TRANSCRIPT OF PROCEEDINGS

In the Matter of:)
)
SECTION 1201 PUBLIC HEARING:)
PROPOSED CLASS 5)
COMPUTER PROGRAMS - REPAIR)
)

Pages: 1 through 86

Place: Washington, D.C.

Date: April 16, 2024

HERITAGE REPORTING CORPORATION
Official Reporters
1220 L Street, N.W., Suite 206
Washington, D.C. 20005-4018
(202) 628-4888
contracts@hrccourtreporters.com

UNITED STATES COPYRIGHT OFFICE

In the Matter of:	)
	)
SECTION 1201 PUBLIC HEARING:	)
PROPOSED CLASS 5	)
COMPUTER PROGRAMS - REPAIR	)
	)

Suite 206
Heritage Reporting Corporation
1220 L Street, NW
Washington, D.C.

Tuesday,
April 16, 2024

The parties convened remotely, pursuant to notice, at 2:35 p.m.

PARTICIPANTS:

Government Representatives:

NICK BARTELT, U.S. Copyright Office
MARK GRAY, U.S. Copyright Office
LUIS ZAMBRANO RAMOS, National Telecommunications and Information Administration

Panelists:

JACOB BLOUGH, FreeICT USA
STEVEN R. ENGLUND, Jenner & Block LLP, on behalf of Joint Creators and Copyright Owners
DENVER GINGERICH, Software Freedom Conservancy
STACEY HIGGINBOTHAM, Consumer Reports
PRIYA NAIR, ACT | The App Association
ANTHONY D. ROSBOROUGH, Dalhousie University, on behalf of iFixit and Canadian Repair Coalition
MEREDITH ROSE, Public Knowledge
KYLE WIENS, iFixit

P R O C E E D I N G S

(2:35 p.m.)

MR. BARTELT: Hi, everyone. Welcome to the Class 5 Computer Programs - Repair hearing. We're just waiting one second. We're going to pull down the opening slide here so you can see the speakers as they rotate through. We're just trying to resolve one quick audio issue, and we'll be commencing shortly.

(Pause.)

MR. BARTELT: Hi, everyone. Sorry about that. Emily, is your audio working yet? If not, I'll just go ahead.

MS. CHAPUIS: You tell me, is it working?

MR. BARTELT: It is. Please proceed, and if it cuts out again on you, I'm happy to take over. Oh, I'm sorry, it looks like it's cut out again. I apologize. I'm not sure what's happening with our audio, and apologies to the panel and to the participants, attendees, but I'll do our intro here and introduce everyone.

Good afternoon. Welcome back. This is the Class 5 Computer Programs - Repair hearing. My name is Nick Bartelt. I'm an Attorney-Advisor here at the Copyright Office. We're continuing Day 1 of the Section 1201 rulemaking hearings.

Before we begin Class 5, I'd like to go over a few logistical items. In this session, our panelists, my government colleagues, myself will ask specific questions and call on participants to respond. To indicate that you'd like to speak, please use the Raise Hand function on Zoom or, if that's not working for you, feel free to wave your hand, your real hand, and we will know to recognize you. Hopefully, no one else has the same sort of audio issues we're experiencing on our end.

So we have a lot of topics to cover, so please do try to focus your responses on the particular question being posed and please keep your comments relatively brief. This hearing is being live-streamed. It is also being recorded and transcribed by a court reporter. The video and transcript will be posted on the Copyright Office website after the hearings conclude. Both for the benefit of our court reporter and for our live participants, we ask that everyone speak loudly and clearly and that you mute your audio anytime you are not speaking.

Finally, for those of you who are listening, on Thursday afternoon, we will have a public participation session that will run from 4 to 5 p.m.

Anyone who would like to participate in that session can sign up using the link in our chat -- hopefully, that'll be up in a second -- and it's also on our website for those who are looking for it. Public comments can relate to any of the classes that are being discussed during this proceeding, but we ask that remarks be limited to three minutes each.

So, again, this afternoon's hearing is on Class 5. This is Computer Programs and Repair. Before we begin, I'd like to invite my colleagues to introduce themselves. Again, I'm Nick Bartelt, an Attorney-Advisor with the Office of General Counsel. I also have, I believe, another colleague from the Office of General Counsel here with me, Mark Gray.

MR. GRAY: Hello, everyone.

MR. BARTELT: Mark is an Assistant General Counsel with our group. And from the National Telecommunications and Information Administration, would you like to introduce yourself?

MR. RAMOS: Sure. Hey, everyone. I'm Luis Zambrano Ramos. I'm a Senior Policy Advisor in NTIA's Office of Policy Analysis and Development.

MR. BARTELT: Thanks, Luis.

And now I'd like to invite the participants to introduce themselves. Let's start with the

proponents of the proposed exemption. Jacob, could you go ahead.

MR. WIENS: Jacob has been messaging me. He's trying to get on but hasn't been able to get on yet, so maybe come back.

MR. BARTELT: Oh, okay, thank you. Kyle, while you're on, why don't you introduce yourself and then we'll rotate back through.

MR. WIENS: Sure. I'm Kyle Wiens. I'm the CEO of iFixit, the free repair guide for everything.

MR. BARTELT: Thanks, Kyle.

Denver?

MR. GINGERICH: I'm Denver Gingerich. I'm the Director of Compliance at Software Freedom Conservancy.

MR. BARTELT: Okay. Thank you, Denver.

Stacey?

MS. HIGGENBOTHAM: Hi. I'm Stacey Higgenbotham. I am a Policy Fellow at Consumer Reports.

MR. BARTELT: Thank you.

And, finally, Anthony, from the proponents.

MR. ROSBOROUGH: Hi. I'm Anthony Rosborough, Assistant Professor of Law and Computer Science at Dalhousie University in Canada and founder

of the Canadian Repair Coalition.

MR. BARTELT: All right. Thank you.

And let's turn to those who are opposing the proposed exemption, so let's start with Steven.

MR. ENGLUND: Hi. I'm Steve Englund of Jenner & Block and I'm here representing the Entertainment Software Association, the Motion Picture Association, and the Recording Industry Association of America.

MR. BARTELT: Oh, I realize I neglected -- I overlooked one person on the proponents side. Bear with me, let's go right back to Meredith.

MS. ROSE: No problem. I'm Meredith Rose. I'm Senior Policy Counsel at Public Knowledge.

MR. BARTELT: Thank you, Meredith. You had floated off my screen with all the people that we have here today.

And now back to the opponents, Priya.

MS. NAIR: Hi, everyone. I'm Priya Nair. I'm Senior IP Policy Counsel for ACT | The App Association.

MR. BARTELT: All right. Well, thank you, everyone. I think that covers our panel. Again, thank you for your patience. And with that, let's start off with the questions. I'll start with the way

we're going to divide this up essentially is into three parts, just to give you a roadmap. First, we're going to have a section just focusing on the scope of the proposed class. After that, we'll move into a section on the proposed non-infringing uses. And then, finally, we'll have a third section that's going to focus us on adverse effects, understanding that there will be some bleed between those sections, but we'd like to try to keep the discussion limited to those three sections. So, if you have comments related to one, please be assured we'll get to them eventually.

So, with that, I'll start off by asking a question that relates to the scope of the proposed class. So the Petitioners, in their initial comments here, provided four index examples of commercial industrial devices. Those were for commercial food preparation, construction equipment, programmable logic controllers, and enterprise IT. So this is a question to any of the proponents. So we'd like you to explain why, in your view, that these four index examples support a class covering all commercial industrial devices and are there any examples of other device types that should be considered? So please raise your hand if you'd like to respond. And maybe

I'm not seeing the Raise Hand function.

MR. RAMOS: Meredith, why don't you go ahead. I'll help Nick with his visuals.

MS. ROSE: Sure, yeah. So the reason we selected these particular four is because we felt that we had a uniquely developed record on the four of them as it was a significant part of it in that, you know, acknowledging that many other sort of sub-types of devices had been brought up in previous attempts at the petition, but the Office's response had generally been that there were specific parts of the analysis or things such as alternatives to circumvention that hadn't been correctly explored in prior petitions. And so we picked them largely because (a) we thought that there was a robust record for each of the four of these; and (b) we felt that it showed both the breadth of the problem in terms of access to repair tools and TPMs or, rather, the inability to repair due to TPMs, while also illustrating the similarities that users face among each of them.

MR. BARTELT: Thanks, Meredith.

And now I see Kyle's hand, so please go ahead.

MR. WIENS: Thank you. Well, part of it was we just really like ice cream and so, right now, six

percent of ice cream machines in Washington, D.C., are not working and that feels problematic. One in five in San Diego right now, where it's warmer, are not working. So we thought that that was an entry into it.

You know, at iFixit, we have repair guides for over a hundred thousand products. We see the spectrum of all the products that people deal with. Fundamentally, if you look inside these things, oftentimes it's the same chip inside different products, so the actual software, the nature of the work, is relatively similar across different industries.

But we wanted to pick different examples. The PLCs, I think, comes up because it a little bit of a unique software development environment with PLCs. Enterprise IT, you know, we had some examples of some data center equipment with IBM and some of the other systems. But, broadly, enterprise IT is similar. So we tried to give you, you know, a set of kind of four cases that I think are pretty representative of the software situation across the commercial and industrial and the electronic space.

MR. BARTELT: All right, thank you. I do have a few follow-ups, but I'm going to ask one more

for the proponents and then I have some questions for the opponents here. So one follow-up I have is about the proponents' initial comment, which said that it doesn't intend to cover devices with scientific uses. I was just curious how you would define "scientific" in this context and what kind of devices you had in mind that might fit that definition?

Go ahead, Meredith, I see you.

