August 2, 2024

Suzanne Wilson
General Counsel and Associate Register of Copyrights
United States Copyright Office
Library of Congress
101 Independence Ave. SE
Washington, DC 20559-6000

VIA EMAIL

To: bkarl@copyright.gov
meft@copyright.gov

Re: Summary of Ex Parte Meeting with the Copyright Office Concerning Docket No. 2023-5, *Ninth Triennial Section 1201 Proceeding, 2024 Cycle, Exemptions To Permit Circumvention of Access Controls on Copyrighted Works*

Dear Ms. Wilson,

We write to summarize the July 26, 2024, *ex parte* meeting held between representatives of the Consumer Technology Association ("CTA"), Cisco, Hewlett Packard Enterprise ("HPE"), IBM, the Information Technology Industry Council ("ITI"), TechNet, and Wiley Rein LLP (on behalf of CTA, "Wiley") (collectively, "the Industry Representatives"), and representatives of the Copyright Office ("the Office"). The meeting focused on four topics related to the "Class 5" proposal to expand the existing Digital Millennium Copyright Act ("DMCA") anti-circumvention exemptions for diagnosis, maintenance, and repair of devices to a broad class of commercial and industrial equipment, including enterprise information technology ("IT"): (1) the uniqueness and lack of commonality of the proposed class; (2) the lack of adverse effects on the proponents of the proposed class; (3) how the proposed use is infringing and is not amenable to a fair use analysis; and (4) unique cybersecurity concerns that weigh against expanding the existing exemption.

In attendance at the meeting were, for CTA, Walter Alcorn and Michael Petricone; for Cisco, Eric Wenger; for HPE, Monica Markov; for IBM, Jamie Klein, Marc Williams, and Yeen Tham; for ITI, Chris Cleet; for TechNet, Ebbie Yazdani; and, for Wiley (on behalf of CTA), Duane Pozza and Scott Bouboulis. Representatives for the Copyright Office included Brandy Karl, Emily Chapuis, and Nick Bartelt. This letter summarizes that discussion and questions raised by the Office during the meeting.

Overview

At the meeting, the Industry Representatives provided views on the "Class 5" proposal seeking to expand the existing DMCA anti-circumvention exemptions for diagnosis, maintenance, and repair of devices to a broad class of commercial and industrial equipment (or, in the alternative, create a new class of exemption). The proposed class includes "enterprise information technology (IT),"[1] which, among other things, represents a broad spectrum of technologies that support the fundamental functions of government and the nation's critical infrastructure.

The Industry Representatives oppose this proposed expansion for four reasons discussed at the meeting. First, enterprise IT is fundamentally different from consumer devices covered under the existing repair exemption, and the proposed class lacks commonality. Second, proponents have not shown that they are adversely affected by prohibitions on circumvention of technological protection measures ("TPMs"), particularly with regard to enterprise IT equipment. Third, the proponents have not shown that the proposed use is non-infringing, and a fair use analysis is not possible across the class for the proposed use. Fourth and finally, there are unique cybersecurity concerns present with commercial and industrial equipment that weigh against expanding the exemption.

The Industry Representatives provided details on each of these arguments as summarized below.

1. The scope of the proposed class of commercial and industrial equipment lacks commonality with the existing class of consumer devices and lacks commonality even among different kinds of technology included in the proposed class itself.

In considering a proposed exemption, the Copyright Office considers whether a proposed exemption defines a class of works with sufficient commonality, whether the class is narrowed by specific uses, and whether users of the class are similarly affected.[2] The proposed class of commercial and industrial equipment includes enterprise-grade IT equipment that is fundamentally different from consumer devices in terms of the equipment itself and its primary uses and users.

---

[1] *See generally* Public Knowledge & iFixit, Initial Comments (Dec. 22, 2023), https://www.copyright.gov/1201/2024/comments/Class%205%20-%20Initial%20Comments%20-%20Public%20Knowledge.pdf ("PK Comments"). For the convenience of discussion, we use this term because it was used by the proponents; however, we do not agree or intend to imply that such a label in itself can simply define a loose and diverse grouping of information and communication technologies.

