LIBRARY OF CONGRESS

IN THE MATTER OF:  

SECTION 1201  
RULEMAKING HEARING

Pages: 730 through 850  
Place: Washington, D.C.  
Date: April 20, 2021

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

IN THE MATTER OF: )
) SECTION 1201 )
RULEMAKING HEARING )

Remote Roundtable
Suite 206
Heritage Reporting Corporation
1220 L Street, N.W.
Washington, D.C.

Tuesday,
April 20, 2021

The parties met remotely, pursuant to notice, at
10:35 a.m.

PARTICIPANTS:

Government Representatives:

REGAN SMITH, General Counsel of the U.S. Copyright Office
KEVIN AMER, U.S. Copyright Office
NICHOLAS BARTELT, U.S. Copyright Office
STACEY CHENEY, National Telecommunications and Information Administration
BRAD GREENBERG, U.S. Copyright Office

Panelists:

MICHAEL AYERS, DVD CCA and ACS LA
KATHLEEN BURKE, Public Knowledge
CARA GAGLIANO, Electronic Frontier Foundation
STEVE INACKER, Transtate Equipment Company and Avante Health Solutions
ROBERT KERWIN, International Association of Medical Equipment Remarketers and Servicers
MARK McHARGUE, Nebraska Farm Bureau
MORGAN REED, ACT | The App Association
KEVIN M. ROSENBAUM, Auto Innovators
KERRY MAEVE SHEEHAN, iFixit
KYLE WIENS, Repair Association
J. MATTHEW WILLIAMS, Joint Creators and Copyright Owners
P R O C E E D I N G S

(10:35 a.m.)

MS. SMITH: I'm Reagan Smith, General Counsel of the Copyright Office, and this is our sixth day of hearings for our Section 1201 rulemaking. Today we are focused on Class 12, which concerns various adjustments or proposed expansions to exemptions for purposes of repair.

We're really excited that we have a big group today. Thank you for coming. We think we'll have a productive discussion.

So to go through logistics for those who might be new, my colleagues and I will moderate this session by posing specific questions. If you wish to respond, probably the easiest way is to use the Zoom "raise hand" button, and we'll try to get through to people in turn. If you're having issues -- some people have been having issues -- you can literally wave your hand or signal in the chat.

For anyone in the audience or a panelist who has an issue communicating in the chat or the Q&A, we'll alert someone at the Copyright Office to reach out to you to provide technical assistance.

For those who are listening or watching as an S-M-B, I guess this is the only session for today,
but there is also a link in the chat if you wish to sign up for audience participation for tomorrow. That is the time for those who maybe didn't sign up for a specific panel but wish to provide perhaps up to three minutes of their own views as to any of the proposed exemptions, and that will be concluding our hearings tomorrow.

And today's event is being recorded. The video will be posted to the Copyright Office website. I think it's also being livestreamed. We have a court reporter transcribing the proceedings, so please try to speak slowly and clearly. I know we're all experts in virtual communication, so mute yourself if you're not speaking.

And I think before we get started, I'd like to ask those from the Government to introduce themselves, so maybe Mr. Amer, Mr. Bartelt, and Mr. Greenberg from the Copyright Office.

MR. AMER: Good morning. Kevin Amer, Deputy General Counsel.

MR. BARTELT: Good morning. Nick Bartelt, Attorney-Advisor.

MR. GREENBERG: Good morning. Brad Greenberg, Assistant General Counsel.

MS. SMITH: And, Mr. Cheney, could you
please introduce yourself?

MR. CHENEY: Sure. Thank you and good morning. My name is Stacey Cheney. I'm a Senior Attorney Advisor in the Office of Chief Counsel at NTIA, Department of Commerce.

MS. SMITH: So next, we're just going to do short introductions of where you are and what organization you may be representing. So I'm going to try to go alphabetically, starting with those who are here in support of seeing expanded exemptions in some form or the other.

So, Ms. Burke?

MS. BURKE: I'm Kathleen Burke, and I'm representing Public Knowledge.

MS. SMITH: Thank you.

Ms. Gagliano?

MS. GAGLIANO: Cara Gagliano, and I'm representing the Electronic Frontier Foundation.

MS. SMITH: Mr. Inacker?

MR. INACKER: Steve Inacker, and I'm representing Transtate Equipment Company and Avante Health Solutions in the medical segment.

MS. SMITH: Mr. Kerwin?

MR. KERWIN: Robert Kerwin, General Counsel to IAMERS, the International Association of Medical
Equipment Remarketers and Servicers.

MS. SMITH: Mr. McHargue?

MR. McHARGUE: Good morning. Mark McHargue.

I'm a farmer in Central City, Nebraska representing American Farm Bureau.

MS. SMITH: Ms. Sheehan?

MS. SHEEHAN: Kerry Sheehan. I am the head of U.S. policy at iFixit.

MS. SMITH: Mr. Wiens?

MR. WIENS: Kyle Wiens, and I am speaking on behalf of The Repair Association.

MS. SMITH: And now we'll have those who have filed in opposition to some or all of the proposed adjustments to the exemptions.

So, Mr. Ayers?

MR. AYERS: Thank you. Good morning. My name is Michael Ayers, and I'm representing the Advanced Access Content System Licensing Administrator LLC, usually referred to as AACS LA, and DVD CCA -- DVD Copy Control Association, usually referred to as DVD CCA.

MS. SMITH: Thank you.

Mr. Reed?

MR. REED: Hi. My name is Morgan Reed. I'm the President of The App Association, and the
Executive Director of The Connected Health Initiative.

MS. SMITH: Mr. Rosenbaum?

MR. ROSENBAUM: Hi. I'm Kevin Rosenbaum, and I'm here today representing The Alliance for Automotive Innovation, Auto Innovators.

MS. SMITH: Thank you.

And, Mr. Williams?

MR. WILLIAMS: Good morning. Matthew Williams, Mitchell, Silberberg & Knupp, representing the Joint Creators and Copyright Owners.

MS. SMITH: Thank you.

So we have a lot of people here on kind of a bigger record for this proposed class, so I want to give a short road map of some of the issues, the order in which we are hoping to get through some of the issues, to make sure we have time to get to it all.

So first, we are going to address questions of the proposed scope of the class, whether it should be one exemption or multiple exemptions, which it currently is.

Secondly, some of the proposals to make it device-agnostic as well as permit modification of devices.

Next, issues specific to DVD or Blu-Ray players, as well as video game consoles.
We have a couple of questions specific to causation; then turning to medical devices; and then, finally, issues related to vehicles.

So we'll try to get to everything, and certainly some issues are going to be cross-cutting, but I thought that might be helpful.

So I guess to begin, it would be helpful to hear either from proponents or opponents with respect to some of the proposals by EFF, or iFixit, or The Repair Association to sort of broaden and condense the two existing regulatory exemptions into a single one that is agnostic as to device.

So we have some precedent for this in an exemption for security research, where the Office concluded that computer programs can constitute a proper class because the use was so tailored.

Is that helpful for us to look at that in connection with repair, or are there different issues going on that we should be cognizant of with respect to the areas at issue in this exemption? So I saw Ms. Sheehan first.

Please go ahead.

MS. SHEEHAN: So I think that's a great analogy. I think similar to how we think about security research, where we're talking about repair,
the purpose of the use is consistently non-infringing,
and the use of the software is virtually identical.
If the purpose of repair is to restore the device to
functionality and all of that, that's a fair use, and
it's non-infringing also under 117.

Continuing with the Office's path of limited
exemption categories that are kind of device
restricted or limited to certain narrow categories of
devices really makes it difficult for these exemptions
to keep up with the increasing number of software-
enabled devices with technological protection
measures.

So from a purely practical level, if we
continue on this route, we're going to be -- us,
iFixit, The Repair Association, EFF, and other
individual users and organizations and advocates are
going to be coming back every three years with a new
roster of devices as the world of software-enabled
devices continues to explode.

And part of the problem that we see with
some of these narrow categories is that sometimes it's
unclear whether a device sits in one category or
another. Is a headphone a wearable? Is it something
else? What about a smart watch?

So the categories don't kind of keep up with
market realities, or how products are marketed, or how many functions they have, and we just have a proliferation of these devices. So three years ago, we weren't really looking at a bunch of smart light bulbs, but now we are, and that's just going to increase going forward.