MS. ROSE: Yeah. So our intention was essentially to exclude things like lab equipment partly because that is an area where we haven't, frankly, been able to have conversations with folks who run labs who use it. And also the bleed-over between lab equipment and things like medical devices was pretty substantial and we weren't sure how to best address that. And so we used the term "scientific" as a little bit of a placeholder to try to address that or to carve out that sort of subset of devices.

MR. BARTELT: Okay, thanks, Meredith.

Again, I had one more question that I'll come back to, but I wanted to give the opponents or the participants who are opposing the exemption a chance to weigh in on the scope of the class question, which was sort of the flip side of this, was to explain why, in your view, the examples and record

provided by the proponents do not support a broad class of commercial industrial devices. And, Steve, I see you have your hand raised. Please go ahead.

MR. ENGLUND: Yeah. So, as you foreshadowed, I do not believe that these examples are representative of the full scope of the class, nor do I think the record is particularly well developed, but we'll focus on the breadth of the class.

When you're talking about commercial and industrial equipment, you're essentially talking about almost everything under the sun that's not a consumer good. And so, as most relevant to my clients, commercial and industrial equipment used for processing creative works includes things like arcade game machines, motion picture projection equipment, systems for transmitting music and motion pictures in commercial buildings and by cable television, satellite broadcasting.

But, even beyond that, Ms. Rose mentioned an exemption for scientific. I think that barely begins to scratch the surface of the critical applications here. Even within the category of enterprise IT, we're talking about systems that are used to control a great deal of critical infrastructure, the electrical grid, power plants. But moving beyond enterprise IT,

I think you're talking about communications, network equipment, avionics equipment on commercial aircraft, water purification systems, everything under the sun. And I don't think there's a sufficient record here to support an exemption for the four categories that have been identified, but certainly haven't made a record on avionics equipment or control systems for nuclear power plants.

MS. NAIR: I would have to agree with that. I don't think that this petition has expressed the full scope of the class at all. Our members are small and medium-sized software developers that provide IoT-based and mobile-type devices that kind of span different industries. Commercial industrial equipment is very limited. And I also don't believe, which I'm sure we'll get into, that the petition even expresses enough evidence to fully prove actual harm here, to actually enable an exemption in this case. So I'll leave it at that.

MR. BARTELT: Thank you, Priya, and thank you, Steve. Kyle, I see your hand raised, but, before we let you in, I just wanted to allow -- we do have our final participant, who's just joined us. I hope he can hear us. Jake, if you'd like to introduce yourself, please do so.

MR. BLOUGH: Yeah. Hopefully, you can hear me.

MR. BARTELT: Yes.

MR. BLOUGH: I had to join from a gigantic conference room, so all you see is a very long table. Jake Blough from FreeICT USA and also Service Express.

MR. BARTELT: All right. Thank you, Jake.

And please go ahead, Kyle.

MR. WIENS: Yeah, I appreciate the opposition comments. You know, when you look at the actual electronics that go into these products, whether it's a water treatment plant or a nuclear power plant, both of those are controlled by PLCs, which are in the example. So, if you dive into the actual products, the actual control boards, the actual software that we're talking about, there's a relatively small number of actual operating systems and actual CPUs that are running these systems.

MR. BARTELT: Thanks, Kyle.

I did want to give my colleague, Luis, a chance to ask a question here as a follow-up to one of our earlier questions. Luis, go ahead.

MR. RAMOS: Yeah, sure, thank you so much, Nick. So just one follow-up on this on scope. I'm curious if the supporters and proponents can talk a

little bit about the ubiquity or the lack thereof of copyrighted software in commercial and industrial equipment today for which an exemption would be necessary. You know, do most commercial and industrial equipment today require a TPM -- require an exemption to bypass a TPM and access copyrighted software? And, opponents, if you also have thoughts on this, please chime in.

MR. BARTELT: Kyle?

MR. WIENS: Yeah. So, if you dive into let's say PLCs as an example because we're talking about them, it's very common for them to have a PIN. It's almost a default. And you have two layers of software. You have the IC running the unit and you have the embedded firmware on the system and then you have any programming controls that you've built on top of it. And there will be a lock above the program controls and then there would be a lock above the actual firmware that runs the unit itself. So, in both cases, the nature of the copyrighted work is the software that runs the system.

I'm in the process of -- we're building a new facility and we have a building automation system and we hired a controls company to write custom software that is just for our building that sets when

the lights turn on and when the HVAC turns on and that kind of thing. It's a work-for-hire that they're doing for me, but the default, when I talked to them, I said, are you going to give me the password to the software that I'm paying you to create, and they said not usually, no. So that's pretty typical.

MR. BARTELT: All right. Thank you.

And Steve?

MR. ENGLUND: I won't hold myself out as an expert on programmable logic controllers, but I did try to read up on the subject in preparation for this panel, and, obviously, they contain software, which I think was the original question from Mr. Ramos. Basically, they're just small ruggedized computers, and so the whole point of them is to execute software.

And, you know, it does appear that there may be a couple of layers of TPMs that are applied to them. The TPM on the device, to the extent I can tell from my reading, should be thought of as more akin to the password on your phone or your laptop than it should be as something designed to keep users out. It's designed to enforce protection for the user/owner. So, for example, I saw that Department of Homeland Security recently released a security bulletin to water utilities encouraging them to change

the default passwords on their Unitronics PLCs because these devices come with a default password of 1111 and DHS determined that due to cybersecurity threats, it was not desirable for water utilities to have all their PLCs have the password set to 1111, it’s not a lockout device.

In terms of software installed by systems integrators, as Mr. Wiens said, these are contractors. I've negotiated plenty of contracts for the procurement of customized software systems, and, in general, people who contract for software that's custom-developed don't get locked out by their contractors. If they do, there's a contract problem. But, to the extent that the systems integrator might be providing proprietary software, it's presumed they're licensed and subject to license restrictions. I'd expect that TPMs would be used to enforce the license restrictions as TPMs are commonly used to enforce restrictions on licensed software.

MR. BARTELT: All right. Thanks, Steve.

And I see, Meredith, you also had your hand up. You'd like to respond?

MS. ROSE: Yeah. I want to make really sort of two discrete points. One is that to your question, Luis, about the sort of ubiquity of software enabled

in these devices, the answer is, yes, everything that we have found. All the current models of construction equipment, for example, come with some kind of diagnostic software that runs and monitors different inputs on the device. You know, everyone's right about the McFlurry machines. I feel, if you've opened Wired in the last two years, you've probably come across a story about the McFlurry machines breaking down.

The other thing I do want to point out here is that, you know -- and I know we'll get into this further in sort of the adverse effects section, but I do just want to bring to top of mind the fact that the Office has repeatedly in the last few triennials declined to consider situations, sort of external regulations and, you know, the purported risks of circumvention for things like either health and safety or cleanliness regulations. So, when we talk about things like nuclear power reactors and water chips, this is a way of getting at the idea that there might be some sort of systemic risk to public safety by mishandling of these devices, and that is something that the Office has firmly come down repeatedly and said that this is not a thing we will consider, there is no cover using the DMCA in order to commit

violations of other safety standards and security law. So I just want to bring that to top of mind.

MR. BARTELT: All right. Thank you, Meredith, for raising that point.

I have a question I'll move on to. This is a question sort of for both or for anyone on the panel and this is, if the Office were to find that insufficient commonalities existed to support the class as proposed, should the Office consider a narrower class limited to the record's examples? For example, does the Office have enough of a record to extrapolate from the Taylor ice cream machine to cover equipment used in commercial food preparation? Again, that's for anyone on the panel. Steve and then Meredith.

MR. ENGLUND: I'll say no because, historically, the Office has really wanted to do a detailed analysis of any kind of use case for which it's considered granting an exemption. And, here, as Ms. Rose said, what we have are a few Wired articles that talk about ice cream machines. We haven't heard from people at Taylor. We haven't heard any kinds of details about how those TPMs work. While I will not hold myself out as an expert on Taylor ice cream machines, again, I tried to prepare for this panel and

it seems like the proponents' complaint about the Taylor machines is that they display cryptic error codes and break a lot. But neither of those is a circumvention issue. There's reference in the comments to a 16-button combination of key presses necessary to access a service menu to apparently demystify the error codes, but the iFixit comments say that that's unrealistic. So I was initially at a loss to even understand what the circumvention is here that's desired.

There is reference in the comments to third-party devices that are apparently helpful to franchisees. Reading the Wired article, cited in the comments, there is apparently a device called a Kytch, spelled K-Y-T-C-H. Apparently, this is some kind of circumvention device. But, if it really is a circumvention device, trafficking in it is prohibited. I can't think of a case where the Office has entertained an exemption to permit use of a prohibited circumvention device. So, even in the case of soft serve ice cream machines, it seems like the exemption is problematic.

MR. BARTELT: All right. Thanks, Steve.

Meredith, you're next.

MS. ROSE: So a couple of things. So, to

the original question, we feel that this as a class is, frankly, as delineated, as clearly delineated as consumer devices as a class, in which case consumer devices, you cannot sort of examine every single consumer device that is on the market. Similarly, we have worked and the Office has worked in previous triennials to use these sort of index cases with deeds and records to establish the similarities across a class, which we discussed extensively in our long comment and in our replies.

To some of the more specific comments, so we actually do go into pretty significant detail in our filing about what the actual circumvention requirement is in the case of Taylor ice cream machines. But, just to re-up that, the Taylor machines, in some cases, can be accessed via this 16-button press, which is not advertised anywhere. It was actually discovered by accident. That is in some cases until there is a firmware update. Now, if the machine has been touched by an official Taylor technician at any point, that 16-button key press no longer works as far as we are aware. These firmware updates come with every single repair. They are not noticed to the owner of the machine, and it also scrambles the codes that are involved. So, no, there is, in fact, no

option but to circumvent these in order to get the codes, as we laid out pretty extensively in our comments.