[2] The DMCA specifies that an exemption adopted as part of this rulemaking must be based on "a particular class of works." 17 U.S.C. § 1201(a)(1)(B). In prior Triennial Reviews, the Copyright Office has stated that, "as a threshold matter, the Register [of Copyrights] 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 across the full spectrum of software-enabled devices." 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"). In particular, the Office considers whether "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." U.S. Copyright Office, Section 1201 Rulemaking: Seventh Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the Register of Copyrights 289 (2018) ("2018 Recommendation"). In 2021, the Office correctly found that there was insufficient evidence of commonality to extend the exemption to commercial and industrial equipment.

Regarding ***the equipment and its uses***, enterprise IT is fundamentally different from consumer devices. Enterprise IT infrastructures are composed of many enterprise IT devices and equipment from different manufacturers, highly interconnected and bound together by software, running multiple business applications. The hardware and operating software are platforms for a customer's choice of business applications. Infrastructures vary enormously from organization to organization, as well as in terms of workloads, and can cost millions of dollars to acquire and operate.

Equipment deployed in enterprise IT infrastructures provide highly critical security protections, data protection and integrity, as well as substantial processing power for entities that operate the backbone of the U.S. economy and that run critical infrastructure – such as banking, government activities, telecommunications, and health care. Enterprise IT equipment is designed this way because businesses as well as Federal, State, and local governments want and need these protections and rely on equipment manufacturers to provide such capabilities. These customers' industries are often highly regulated and often deal with additional security and data protection requirements. A single machine may process information for millions of people an hour – as well as other highly sensitive information – and keep the critical functions of government, business, and our economy running. The impact of any issues with enterprise IT devices or infrastructure – including security incidents – could be serious and may be of a thoroughly different scale than an attack on an individual's consumer device. These issues are underscored by the recent CrowdStrike outage, which demonstrates how a single event can have far-reaching impacts across interconnected machines and networks.

This equipment also needs round-the-clock support to maintain operations. Enterprise IT infrastructure cannot go offline for a repair and must have both redundancy and equipment designed to be repaired on location with no impact to the operation of the environment. Manufacturers, third parties, and customers supporting their own environments often provide 24/7 support, with response times that can run to minutes. In such ways, enterprise IT equipment differs from consumer devices.

Regarding ***users***, enterprise IT infrastructures and enterprise IT equipment do not have "users" analogous to users of consumer or small office products. Actual users of an IT infrastructure and related equipment run into millions of individuals daily. Enterprise IT infrastructure also requires specialized knowledge by professional users to deploy, configure, and maintain. Access to the IT environment is strictly controlled, as maintenance and service activities are limited to specialized teams operated by the customer themselves, the manufacturer, or contracted business partners. The equipment often requires tailored diagnostic capabilities, and specific engineering experience and expertise. Additionally, the parties involved in enterprise IT equipment procurement and use are differently situated than for consumer products, as these products are intended solely for business-to-business or business-to-government users.

In sum, enterprise IT equipment is significantly different in kind from consumer devices and has fundamentally different uses and users than consumer devices.

Despite what is argued by proponents,[3] enterprise IT equipment also varies widely from other technologies ***within the proposed class*** of commercial and industrial equipment, which is overly broad and lacks commonality. Enterprise IT equipment is significantly different from other

[3] *See, e.g.*, PK Comments at 9.

commercial and industrial equipment, such as ice cream machines, industrial food preparation equipment, or construction equipment. The hardware components, chips, and software involved in enterprise IT equipment involve different technologies, complexities, levels of scale, and proprietary designs from those used in other industrial equipment. Technical cybersecurity protections that are expected and provided in enterprise IT equipment go far beyond what is standard in other kinds of industrial equipment. A separate class for commercial and industrial equipment therefore cannot be justified, or, at a minimum, enterprise IT equipment should be excluded from such a class.