And I'll say that similarly to the exemption for encryption research and security research, when we're talking about looking at this broad category of devices, for each of these devices, the purpose is still non-infringing, and the copyright analysis is the same. The purpose is repair. Repair is non-infringing. And that doesn't differ between whether it's a phone, or a tractor, or a light bulb, or a smart litter box.

MS. SMITH: Thank you.

So I'll call on you next, Ms. Gagliano, but one thing to pick out -- I thought Ms. Sheehan is stressing the purpose being shared, but I wonder if you could also address whether there is a similar causation effect. So do the TPMs work in the same way?

And another element, of course, for considering is the effect on the market for copyrighted works and whether or not there's
sufficient commonalities to assume they're all going
to have a similar effect.

    MS. GAGLIANO: Yeah. Thank you. So I agree
with everything that Ms. Sheehan just said, and to
some of your points would add that, yes, I think that
the causation issues are very much the same, and the
effect on the market, and part of that is because like
security research and that exemption, we're already
limited to a subcategory of literary works and have
this specific purpose.

    But not only that, we're limited further.
It's not all computer programs. It's just firmware,
embedded software that's controlling the operation of
physical devices.

And that unifying feature is what really
unites the entire class in terms of common issues with
all of the statutory factors, including market
effects, because the thing about firmware that's
unique relative to a lot of other kinds of computer
programs is that there really isn't a separate market
for firmware outside of the physical devices it's
attached to. That is just inherent to the nature of
firmware. It's what makes it firmware, it is attached
to, sold with, a specific device.

    And any kind of modified firmware, repaired
firmware, that's being produced through this exemption isn't something that is going to act as a market substitute for firmware, because you would still have to buy the physical device or otherwise acquire the physical device in the first place with that original firmware already on it.

So the copyright owner has already been compensated. They aren't selling any fewer copies of the firmware, because the number of firmware copies is inherently tied to the number of devices sold, and modified firmware is useless without that.

MS. SMITH: Let me ask you one question, and then I think I'll move on to make sure everyone has an opportunity to wave in. You're using this word "firmware," and the two exemptions now discuss computer programs that are contained in and control the functioning of a lawfully acquired "blah" -- with "blah" being what's in dispute.

Do you think that "contained in" and "control the functioning" is synonymous with firmware? Or are you sort of narrowing the description a bit more?

MS. GAGLIANO: I think it is essentially synonymous. You know, to the extent that the definition you mentioned, "contained in" and "controlling the operation of" could be understood to
be broader. You know, that's really not what we mean. We're not talking about like apps. Even if you could think in some sense, "Well, an app in some way controls the operation of the product," but that's not what we're talking about. We're talking about what is the industry term of firmware or embedded software.

MS. SMITH: Okay. So it sounds like you might not object to an effort to sort of clarify that to the extent that might put Mr. Reed, for example, at The App Association -- give him a little bit more comfort. Is that right?

MS. GAGLIANO: Sure.

MS. SMITH: Okay.

So I think to keep going in order, we'll go to Mr. Wiens and Mr. Williams. But, Mr. Wiens, I want to press and give you the same question I asked Ms. Gagliano, because I still think one area -- to take the analogy to other exemptions, is we similarly concluded in the unlocking process there just weren't other examples of devices that needed to be unlocked. There were not TPMs effectively controlling access.

And so that is a question we have here, whether there is the same showing of causation or
adverse effects across these categories, because if
there's not TPMs, it doesn't make sense to have a
regulatory proceeding and sort of make it seem like an
exemption is needed if one is not, for example.

And we also want to see whether there are
other alternatives, even where there may be TPMs. So
can you provide a little bit more color about the
other types of devices you think are not being able to
be accessed, notwithstanding the current exemptions?

MR. WIENS: Absolutely. Great question.
What I think is interesting about this is we're
talking about all of these devices, all kinds of
different devices. What's sort of amusing to me
technically about this is that the software, the work
that we're talking about, is substantially precisely
the same in all of these cases, even though they're
different devices. It's Linux.

Linux is the work that is being protected in
almost all of these cases, whether it is a nanny cam,
or a smart coaster, or a industrial SCADA system.
They are running on Linux. And I like to call the
internet of things "the internet of outdated Linux
distributions."

And what's happening is you hear about all
of the kind of security problems that we have with the

Heritage Reporting Corporation
(202) 628-4888
internet of things. It's because these devices are outdated and not patched. And in response to all of the security vulnerabilities that have been found, manufacturers are locking these devices down.

It's interesting that like traditionally, the Copyright Office is focused on TPMs, where you have a DVD. You have copy protection put on the DVD. The copy protection is there to protect the work from being copied. In this case, it's generally there to prevent malware.

And so are there TPMs on all of these devices? There should be. If a manufacturer is doing their job, if it's a nanny cam, you don't want that stream ending up on the public internet. You want it locked down. If it's a building automation system, you don't want anyone on the internet to be able to log in and unlock the doors. You need to lock it.

So I would say the default case is, yeah, there are locks. The locks are not intended to prevent owners from accessing and modifying and unlocking a door in a building automation system. The locks are there to prevent unauthorized third parties.

So if you look at the world of internet-connected devices going forward, if I was designing them all, if I had sort of my druthers, I would put...
locks on all of them. And I think that you will see,
sort of the security best practices, that there should
and will continue to be locks on these devices.

MS. SMITH: Is there an issue, for example,
with the SCADA systems of not being able to repair
them or even lawfully modify them because there's an
inability to get permission?

I mean, we had a specific record on that,
for example, with the security research classes, that
there was a need to have good-faith security
researchers on those types of systems, and I don't
know if we have a similar record in this class of the
effect of 1201 on non-infringing uses for some of
these types of devices.

MR. WIENS: Yeah, we -- so one story that we
mentioned on the record was a school. This was, I
think, an elementary school. And the facility's
maintenance person passed away, and he had the
password to the whole system. And it turned out that
this particular system, there was no way to reset that
password.

What you had to do was wipe out the
programming for the entire system and reprogram it,
which if -- so I've configured some of these building
systems, and like for our office, it took like a month
of programming to set it up. It controls the lawn
sprinklers. It controls timing on the doors, who can
go in and out. There's different timing settings. If
someone unlocks the door at 3:00 a.m., different
security settings go off, and otherwise. It controls
the air conditioning. In a larger -- like in a
school, it might control a water treatment system.

So it is a huge amount of work, so in that
case, where you need to be able to basically break
into your own system to change the password, if they
couldn't do that, you're talking about like probably
not the kind of repair that could happen in a weekend.
It might take a professional or someone really good at
this a week to go in and reprogram everything. So the
ability to circumvent that would be very important.

Another example that's personal to me, we
have a building automation system that only supports
99 key cards, and we have more than 99 people. We
need to change it.

MS. SMITH: Do you know why it only supports
99 key cards? Is that part of a license?

MR. WIENS: No, there's no way to pay more.
The company just doesn't support it. I think it was
an artificial limit put in by some software engineer.
I want to find that person and smack them upside the
head, because it's very frustrating. But it's a limit, and I've asked. There's no amount of money that we can pay to change it.

And another thing that I would mention, because we're talking about sort of third parties you sort of have the branded folks, the folks who maybe have been trained by manufacturers to come in and do some of this work. We've had extensive experience with a lot of these folks and have had repair problems with our building automation system that the trained service technician from the factory can't figure out. They've been out a dozen times and can't figure out problems.

MS. SMITH: And just to make sure I run down your example that you provided of the school, you can't call someone and say, "You know, the guy who had the password has left, can you reset it?" Because I think that's something we find ourselves having to do with a variety of technology now.

MR. WIENS: Right. In this case, the system just wasn't designed that way. And I think that you will find that is fairly common. A lot of these -- I mean, particularly -- we're kind of in the early days of all of these technologies. A lot of them are relatively primitive. And so in this case, the
software just didn't have that feature. And so the factory technician is going to come out and say, "Your option is to wipe all the settings or cough up the password."

MS. SMITH: Okay, thank you. So I know you talked for a little bit.

Mr. Williams, you've had your hand up for a while. So please feel free to comment on the past speakers or any of the issues I've posed.

MR. WILLIAMS: Yeah, thank you. I mean, I'm glad to hear Mr. Wiens acknowledge that the use of locks is a best practice, really, with devices across industries and is not something to be critical of in the abstract.