The idea that because we have not heard a response directly from Taylor means that the Copyright Office must abandon a petition is unprecedented and, frankly, just unworkable by the standards of any of these proceedings. We have had many, many instances, frankly, in which, you know, companies that are affected decide not to weigh in on this and deliberately as a way to obscure access to technical information. And if that were the case and that were the standard that we were working on, then there would be simply no exemptions. Just the option to defeat an exemption by sitting it out is not something that the Copyright Office has ever recognized, nor do I think they should start now.

MR. BARTELT: All right. Thank you.

And I see, Kyle, you also had your hand up. Please go ahead.

MR. WIENS: Thank you. Yeah, I might explain what the Kytch device does. This is the aftermarket hardware that connects to the ice cream machine because maybe it's indicative of the kind of innovations that consumers might want to create. So,

in the case of Kytch, they made a tool and they were selling a tool, so that would be trafficking. In this case, Kytch had permission from Taylor to create and traffic that tool, so it's not relevant, that particular device isn't relevant to the proceeding in terms of being a violation, but I think it's indicative of the kind of tool that you might want to do. So the Kytch tool, kind of like an OBD reader for your car, you plug it in and then you have a phone app and you can see what's going on. The Kytch tool plugged into the ice cream machine and then decoded these crazy, incredibly baroque error messages and it was kind of a user aid to help you navigate the system.

So you can imagine a franchise owner that owned the machine and has a whole lot of, you know, high school, college students working for them. They would need to make the interface easier to use so that they could manage the pasteurization system. As a software engineer myself, I might want to tinker with my machine, reverse engineer it, re-enable those diagnostic screens, or even create a separate interface so that my employees could manage the machine better.

And so I think it's a good proxy to see how

you have this embedded software device that is not intuitive to work on. I, as the owner, might want to find a way to make it easier to work on, provide that to my employees. And you can see how that type of approach might be highly relevant to say a contractor who has a piece of construction machinery, it's difficult for his employees or maybe some of his subcontractors to use, and so you might want to create an interface for them to make it easier to work on. Same thing for a water treatment plant or anything else.

So I think the exact types of use cases that we're talking about, being able to bypass a lock to improve diagnostics or in the case of maybe you have a pass code, the employee who set the pass code doesn't work for you anymore -- we had an example of a school district where the janitor, the employee who set up the building automation system, passed away and then the school didn't have access to the code with all the programming and the only way around that without bypassing a TPM, they were going to have to wipe the entire programming for the building, so the school would be shut down for a few days while they recreated all the programming from scratch. It's far better for the site owner in this case to bypass the password and

reset it themselves. And we provided in the record a few examples of how you might do that with a PLC.

MR. BARTELT: All right. Thank you, Kyle.

And I see, Steve, you have your hand raised, and after that I want to give one of my colleagues a chance to ask a question, but go ahead, Steve.

MR. ENGLUND: Just quickly, I think Mr. Wiens said that this Kytch device for the Taylor machines is licensed, and it would be very strange, indeed, to adopt an exemption for Taylor machines designed to enable to use the Kytch device when the Kytch device is licensed. It seems like that's proof that a Taylor exemption is not needed.

MR. WIENS: The idea is I want to able to make my own. The Kytch device isn't available for sale anymore.

MS. ROSE: Yeah. It's worth noting the Kytch device is currently tied up in litigation due to other reasons.

MR. BARTELT: Well, speaking of that, I think that my colleague, Mark Gray, has a follow-up question relating to the Taylor ice cream machines.

MR. GRAY: Sure. So I wanted to turn back quickly to something you said a minute ago, Meredith, which was, in your initial comment, you mentioned, I

think, in one or two places that when Taylor technicians come in and actually repair the device, sometimes they will just update the firmware without necessarily knowledge of the consent of the franchisee. Jumping a little bit ahead to adverse effects, what is that representation based on? Like, have you had conversations with franchisees? Like, sort of how do you know this?

MS. ROSE: I believe this was covered in the mass reporting about it, but Kyle, I think, may have had one-on-one conversations as well.

MR. WIENS: Yeah, I didn't have that conversation. I can look that up and find that for you later, but I don't off the top of my head know the source for that.

MR. GRAY: Okay, great, that's helpful.

MR. BARTELT: Thanks. I wanted to follow up. I think we got a little sense of this earlier maybe from Steve, but either for Steve or Priya, I'm wondering if there were any device types that should maybe be specifically excluded from this class. Again, are there any specific device types or fields that raise unique considerations or are sufficiently distinct from any of the examples offered by the proponents here? Steve, go ahead -- oh, sorry.

MS. NAIR: Go ahead.

MR. ENGLUND: First of all, I assume that the existing language in the exemption concerning circumvention to access creative works would be maintained and that it's not my understanding that the proponents are proposing to change that. That would obviously be very important to my clients.

But looking at the proposed class more broadly, I think the enterprise IT category is extremely problematic because, here, the example that the proponents give is IBM mainframes, and the IBM mainframe, obviously, a general purpose computer, a very expensive one subject to individualized negotiations between parties of significant bargaining power. I've negotiated licenses with IBM in the past and they are negotiated, to contrast mass market consumer licenses. And the software is separately priced, and so it has market value distinct from the box, which has been significant to the Office's consideration of proposed classes before. And the TPMs are typically associated with the preservation of license restrictions. And the class is stated very broadly here, so it looks like any software on an IBM mainframe could be circumvented or have the TPM circumvented if it was swept up in a repair effort.

The comments also referred to an upgrade key as one of the security measures on the IBM mainframe and, typically, upgrades would be priced. You would get them if you have a maintenance contract, you would get them if you paid for them. And I understood the proponents' comments to say, well, part of a repair effort, we could put a pirated copy of an upgrade on by circumventing the upgrade key, and that's kind of a radical proposition.

So, beyond that, the IBM mainframes are used in a lot of critical applications and designed for security in a way that consumer products typically are not. And so the thought of having unauthorized circumvention of security measures on a product that's designed for security and used in critical applications, including all critical infrastructure, the banking system, communications systems, ought to be scary to everybody.

MR. BARTELT: Thanks, Steve.

And I know, Priya, you were coming off mute a second ago, so I'm going to go to you, then come back to Jake, then Denver, and then I had a question from Luis at NTIA. So go ahead, Priya.

MS. NAIR: Thank you. Just to back up a little bit, I want to explain something of why we're

here, why The App Association is here, today on this specific topic. Right-to-repair exemptions in the past and even this one are overly broad. They're very expansive on a process that is supposed to be narrow, necessary, and have a high burden. We don't believe that they have met their burden of proof here.

And I think what's fundamentally wrong here with this petition and also broadly looking at legislative proposals federally and state-wide is that there is a framing of copyright and copyright-related protections as anti-competitive, and that's just not true without more. We don't believe that there is enough evidence here to show that market solutions are ineffective or that there aren't any market solutions at all.

And so kind of going back to what was previously said about enterprise IT systems, the harm that this petition poses on critical infrastructure that lay the foundation for the functioning of the U.S. Government for our economy outweighs the ill-defined harm proposed in this petition. Cyber attacks are becoming more prevalent and larger scaled, and the U.S. Government is trying to provide tools and legal obligation to allow businesses to deploy secure products on the market, and as these cyber attacks

become more advanced and complicated, as TPMs become more advanced, the United States has provided for both federal and state laws, and some of those are the National Cyber Strategy, the Secure by Design initiative, and the Biden Administration's May 2021 Executive Order on the nation's cybersecurity.

So we would really implore the U.S. Copyright Office to consider these kinds of harms that can come from a petition like this if accepted.

MR. BARTELT: All right. Thank you, Priya.

Jake, I see you had hand raised next. Go ahead.

MR. BLOUGH: Yeah, and I'd like to kind of maybe clarify a mainframe comment and then speak to the comment Priya just made. So the mainframe comment, I actually would agree that upgrade keys really aren't the thing to deal with, but there are items on the mainframe that you cannot repair the unit without passwords and without bypassing. So it means that a customer that has invested in this platform literally cannot repair it once IBM has decided that they no longer want to support it. So this is a risk to the business which forces them into unplanned upgrades because these passwords are not put in for security. They're put in by engineering to lock it

in.

To speak to Priya's point, a similar situation that actually did involve the federal government is their enterprise storage arrays, the only way that you can repair them, including replacing spindles, is to go through an RSA encrypted login on the machine. EMC decided they no longer wanted to maintain it and so the federal government was abandoned and they could not repair their own machine, and anyone who goes into bypass that system would be at risk of running afoul of this section, which is why, like, you know, I believe in the petition we talk about it's about diagnosis, maintenance, and repair. It's not to unlock upgrades. It's not to unlock software. But, once a manufacturer has abandoned a product, they should not be able to continue to lock the device so that no one else can fix it, and that is a risk to the federal government, that is a risk to American business, that's a risk to our financial system because that is who uses those machines.

MR. BARTELT: Thank you, Jake.

And Denver?

MR. GINGERICH: Yes, thank you. I just wanted to comment on the IBM mainframe example as well. I think the example provided, that the only

possible use of bypassing an upgrade key would be to install an infringing copy of IBM's mainframe software, I think that's somewhat unreasonable because there are many other things that you could install that do not violate any licenses. For example, there are many companies out there that have built on Linux, which is a freely licensed work that allows you to build on and improve it, and the point here being that all of these companies that are building on that and creating alternatives to the software that's running on the IBM mainframe should not be prohibited from installing this software for, you know, competitive reasons and many other reasons, especially, as Jake said, if IBM has chosen to simply not support it anymore. The mainframe could become vulnerable to various security exploits, and it should be up to the owner of the mainframe to maintain the functionality of the mainframe using whatever software they wished. And so it would be unreasonable to allow IBM to lock that down so that you couldn't install something else on it if it was, of course, properly licensed.

MR. BARTELT: All right. Thank you, Denver.