Notably, consistent with these distinctions, states have expressly limited the scope of laws related to "right to repair" for digital electronic equipment to consumer products, or have excluded from these laws IT equipment used in critical infrastructure, recognizing that enterprise equipment raises different issues than consumer devices. For example, the Minnesota legislature decided to include an express exclusion for IT equipment intended for use in critical infrastructure in its repair law.[4] Likewise, the New York Governor and the legislature excluded business-to-business and business-to-government contracts from the repair law out of concern about the impact of the law on critical infrastructure.[5]

2. Proponents have not shown that they are adversely affected by prohibitions on circumvention of TPMs – particularly with regard to enterprise IT equipment.

The DMCA exemption process requires that petitioners show that they are "adversely affected . . . in their ability to making noninfringing uses" by the prohibition on circumvention, and they must identify "distinct, verifiable, and measurable" impacts.[6]

In prior Triennial Reviews, the Copyright Office has explained that proponents can satisfy the adverse effect requirement through one of two methods. First, they can demonstrate that a "'substantial diminution' of the availability of works for noninfringing uses is 'actually occurring' in the marketplace," and that evidence of "mere inconveniences" or "individual cases" will not suffice.[7] Second, proponents can demonstrate that the prohibition will result in future

[4] Minn. Stat. § 325E.72, Subd. 6(g) ("(g) Nothing in this section applies to information technology equipment that is intended for use in critical infrastructure, as defined in United States Code, title 42, section 5195c(e).").

[5] N.Y. Gen. Bus. Law § 399-nn(1)(b). California's and Oregon's digital equipment repair laws are limited to the kinds of equipment generally used for personal, family, or household purposes. *See* Cal. Pub. Res. Code § 42488.2(j)(3A-B); S.B. 1596, Section 1(1)(b), Reg. Sess. (Or. 2024). Colorado recently enacted a digital electronic equipment repair law, and until a late Senate amendment, was limited to consumer digital electronic equipment. H.B. 1121, Reg. Sess. (Colo. 2024). In response to concerns about cybersecurity risks to enterprise equipment used in critical infrastructure posed by repair obligations, the Governor in his signing statement acknowledged these concerns and encouraged stakeholders to work to ensure that before the law goes into effect, it contains the "full list of exclusions [] appropriate and exhaustive." CO Governor Polis's Signing Memorandum for H.B. 1121 (May 28, 2024).

[6] 17 U.S.C. § 1201(a)(1)(B); Digital Millennium Copyright Act of 1998, H.R. Rep. No. 105-551, pt. 2 at 6 (1998).

[7] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Notice of Inquiry, 79 Fed. Reg. 55687, 55690 (Sept. 17, 2014); 2021 Recommendation at 12.

impacts, but "only in extraordinary circumstances in which the evidence of likelihood of future adverse impact during that time period is highly specific, strong and persuasive."[8]

Petitioners, as well as the Federal Trade Commission ("FTC") and Department of Justice ("DOJ") in their comment, present ***no evidence that enterprise IT customers lack responsive maintenance and repair.*** Instead, the sources cited simply discuss costs of downtime – notably including from security compromise or poor skills – without suggesting that lack of repair availability was a cause.[9] Contrary to what proponents claim for certain products, there is no lack of availability for repair of enterprise IT equipment.

In fact, even beyond direct contracts with a manufacturer for maintenance and repair, ***access to individual enterprise IT hardware repairability is robust***. For example, manufacturers today make available information to conduct most repair of enterprise IT equipment. This information is available online or comes with the purchase of the equipment. To give a specific example, HPE provides a variety of diagnostic capabilities as well as the relevant service and repair manuals and lookup tools so that a failed part can be identified, and videos are available on how to actually replace the part. Parts can be ordered directly through the HPE parts store or through authorized parts suppliers, in order to help protect against counterfeit parts that can damage the integrity and security of equipment.[10] HPE is already providing repair options for devices where there are no cybersecurity concerns, without the need to circumvent a TPM. Other OEMs also provide similar resources.