And I think your question goes to whether all devices are the same or there are distinctions, and I think the records over the past few cycles have demonstrated that there are distinctions, and you put your finger on a few of them with your questioning.

For video game consoles, for example, there's an established consistent record that those TPMs are in place to protect security of the devices, privacy of users, prevent cheating, but also primarily, and importantly, to prevent infringement, and that the value of the device firmware is decreased.
by circumvention of these access controls, which
impacts the fair use analysis and also the 1201
factors analysis.

In addition, you've determined there are
alternatives to circumvention in certain respects with
respect to repairing video game consoles, and that's
not consistent across all of the devices that you've
looked at here. And I think Mr. Wiens's examples just
show you the wide variety of questions that can come
up when you go from one device to the other device, or
to a system.

Your question was quite good about, "Is that
a license? Could you pay more for 200 users instead
of 99 users?" The answer may be very different for
different situations. And so just focusing on the
video game console space, I don't think there's
anything in the record to deviate from prior
decisions, and I think you've been wise to go at least
device by device in terms of categories.

I mean, you haven't been myopically focused
on individual devices. You have acknowledged that
there are distinctions between categories of devices,
and those distinctions can have a lot of import,
whether it's under 117, or 107, or alternatives to
circumvention, and so I think that's been the right
approach.

And I don't see it as analogous to security research. In part, I feel the security research exemption has been granted because there's a statutory provision that you were building off of, and you felt that over time that provision was no longer doing its job. You know, whether I agree with that or not, I think that's how that progressed in the way it did. And I think this is a distinct situation.

MS. SMITH: Okay. Can I stand you with two follow-up questions that are rather pointed and then get to everyone?

So why or why not was it helpful to hear suggestions that the proposed exemption is limited to so-called firmware or something, Linux specifically? Does that help address your concerns at all, or not? And if not, why?

MR. WILLIAMS: No, I don't think limiting it to circumventing access controls on firmware would fix our concerns, especially in the video game console space. When you circumvent those access controls, you undermine the security scheme that's in place to do a lot of different jobs but, importantly, protect the copyright integrity of the system, and so that would not fix our concern there.
Perhaps if you're in another space --
printers or litter boxes -- maybe the firmware doesn't
have any other copyright purpose, but I think you've
been right to acknowledge in the past that in the
video game consoles it does.

MS. SMITH: Okay, thank you.

Mr. Rosenbaum?

MR. ROSENBAUM: Thank you very much. I know
we're going to get to vehicles in a different segment,
but I just wanted to make the point, sort of following
on Matt's point, that there are distinctions,
particularly with the automobile industry. My
comments address only that industry. We don't have
any position on any other devices here.

But just, for example, there's no evidence
that users of automobiles are having any difficulty
getting their automobiles repaired. There's a
thriving aftermarket going on. Seventy percent of
post-warranty repair work is done by independent
repair shops.

There's, of course, the MOU under which auto
manufacturers are required to provide automobile
owners and independent repair shops with the same
repair and diagnostic information and tools that are
provided to franchise dealers.
And then, of course, the other distinction is the auto industry is very highly regulated, and the access controls also protect software that relates to safety and environmental regulations, and those are critical, which the Office recognized in its promulgation of the existing exemption.

And so what's at issue here is relaxing some of these important restrictions on the existing exemptions, so I just wanted to point out that there are some real distinctions here with the auto industry.

MS. SMITH: Thank you.

And I see we have a lot of hands raised. I'm going to keep moving on.

So I think, Mr. Ayers, I will go to you next. The one question I'm wondering, and it's maybe part of what you're already prepared to comment upon, is piggybacking off Mr. Rosenbaum bringing vehicles into this, the current exemption for vehicle repair, accepts TPMs protecting works that are accessed on a subscription service such as radio, sort of expressible content, and that's an approach the Office has taken to some exemptions, including also saying that circumvention -- for example, in the jail-breaking context of audio speakers -- cannot be
accomplished for the purpose of gaining access to other copyrighted works.

And so I think sort of anticipating what you might be saying, and also listening to what Mr. Williams said, is that an approach that is useful for the Office to consider, to sort of carve out the video game consoles or DVD or Blu-Ray players, or things where the TPM circumvention -- if the record shows it will be more likely to have an adverse effect on the unlawful distribution of copyrighted works and, perhaps the nanny cam?

MR. AYERS: Thank you. Well, certainly, to the extent there's an inclination to grant the requested expansions to the exception or to the exemption, it's better to have limits than no limits, and the concern of my clients is geared towards those devices with optical disk drives that play back expressive content like DVDs and Blu-Rays, so including game consoles.

So certainly, we still continue to maintain our position, but to the extent that there's an inclination to go that way, carving out those devices certainly relieves the pressure, to a certain extent, on my clients.

And I would just note that a couple of other
issues that have come up in the comments we've talked about that we've had today -- one is what we keep calling as a repair exemption. A number of the examples in the conversation today and in the comments received so far have actually gone well beyond repair and have included modification of devices beyond their original functionality.

And one of the concerns that we would have would be the extent to which a repair is then geared towards changing the functionality of a device, which uses AACS or CSS to circumvent those technologies and present pirated content in a manner in which it's not authorized.

I would also note that there was also the comment that I thought was a very salient one, that locks are not always bad, as has already been said, and that, certainly, to a large extent, the protections on firmware and devices are often to protect the users of those devices against intrusions by malicious third parties, and that's certainly a good thing.

But also, to piggyback a little bit on other comments that have been made, there are other purposes for the firmware, and so for instance, in the context of DVD and Blu-Ray, the firmware is used to protect
the decryption -- cryptographic values, and device
dkeys, and certificates that are used to render the
device a good citizen in the entertainment content
world, making sure that it's a secure platform that's
available for a content owner to release high-value
content in that format.

And to the extent that the ability of the
device to protect those cryptographic values is
rendered less, is rendered less effective, it reduces
the attractiveness of the formats to content owners.

MS. SMITH: Okay, thank you, Mr. Ayers.

So I'm going to try to get to everyone who
hasn't spoken yet, but then go back to you Ms.
Sheehan, Ms. Gagliano, I understand this is something
that you wish to respond to.

So, Ms. Burke, can we piggyback on what Mr.
Ayers brought up, which is modification? And what are
your thoughts? You can comment on what some of the
prior commenters have said, but with respect to video
game consoles in particular, do you see a need for
modifications? I'm not sure that's part of what
Public Knowledge is supporting with respect to video
game consoles for this exemption.

MS. BURKE: Yeah. So with respect to
modification, to the extent that you might need to
modify the software in order to like repair or relock
the optical drive once you change it out, I think that
modification would be potentially necessary, depending
on what the anti-circumvention technology ends up
doing.

I know as an analogy, there are some times
when you might need to reprogram like in the software,
like how -- what the function of a button is, and so
that might require modification. But in terms of
modification for a functional purpose, not
modification to allow you to play pirated DVDs.

And I just want to address that concern
there, that somehow allowing these -- changing out the
optical drive and being able to repair that optical
drive is going to jeopardize the security of the whole
system: the lock that pairs an optical drive to the
motherboard exists on the daughterboard connection
between the two devices. And it's my understanding
that unlocking that so that you can pair a new optical
drive is not going to then jeopardize the whole
ecosystem of a video game console and its security
protocols.

So I think that that's something that's
particularly relevant here, since this idea that all
of a sudden changing out an optical drive is going to
make it easier to pirate content. It just doesn't seem like that works within the realities of how these systems are constructed.

MS. SMITH: Thank you.

Mr. Reed?

MR. REED: Hi, hopefully your cat is getting out of the way.

I think there are a couple things. I want to actually note, I agree with Kyle Wiens. I thought his use of the concept of unpatched Linux is great, and I just think about the GRUB bootloader and the problems we've had there.

But it actually points to the problem, Regan, that you hit on exactly, which is any tools that you build to go against the TPMs open up a case for infringement that's pretty significant.

You asked a great question, which is if that house software or that building software uses as part of its marketing "pay this much for 99 users, pay this much for 200," in Mr. Wiens's example, there wasn't that option. But the tools have to be created in a way that would make access to it.