And before we go to Luis, I actually have Mark Gray has a question for one of our panelists.

MR. GRAY: Sure. Priya, I wanted to follow

up really quickly on your point a moment ago about cybersecurity issues. So we noticed in your comment from The App Association you mentioned sort of similar issues, cybersecurity, you know, other issues that generally we would describe as sort of non-copyright harms. Earlier today, Meredith mentioned that in the past, particularly in our 2017 Section 1201 policy study and in subsequent recommendations, we have generally tried to focus more on the Title 17 and copyright issues when we're going through this exemption process, and so I understand your point on the Administration's cybersecurity Executive Order. But we've also gotten comments in this proceeding from the Federal Trade Commission, from the Department of Justice Antitrust Division. Our colleagues at NTIA are the information advisors to the President. How should the Office look at the Administration's interest in cybersecurity but also what the Administration has been telling us during this proceeding about the repair and competition aspects that they have made a priority for the Administration?

MS. NAIR: Absolutely. Thank you for that question. I think the fact that the FTC and the DOJ and the Administration have weighed in justifies the fact that the DMCA triennial review process is

actually not the right venue. This is why. As I've mentioned, there are many state proposals, many that have also been implemented, and then some federal proposals in the past on right to repair. There are more issues than just copyright here. It's cybersecurity, it's consumer privacy, it's child protection, it's competition. If that is true, then we need comprehensive frameworks in policy or a federal legislative proposal that is more balanced.

The copyright process here for Section 1201 is primarily to protect copyright-related protections, which are technical protection measures. The exemptions are checks and balances for the system in order to allow the DMCA to evolve with our digital landscape. That's what it's for. And we do have permanent exemptions in the DMCA that are very narrowly tailored and necessary and actually promote innovation, and our members use it for security research, reverse engineering. These are things that promote innovation. But, to the extent that the petition is overly broad or doesn't provide enough information on actually why there is an actual harm here, I don't see a reason why this should be accepted.

MR. GRAY: So I see Meredith has her hand

up. Before we let her speak, I guess the question I have is, certainly, the DMCA process is a balancing process and I take the point that the scope of all of these "non-copyright harms" might be a reason why it makes more sense for this to be a matter of state legislation or federal legislation.

In our role as the Copyright Office advising the Librarian of Congress, you know, this is a petition we have in front of us and we have to make a recommendation. So is your argument essentially that because there are all these non-copyright issues, we should decline to recommend? Is it that regardless of the non-copyright issues, there is simply not enough factual evidence that there has been a showing of likely adverse effects to a non-infringing use? Or is it something else?

MS. NAIR: I would say that there is not enough evidence to show that there is a adverse effect here to non-infringing use. I do think the Copyright Office should weigh in on a comprehensive framework here, but I don't think this petition is the right venue.

MR. GRAY: Great. Thank you.

Meredith?

MS. ROSE: Yeah. I actually -- you know,

just to sort of reiterate -- I can talk everyone's ear off about the fact that sort of non-copyright regulatory matters are outside the scope of the Copyright Office's purview and, if they weren't, frankly, you know, you guys who are already under a pile of work would be swimming in it for several more weeks at a minimum.

You know, I will point out that the primary or at least many of the issues that Priya mentioned are specifically within the purview of the DOJ and the FTC, who, despite this, came out not only with very full-throated support for the petition without us contacting them -- this was entirely sui generis from the FTC and the DOJ as far as we can tell -- but they actually argued that the repair exemptions should expand even in more of a blanket than we petitioned for in the first place. So, to the extent that the federal government is concerned about things like security, safety regulations, those are best dealt with under the respective jurisdictions of the agencies that have taken responsibility for them. And the FTC and DOJ, as primary, you know, contact points for all of these concerns, have taken it under consideration and decided that the Copyright Office, you know, for the purposes of deciding the copyright

question, should recommend the class.

MR. BARTELT: Thanks, Meredith.

And before we go to Steve, I think, Luis, you had a follow-up here.

MR. RAMOS: I did. I want to follow up on sort of cybersecurity concerns and other concerns, and this question is for opponents, perhaps Priya or others. There have been several repair exemptions now, for several years now, going to multiple rulemakings ago. Is there evidence that these concerns have materialized following the granting of those exemptions, and how should such evidence or the lack thereof inform our analysis? Thank you.

MR. BARTELT: And, Steve, you already had your hand raised.

MR. ENGLUND: I had my hand up to address the larger point, but I will try to --

MR. BARTELT: Priya, we'll go to you next too.

MR. ENGLUND: -- turn to Mr. Ramos's point as well. So I think, on the merits, I actually didn't find the DOJ/FTC letter very persuasive. It seemed like mostly what it did was describe the Public Knowledge/iFixit filing, and so it doesn't really add much to the record. But I think it's really notable

here that other government agencies are just sending mixed messages on the topics here. As Meredith said, the Administration has very much made cybersecurity an imperative, and so I think you shouldn't lose sight of that message just because competition authorities are in favor of competition.

But even the FTC is sending mixed messages. There's a report from the FTC cited in Note 2 of our comments called "Nixing the Fix," where the FTC suggests that there's not a one-size-fits-all approach to extending right to repair beyond consumer goods to the kinds of things that are the topic of this class. So perhaps the FTC has had a change of heart, but, again, mixed messages.

You know, concerning Mr. Ramos's question, I think the nature of the cybersecurity risk that is posed by this proposed class is very different from any other class that we've seen. Enterprise technology that is used to control critical infrastructure is very different from consumer goods or even medical devices and motor vehicles. So the fact we haven't seen a massive cybersecurity problem associated with consumer goods, or at least I haven't, doesn't suggest to me that it would be a good thing to encourage circumvention of security measures on

products that are designed to be secure because they secure important infrastructure.

MR. BARTELT: All right. Thanks, Steve.

Priya, I think you were about to speak before we went to Steve. I don't know if you wanted to jump back in here.

MS. NAIR: No problem. Yeah. So, as for prior petitions on the right to repair consumer devices, we have always opposed that, particularly because they're often too overbroad.

As far as cybersecurity threats matriculating from them being accepted, we don't have any specific examples on that and would be happy to follow up a bit on that. But I will say that cyber attacks have advanced in the past maybe five years, a lot of ransomware attacks, one of which happened in 2017. It was a global ransomware attack that used an NSA hacking tool, EternalBlue, to attack Microsoft Windows. I think it infected between 200,000 to 300,000 computers. This was also within corporate and government networks. These kinds of things happen more and more frequently.

In fact, two days ago I was reading an article from the FBI where they suspect or they estimate a global loss of one billion U.S. dollars per

year due to ransomware attacks. This should be enough to support the idea that technical protection measures have to have strength to them and every time that they're being cut away, there is more cause for these types of cyber attacks.

MR. BARTELT: Thank you.

And I see, Stacey, you have your hand raised, as well as Anthony. Go ahead, Stacey.

MS. HIGGENBOTHAM: Okay, thank you. On the cybersecurity front, I do want to make a distinction between the types of attacks on OT networks that would happen because of access to the PLC and the type of, like, circumvention we're talking about versus something like EternalBlue, which was a ransomware attack against Microsoft Windows software. So I do want to say, on the cybersecurity front, the questions we should be asking should be about attacks at the PLC level because that's what we're trying to protect here. So those are far more expensive and less common than the majority of the attacks on critical infrastructure that we see today. So having a cybersecurity exemption here, I don't think it's as relevant or as important.

MR. BARTELT: Thank you.

Anthony, go ahead.

MR. ROSBOROUGH: Yeah, thank you. I just wanted to echo some of the statements of others, you know, pointing to the caution, I guess, of using this process as a means to sort of mitigate the cybersecurity merits of a certain exemption. And I think, you know, it's not only important that cybersecurity concerns are not part of that consideration but that they're, you know, explicitly ignored and left to other regulatory instruments to deal with that.

And just on a sort of anecdotal point, I think that, you know, to the extent that there are cybersecurity risks that are presented by allowing circumvention of TPMs, you know, I would think that those who are willing to carry out widespread cybersecurity attacks or threats would not be terribly persuaded by a TPM violation under copyright law.

MR. BARTELT: All right. Thanks, Jake.

I'm going to pivot here a little bit in the questions and this is a specific question maybe more for Meredith and Kyle for the petition. What we are looking at here was the petition for the class said that it wanted to expand the current repair class to commercial and industrial equipment, which would presumably involve the same regulatory text. We're

looking to see if you wanted to clarify here. Are you proposing to amend the consumer device exemption, or are you proposing a new regulatory paragraph that uses the same text as the consumer device exemption but which applies to commercial and industrial equipment?

MS. ROSE: So our primary thought was to expand based on the consumer devices exemption and just incorporate that. However, we are open to, you know, regulatory text that gets at a similar end if it would be easier for drafting purposes just to separate that into two categories.

MR. BARTELT: Okay, thank you. Another maybe sort of clarification here too, and I don't know that you actually requested this, but the current exemptions permit lawful modification for vehicles, including agricultural equipment, but do not permit modification of other types of devices, including medical equipment. So, if the Office recommended an exemption that did not permit modification in line with medical equipment, would that be an issue for any of the proposed uses that you seek to engage in?

MS. ROSE: I don't believe so, but, Kyle, you can correct me if I'm wrong there.

MR. WIENS: Saying modification of any kind?

MR. BARTELT: Right, or I guess we have

lawful modification for vehicles, including agricultural equipment but under the other exemptions. Just if modification was required in order to execute any of the repairs, if that's what you mean.

MR. WIENS: Modification would be helpful. Let me give you an example. We have a building automation system that has access controls, so your badges to get into the building, and the manufacturer who built the system has abandoned the system. They don't make security updates available and so we have to, like, separate the thing off from the Internet because we don't trust it because it doesn't have security updates available, and it had a 99 key card limit. So, when I hired my 100th employee, we didn't have a way to give them access to our building anymore. And so that would be the kind of thing where I would want to go in and modify and find where is this crazy 99 limit and be able to modify and improve it. And I think that's often the case. I mean, if you look at construction equipment, it's very common. You're modifying the equipment physically to accomplish the task. I think it would make sense to allow modification of the software as well.

