.

---

[29] Existing statutory definitions may be useful in framing the class. 42 U.S.C. § 6311 defines industrial equipment in part as a device "which, to any significant extent, is distributed in commerce for industrial or commercial use." The Occupational Health and Safety Administration identifies manufacturers of "Industrial and Commercial Machinery and Computer Equipment" to include facilities that are engaged in "the manufacture of engines and turbines; farm and garden machinery; construction, mining, and oil field machinery; elevators and conveying equipment; hoists, cranes, monorails, and industrial trucks and tractors; metalworking machinery; special industry machinery; general industrial machinery; computer and peripheral equipment and office machinery; and refrigeration and service industry machinery." Major Group 35: Industrial and Commercial Machinery and Computer Equipment, Occupational Health & Safety Admin., https://www.osha.gov/data/sic-manual/major-group-35 (last retrieved Dec. 20, 2023).

[30] Although we believe that "commercial" is an easy and appropriate shorthand to describe the class of users, the devices listed--most notably enterprise IT and construction equipment--are also used by non-profit organizations. We caution the Copyright Office not to adopt exemption language that may accidentally exclude this class of users.

[31] 2021 Recommendation at 202.

[32] U.S. COPYRIGHT OFFICE, SOFTWARE-ENABLED CONSUMER PRODUCTS, REPORT OF THE REGISTER OF COPYRIGHTS 39 (2016) ("Software Study").

The first factor, the purpose and character of the use, favors fair use. Accessing and utilizing the copyrighted software is necessary for the diagnosis, maintenance, and repair of the devices containing (or operated by) said software. Specifically, the use is necessary in order to achieve full functionality, and "restore a device[]... to its previous working state."[33] Modification, optimizing, and "tinkering" fall outside the scope of our proposed exemption.

The second and third factors also favor fair use. Control software for industrial and commercial equipment is "essentially functional," and "not meant to be consumed as a creative work."[34] Moreover, "use of the entire software work" in diagnosis, maintenance, and repair "is reasonable because it often requires analysis of the full software program, and the ultimate product does not contain infringing copies."[35]

Finally, as with consumer devices, there is no separable market for the underlying software. The software is specific to the make, model (and occasionally, the specific item or factory configuration) of the physical device in which it is embedded. Instead, repair bolsters the market for the copyrighted works, as "repair supports—rather than displaces—the purpose of the embedded programs that control the device."[36]

Taken together, the four factors significantly favor the proposed exemption.

---

[33] 2021 Recommendation at 201, citing iFixit & Repair Ass'n Class 12 Reply at 4 (citing *Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc.*, 421 F.3d 1307 (Fed. Cir. 2005); *Sony Computer Entm't v. Connectix Corp*., 203 F.3d 596 (9th Cir. 2000); *Sega Enters. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992)).

[34] 2021 p 201, citing iFixit & Repair Ass'n Class 12 Reply at 5.

[35] *Id.*

[36] Software Study at 40.

Adverse Effects

First factor: the availability for use of copyrighted works.

Commercial Soft Serve Machines

Malfunctioning Taylor machines are not an isolated problem; the issue is so widespread that it has become a news story in its own right[37] and spawned an entire website dedicated to identifying locations with broken machines.[38]

Users attempting to diagnose a broken Taylor soft serve machine without circumvention have two options, neither of which are remotely realistic. First, they can attempt to consult the user manual that shipped with their machine. However, as noted above, the manuals themselves are often outdated and incomplete. Error codes change with each firmware update, and the Taylor practice of having technicians install firmware updates at each visit means that owners may not even know how out of date their manual is. Many codes are not listed in the manual at all, but are only available to authorized technicians, and are locked behind a TPM via an on-device service menu.

The second (unrealistic) option for users is to identify and execute a complex, undocumented 16-press button sequence which may or may not operate after a given firmware update. Neither of these are viable alternatives to using external tools to circumvent Taylor's TPM protecting the secret technician menu.

The financial harm suffered by a franchisee faced with a broken machine is significant. As one blog notes, "You could miss out on 200 or more item sales in a day equaling $600 in sales and $450 in gross margin profit. That one equipment breakdown just cost you $625 in sales in a single day."[39] Franchisees have reported long wait times for needed repairs, and a visit from a Taylor licensed repair technician costs over $300 per fifteen minutes.

---

[37] Greenberg, supra n 6.

[38] MCBROKEN, https://mcbroken.com/ (last retrieved Dec. 20, 2023). At the time of writing, five of the 27 McDonald's soft serve machines within the District of Columbia (18.5%) were broken or "inconclusive." New York City was the most beknighted metropolis, with more than a quarter of the city's soft-serve machines down.

[39] McMillen, supra n 27.