All of the software that my members are making now, we're doing a lot of products that are essentially by the sip, right? You right-size your
product. You right-size the price of your product. If the TPMs can be violated, and tools are widely available that allow that to be broken through, then of course the other modifications that can be made are, "Well, I don't want to pay for 200 licenses. I'll buy one for one license and I'll use TPM-breaking tools to increase that number to 99."

Our entire app ecosystem business model essentially exists on these concepts of right-sizing an in-app purchase, a purchase that you make to get exactly what you want and not pay more for it. The TPMs that are in place, as he noted, for safety and security also secure the framework that allow for the appropriate licensing and right-sizing of the products.

I think the one other comment that goes along with it, though, on the comment we just heard about the daughterboard and where the technology exists, is valid, but at its core, she's essentially saying, "Hey, guys, you need to rewrite your software. If you're not doing it this way, then you as an industry need to change the way you behave."

And I don't think that meets the test that the Copyright Office is setting. Those of us who are writing the products should not be forced to modify
our software to meet this change that they want. So
the fact that in some cases the connection is on the
daughterboard or on the physical device may be
something that software refers to when checking other
things.

So the request here is not just, "We'd like
to hack it ourselves." Her point was, "Well, you can
make this real easy change to your software, and if
you do that, then there won't be a problem." That's a
bar that the Copyright Office shouldn't be making,
shouldn't be telling us to change our software in
order to accommodate someone else's ability to break
into it.

MS. SMITH: Can I ask you, while I have you,
so the way we've structured the current vehicle
exemption does not extend to TPMs protecting
subscription services, and you could see sort of a
similar description of --

MR. REED: Yep.

MS. SMITH: -- you know, exceeding terms of
use, and some of the issues you're talking to. Is
that a helpful way we can think about these internet
of things software-embedded devices? Or is there a
technological reason to suspect that enabling repair
to the --
MR. REED: Right.

MS. SMITH: -- original state is --

MR. REED: It's a great question.

MS. SMITH: -- going to somehow -- yeah, go ahead.

MR. REED: Yeah, so I'll give an example.

One of the problems that we're running into right now is -- and this gets into TPMs -- is we can't actually avoid piracy by giving our products away for free.

So to your question about can you isolate it into these camps because, well, a TPM that's strictly for this use is bad, we're actually seeing a situation right now where software is developed and distributed for free, ad-supported, where the TPMs are being broken, and then that software is being hijacked and an additional ad network is placed underneath it.

So literally, I give my software away for free, and it is being pirated and an additional ad network is being installed underneath it. So your point about well, can we isolate it into a copyright infringing use, that's an example that violates my copyright, but it's not one that has to do with how much I'm charging or where I'm doing it.

I'm literally giving my software away for free, and people are still going to break it and use

Heritage Reporting Corporation
(202) 628-4888
it in a way that disadvantages me. So I think to your
point, I think that obviously what you've done so far
has worked, but I would be very concerned about any
expansion of that across multiple sectors, because I
think it's hard to keep that from breaking into
harmful uses.

MS. SMITH: Okay. Thank you, Mr. Reed.

So, Ms. Gagliano, I think you've had your
hand up for a while, so whatever -- okay, thank you.
If you would like to comment on what you had your hand
raised for as well as particular -- how the Office can
think about modification as a lawful use across these
devices, and maybe address some of the comments raised
about distinguishing between lawful modification on
the one hand, and the derivative right on the other.

MS. GAGLIANO: Yeah. So I think in
particular, responding to what we've been hearing a
lot of from opponents about how "look, if you let
people get past these TPMs, they're going to
infringe," infringement is going to happen, even if
that means having to bypass another TPM, which the
exemption would not permit, even if that means having
to go another step and do the exemption for purposes
that the TPM does not permit. I don't think it is
appropriate for the Office to consider in deciding is
this an appropriate exemption to consider whether people will then break the law and actually go beyond the scope of that exemption.

I mean, you could have said the exact same thing about the security research exemption, and I think many opponents did. The security research exemption applies even to video game consoles, to DVD and Blu-Ray players. We haven't heard anything from opponents about increased infringement since 2018 attributable to granting that exemption.

So when people are using these exemptions, it is to do the -- make the non-infringing uses that were being adversely affected. And the fact that someone might go further and try to say, "Well, this exemption protected part of what I did" isn't really relevant. It's still assuming that someone is going to violate 1201 either way.

And in terms of the concern that someone would -- that a possible modification of the firmware would be to make the device changed in a way that would enable piracy, one simple tweak to our language that would get maybe more at what we actually had in mind is saying, for -- it would be circumvention not only for purpose of non-infringing modification, in which case we mean the actual creation of the
modification would be non-infringing, but it could
also be for a non-infringing purpose.

So the exemption doesn't have to cover
modifications that would be for the purpose of
enabling piracy, getting access to other copyrighted
works. But either way, the exemption is not giving
anyone permission to circumvent TPMs on any work other
than software. It's not giving permission to
circumvent TPMs for the purpose of infringement.

And we have heard the same argument in every
rulemaking cycle against many of the exemptions that
have already been granted, like all the jail-breaking
exemptions, the past exemptions for vehicles. Last
year, it was the exemption for repair of certain
consumer devices and home appliances. Every time,
opponents say, "This is going to make everyone
infringe." There's still absolutely no evidence of
that, and I think the absence of that evidence --

MS. SMITH: Okay.

MS. GAGLIANO: -- is a form of evidence
itself.

MS. SMITH: Thank you.

I'm going to try to just keep our comments a
little bit shorter if we can going forward, to make
sure we have time to get through everything.
Ms. Sheehan, did you want to speak to the question of lawful modification? I know the Office has had some hesitancy in the past to conclude that that's the right defining phrase for that, with level of specificity. We would welcome your thoughts.

MS. SHEEHAN: Absolutely. Do you mind if I also address a couple of your earlier questions? So I'll start with your first question about the causation issue, your question about whether there are TPMs in every software-enabled device, and to the extent that those obstruct repair.

And I would say that if there's not a TPM in a device, it's not part of this conversation about the exemption. So the scope of the exemption is only for circumvention of TPMs that exist in a software-enabled device and that obstruct repair. Right? So the fact that some devices might not have TPMs, the fact that those devices exist, doesn't obviate the need for circumvention where TPMs do obstruct repair. So, first question.

Second, I'd like to address what some of the other panelists have talked about in terms of devices that play back A/V or expressive content, and I'll say that as Ms. Gagliano very correctly identified, that the subject of this exemption is the software. It's
the embedded software in the device. It is the firmware. It is not the copy controls on the content, and it is not the TPMs that protect that content from infringement.

Furthermore, repair of devices that play lawfully acquired copies of expressive content increases the accessibility to both the functionality of the software and the lawful performance of those lawfully acquired works. And the only purpose for the circumvention that is acknowledged and permitted within the exemption is for repair.

So an exemption like this, as Ms. Burke, as Ms. Gagliano said, would not authorize circumvention for the purposes of piracy, so on and so forth. And I think the Office itself has acknowledged that in the 2018 Recommendation when it addressed expressive content on vehicle infotainment and telematics systems.

And so the concerns about piracy in those contexts related primarily to abuses of circumvention that are outside the scope of the proposed exemption, and I'd say that's true here as well.

In terms of alternatives, Mr. Williams raised the specter of alternatives to circumvention, and I'll say that the existence of alternatives to
circumvention is not fatal to prior exemptions and shouldn't be fatal here. The Office granted the motorized land vehicle exemption despite the existence of other alternatives, and we know that those alternatives often prove inadequate. That's fully documented in our record.

But I'll also state that in Chamberlain, the Federal Circuit decided that section 1201 did not grant copyright holders another exclusive right. It only protected the exclusive rights that they already had under 106. And so section 1201 does not give copyright holders the right to control the market for repair services, and the right to require that you use their own branded repair services.

To deny an exemption on the basis of the existence of those manufacturer-branded alternatives would be to grant a new right, would be a grant of new right to exercise anti-competitive practices and control an entire market.

Moving on to the question of --

MS. SMITH: Can I ask you, just on that one --

MS. SKEEHAN: Yeah.

MS. SMITH: Just on that one point before we get to modification, do you think it's relevant
whether there's an additional charge or terms or
something connected to repair, or whether it's sort of
open in terms of the purchase for the initial license?