MR. BARTELT: And I'll just give the opponents a chance to respond, whether modification

raises any specific concerns, you know, as it's allowed for vehicles or as applied to the commercial and industrial device class.

MR. ENGLUND: So, yes, it isn't something that the proponents asked for, so it isn't something that we have had occasion to think about and vet to any length. But modification is certainly something that the Office treated at great length in one or more of the prior proceedings before limiting it to just the motor vehicle class, and all of that analysis speaks for itself.

But, you know, for example, in the enterprise IT category, all the software we're talking about is licensed, so the licenses would typically prohibit modification. So saying that we will permit circumvention to enable modification, it's a violation of the licenses for mainframe software, doesn't seem like something that's consistent with the copyright principles that the Office applies in these proceedings.

MR. BARTELT: All right. Thanks, Steve.

And sorry, Denver, I had overlooked, I saw you had your hand up. Please go ahead.

MR. GINGERICH: Yeah. So I just wanted to comment on that. I think, in chatting with Kyle, just

to clarify, the 99 user limit was simply a restriction built into the software. There was no licensing --

MR. WIENS: That's correct.

MR. GINGERICH: -- on top of that. So it wasn't like Kyle could pay more to get more users. It was just simply not allowed by the software.

MR. WIENS: I couldn't pay more of any kind because they totally discontinued their support of the product, so yeah.

MR. GINGERICH: Right, and that's another --

MR. WIENS: And that wasn't an arbitrary license in the first place. It was purely just a limitation of the system.

MR. GINGERICH: Right. And speaking to limitations of the system, I just wanted to follow up on that, indicating that one of the issues too is with, as was said, some of the modifications. You know, when we're talking about modification versus repair, it's important to consider what baseline functionality you're looking at, and I think one thing that has been noted a lot is that if the baseline functionality is do not be vulnerable to known exploits, then some amount of "modification" per se is required in order to maintain that level of functionality. And as Kyle was talking about, you

know, when these things become unsupported, it's extremely important for the owner of the device to be able to remedy that by using alternate software if necessary and, of course, appropriately licensed, but it may not always come from the manufacturer of the device since others with appropriate expertise can create software that is compatible with that hardware as well.

MR. BARTELT: All right. Thank you for clarifying that, Denver.

Anthony, I see you have your hand raised. Would you like to go ahead?

MR. ROSBOROUGH: Yeah, just very quickly. I think Denver kind of beat me to most of what I was going to say, but, you know, the distinction between circumvention that has a indefinite effect -- you can think of so-called jail breaking -- and modification on the other hand, that distinction can be quite tenuous, and I would caution against, you know, singling out modification as being distinct from a kind of indefinite circumvention.

MR. BARTELT: Thank you. Continuing with -- well, off of the regulatory text, but continuing with sort of scoping the proposed class, and we've touched on some of this already, but I wanted to just circle

back to it, was it's more about -- I know, as this is somewhat a broad class, we have some of the index examples. I was curious if maybe for the proponents, but also to the extent that opponents have knowledge here, if the copyrighted works, meaning in most cases the software, possibly in some cases manuals, are installed on the equipment in all cases or if in some instances it might be just installed on some other type of device ancillary to the equipment being repaired.

All right, Jake, I see your hand is raised, and then Kyle.

MR. BLOUGH: Yeah. In the experience that we have in enterprise IT, these are things that are built typically into the firmware that interfaces to the hardware to enable repair, diagnosis, or maintenance. They may be on what they would call a management console which may be physically separate from the unit but interlinked.

MR. BARTELT: All right. Thank you.

And, Kyle?

MR. WIENS: Yeah. Most of my experience is the software is installed physically on the thing, so a PLC is a physical object that has the computer and the controls on it. I'm sure there are cases where

it's a situation like you described, but most of the equipment that we see, the software comes pre-loaded on the physical artifact, whether that's a piece of machinery or controller.

MR. BARTELT: Thanks, Kyle.

And, Jake, did you have a follow-up, or was your hand just still raised from a moment ago?

MR. BLOUGH: It was still raised. I'm good.

MR. BARTELT: Okay, that's all right. Continuing on with this line of questioning about sort of the specifics of where the software is installed, we also were curious about who or what entity typically develops or owns the commercial industrial equipment software -- for example, it could be the manufacturer, a vendor, a system integrator, or the purchaser -- and whether this varies depending on the type of device. For example, with the PLCs, something in the record suggests that the device owner might commission custom software to be installed on the device. In that instance, does the client then own the software as a work made for hire or -- Kyle, I see you came off mute. Go ahead.

MR. WIENS: Sure, yeah, a good question. So I think we have to frame this as like devices that are programmable, where you're writing software on top of

it, and devices that are not. Probably the majority of the category, you're not writing software on top of it if you have a software. The Taylor ice cream machine, for example, doesn't have a software development environment on top of it. It's just the machine.

But, in the PLC situation, they're building automation software, very, very common. Actually, I have a systems integrator working for me right now writing software on top of a machine, and in this case, it's a work for hire. But I have to admit, you know, having negotiated a lot of contracts, I couldn't tell you what the exact terms of the work-for-hire contract of this guy that I'm paying tens of thousands of dollars. It didn't cross our mind as we were designing a building that we would need to be focusing on the IP licensing in the process. And we're learning regularly that it's very common for an owner not to be given the access code to the software. So I think I will defer to the lawyers in the room. I'm not one to talk about what the default kind of ownership of that software is.

But the experience of an owner is, five years down the line, the integrator will be gone. They wrote that software that sat on top of the

software written and owned by the device manufacturer. I have the physical device. There's boutique software that was written and there's really only generally one installation of that particular set of software in the world. It's operating my facility and I'm going to need to be able to go in and change a parameter, and if I don't have the password, I'm going to have to break a lock to be able to get at it.

MR. BARTELT: Thank you.

And, Steve, I see you have your hand raised. Please go ahead.

MR. ENGLUND: Yeah. The thing to remember about the PLC is they are just general purpose computers. They're small, they're inexpensive, they're in a rugged form factor so that you can hang them on a factory wall next to a piece of equipment. But, in terms of computational power, think of a laptop and so totally programmable. They are secured for reasons that made total sense. You think about a factory with laptops sitting around next to every piece of equipment. You wouldn't want somebody to walk by and screw things up, tamper with them. The factory owner should want them locked down so that people can't tamper with the software that's on the computer. And so some of what Mr. Wiens is talking

about, kind of cases where an ordinary and desirable anti-tampering function is creating problems because somebody dies and nobody has written down the password, that's a management failure. But, you know, in general, security for the software is a good thing.

In terms of the software ownership, because they're general purpose computers, like your laptop, the answer depends where the software came from. The manufacturer isn't trying to keep people from running software on its device any more than the manufacturer of your laptop is trying to keep people from running software on your laptop. But a systems integrator, a contractor hired to put together a system -- you know, take your pallet full of PLCs and wire them together to control a factory -- may have proprietary software, may create custom software, it depends how the factory works.

But I do have some experience negotiating contracts for large IT systems. I've spent the last year and a half working on one for the refurbishment of a factory. It's a very big and thick contract with lots of elaborate controls at every stage and licensing provisions where there's proprietary software, work-made-for-hire terms, and requirements to deliver all kinds of detailed technical information

to the owner at the completion of the process. So this is the sort of thing that the market at least sometimes functions to address by giving owners a great deal of control over the systems that they're paying a great deal of money to have developed and installed pursuant to highly negotiated contracts.

MR. BARTELT: Thanks, Steve.

I see, Stacey, you have your raised, and then I think we have maybe one last question from Luis in this section on the scope of the class. But go ahead, Stacey, first. Oh, Stacey, I think you're on mute. Please unmute.

MS. HIGGENBOTHAM: Sorry. All right.

MR. BARTELT: No, that's okay.

MS. HIGGENBOTHAM: I just want to clarify the PLCs are not like your laptops or the chips in your laptops. These computers are usually highly proprietary, very designed. They run not traditional operating systems like Windows or Linux or Android. A lot of times, they run these -- they're called real-time operating systems, super proprietary, which does get to the competitive nature of kind of how a vendor who uses a PLC can actually lock a company in through, like, repairs because it is very hard to program these or it requires a set of expertise to program these.

So I just want to make that fairly clear here.

MR. BARTELT: Thank you.

And, Luis, you had a question here?

MR. RAMOS: Yes, thanks, Nick. I'm curious, is there commercial and industrial equipment that is already covered by one of the other exemptions for repair? And the reason that I ask that, and this is both to supporters and opponents, are concerns related by granting an exemption related to commercial and industrial equipment already addressed in the language in other exemptions? Thank you.

MR. BARTELT: Okay. Steve, I see you have your hand raised. Go ahead.

MR. ENGLUND: Yeah. So, to some extent, yes, and I would point you to Exemption 13 for vehicles and farm equipment. Some of that seems to be -- or some of what is addressed in the current category seems to be addressed in Exemption 13 and that I think is a matter of good regulatory practice. One shouldn't have two exemptions covering the same topic, but I don't have a particular view on how commercial vehicles and farm equipment end up getting classified.

MR. BARTELT: All right. Before we conclude this section, I just want to see if anybody else had

responses to Luis's question or --

MR. WIENS: I think there is, I mean, so many products that are used in a commercial setting, a dishwasher or just about anything else, like most products are used in a variety of consumer, industrial, and commercial applications.

MR. BARTELT: Okay. Thank you, Kyle.