Notably, ***enterprise IT manufacturers make available broad, flexible, and affordable offerings*** for maintenance and repair under commercial terms and have every incentive to make sure their equipment remains functioning, updated, and secure, so that customers (and the equipment manufacturer) do not suffer reputational or other harm.

Proponents attempted to assert in the hearing that manufacturers abandon older equipment, leaving customers without options, forcing them to buy new equipment.[11] This assertion is not accurate. Customers of enterprise IT invest millions of dollars in the infrastructures that run their organizations and have an ongoing interest in maintaining that equipment and planning migration to new technologies to address their needs. Notably, IT equipment manufacturers engage with their enterprise customers regularly to discuss enhancements reflected in development roadmaps to respond to their customers' evolving technology needs as well as ongoing maintenance. It is generally acknowledged that while manufacturers continue to provide support, and as they introduce new safer products, at some point old equipment is not secure to use, and customers understand the need to migrate to new equipment rather than use old iterations. Particularly in the enterprise IT/critical infrastructure arena, enterprise IT users are driven by a need to keep their technology environments safe, reliable, and secure against quickly emerging threats.

Further – and contrary to a proponent's statements at the hearing – while an "End of Service" or "End of Life" date indicates that IT equipment is at a point in its lifecycle where it is no longer

---

[8] *Id.*

[9] *See* PK Comments at 15-16.

[10] *See, e.g.*, *HPE PartSurfer*, HPE, https://partsurfer.hpe.com/ (last visited July 26, 2024).

[11] *See, e.g.*, In the Matter of: Section 1201 Public Hearing: Proposed Class 5 Computer Programs – Repair, Transcript of Proceedings at 74-75 ("Hearing Transcript").

sold or supported in a standard manner, it does not necessarily mean that a manufacturer or a service provider will "abandon" the machine. For example, a proponent correctly stated that the IBM z13 mainframe End of Service date was announced to be December 31, 2024. However, the proponent's misplaced statement that IBM "will abandon that machine and will no longer sign service contracts and that machine will be un-repairable on January 1, 2025"[12] is objectively false. IBM will – and continues to – support z13 systems (and even older mainframes and equipment) under commercial Hardware Service Extension contracts, and customers continue to use and maintain such older machines until they are ready to take next technology steps.[13]

Additionally, ***independent service providers servicing enterprise IT equipment have not been harmed.*** In fact, such providers have been very successful. These providers who service enterprise customers are not the same firms that service local communities, small businesses, or individuals. For example, Service Express (one company represented among the proponents testifying at the hearing) employs over 1000 individuals and is estimated to have earned over $200 million in 2023.[14]

3. The proponents have not shown that the proposed use is non-infringing, and a fair use analysis is not possible for the proposed use.

To establish a case for an exemption, "proponents must show at a minimum (1) that uses affected by the prohibition on circumvention are or are likely to be noninfringing…"[15] More particularly, "[i]t is not enough that a particular use could be noninfringing. Rather, the Register will assess whether the use is likely to be noninfringing based on current law."[16]

First, the highly variable number of use cases makes it impossible for any court or person to identify a proper categorical outcome for fair use.

The breadth of the proposed exemption makes it impossible to engage in a fact-based analysis of the fair use factors in relation to the class, since many of the factors are unknown if not

---

[12] Hearing Transcript at 77-78.