MS. SHEEHAN: I don't understand your
question. Do you mind rephrasing?

MS. SMITH: Well, I guess you've expressed
care about a branded repair market, and I guess
we're looking at this through the 1201 lens and
whether there's an adverse effect created by TPMs. Did
you think it's relevant whether there's conditions
imposed upon the manufacturer-provided repair, or --

MS. SHEEHAN: Absolutely.

MS. SMITH: -- or it doesn't matter?

MS. SHEEHAN: No, absolutely. And I think
that goes to the kind of tangible, practical adverse
impact on users of software-enabled devices. You
know, in our experience, we talk to repair shops,
we're kind of deep into the repair industry over at
iFixit and the Repair Association.

And our experience with manufacturer-branded
repair is that the types of repairs that they can
carry out are limited, meaning if I take a tractor to
the John Deere dealership, they can only do certain
repairs. If I take my iPhone to an Apple-authorized
repair provider or an Apple IRP provider, they can
only do simple, basic repairs before they either encourage me to buy a new device or have to send it back to Apple.

Some manufacturer-branded services may be extremely costly, more expensive than an independent, and in the medical device sector, it was found that manufacturer-branded medical device repair could cost 30 to 50 percent more than an independent service organization's repair. It can also involve long delays if you have to schedule or ship a product back to a manufacturer, and in some circumstances, you might not be able to get a repair at all.

So Kyle mentioned earlier our kind of industrial premises control systems. We are completely outside of a service network for our manufacturer on some of those systems, and so if we were to depend on manufacturer-branded repair services, we would be completely out of luck.

MS. SMITH: Okay, thank you.

MS. SHEEHAN: Is it okay if I address modification?

MS. SMITH: And modification.

MS. SHEEHAN: Ok yeah. So I just wanted to say briefly, I think Ms. Gagliano addressed that pretty well, extremely well, and I would just say that
in *Sega v. Accolade*, the Court found that modification of a software-enabled device is not infringing, especially when it is a reasonable step to a transformative use such as repair.

So when a modification is carried out for the purposes of repair or for other non-infringing uses, then it should also be understood as non-infringing.

Can I say one --

MS. SMITH: Okay.

MS. SHEEHAN: -- more thing? Just one more quick -- I'll be quick, I promise.

MS. SMITH: Extremely limited, because I do see a lot of hands raised and we've got to move on.

MS. SHEEHAN: Okay.

MS. SMITH: Extremely quickly.

MS. SHEEHAN: I just wanted to respond really briefly to both Mr. Williams's and Mr. Reed's comments about the necessity of TPMs to prevent cheating, to protect privacy, or to protect safety and emissions, and I would say that absolutely none of those things are part of the Copyright Office's very copyright-based inquiry on whether a 1201 exemption should be granted.

And I'd actually be interested to know
whether the clients that Mr. Williams and Mr. Reed represent are actually using 1201 to go after people for cheating, or violating emissions controls, or violating a user's privacy, because I'm unaware of any cases like that.

MS. SMITH: Okay, thank you.

Mr. McHargue?

MR. McHARGUE: Well, thank you. I just want to remind people that I am a farmer. I'm not an attorney. So this is a very interesting conversation to me. You know, on our farm, one of the things that we're really concerned about -- someone mentioned the use of tools.

And as our ag equipment gets more complicated -- every day, it seems like -- there's an increasing need to have users, or I'd say third-party experts, develop a tool that can work on my tractor. I know there's difficulties, in our area anyway, that the dealerships or the authorized dealerships say they will provide tools, but they're really not the tools to the extent that we can come in and actually fix our equipment back to actually operating state. And so I just wanted to say that that was one of the things that we're concerned about in the ag sector.

The other thing is there was a conversation
about modification that may not quite fit into this
category, but we're clear at American Farm Bureau that
if there's modification that involves environmental or
safety issues, I think we have to be very careful when
we start going down that route. If we're talking
about things that we can improve potentially -- but we
have to be very careful when it gets into
environmental and safety issues.

MS. SMITH: Thank you. I appreciate your
thoughts.

So I think the next person who had their
hand raised is Mr. Ayers, but given our time, I'm also
going to shift some of the questioning to my
colleague, Mr. Amer, so that we can wrap up
modification discussion but segue into some of the
device-specific categories of the media players or the
video game consoles.

So, I don't know, Mr. Amer, if you wanted to
pose any additional questions, but I do think it is
Mr. Ayers's turn to respond.

MR. AMER: Yes. Well, actually, my first
question was going to be about DVD players anyway.

So maybe, Mr. Ayers, you could speak to
this. So I wanted to sort of make sure I understand
what seems to be kind of a factual dispute,
potentially, about what the TPMs protecting firmware in DVD players controls access to.

So I know that the proponents have said that their proposed exemption would apply only to software that controls the operation of the device and would not permit circumvention of separate TPMs that protect access to the DRM-protected media.

Now, today, earlier on, you talked about, I think, the cryptographic values that exist in DVD players, and I think you said something about if those are altered, that makes the device sort of a less attractive platform for manufacturers. Could you sort of elaborate and explain a little more, explain sort of what these cryptographic values protect and what they don't protect?

MR. AYERS: Sure. Thank you. So the concept with content protection technology in consumer electronics devices in the entertainment content space is that the content owner and the device manufacturer are both engaged in an ecosystem where the content owner is sufficiently trustful, finds the target device sufficiently trustworthy, that the content owner will release its high-value content in the format played by that device.

In the context of movies on optical disk,
that includes authoring and manufacturing the movie
and the disk with certain cryptographic values that
are used to encrypt the movie. Corresponding
cryptographic values such as device keys are embedded
in the device by the manufacturer during the
manufacturing process that are then used to decrypt
the content on those disks.

So you put the disk in the machine. The
machine has decryption keys that allow it to decrypt
the content on the disk that has been encrypted with
the encryption keys. So this provides a benefit for
consumers, as has been mentioned in other hearings.
DVD was one of the most successful consumer
electronics products in history, in the history of
consumer products, and it certainly laid the
groundwork for commercial success for multiple
industries since then.

But to the extent that those devices become
compromised and are no longer able to be trusted, it
presents a problem for the content owners in investing
a ton of money in very high-value content such that
it's no longer as good an investment, because the
content is less secure.

And certainly folks might look at, "Well,
they're movie studios. They have a lot of money
anyway." And I think the idea here is look, these are investments of significant resources both on the device side and on the content side to make sure that this all works together, so that the end result is an extremely attractive proposition for the consumer. And so to the extent that this compromises it, we have less of an attractive setting.

And just a quick follow up on an earlier comment.

MR. AMER: Well could I just follow up on that --

MR. AYERS: Sure.

MR. AMER: -- first, though? So are you saying that if someone were to circumvent TPMs protecting the firmware on a DVD player, that would necessarily expose these cryptographic keys you're talking about, and it would therefore allow people to play unauthorized DVDs?

MR. AYERS: That's essentially the concern. I mean, the exact way that each device manufacturer implements the storage of the applicable cryptographic values is somewhat flexible to allow for the realities of device manufacturing in different contexts, but that's the essential concern.

And in that case, what you've done is when
the key is exposed, you're no longer looking at onesie-twosie situation where you may be compromising a movie at a time, which is itself not desirable at all, but because it's a decryption key that could decrypt any DVD or any Blu-Ray disk, it potentially endangers the entire ecosystem, because now you've enabled a circumvention tool for the high-value entertainment content.

MR. AMER: Okay.

Ms. Burke, could you respond to that?

MS. BURKE: Yes. It's our understanding that the limited request that we've asked for, which is the exemption to unlock an optical drive, replace it, and then relock that pairing, would not cause that kind of decryption of what protects the Blu-rays and the DVDs at question here.

Rather, I think it's important to note that this TPM that locks and pairs an optical drive to the rest of the video game console is unique to these optical-drive-driven video game consoles. Other devices that have optical drives don't necessarily have these same locks. So if you wanted to replace your optical drive in your computer, you could go get a new optical drive, put it in your computer, and plug it in, and change it out pretty simply, without having
to circumvent this kind of TPM.

So these optical drives, being able to change them out doesn't really implicate the same concerns when it comes to that type of a situation, with being able to change out your optical drive. So what makes a video game console so unique? It's our understanding that these TPMs that are protecting the optical drive don't actually protect the content that could be played on an optical drive. Rather, it just protects this particular pairing.