So, with that, we're going to move on to a few, just a few questions on non-infringing uses, and then I think the majority of the remainder of our time we'll spend on adverse effects, though, obviously, we've already gotten into some of that in our earlier discussion here. So I'll start off with a question -- this is really open to anyone on the panel -- how does the fact that the users of commercial industrial devices are more likely to be commercial actors affect the fair use analysis? In other words, does the commerciality of the use change the fair use analysis specifically with respect to the first factor? And the first hand I see is Meredith. Please go ahead.

MS. ROSE: Our opinion is it does not change the analysis. This is a repair just the same as if you were repairing a home device because there exist potential extraneous repairs. For some reason, it told me I am done talking.

MR. BARTELT: No, we can still hear you. You're welcome to continue your thought.

MS. ROSE: No. So my point is that I don't believe this does affect the analysis just because they are commercial actors, frankly. Consumer devices at home are used in commercial contexts semi-regularly. As Kyle pointed out, dishwashers exist in restaurants as well as in homes. People run commercial enterprises out of their home all the time. And so I think, to the extent that we're going to start drawing lines around whether or not motive that is potentially implicated by the use of the machine in the first place, it becomes so attenuated that it bears nothing to the analysis.

MR. BARTELT: Thank you, Meredith.

Steve?

MR. ENGLUND: You wouldn't be surprised that I disagree. Since the Office last addressed this question, the Supreme Court has reminded us in Warhol that the commercial components of the first factor matters, and, here, it's all about commercial actors. You have commercial users of the commercial products and you have commercial third-party service providers that would like to service products, and so it's fundamentally a dispute among commercial actors. And

that's not something that the statute permits you to ignore when analyzing the first factor.

I think the analysis of the other factors can be affected also. I don't know if you want to get into that or not, but just to put it on the table --

MR. BARTELT: Sure.

MR. ENGLUND: -- the second factor, the court has -- or the Office, rather, has historically found that repair exemptions are focused on very functional firmware built into devices. That's not what we're talking about here, at least in some of these categories, for the enterprise IT in particular and to some extent the PLC exemption. We're talking about licensed software, applications potentially, and so that implies a very different second factor analysis than the Office has previously applied when thinking about repair exemptions.

And, similarly, with respect to the fourth factor, the Register's fourth factor analysis has always turned on the fact that firmware embedded in consumer grids or motor vehicles doesn't have uses or value that is separate from the products in which it's embedded. But, when we're talking about industrial commercial equipment, that's not true, not always true, particularly again in the case of the enterprise

IT. It's all licensed software. It's all separately priced. And when people are talking about circumventing the TPMs on licensed software, it's a violation of the license agreements and potentially runs into the economics of the licensing models. And so that's a very different fourth factor analysis than the Office has previously employed.

MR. BARTELT: All right. Thank you, Steve.

And I see we have a couple hands raised, so I'll go with Anthony next, then Meredith, then Priya.

MR. ROSBOROUGH: Yeah. Just very quickly, it's important that we characterize what is commercial about this, about a repair, you know. And if we're talking about commercial repairs carried out by independent service providers, I mean, we're not talking about commercial uses of software necessarily to the extent that it is unauthorized distribution or reproduction of that software. So I just think it's important that when we're talking about fair use in the context of commercial software that we're clear that the commercial relationship we're talking about here is delivering -- well, is in carrying out commercial repairs and not necessarily in unauthorized commercial uses of protected works.

MR. BARTELT: Thank you, Anthony.

Meredith?

MS. ROSE: Yeah. Just to speak directly to the Warhol concerns. So Warhol is inapposite in this case. Warhol, the case in Warhol, the work in that case was, like, highly creative expressive work, which, again, the software at issue is not, frankly. Like, we've discussed this at some length in our petition and the Copyright Office has dealt with this before. The work in Warhol was extremely creative and expressive and then it was copied, modified, and put into commerce directly in competition with the original work upon which it is based. That is not the fact pattern we're discussing here by a country mile.

What we're discussing here is access to copyrighted software which is unexpressive. It is done specifically for the purpose of controlling inputs and diagnostic materials happening within a physical object in order to run the physical device, and there's no copying and modifying it and putting it into circulation. To the extent that there's any copying or modifying being done, it is being done to restore the original functionality of the product.

It is totally unrelated to the fact pattern in Warhol, which I will also add the Supreme Court bent over backwards several times to say that they are

cabining this specifically to the fact pattern at issue in Warhol and expressly warned against trying to apply it elsewhere.

MR. BARTELT: Thank you.

And, Priya, go ahead.

MS. NAIR: Absolutely, thank you. I'm going to kind of shift a little to the fourth factor but maybe more broadly. I think we should all be careful not to make blanket determinations about fair use. You know, this is always going to be a case-by-case determination, a fact-specific determination. And although Warhol does apply a bit more broadly, I think we should keep that in mind.

I think, when it comes to right-to-repair exemptions, really thinking about where this fair use analysis kind of leans on, I look at the fourth factor as a very important one and that's the effect of the use upon a potential market. And the Copyright Office even says, in assessing this factor, courts consider whether the use is hurting the current market for the original work and/or whether the use could cause substantial harm if it were to become widespread.

We've kind of detailed in our comments that there are harms to the current market. If a device maker has an unauthorized or unlicensed third-party

repair shop and they repair their device in a way that would either expose information on their software or provide the consumer a bad product, that would inflict upon their current market. I would also say that the ability to repair your own devices kind of falls within the copyright holder's rights to establish and benefit from these derivative markets.

MR. BARTELT: I have a follow-up question on market harm then, is whether there's any market for any of the commercial or industrial device software separate from the use within the device itself, and that can be either to you, Priya, or to anyone on the panel.

MS. NAIR: Happy to follow up on that.

MR. BARTELT: Go ahead.

MS. NAIR: Yeah. For the specific class here, the commercial industrial equipment, again, we are experts on a category separate from that, but happy to follow up on that specific one.

MR. BARTELT: Okay. Thank you.

And I see, Meredith, you have your hand raised. Go ahead. And then, after that, Steve.

MS. ROSE: Just quickly, so the answer as far as we're aware is no, that all of these software programs are designed specifically for the device in

which they are embedded. Doubly so for PLCs, which are often bespoke to the point of, you know, as Kyle's point was, they are designed specifically to take into account the various connectivity they're going to need to other systems. And so, as far as we are aware, no, there's not a situation where you could take, say, a Caterpillar operating system and switch it into a Sennebogen or something similar. They are all specifically made to the particular array of sensors and functions that is present within the device in which they are embedded.

MR. BARTELT: Thank you, Meredith.

Steve?

MR. ENGLUND: Well, I'll just highlight as I have several times previously that the enterprise IT category is different in some respects from the other kinds of products we're talking about here. And I think it is probably true that software applications that are intended to run on an IBM mainframe only run on an IBM mainframe, but they are licensed for a great deal of money to run on an IBM mainframe. And so that doesn't mean that there's not a market and a very important commercial market even if they're technically incompatible with the operating systems on different computers or the operating system being

compatible with the hardware on different kinds of computers.

MR. BARTELT: All right. Thank you. And I just wanted to see if -- I'll turn the mic for a second to my colleague, to Luis, and see if -- I think maybe he had a question about negotiated license potentially here, so, Luis, if you want to go ahead and ask that question. We're about to move on to the adverse effects for the remainder of our time here, but I'll let Luis maybe proceed with his question and then we'll go into adverse effects.

MR. RAMOS: Sure. I just want to get a better sense of the landscape here and how it's different maybe from consumer devices, specifically whether there are repair agreements between the manufacturer and developer and the purchaser and more so than the consumer device space and whether that sort of impacts either market harm under the fourth factor or under the 1201 statutory factors. Thank you.

MR. BARTELT: And I see, Steve, you have your hand raised, and then Kyle.

MR. ENGLUND: So I don't have the factual basis to address this comprehensively but can say a little bit about it. I think the short answer here

is, yes, that, in general, my sense is that commercial industrial equipment tends to have long warranties, and because it is used in important commercial industrial applications, tends to have even some service arrangements that are kind of part of using such devices. And so, to take the category I know best, the enterprise IT, people who have spent millions of dollars on IBM mainframe tend to have maintenance contracts for the hardware and the software. And, you know, my experience has been that owners of devices like that tend to view it as very important that they have access to very quick maintenance and so they bargain over service level agreements to ensure that if they experience any downtime it is brief. They also make disaster recovery arrangements to mitigate the effects.

In the case of some of the other equipment, I just in preparing for this hearing noticed that Taylor ice cream machines have a five-year warranty, and I'm under the impression that some of the heavy equipment manufacturers in construction have various kinds of maintenance offerings. So this is very different from a child's toy or even a dishwasher in the sense that you have sophisticated users who are depending on equipment for important commercial

applications and have in place commercial arrangements that the OEMs provide.

MR. BARTELT: Thanks, Steve.

Kyle, go ahead.

MR. WIENS: I mean, the short answer is all of the above, but I don't see how it's fundamentally different than the consumer market. I bought a TV at Costco yesterday. The default was it came with a three-year warranty. They wanted to sell me a five-year warranty for another $35. Consumers have options. Consumers have the ability to go and hire repair services. I have a feeling the McDonald's franchise owners, when they're buying a Taylor ice cream machine, are not looking at a software licensing agreement or, if they are, they're spending the same amount of time as you did when you clicked through the Microsoft Word license agreement, which is we all spend very little time.

It's kind of amazing how similar these cases are to consumer products, even to the -- a couple of members of the Department of Defense procurement arm wrote an op ed in the New York Times a few years ago talking about how military procurement was basically the same as consumer procurement, and they were asking all of us advocates to try to improve the terms that

consumers were getting around repair access over the long term because it would help military equipment. So I think, yes, there are cases where it's negotiated. There's additional software that's built. But, even in those cases, it's not clear at all what the kind of ownership and maintenance of it is going to be over the long run.