Construction Equipment

Users attempting diagnosis, maintenance, or repair on construction equipment have no realistic alternative to circumvention. Liebherr machines are only accessible via the company's proprietary LiDIA and SCULi systems. The standard wait time for a Liebherr technician to visit some dealers is approximately 90 days; technicians have also implied to dealer representatives that they have been given explicit instructions not to support equipment sold by these dealers. As noted above, Sennebogen similarly refuses to sell its SenCon diagnostic equipment to dealers.

Caterpillar sells a consumer version of its CAT ET diagnostic equipment; however, its capabilities are significantly limited. Maintenance affecting the electronic control module (ECM) in a CAT machine--such as resetting a machine's working hours, after its engine has been rebuilt--requires dealer-level CAT ET access, which is available only to authorized dealers.[40]

Third-party laptop systems, such as those made by Jaltest,[41] provide only limited diagnostic capabilities. They cannot interpret the full range of fault codes; so-called "event codes" on Caterpillar machines, for example, can only be cleared with the dealer license of CAT ET. The official public description for most event codes reads simply, "Contact your local Caterpillar dealer to clear this event code."[42]

Programmable Logic Controllers

PLCs are often customized for a specific installation, with code and parameters specific to that location. While the exact arrangement depends on the manufacturer, integrator, and/or vendor, it is possible for an owner to get into a situation where they have no alternative than to bypass the lock or replace the unit. As noted above, system integrators write custom code to control a machine, and sell it as a package to the customer. That code is protected behind the

---

[40] Tyler Robertson, *Heavy Truck Engine ECM Programming*, Diesel Laptops (May 7, 2020), https://www.diesellaptops.com/blogs/news/heavy-truck-engine-ecm-programming ("Your only option when it comes to CAT ECM programming is to bring it to your local CAT dealer or distributor.").

[41] Jaltest OHW, Jaltest, https://www.jaltest.com/en/diagnostics/jaltest-ohw-construction-machinery/ (last retrieved Dec. 20, 2023).

[42] See, e.g., *Table 4. Event Codes, Manual for Caterpillar Front-Loader*, https://constructionloader.tpub.com/TM-5-3805-291-23-1/TM-5-3805-291-23-100438.html.

password. TPM practices (and opinions) among integrators vary widely, while owners almost universally believe they should have full access to the systems they have paid to create.[43]

In some PLC models, circumvention is unavoidable. Newer models of the Siemens Simatic Step 7/S7, for example, cannot be accessed without the password. If the password is lost, the module must simply be thrown away and replaced, losing all code and customizations.[44]

For some models, access without circumvention is technically possible, but unrealistic. Older models of the Siemens S7, for example, can be bypassed by swapping out the memory module. However, this largely obliterates the usefulness of the underlying program, as comments and local variables are completely wiped from the resulting reboot.[45] Users have noted that suppliers have become increasingly reluctant to share passwords in recent years,[46] citing reasons that range from fears of Chinese IP theft, to protecting "proprietary" code,[47] to liability issues,[48] to vague, generalized legal reluctance.[49]

---

[43] User rnav24, supra n 19.

[44] Comment of user Marcjan, *s7 300 password reset*, Siemens Industry Online Support (Dec. 17, 2013), https://support.industry.siemens.com/forum/WW/en/posts/s7-300-password-reset/101658/?page=0&pageSize=10 (last retrieved Dec. 20, 2023).

[45] Comment of user Marcjan, *PASSWORD PROTECTED MMC*, Siemens Industry Online Support (Mar. 11, 2014), https://support.industry.siemens.com/forum/WW/en/posts/password-protected-mmc/105121?page=0&pageSize=10 (last retrieved Dec. 20, 2023).

[46] MagnaVoxx, supra n 18 ("It's become more common the last few years for some reason. 10-15 years ago there was not nearly as much resistance to this.").

[47] User TheRealTogaKing, *Serious Question. Why do OEMs password lock their programs?*, Reddit (2021), https://www.reddit.com/r/PLC/comments/s2khxp/serious_question_why_do_oems_password_lock_their/ (last retrieved Dec. 20, 2023).

[48] User pickpack_paddywhack, *Supplier wont supply safety password*, Reddit (2023), https://www.reddit.com/r/PLC/comments/16gjjrw/supplier_wont_supply_safety_password/ (last retrieved Dec. 20, 2023); Comment of user SpaceAgePotatoCakes, *When documentation is gone and past integrators password protected the devices,* Reddit (2023), https://www.reddit.com/r/PLC/comments/12ck3cl/when_documentation_is_gone_and_past_integrators/ (last retrieved Dec. 20, 2023) ("At my last job it was a liability thing, we'd lock down the safety system to ensure nobody did something dangerous like bypass a trip. If the customer wanted access they could sign the paperwork to unlock it and then if they blew something up it was on them.").