And so the TPMs that need to be circumvented here they're really just protecting or preventing people from being able to repair an optical drive, which is a harm to consumers, because optical drives are the most frequent thing to fail in a video game console. Replacing one is fairly cheap, as opposed to having to purchase a whole new device.

And so it's our understanding that these TPMs really aren't protecting content so much as they are preventing these types of repairs which consumers have a right to do. When you own a device, you should be able to repair it, and copyright should not be a tool that prevents you from being able to do that. It's not intuitive, and it doesn't make sense with regard to what copyright is intended to protect.
MR. AMER: Okay, thank you.
I think, Mr. Cheney, do you have a question?

MR. CHENEY: Thank you. I think this has been a helpful discussion, and I think it's been helpful for me to hear this a little bit on these game systems and DVD players.

For example, one of the questions I had with these cryptographic values that potentially are exposed or may be misused, can you describe what that might be like in the sort of repair that has just been described?

I think, Mr. Ayers, you may have the best answer here. Are they allowed to be copied and reproduced? I mean, what is the possible path to piracy here if they are, indeed, exposed in this repair? Is it on the device itself, or is it something that would be a broader piracy possibility?

Can you describe that a little bit more? Because I'm not sure I'm getting where that value gets exposed here. Can you help me out here? Thanks.

MR. AYERS: Yes, thank you. So it is in the broader context that we're most concerned about this. So when the device key, we'll call it, is extracted, is exposed and extracted from a particular device, that key can then be incorporated into, for instance,
a software circumvention tool, and that is essentially how various of the current unauthorized circumvention tools operate today.

They use stolen keys that have been taken out of otherwise legitimate products, and then those device keys are incorporated into a circumvention tool, usually a software product. That then we're now not talking about one device being able to play back any movie that it wants to, which it was already able to do because it had a device key in it in the first place, but it's now enabling a whole market full of circumvention tools in the form of software that provides a much bigger avenue for piracy than might have been possible with that single device.

MR. CHENEY: Thank you, Mr. Ayers.

Does anyone else have some input on that particular question? And particularly, does this repair on those players expose those cryptographic keys? And I understand potentially how it might get out there, but if that can help direct the question. Thanks.

Mr. Reed, I think I see your hand, if that's okay.

MR. REED: Yeah. I'll just add this. So while everyone was talking, I just put into my Google
search engine "hack my Xbox drive." Here's the one that comes up first: "Flash the light on disk drive used by some Xbox consoles for hacking. If you're tired of paying $60 for a new Xbox game or waiting years for them to get cheaper, you should probably mod your system."

That's literally the first thing that comes up, and it goes through and has a video of how you actually flash the drive by installing a different DVD player into your box, and flash the drive to allow you to play disks that violate the copyright.

So at the core of your question, "Is this a vector by which people can use it," well, literally that's the first thing that comes up on your Google search when you put in "hack your Xbox drive." So whether or not we can talk about which case law applies, the search engine bar will tell you how quickly and easily it's there and why that is a primary vector.

So you know, in this case, Google is your friend. Find the answer, hack your drive, flash it, and run disks that you want to play for less than 60 bucks. It's right there. First output.

MR. AMER: Okay.

So we have lots of hands up. So I'm going
to try to get to everybody, and I would ask everybody
to just be relatively brief.
    Mr. Wiens, maybe you could go next.
MR. WIENS: Sure. I would encourage Mr. Reed to go ahead and give that site $60, and then
they're going to sell your credit card number on the black net. It's a scam. There isn't such a hack.
    There are a lot of wonderful sites that will like trick you and make you think that they will help you hack your Xbox. They will happily take your credit card number and then not help you hack your Xbox. The Xbox One, the PlayStation 4, PlayStation 5 haven't been cracked, so that's a non-issue.
    I think that if you think about this in the context of what you can do with a P.C., a Blu-ray drive on a P.C., we have the ability to do the work on those. It's not implicating or creating any challenges.
    You know, those encryption keys are on the drive. They're fine. That's not what we want to access. All we want to be able to do is restore the device back to functionality. And I would note that functionality -- from my perspective, the device isn't repaired unless the copy protection is restored. Like we don't want to remove the copy protection. We want
to get the device working exactly as it did from the factory.

So when these devices are provisioned in the factory, in the Xbox or the PlayStation factory, they take an off-the-shelf drive, install it in the machine. They run a software tool that pairs that optical drive to the machine. That's all that we want to do, is just do that pairing. You know, I think that this has gotten more complicated than it really is. We just want to fix the thing.

MR. AMER: Okay.

Mr. Inacker, I think you've been waiting.

MR. INACKER: Thank you. Similar to Mr. McHargue, I am not a lawyer, and I have found this conversation very, very interesting. But talk about Xboxes and DVDs and everything else is very interesting, but we are all consumers of health care.

Our businesses that we have within Avante Health Solutions -- we repair vital medical equipment, and we do it as independent service organizations. And as all of us as consumers of health care, it should be of great value for you to understand that we do it much more responsibly, much more safely, and, in many cases, much, much more cost effectively than the original equipment manufacturers do.
Yet they have put restrictions in place through these TPMs to prevent us from being able to service it. No different than your automobile, no different than your agriculture equipment. We need to have the right to repair the equipment for our customers and have access to do so on a readily available basis.

This is a patient safety issue. When we can't get access to the equipment that we need to service, patients wait. When an MRI is down, or a C.T. is down, or a cath lab is down, or a piece of diagnostic equipment is not working, patients have to wait, and that harms their care.

MR. AMER: I just want to --

MR. INACKER: Vital issue for our industry.

MR. AMER: I appreciate it. I want to stop you there because I wanted to ask about DVDs and video game consoles. We're going to get to medical devices in just a little bit. So hold that thought, if you would.

Let's go to Mr. Williams.

MR. WILLIAMS: Thank you very much. A lot's been said, but I'll try to stay brief. So the video game consoles, as Mr. Ayers mentioned, have some of the same concerns with respect to keys, because they
play disks with motion pictures on them. But they also have the concerns that you've identified in previous proceedings related to either installing and playing illegal copies of games or using illegal disks, and I appreciate Mr. Reed's comments on that.

You know, one difficulty from the comments that we have is that there's no real specifics about the procedures that they say they can implement to repair or replace the optical drives. They seem to lay out two scenarios. One is using an application of some sort to flash the device, and one is a more manual procedure.

Going back to, I believe, all the way to 2012, the Office has concluded that there has not been evidence that you cannot replace or repair an optical drive without circumvention, and so depending on the different approaches that they take, there may be alternatives to circumvention here.

The other issue is they say that they will restore all of the functionality of the TPMs, but there's no explanation of exactly how that's going to happen either, and my understanding is that this is of concern to the console manufacturers, not only whether they can actually restore the functionality to its original state, but also that the use of an
application to open up the system for the purpose of replacing or repairing the optical disk drive could lead to the use of unauthorized applications or disks.

    Just very quickly, Ms. Sheehan asked about cases where the industries have pursued issues under 1201. I think you know there are quite a number, but in the video game space two of the biggest names are the MDY case and Davidson v. Jung. They go all the way to the appellate level. And so 1201 has been enforced, including by the Department of Justice, and there's a case in our comments on that.

    MR. AMER: Let me just jump in.

    MR. WILLIAMS: The harm to consumers here is not from the manufacturers.

    MR. AMER: Mr. Williams, could I just jump in? Could I just jump in? Because I wanted to ask about something you said earlier. Because there does seem to be, again, this factual question about restoring the TPMs.

    So I believe it was Public Knowledge's reply comments that said a video game console will only function if the two portions of the console unlocked by repair, the motherboard and the optical drive, are relocked. Is there any dispute about that? They seem to be saying that in order for a repaired video game
console, at least with respect to the optical drive, to work at all going forward, you have to restore the TPMs. Do you have any information on that?

MR. WILLIAMS: So to my understanding, it may depend on what your definition of "function" is. If you want to restore it to full functionality, to where it is capable of interacting with authentication servers, et cetera, that may be true.

Without repairing those TPMs, whether you could still play offline infringing games, I think's a different question. If you gave me a post-hearing letter on that, I could probably give you more specifics, and it may be different from console to console, the exact answer. But that's my understanding.