[13] *See, e.g.*, *IBM Technology Lifecycle Services*, IBM, https://www.ibm.com/downloads/cas/0WG1YGJZ. At the hearing, proponents tried to imply that enterprises customers contribute to waste by "just throwing out products because the software is not useful even though there's nothing wrong with the hardware." Hearing Transcript at 74. However, there is no evidence that there is an e-waste problem with respect to enterprise IT equipment. In fact, most OEMs have active recycling programs for their equipment where customers can turn in their equipment for free. *See, e.g.*, *HPE Take Back & Recycling*, HPE, https://www.hpe.com/us/en/about/environment/product-recycling.html; *The Cisco Takeback and Reuse Program*, Cisco, https://www.cisco.com/c/en/us/about/takeback-and-reuse.html. In addition, customers often choose to sell their used enterprise IT equipment to third-party brokers or recyclers who have recognized the value of downstream sales.

[14] *Service Express Revenue and Competitors*, Growjo, https://growjo.com/company/Service_Express#revenue-financials (last visited July 31, 2024).

[15] *See, e.g.*, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Final Rule, 86 Fed. Reg. 59627, 59628 (Oct. 28, 2021).

[16] U.S. Copyright Office, "The Triennial Rulemaking Process for Section 1201," at 6, https://cdn.loc.gov/copyright/1201/1201_rulemaking_slides.pdf (last visited July 28, 2024).

unknowable.[17] Because of the vast number of different commercial and industrial systems captured by the proposed class, the fact-specific analysis needed for a fair use analysis is not possible. As one example, it would be exceedingly difficult to determine how much of the work would need to be "taken," for purposes of a fair use analysis across the proposed class. These concerns frustrate any attempts at a fair use analysis across the class, and provide a sufficient basis for the Copyright Office to deny proponents' request for expansion of the Class 5 exemption.

Second, circumvention for repair is done for commercial purposes and is non-transformative, and therefore an exemption would facilitate infringing uses.

The Office also must consider whether uses that would be permitted under the proposed exception are actually fair use, which takes into account the purpose and character of the use, including whether it is a commercial use.[18] In fact, the uses cited by the proponents are *commercial* in nature, and an exemption would therefore encompass many uses that actually would be infringing. The proponents' stated reasons for an exemption are not, for example, good-faith security research, which already has an exemption.[19]

While consumer product users may circumvent access controls for non-commercial reasons, users and repairers of commercial and industrial systems would circumvent access controls solely for commercial motivations. That is, granting an exemption would advance the interests of those with only an economic interest to potentially win commercial contracts with commercial customers. Independent service providers for enterprise IT equipment do not provide these services free of charge, and they benefit commercially.

Further, it is clear from the hearing record that different proponents seek the exemption for different commercial purposes – notably, many of which are not for diagnosis, maintenance, and repair. Some would like to circumvent protection measures to sell their own upgrades or to remove the original software to replace it with their own or others' software or services. Others propose to modify existing software to add capabilities. It is even unclear if the proponents want to bypass the TPM in order to copy or distribute unauthorized copies of firmware so they can perform the commercial repair. In short, it is not clear what all proponents' goals would be for bypassing the TPM, but they all seem to be for commercial reasons.

Third, circumvention of TPMs for enterprise IT would adversely affect the market for the underlying software and enable commercial, infringing uses of the software.

---

[17] A fair use analysis looks to a balanced application of four factors: (1) the purpose and character of the use (transformation), (2) the nature of the copyrighted work, (3) the amount and substantiality of the portion taken, and (4) the effect of the use upon the potential market. Fair use analysis is highly fact-specific and must be performed on a work-by-work basis.

[18] *See* 17 U.S.C. § 107(1) ("purpose and character of the use, including whether such use is of a commercial nature"). Indeed, as part of the exemption analysis, the DMCA requires consideration of the impact of the prohibition on circumvention on "criticism, comment, news reporting, teaching, scholarship, or research." 17 U.S.C. § 1201(a)(1)(C)(iii).

[19] 37 C.F.R. § 201.40(b)(16).

In deciding whether to grant a DMCA exemption, the Copyright Office must consider "the effect of circumvention of technological measures on the market for or value of copyrighted works."[20] The 2021 Recommendation noted that the expansion of the repair exemption to commercial and industrial equipment could "contravene negotiated licensing terms between commercial actors."[21] These actors are businesses and governments that are able to negotiate on fair terms for commercial IT equipment. Ultimately, allowing infringing uses would result in a reduction in value of the software.