Broadly, we're running into the same challenges when the Copyright Office investigated the software embedded in electronic devices. That's what we're running into with all the commercial products. And the historical expectation maybe with consumer products is they last for 10 years. With commercial industrial products, they last for 30 or 50 years. But we're in a new age where software is in everything and nobody knows how to maintain software that's going to last for 30-plus years. Certainly, manufacturers aren't planning on providing a path for dealing with that. And I'll maybe pass it to Jake because that's what his company does, is pick up when the manufacturers leave off.

MR. BARTELT: Perfect. Thanks.

Go ahead, Jake.

MR. BLOUGH: Yeah, and it's like -- I think, like, two kind of points here. One is there's a lot

of talk about mainframe and that is the smallest slice of enterprise IT. It's like 2500 of them in the United States. There's 40 million of the rest of servers and storage devices and everything else that run the economy. So there's kind of an over-reliance there on this one example.

And the second bit of it, you know, kind of speaking to what Kyle was saying, is, you know, one, this isn't, you know, licensed software modification. This is processes that must be used on a machine to keep it operating and to keep a business running, and that is the repair, diagnosis, and maintenance portion where this has been locked off from the rightful end user and buyer of the product, and it's being hidden behind this concept of, well, this is a licensed software. So I think there's a distinction there between what -- and I think Meredith said this -- of returning it to the state that it was in before it had a failure. So I want to make sure that we have that distinction where we're talking about enterprise IT and it's not about mainframe. It's about everything in IT. Thank you.

MR. BARTELT: All right. Thank you, Jake.

With that, I am actually going to turn over the questioning to my co-moderator, Mark Gray, who's

going to ask some questions about adverse effects and any other follow-ups he might have.

MR. GRAY: Great. Thanks, Nick. And just to sort of sign for us where we are for everyone here, you know, we have 30 minutes scheduled left for our time today. As Nick mentioned, we wanted to sort of wrap up our roadmap today with adverse effects, but we can obviously answer any additional questions or see where the conversation takes us.

For our next question, I would like to turn to the proponents and ask you to provide sort of a clear overview of, you know, when we're talking about all these different categories of enterprise or industrial equipment, what specific kinds of technological protection measures are you seeing and are you looking to circumvent that are restricting access to copyrighted software? And to the extent that that differs by a device or category, please elaborate on that as well.

MR. WIENS: So maybe I can start and then pass it off to the other folks. It depends on the category of products. So, in the case of the Taylor machine, we're talking about there's a touchscreen on it and there are pass codes. There's this diagnostic code that disappears. And so the thought would be to

make a modification of the firmware on the device to re-enable that diagnostic service. What exactly the form of the TPM is on that is going to depend on the specific micro-controller that's used.

With PLCs, there's a password that you're bypassing. And it's interesting, some of the PLCs, I think we said it in the record, there's a bypass where, like, you push a button or you reset a certain amount of RAM or you remove a memory module and then it resets the password and then you can go, where, with other devices, there isn't a way and so you would need to go and make a modification again to the firmware to be able to bypass that password.

With a lot of machinery, I think it's going to be similar to the record around John Deere and the agriculture equipment, where you have an ECU or some equivalent running. You can imagine John Deere makes generators maybe that would be included under this and maybe they're using very similar software on generators that they do on their tractors.

For the enterprise IT equipment, again, I think I'll pass it to Jake to describe how that works because this is his day-to-day.

MR. BARTELT: Jake?

MR. BLOUGH: Yeah. Thanks, Kyle. So we

see, you know, maybe three common things. The first thing, like Kyle said, is a password. So there is a diagnostic or repair function built into the machine that is already there, but you cannot access it without a particular password and that password is not shared with anyone outside the manufacturer.

The second version of this is a separate login to a management software, like in the EMC world, there's a thing called SymmWin, that exists on the machine. All of the repair functions are on the machine, but you cannot access it without going through an RSA encrypted login. So you cannot replace a component without having this special login and password, which is not shared outside of the OEM.

And the third one is sort of a modification of that where there are menus to be able to perform diagnostics and it's not an RSA encryption, but it is a rotating password that you have to call the manufacturer to get, and you cannot receive that from the manufacturer. This is specific to peer storage. You cannot receive that unless you have a maintenance contract, which, you know, to Steven's point, yes, you can have a maintenance contract, but it also means you're locked in forever. And when they decide they will no longer service it, you will no longer receive

those passwords. So it would be the ability to access the service menu to be able to perform repairs without running afoul of the law.

MR. GRAY: Anyone else on this one?

(No response.)

MR. GRAY: All right. The next question I had, starting with proponents and then I'd like to hear from Priya and Steve, after these types of technological protection measures are circumvented just as a general matter, are those technological protection measures essentially in a state of being bypassed, or is it just sort of a one-time circumvention? Or to put it another way, after you circumvent a TPM to repair some sort of device or equipment, is that TPM restored, can it be restored, or is the device essentially permanently unlocked? And to the extent that this differs by category, again, you know, please, that information is helpful.

MR. BLOUGH: In the enterprise IT space, the machine must be returned to its original state for it to continue to function properly, so it is not permanently disabled. It's getting through it the first time is the issue.

MR. WIENS: Yeah, that's correct, and that's with a building automation system, right, the idea

that the maintenance person is no longer around. We need to bypass the password. We want the password on the system, so it's repair. The goal is to, you know, bypass the TPM, make whatever changes you need to the system, and then relock it with a password that you know this time, and same thing for a PLC.

MR. GRAY: Great. Before I turn to Steve and Priya, so let's say hypothetically the Office was inclined to recommend this exemption. If we imposed a requirement along the lines of requiring the TPM to be reinstated or restored, (a) is that something that would be technically feasible for all the use cases you have in mind, and (b) would that still enable the kinds of uses you're trying to engage in?

MR. WIENS: Good question.

MR. BLOUGH: Go ahead, Kyle.

MR. WIENS: Go for it, Jake. I'm thinking about it.

MR. BLOUGH: Yeah, and I'm trying to think of the way to phrase it. So, Mark, maybe could you rephrase that question for us real quick?

MR. GRAY: So, essentially, say there's a TPM protecting some sort of piece of industrial equipment, maybe it's a password, you know, you disable the password. If we recommended a repair

exemption of some sort -- and, again, this is hypothetical; this is not to say that we want to -- would it be an issue for us to require that that technological protection measure be restored?

MR. BLOUGH: So I think my answer, which kind of echoes Kyle, is we want a password on it. We absolutely want a password. We do not want a password that's 1111. So I believe that we would want it to have to be restored. Like, there has to be some sort of security there. You don't want to just disable it to do your thing. I think the big thing is, is if you can understand how to do the password or you can understand how to change the password, but you still want the protection on the machine.

MR. GRAY: Okay.

MR. WIENS: So I generally agree with Jake. Generally, we want the lock. But I'm not sure that we can do it in all cases. A good example would be a device that is out of security -- it's not supported by the manufacturer anymore. There aren't security updates. And so what we're going to do is bypass the TPM, maybe wipe the software off of it and install Linux or something else. In that case, there would be no way to restore that TPM. The device wasn't secure anymore and so there was just no other way. You had

to install something totally different on it.

MR. GRAY: All right. Anyone else from the proponents on this one? Meredith?

MS. ROSE: Yeah. I mean, my understanding, you know, from what I heard Jake and Kyle saying is that I don't know that there would necessarily need to be a requirement to reinstall a TPM given that most rational folks would want there to be, you know, a TPM, albeit one that they can deal with when they need to repair things. So I'm not sure that that would necessarily be, like, you need a requirement within the regulatory text in order for that to happen. It just sort of seems like something that would happen regardless in the rational actor situation.

MR. GRAY: Stacey?

MS. HIGGENBOTHAM: So, broadly, from a cybersecurity perspective, we've actually been legislating and focusing on moving away from hard coded passwords inside something like a PLC, so it kind of moots some of these questions that we're asking about and especially going forward.

MR. GRAY: All right. Steve or Priya, do you agree that that would not be necessary to impose as a requirement if we recommended an exemption of some sort for repair?

MR. ENGLUND: So mostly I think you should not recommend an exemption for repair. And the last few minutes of discussion illustrate for me the lack of commonality both within the commercial industrial category of equipment versus consumer goods because I think, for consumer goods, you wouldn't be having a conversation about whether owners actually desire passwords. And because of the breadth of the class, it's a little bit hard to kind of conceptualize the full range of things that we're talking about.

But, to the extent that we are talking about TPMs on software that secures content on devices or that secures licensed software on devices, I think you would want to ensure that that content or that software is not left in the clear because it presents obvious infringement risk.

MS. NAIR: I would agree. And I also want to go back to just hearing a few things that were said on the proponents' side. What I'm failing to hear, quite frankly, is where the actual harm is to the lawful use of these copyrighted works, and that also includes how market solutions are ineffective or if there aren't market solutions, like I've said before.

It seems like there is a categorization that manufacturers and developers abandon their equipment

or have any kind of warranty for their customers or the end user of their product, and that just can't be true. I would really love to see the statistics on that. Manufacturers and developers have incentives that third-party repair businesses don't have. They have the incentive to secure their customers' privacy and security on their devices. They also have the incentive to provide authorized repair options for the end user of their product, and that's simply because they want their product to be strong in the market. And so it would be interesting to see kind of what the statistic on manufacturers that abandon their product or don't provide sufficient options.

MR. GRAY: Great.

Denver?

MR. GINGERICH: Sure. I just wanted to respond to that a little bit. I think that the common reason that manufacturers stop supporting their devices is that they want you to buy a new one, and that's the standard lock-in mechanism that is used widely across the industry. And it's unfortunate because it leads to a lot of waste, people just throwing out products because the software is not useful even though there's nothing wrong with the hardware. And so that's why it's especially important

that people be able to unlock their device to install different software to maintain the functionality beyond any period that the manufacturer may wish to support the device for, because the device owner could then support it themselves or hire someone else to support the device using the existing software or replacement software that is obtained under an appropriate license.