[49] *Id*. ("They claim their Legal department wont allow them to share the password, even tho we suggested that we sign document saying supplier responsibility is connected to the checksum." [sic])

Manufacturing, like agriculture, is extremely time-sensitive. While the loss of use and time required to rebuild the necessary programming may not be a significant burden for consumer devices, the work stoppage needed to rebuild a process-critical manufacturing PLC could permanently damage the business. Downtime is expensive: the 2019 average estimated cost of unplanned manufacturing downtime was $260,000 per hour,[50] while automotive manufacturing stoppage costs approximately $22,000 per minute.[51] It also harms businesses' relationships with their customers; a 2019 survey found that, during periods of stoppage, "46 percent couldn't deliver services to customers, 37 percent lost production time on a critical asset, and 29 percent were totally unable to service or support specific equipment or assets."[52] As one user noted,

> This is a matter of ownership first for us, secondly it's a matter of uptime. If we paid 20M+ EUR for a machine we pay for the whole machine, not for a 3rd party (that may not even exist 5-10 years from now) holding the keys to it. If we have to do a repair of the PLC, even if we don't do it ourself [sic], we can't rely on the supplier to get some commissioning guy that may be in China for 3 months first.[53]

The need for circumvention is not something that can be adequately contracted around or ameliorated by competition. While a physical PLC unit may be bog-standard, its software must be custom tailored to the specific plant and interfacing equipment. This means that PLC integrators and vendors are often specialized to certain kinds of fields. And contracts do not prevent integrators, manufacturers, or password-holding vendors from going out of business.

Internet forums are filled with countless stories of users being stymied: passwords held by a long-departed administrator,[54] suppliers going out of business and becoming unreachable. The Office has previously noted that the need for circumvention in industrial and commercial

---

[50] *The actual cost of downtime in the manufacturing industry*, IIOT WORLD (Nov. 14, 2018), https://www.iiot-world.com/predictive-analytics/predictive-maintenance/the-actual-cost-of-downtime-in-the-manufacturing-industry/

[51] Ravande, supra n 28.

[52] IIOT World, supra n 50.

[53] MagnaVoxx, supra n 18.

[54] User dyalndlaotn, *Locked out of PLC*, Reddit (2022), https://www.reddit.com/r/PLC/comments/zj6bb6/comment/iztul5y/?utm_source=share&utm_medium=web3x&utm_name=web3xcss&utm_term=1&utm_content=share_button (last retrieved Dec. 20, 2023).

contexts may be less, because equipment buyers enjoy greater negotiating power with manufacturers. While this power dynamic may be true, it is also only half the picture.

Moreover, the impact of PLC locks can be significant, as a recent problem with the Polish passenger train system illustrates. A Polish regional train operator purchased 11 trains from manufacturer Newag. Although Newag won the production bid, they lost the bidding process for the associated maintenance contract, which went instead to a well-established independent repair company called SPS. During routine maintenance, SPS began noticing "mysterious errors" that prevented the trains from running. At a loss, they hired a security research firm to try and diagnose the issue. As the security researchers later described it, "we discovered a 'workshop-detection' system built into the train software, which bricked the trains after some conditions were met (two of the trains even used a list of precise GPS coordinates of competitors' workshops). We also discovered an undocumented 'unlock code' which you could enter from the train driver's panel which magically fixed the issue.'"[55] The security researchers were ultimately able to bypass the measures and fix the trains.[56] They also released a detailed report on their work (in Polish), including documentation of the kinds of DRM they encountered, and presented their results at the Oh My H@ck conference this December.[57]

Enterprise IT

Enterprise IT equipment is frequently installed in critical applications, where a storage array failure can result in loss of access to medical records or business data. A study commissioned by

[55] Jason Koebler, *Polish Hackers Repaired Trains the Manufacturer Artificially Bricked. Now The Train Company Is Threatening Them*, 404 Media (Dec. 13, 2023), https://www.404media.co/polish-hackers-repaired-trains-the-manufacturer-artificially-bricked-now-the-train-company-is-threatening-them/.

[56] *Dieselgate, but for trains – some heavyweight hardware hacking*, BadCyber (Dec. 5, 2023), https://badcyber.com/dieselgate-but-for-trains-some-heavyweight-hardware-hacking/.

[57] *Hakerzy odpowiadają Newagowi*, Rynek Kolejowy (Dec. 5, 2023), https://www.rynek-kolejowy.pl/wiadomosci/hakerzy-odpowiadaja-newagowi-116487.html.