Regardless of where the TPM might sit within the different layers of hardware components or software, permitting circumvention would contravene the commercial license as well as have an effect on value or market for the software. Enterprise IT equipment is comprised of complex devices with multiple layers of hardware components and software, coming from various sources, and TPMs may be implemented in any of these layers to govern authorized/licensed use, add functions to the device, as well as to protect the machine or its components against security threats. A TPM may take any number of forms, depending on its intended use. In the commercial context of enterprise IT equipment, associated software is licensed between the commercial customer and manufacturer. Such software may be separately priced, or its value may initially be included as part of a hardware purchase. However, ongoing software updates to maintain or repair either the hardware or software are subject to additional license terms and often separate commercial support agreements (either for long periods or for short duration) that have their own charges. In some circumstances, firmware updates may be licensed by manufacturers for a fee. Permitting circumvention could therefore undermine existing software licenses and adversely affect the market for the software.

4. The Copyright Office should consider the unique cybersecurity concerns present with commercial and industrial equipment in determining not to expand the current repair exemption.

The DMCA requires consideration of other factors deemed "appropriate" in determining whether to grant exemptions.[22] In this case, there are strong cybersecurity policy considerations against expanding the exemptions to allow circumvention of TPMs for enterprise IT systems. Given the impact and ever-evolving nature of cyber threats, there is an intense national focus on mitigating cybersecurity vulnerabilities in critical infrastructure, on assuring that the confidentiality and integrity of these systems are protected, and that these IT systems that power our economy are consistently up and available. Customers as well as the public are depending on manufacturers to focus on the safety and security of critical infrastructure IT systems. The U.S. government has sought to push manufacturers and service providers to make their products *more* secure, not less, particularly in the case of critical infrastructure. One example is the Biden Administration's May 2021 Executive Order ("EO") on Improving the Nation's Cybersecurity.[23]

---

[20] 17 U.S.C. § 1201(a)(1)(C)(iv).

[21] 2021 Recommendation at 197-98.

[22] 17 U.S.C. § 1201(a)(1)(C)(v).

[23] Executive Order 14028, 86 Fed. Reg. 26633 (May 17, 2021) ("Cybersecurity EO").

Security of "critical software" (which includes firmware and other embedded software) is a particular focus of the EO.[24] The EO, through a phased approach, created a set of requirements that are to be followed by those who sell to the government.[25] Companies are currently in the process of making attestations that the software they provide meets these requirements. These new obligations include, among other things, build environment security for developing and checking code as well as to lock down code after attestations have been completed.

To allow third parties to defeat these new security requirements contradicts the very purpose of these actions. Enterprise hardware manufacturers have made significant advances in securing the technology stack from the silicon board all the way up to the application and data layers. When properly utilized, Trusted Platform Modules or Trust Anchor Modules ("TPMs/TAMs") allow the system to validate its hardware configuration to prevent modification with counterfeit or tampered components. The system can next validate the first software to run on the system – e.g., Basic Input Output System ("BIOS") and firmware. This important step helps to ensure that only validated and genuine software runs on the system, and also prevents persistent attacks that could be otherwise possible. For example, an advanced persistent attacker capable of tampering with or substituting firmware would be capable of writing exploit code that would survive even a complete shutdown and reboot of the device – and even reinstalling the operating system ("OS"). Once the hardware and firmware have been validated, it becomes possible to leverage the unique cryptographic signing capabilities enabled by TPMs/TAMs to then validate and securely load the hardware configuration, firmware, and OS – e.g., Windows, Linux, or MacOS – in a manner that dramatically cuts risk that exploits persist on system restart. Requiring that signing keys be shared out to non-OEM authorized repair services would sever the connection between the TPM/TAM and the firmware or between the firmware and the OS – undoing the significant advancements in security that have been achieved after significant investments of time and resources.