MR. GRAY: Thank you.

Meredith?

MS. ROSE: Yeah. I mean, you know, at the risk of sounding like a broken record, we do talk pretty extensively about the actual documented harms of breakdowns and the lack of repair options in our comments, but just sort to re-up some of the numbers that we have on this, you know, it is worth noting that while -- you know, I believe the figure that we found for a McFlurry machine breaking was something along the lines of about $650 in lost sales in a given day. You know, we talk about things like PLCs, where, you know, once you have a manufacturing breakdown, time is absolutely of the essence in getting this working again. I mean, this is a similar situation to what we see with agriculture, where you have crops that can literally rot in the field. It's extremely

time-sensitive.

And so, the extent that we have these breakdowns in PLCs on manufacturing situations, you can have, I believe -- sorry, I'm control F'ing here -- automotive manufacturing stoppage costs $22,000 per minute in terms of, like, just trying to bring that back up online. In 2019, the average estimated cost of unpinned manufacturing downtime was $260,000 per hour, and that's not even the most expensive. That's manufacturing as a whole as compared to automotive specifically. So there is significant financial and logistical costs associated with breakdowns in situations like PLCs.

Enterprise IT, you know, we went through a whole litany of incidents from 2009 all the way up to 2018 where, you know, mainframe programming error costs, you know, crashed an entire ATM system throughout Taiwan. You know, lost profits damage reputations. This is a significant cost, and, frankly, even $650 in lost sales in a day is a hugely significant cost when you're a small franchisee of a McDonald's.

So there are lots of documented harms. We've pulled quite a few examples from this, and these are all directly tied to the inability of individual

business owners and users of these machines and these various kind of equipment to be able to effectuate a quick repair rather than having to wait for, for example, the John -- we're all very familiar at this point with John Deere and the John Deere repair services and the timeframe that they took to get out and repair a tractor. You know, if you're talking about a Taylor soft serve machine, we found the average cost for a 15-minute visit, I believe, was something like $300 and there could be multi-week wait lists. So this is really not a situation -- you know, we can talk until the cows come home about how manufacturers have every incentive to provide prompt and fast and affordable repair, but that's just not the reality of what's happening by any measure.

MR. GRAY: Great. Thank you.

Jake, if you could keep it really quickly. You know, we have 10 minutes and then I think we have another question or two, and then, Steve, we'll get to you afterwards.

MR. BLOUGH: Yeah. Yeah, I'll be super brief. Yeah, the concept that manufacturers don't abandon, they literally have nomenclature called end of support, end of service life that they post for every single piece of equipment that they ever made.

The IBM C-13 goes end of support December 31, 2024. They've already posted it. They will abandon that machine and will no longer sign service contracts and that machine will be un-repairable on January 1, 2025. Thank you.

MR. GRAY: Great. And, Steve, before we go, given where we are on the time, I'm also going to open with the next question for you, and so you can answer, you can share what you have right now, as well as answer this question, which is pretty related.

So it sounds like at least on the proponents' side, one of the concerns here is that there is a significant issue with lack of original manufacturer support. You know, one of the things that we frequently ask about in this process, in this rulemaking, is, you know, what kinds of reasonable alternatives there are to circumvention, which would include things like, you know, warranty repairs or authorized repair technicians. You know, to what extent are those avenues reasonable alternatives to circumvention or to what extent are they not?

And, Steve, we'll start with you and then we can circle around.

MR. ENGLUND: Yeah. So I raised my hand to respond specifically to Ms. Rose's recitation of the

various numbers on the cost of downtime. I think important to recognize that the cost of downtime is not the same as the incidence of downtime, which is important to recognition of harm. So the proponents have provided lots of data about the cost of downtime, very little about the incidence of downtime, and really not made a showing that across broad categories of industrial and commercial equipment or even in specific ones that there are significant problems with owners being unable to get timely repair and maintenance. And AED filed some comments in this proceeding -- it isn't represented here today -- but those comments suggest that, you know, owners of construction equipment are typically able to make repairs to their equipment on their own or at least with few exceptions. So we should not assume that the fact that any commercial or industrial device breaks means that there's massive downtime and harm. I think it's more reasonable to assume that maintenance is available or because of the cost that owners make arrangements to put in place the arrangements necessary to avoid things, redundancy. So, you know, if your PLC fails, you replace the PLC.

But, in terms of alternatives, I think it's impossible to answer that on a general basis because

this proposed exemption covers everything under the sun, and different manufacturers are going to have different practices. But all the information I have, all my experience in representing clients in procuring technology suggests that there are maintenance options for a lot of products, and it may be that products reach the end of their life and sometimes need to be replaced, but that's kind of the ordinary cycle of commercial users' planning because they want to be able to run the next generation of software that will require the next generation of hardware. And so companies make budgets and have IT roadmaps that extend out years, and the reason IBM publishes the end-of-life date for a mainframe is so users can spend a couple of years planning for that event. And so I just don't see evidence in the record here that despite the costs of downtime, that there's really an inability for owners broadly across the full spectrum of this class to get timely maintenance and repair.

MR. GRAY: Thank you.

Does anyone want to respond on this?

MR. BLOUGH: I think my response there just to Steven's comment is that the harm is they don't need to buy a new one. The equipment that they have fits their bill, it does what they need it to do, and

they are being forced to spend millions of dollars that they should not have to spend because it is not repairable.

MR. GRAY: All right. Next, I'd like to turn it over to Luis.

MR. RAMOS: Yes, thanks, Mark. So I actually have an overarching question that I think goes to the three topics that we've discussed, and that's about the idea of commonalities and how we should think about commonalities. Proponents have, you know, stated that sort of their petition kind of falls within sort of the way that commonalities have been analyzed in previous rulemakings. But I'm curious from both sort of supporters and opponents, should that approach to commonalities, you know, remain the same as the 2021 rulemaking, or what is essential in order to have commonalities to form a class, or are there things that we should consider when evaluating commonalities in this process?

Meredith?

MS. ROSE: Sure. Sorry, I wasn't sure if I should just start or not. No, we think that the current approach actually is appropriate. Frankly, you know, if anything, I think it might be easier to have it restated as a single rule. We sort of

attempted to synthesize the position of the Copyright Office from a couple of different rulemakings, as well as the software-enabled devices report, in order to try to synthesize a standard in one place essentially.

You know, to the extent that, you know -- the way we ended up doing it essentially said that it's appropriate wherever the record establishes that users of such work are similarly affected by the prohibition on circumvention and the class is further narrowed by a reference to particular types of uses and commonalities among different device types. We think that's actually a pretty useful standard, frankly, you know, commonality of uses, commonality of users, and commonality among devices, and we found that to be particularly helpful.

MR. GRAY: Okay. Kyle, go ahead.

MR. WIENS: My other point on that would be we're talking about embedded software. The nature of the work here is the embedded software on these devices. We're here, we're 26 years into the DMCA, and we really haven't seen harms ever come from users modifying this embedded software. You're not seeing piracy of embedded software. The nature of the work is kind of irrelevant to the task that everyone wants performance. My broad argument would be this is about

all software running that's embedded in hardware.

MR. GRAY: Thank you, Kyle.

And, Steve, I see your hand raised. Go ahead.

MR. ENGLUND: Yeah. So it's right to focus on commonality because that has been a critical factor in the Office's discussion of proposals for an exemption like this the last couple times the Office has rejected them. And when I look at this class, it seemed like there are obvious differences between consumer goods and commercial and industrial in the sense that size and price point, the nature of consumer use implies a very limited set of products as compared to industrial equipment, where that could potentially be everything under the sun.

And as a result of that, the Office's decisions do not stand alone in distinguishing between consumer goods and commercial and industrial equipment. The Office's software-enabled devices study focused on consumer devices. That was the assignment received from Congress, but, nonetheless, that was the assignment received from Congress. The FTC, in the study I mentioned earlier, distinguished consumer goods from commercial and industrial and noted the complications and the lack of commonality

with commercial and industrial equipment and suggested that a one-size-fits-all approach wouldn't work.

And I'm under the impression -- I'm not an expert on the state right-to-repair laws -- that states have grappled with this distinction as well and sometimes excepted out commercial industrial equipment or categories of commercial industrial equipment, including that which provides critical infrastructure.

So there are obvious differences here and differences in the product design as well. And we talked earlier about cybersecurity and don't need to repeat all that discussion. But industrial equipment is designed to be secure in a way that consumer equipment very often is not, and that's certainly a key feature of the products and I think one that the Office should not ignore.

MR. BARTELT: Thank you, Steve, and thank you to all of the participants today. I think this was a really helpful discussion and helped us to get a lot more out of the written comments that we had already received to date. So, with that, I'd like to adjourn our hearings for today. And I think what we have scheduled is, for tomorrow, we're going to reconvene the hearings at 11:30 a.m. to discuss the proposed Class 3, which relates to text and data

mining for motion pictures and literary works. So, with that, again, I'd like to thank everyone for participating today, and we'll see those who are interested tomorrow.

(Whereupon, at 4:30 p.m., the hearing in the above-entitled matter was adjourned.)

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

REPORTER'S CERTIFICATE

CASE TITLE: Section 1201 Public Hearing: Proposed Class 5, Computer Programs - Repair

HEARING DATE: April 16, 2024

LOCATION: Washington, D.C.

I hereby certify that the proceedings and evidence are contained fully and accurately on the tapes and notes reported by me at the hearing in the above case before the United States Copyright Office.

Date: April 16, 2024

Alexis Robinson
Official Reporter
Heritage Reporting Corporation
Suite 206
1220 L Street, N.W.
Washington, D.C. 20005-4018