IBM estimated the cost to businesses of planned mainframe outages at $1.5m per quarter.[58] A 2016 study estimated that unplanned outages, by contrast, cost nearly $9,000 per *minute*.[59]

These incidents are neither rare nor novel. New Iron Solutions, an IT staffing company, describes some historical incidents caused by unplanned mainframe downtime:

> Nielsen: In 2009, a mainframe glitch at the start of the television season brought down all of this company's primary TV ratings services for several days. The problems were traced to the relocation of Nielsen's mainframe computing system. A client described the situation as 'continuous chaos.' Nielsen lost millions of dollars and suffered lingering damage to its reputation.
> HSBC Bank: In 2010, customers of this international bank were unable to perform online banking or use ATMs because of a mainframe outage. It was the second such crash in six months. Similar problems occurred at HSBC three years later in 2013, affecting millions of users. The bank lost money and customers.
> Taiwan: In August 2018, ATMS throughout Taiwan crashed for two hours because of programming errors in the IBM mainframe and crippled inter-bank transactions, resulting in lost profit and a damaged reputation.[60]

> Second and third factors: the availability for use of works for nonprofit archival, preservation, and educational purposes; the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research.

As noted previously, "these factors have limited relevance to the proposed uses."[61] However, as an exemption would remove significant impediments to training and research into these

[58] *The Real Costs Of Planned And Unplanned Downtime*, Forrester (Aug. 2019), https://www.ibm.com/downloads/cas/L57KW7ND (last retrieved Dec. 20, 2023).

[59] *Cost of Data Center Outages*, Ponemon Institute at 14 (Jan 2016), https://www.vertiv.com/globalassets/documents/reports/2016-cost-of-data-center-outages-11-11_51190_1.pdf (last retrieved Dec. 20, 2023).

[60] *The High Cost of a Mainframe Going Down*, New Iron Solutions, https://newironsolutions.com/the-high-cost-of-a-mainframe-going-down/ (last retrieved Dec. 20, 2023).

[61] 2021 Recommendation at 215.

systems and the devices they operate by removing the threat of liability, these factors "weigh slightly in favor of an exemption."[62]

Fourth factor: the effect of circumvention of technological measures on the market for or value of copyrighted works

The copyrighted software at issue is customized to the particular make and model of equipment in which it is installed. These are not generalist, plug-and-play systems; they are customized, and in the case of PLCs, often bespoke to the particular combination and uses of equipment under its control. There is no independent market for the software or firmware being accessed.

Fifth factor: such other factors as the Librarian considers appropriate.

The Office has recognized that TPMs "can have an anticompetitive effect on independent repair and self-repair."[63] This has become even more high profile since the last proceeding. The Freedom to Repair Act of 2022 proposed exempting TPM circumvention for all repair, diagnosis, and maintenance purposes.[64] The Intellectual Property subcommittee of the House Judiciary Committee held a hearing on Right to Repair in which they considered the original purpose and unintended anticompetitive effects of TPMs; original DMCA coauthor Rep. Zoe Lofgren said in this hearing, "We didn't do TPMs so monopolies could control products. That was never the intent."[65] A letter to Congress on March 24, 2023, signed by 28 attorneys general, decried anticompetitive software and diagnostics restrictions: "OEMs often control access to these electronics parts, creating unfair restraint of trade and a monopoly on repair."[66]

---

[62] *Id.*

[63] 2021 Recommendation at 218.

[64] H.R. 6566, 117th Cong. (2022), available at https://www.congress.gov/bill/117th-congress/house-bill/6566.

[65] I*s There a Right To Repair?: Hearing Before the Subcomm. on Cts., Intell. Prop., & the Internet of the H. Comm. on the Judiciary*, 118th Cong. (Jul 18, 2023). Hearing page available at https://judiciary.house.gov/committee-activity/hearings/there-right-repair.

[66] Letter from 28 State Attorneys General to Reps. Cathy McMorris Rodgers and Frank Pallone, and Sens. Maria Cantwell and Ted Cruz, (Mar. 24, 2023), https://oag.ca.gov/system/files/attachments/press-docs/3.24.2023%20Right%20to%20Repair%20Ltr.%20to%20Congress%20FINAL.pdf.

Commercial and industrial equipment covered by the proposed exemption would still be subject to all applicable health and safety laws and regulations. The Office has noted that "it will generally decline to consider health, safety, and environmental concerns as part of the triennial proceeding," recognizing that "an exemption provides no defense to those who use it as an excuse to violate other laws and regulations."[67]

DOCUMENTARY EVIDENCE

N/A

[67] 2021 Recommendation at 218, citing U.S. COPYRIGHT OFFICE, SECTION 1201 OF TITLE 17: A REPORT OF THE REGISTER OF COPYRIGHTS at 126 (2017).