MR. AMER: Okay.

Ms. Gagliano, I think you've been waiting.

MS. GAGLIANO: Yeah. I just wanted to respond to a point Mr. Ayers was making about the DVD and Blu-ray context, saying that even if the exemption itself doesn't permit piracy within its scope, that the movie studies, the content providers just knowing that people are allowed to circumvent the TPM, and that that would make the system less secure, would be less willing to license their content for release on
DVD and Blu-ray, which is a little confusing to me, because I think we all know DVD CCA and AACS LA even brought up in their opposition comments DeCSS, the still widely available program for decrypting DVDs.

And since at least 2007, the decryption keys for Blu-Ray encryption have also been out there widely publicly available, you know. It may be not be legal to distribute and use these, but it also would not be legal to be bypassing the content protection TPMs under the proposed exemption.

And I have not seen or heard any evidence that since those keys have become publicly available through various means that there actually has been any decrease in content providers' willingness to license their works for release on DVD and Blu-ray. So I just don't think that point really seems to hold up based on what we know from the real world.

MR. AMER: Mr. Ayers, do you have a response?

MR. AYERS: Thank you very much. And actually, part of why I had my hand up was to address the earlier comment that was made, that there's no evidence of increased piracy. Just I would note that specifically in the game console space, one of the most popular platforms for the playback of
Unauthorized content is an application that's a direct descendant of early efforts to hack and modify the Xbox console.

And similar to the Google search we were introduced to a little earlier in the conversation, a similar search regarding this product will yield the result that yes, the distribution of the playback platform itself is -- we'll make comments about not pirating content. However, every single reference you find in association with that platform in a Google search talks about getting free movies and T.V. And so we see the technical compliance effort versus the real world in that case.

And to address the more recent comment about what action has been taken, actually, action has been taken. And while certainly my clients are not ones to seek the limelight and do perp walks, for instance, in cases like this, there are certainly efforts that are taken. A successful content protection effort involves technical elements as well as legal elements, and my clients have pursued both in a number of cases.

And then to look at the content industry as "because it still continues to release Blu-rays as therefore it must not be a problem," I think is a gross oversimplification of how the market works in
this case, and the realities of content distribution.

MR. AMER: Mr. Wiens?

MR. WIENS: I just wanted to make myself available if you have additional technical questions on like where the encryption keys are stored and how that works.

MR. AMER: Well, do you have any information that you could offer on this question of the need to relock video game consoles if you're repairing the optical drive?

MR. WIENS: Yeah, the game console would not work to play off-the-shelf games unless you restore the TPM, unless you restore its ability to have those keys and to have that communication, right? Because if I buy Call of Duty, it's encrypted. So that's all we want to do, is keep it in place.

And I think that the point that the Blu-ray keys have already been leaked is poignant, because we're talking about not allowing people to get in and access something. Well, that secret is already out there. The criminals are doing the criminal activity. What we're saying is we just want to be able to do the legal activity.

And I would say like the market harm here is real. I have an entire shelf full of about a hundred
PS4 optical drives and main boards, and we have to sell those together. So I have to take main board and an optical drive, sell it as an expensive part. We are completely supply constrained. The number of people out there that can fix their game consoles is completely limited to the number of game consoles that end up at recyclers.

Then those two pieces together both work, and we can get out there. So it's like there are maybe hundreds of people a quarter that can fix their own game consoles when, in the market, there are millions of people that potentially have these problems. So this is a very real and kind of dire problem. Every time I talk with a repair professional, I mention the game console thing. They just get sad.

MR. AMER: Okay. Thank you.

Let's go to Ms. Sheehan and Ms. Burke quickly, and then I think we'll move to another question.

MS. SHEEHAN: I just wanted to endorse what Ms. Gagliano and Mr. Wiens had said. On one side of the scale, it's a little bit late for hand-wringing over access to decryption keys, as Ms. Gagliano and Mr. Wiens said. The horse is kind of out the barn
door with that. They're widely available. And restricting people from being able to repair their consoles isn't going to protect them any more.

I think one thing to note, to recognize there, is that people who are going to infringe copyright deliberately or who are going to hack their consoles in order to infringe copyright are already doing that. They're not waiting for a 1201 repair exemption to be able to do that.

The lack of a repair exemption to 1201 only really impacts people who are interested in doing the lawful activity of repair. And in this case, we're talking about really just replacing an optical drive on a machine where the optical drive is broken, and then reenabling the TPM protection there. So we just want to fix our consoles.

And as I mentioned before, we talk to repair shops all around the country and all around the world, and we talk to folks who specialize in video game repair, and they tell us that they have storage rooms full of hundreds of consoles that they've been unable to fix for their customers, because without the ability to replace a broken optical drive on its own, the repairs are too costly, too risky, and the parts are too hard to find.
MR. AMER: Thank you.

Ms. Burke?

MS. BURKE: Yeah. I just wanted to echo what Ms. Sheehan and Mr. Wiens and Ms. Gagliano have said here today. What's interesting here is that the conversation that Mr. Reed had earlier about people pirating games even that they had given away for free, and the wide availability of these decryption keys, kind of demonstrates that these locks aren't preventing pirates from pirating. They're not preserving the copyright of these creative works.

What they are actually doing is they are preventing law-abiding citizens who want to do law-abiding things such as repair their devices. And so I think like that's particularly relevant when looking at this exemption request, that what we're asking for is an exemption for a limited purpose, to perform a repair. We are not asking for an exemption to pirate content.

And the underlying work that is being protected by this TPM, it isn't the movies on the Blu-rays or the DVDs, or even on the video game disks. It's the software, the firmware that is controlling this lock itself. So I think that's also particularly relevant here when we're talking about like what
copyright work is actually being protected here with
this lock on the optical drive to the motherboard.

So there's just this over -- the concerns
about piracy here feel more like fearmongering as
opposed to actual realities of what is at stake.

MR. AMER: Okay. So thank you.

That raises an issue that I wanted to follow
up on quickly, and then I think we'll move to the next
topic, and it's this idea of sort of the relevance of
what the purpose of the circumvention is, and I'm
interested in particularly the opponents' response to
this.

So I mean one argument that I think we've
heard today from the proponents is that the existing
temporary exemptions, for example, for security
research and jail-breaking, and also the permanent
exemptions for things like security testing and
encryption research, all refer to the purpose of the
circumvention, right?

They turn on whether the circumvention is
undertaken for an accepted purpose. So you know,
certainly with the vehicle repair portion of this
exemption, we've included language that tries to state
clearly that the circumvention may not be undertaken
for the purpose of gaining access to other types of
works.

I wonder if that approach -- the opponents seem to be saying that approach is not sufficient here and that DVD players and video game consoles are sort of an entirely separate category.

But I wonder if you could speak to this question of well they certainly aren't immune from the statutory exemptions that already exist, which are based on the purpose of the activity. So I wonder if you could speak to that apparent discrepancy, Mr. Williams?

MR. WILLIAMS: Yeah, thank you. And I'll just say quickly, some of the comments made it sound like video game consoles can't be repaired at all, ever, and that's just not true. If you take a look at our comments, you'll see that there is still warranty repair and post-warranty repair available for consoles.

On this question of the limiting language that you mentioned, I mean, of course, that language is helpful to an extent, and we prefer exemptions that have it, but it doesn't really solve the problem. And I think if you look back at the records on video game consoles specifically, there's been a lot of evidence that jail-breaking a console almost inevitably leads
to piracy, that infringement is the number-one reason to open up a console.

And so just saying in an exemption that it doesn't apply unless -- as long as they -- no one intends at the time to access content illegally, that's very difficult to police, number one. And number two, there's all kinds of questions about timing. So when you put that language in there if someone makes a repair, say, and then a year later they start using it for infringement, how does that work?

So the language, while helpful, while I appreciate your efforts to try to rein in some of these exemptions, it really doesn't address our overall big picture concerns that the 1201 statute really sets a marketplace expectation for typical consumers. And when you alter that underlying marketplace expectation, bad things tend to happen, even if you've got language of that sort in the exemption itself.

MR. AMER: Okay, thank you.

I want to, Mr. Ayers, give you a chance to respond, too, and then I do, just in the interest of time, want to move to the next topic.