By undermining the security of the enterprise IT devices, TPM circumvention therefore directly damages the value of enterprise IT equipment and the infrastructure it resides within. These machines are designed and marketed for security and data integrity purposes and are used in critical infrastructure because of these attributes. Critical infrastructure customers rely on manufacturers' judgment as to what repair information to make safely available, recognizing that manufacturers may choose to make parts of the enterprise IT more secure rather than broadly accessible.

One proponent has argued that bad actors are not discouraged by a prohibition on circumvention.[26] In this case, bad actors will be attracted to a new, target-rich environment of vulnerabilities if they know that TPMs might be compromised or left open permanently because an array of service providers are circumventing the protections. An exemption would further embolden hacking into IT systems intended to run critical infrastructure – not by skilled security researchers, but bad actors and those less skilled who could do any number of things

[24] *Id.* at 26638-39.

[25] *Security Measures for EO-Critical Software Use*, NIST, https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use (last visited July 26, 2024).

[26] Hearing Transcript at 40.

within the system.[27] This may result in permanent compromise of cybersecurity protections, leaving systems vulnerable to cyberattack. In addition, if modification is permitted as to any aspect of the system, including trusted platforms on which the system operates, this would allow for further cybersecurity vulnerabilities and potential compromise.

Finally, as previously noted, enterprise IT infrastructure is deeply interconnected. If more parties are able to make changes to software embedded in enterprise IT equipment, it could create unintended consequences with massive ripple effects, as underscored by, for example, the recent CrowdStrike incident.

Question and Answer Portion

In the question and answer portion of the meeting, representatives from the Copyright Office asked whether device firmware is provided with the hardware, is proprietary, and licensed separately.

Industry Representatives noted that, as part of the overall software stack on a machine, firmware is a type of software embedded in a device's hardware. In order to operate, firmware must be initially shipped with enterprise IT systems. However, updates to firmware are made available separately from the initial hardware, and it is up to the customer (or their service provider) to choose to download such code to update their systems. In addition, such firmware updates include not just bug fixes or security fixes but may also include additional features and functionalities that were not present in the initial version shipped with the hardware. Depending on the manufacturer and the particular machine, the manufacturer may make such firmware available only as part of the commercial support contract fees or may charge separately for the firmware updates or replacement.

Conclusion

Industry Representatives thank the Copyright Office for the meeting and its attention to these important issues, and are happy to answer any additional questions that the Copyright Office may have.

Sincerely,

/s/ Walter Alcorn

Walter Alcorn

[27] Given the dissonant and varying nature of the testimony provided about what technical layer might be touched or what activity may be conducted under such circumvention permission (e.g., Hearing Transcript at 16-18), it is questionable whether an enterprise client would be accurately informed – let alone would consent to – the circumvention being conducted. Similarly, we believe permitting modification of software is very dangerous. There are reports where individuals, as well as adversarial nation states, have introduced backdoors or vulnerabilities into code without users or other developers being aware. *See, e.g.*, Andy Greenberg & Matt Burgess, *The Mystery of 'Jia Tan,' the XZ Backdoor Mastermind*, Wired (Apr. 3, 2024), https://www.wired.com/story/jia-tan-xz-backdoor/; Ravie Lakshmanan, *Iranian Hackers Deploy New BugSleep Backdoor in Middle East Cyber Attacks*, The Hacker News (July 16, 2024), https://thehackernews.com/2024/07/iranian-hackers-deploy-new-bugsleep.html.

Vice President, Environmental Affairs and Industry Sustainability
Consumer Technology Association

/s/ Chris Cleet
Chris Cleet, QEP
Vice President of Policy, Environment, Sustainability & Regulatory
Information Technology Industry Council (ITI)

/s/ Ebbie Yazdani
Ebbie Yazdani
Counsel and Director, Federal Policy and Government Relations
TechNet