I think we've had some comments on this
point before, so I think we'd like to wrap it up after
-- oh, Mr. Ayers, did you no longer --

MR. AYERS: No, I'm sorry. I was just
removing my hand just in -- it's still up.

MR. AMER: Okay.

MR. AYERS: It's still up. Sorry.

MR. AMER: So let's go to you, and then
we'll go to the next topic.

MR. AYERS: Thank you, and I'll be very
brief. Just to note that, again, limitations are
better than no limitations in this context, and
certainly, if there's an inclination to grant the
request, properly bounding them is important.

But I would note that, again, we've got
multiple situations where the word "repair" has been
used in relation to activities which are arguably
modifications or expanding the functionality of
devices.

Also a little bit concerned about restoring
a device to its original condition. Does that include
if the device had a revoked device key because it's
been inappropriately used? Does that mean restoring
that device with an unauthorized device key that's
been retrieved from another source?

And again, to note that the difference
between other contexts and the optical disk drive context here is that we've already seen, for years now, the proliferation of piracy that occurs. And again, noting specifically in the game console space that the most used and popular platform today for playing unauthorized content is a direct result of original efforts to hack and modify the Xbox.

MR. AMER: Thank you.

And I see that we do have a couple of other hands up, and so you can potentially incorporate your answers here into the next questions, but I'd like to turn it over to my colleague Mr. Bartelt to ask about some other types of devices.

MR. BARTELT: Thanks.

Hi, everyone. Following up on some of what Ms. Smith alluded earlier about questions concerning causation, in the 2018 rulemaking there were some device types that, in the recommendation that the Office issued or the acting register issued, we had found out there was an insufficient causal link.

So I wanted to probe a little bit about maybe what's changed since the 2018 rulemaking and see if there's an additional record supporting the causation that relates to these devices.

The first one I'd mention is a category that
we refer to as consumables. There, we found that the
prohibition against circumvention -- it was not clear
from the record whether the prohibition against TPMs
was causing adverse effects on non-infringing
activities relating to replacement cartridges for ink,
coffee, litter boxes. I think we had a few other
examples. I believe this came up primarily in the EFF
submission.

So I'd like to first, I guess, direct my
question to Ms. Gagliano, whether there's the
additional record in this rulemaking that you can
point to that shows a causal link between the TPMs
inhibiting repair activities as it relates to these
devices that use consumables.

And then maybe after that, I can turn to
you, Ms. Burke, to see if you have additional
comments.

Ms. Gagliano?

MS. GAGLIANO: Sure. Yeah. If you look at
our initial longform comment, I'd say that both the
CatGenie cat litter box example that you mentioned and
the printer example both go to consumables.

And you know, as opposed to last time my
understanding then was that the Office was not saying
so much, "Well, that's not enough examples," as it
was, "You didn't give us enough detail about what the
TPMs are, whether they actually are access controls,"
you know, "how the circumventions would work and," you
know, "what's the full fair use analysis, statutory
analysis?"

So this time we have given you all of that
in perhaps excruciating detail, so I think if you look
there, you'll see for both of those examples and for
printers it's not just one printer, but we discuss
multiple kinds, including H.P., I believe, also
Lexmark, and a couple others that are using TPMs.

And we discuss in more detail what those
TPMs are, how they are actually access controls, and
how 1201 adversely affects modifications that people
want to be able to make.

MR. BARTELT: Thank you.

Ms. Burke? I'm not sure if your comments
are specific to these causation issues, but --

MS. BURKE: As far as to the changed
circumstances question, with -- well, first, as a
matter of just -- I know opposition replies to our
comments with regard to the video game console had
suggested that we should be barred from bringing such
a petition because it had been denied in the past.

And as a matter of course, I want to point
out that there are no pseudo-standing kind of
threshold issues at play with regard to this 1201
hearing. It's not in the statute. It's not in the
legislative intent. And so I just think, as a matter
of course that that's -- it just not in keeping with
what this hearing is about.

Congress intended for these reviews to
happen every three years because it understood that
technology changes quickly, and the context and
circumstances of our understanding of when an
exemption might be necessary could change with those
times.

Now, to the extent that it's something that
the Librarian would want to consider under the fifth
factor of the 1201 statutory analysis with regard to
video game consoles, there have been significant
changes since the 2018 review. Most notably, one of
the reasons that the video game console exemption was
denied in 2018 was because of the availability of
official repair channels.

And I know that Mr. Williams had kind of
gotten into this a little bit, but the facts there
simply aren't true. In 2019, Microsoft announced that
it was no longer going to repair devices that didn't
have in active production, and the Xbox 360, the Xbox
One, the Xbox One X can no longer be repaired through Microsoft. So there are no official warranty repair options or even outside of warranty repair options with regard to many of these consoles, so consumers have no choice but to either buy a completely new console or to just throw it out, basically.

Then as far as like other things that have changed, I think with regard to not just to video game consoles, but with regard to all devices, when it comes to the necessity of repair, over the last 13 months our understanding of global supply chains and the availability of devices has definitely shown that it's much more vulnerable than we could have possibly believed before, not just from COVID but our relationships with China when it comes to trade and the recent incident in the Suez Canal demonstrates that our ability to get devices, new devices, when we need them and to get even official repair parts, et cetera, can be significantly challenging.

And when there's a crisis at hand, it's really important to be able to repair what we have, given some of --

MR. BARTELT: Okay.

MS. BURKE: -- the increased concerns.

MR. BARTELT: Sure. Thank you, Ms. Burke.
I do have a question for Mr. Wiens that also sort of relates to this question of changed circumstances and from 2018 where the -- in the recommendation, the Office had found that for computing peripherals, I think the instance that was before us then was related to a hard drive that people were trying to access, that it wasn't actually inhibiting the ability to circumvent.

And I just was curious if there were any examples that you could provide relating to computing peripherals that would show that TPMs are, in fact, inhibiting access or are effectively controlling access to these types of devices. The hard drive would be, of course, one example. But if you have others, please provide those.

MR. WIENS: Absolutely. You know, you think back over the last three years, it's hard to think about what the world was like almost before 2020. Like so much has changed, and so much has changed in this sphere. I like to say if something can't have software added to it, it will. And the kind of new adage is if something can have a lithium battery in it, then they're going to add a battery.

And so the whole world of gizmos have consumables, have batteries. I'll get to the
peripheral question in a second, but an example of a consumable that we haven't discussed before is robot vacuums. So the iRobot vacuums have batteries in them. The batteries have a TPM that ties the manufacturer sort of branded batteries, and if you install an after-market battery, the vacuum won't recognize it.

And that's not just the case there. I mean, we see that -- Apple does this with the batteries in the iPhone. Increasingly, these battery consumables are being tied to the device purely to monopolize sales of after-market parts, just like we see in inkjets.

You know, it's also interesting to think about, like we all -- we do this every three years. Man, it would sure be nice if this was more often than every three years, because the technology world changes so quickly. I think we realized about a month after the last kind of hearing that as we were talking about all the things that we could repair, nobody asked for an exemption for computers, for laptops.

And like all the computers and everything that we're talking to now, we don't have a repair exemption for them. And we were all kind of shaking our heads, like how did we not think about that? And
the answer is that historically, computers haven't had
TPMs. You know, your bog-standard P.C. you can get
in. You can access. You can replace anything.

But what we're starting to see now is Apple
has taken the T2 security chip from iOS devices --
this is maybe the thing we have to jailbreak in iOS
devices -- and they've put it on their computers. And
we're seeing more secure boot techniques across the
board in all kind of general purpose computers.

So where historically there wasn't a
circumvention needed to do service, now overwhelmingly
it is, and that's been a huge sea change in the last
three years. There have been lots of other changes to
areas where -- go ahead.

MR. BARTELT: Okay. No, I was just going to
say, I was going to give Mr. Williams an opportunity
to respond, and then what we'll do after that is where
we're going to change -- as Ms. Smith mentioned
earlier, we're going to discuss medical devices. I
believe we have some comments on that. But we'll
focus a little bit more on that and then conclude with
discussing vehicles.

So, Mr. Williams?

MR. WILLIAMS: Yes, thank you. I wanted to
respond quickly to what Ms. Burke was saying. If you
go to support.xbox.com, you'll see that the Xbox One S, the Xbox One X, they're still being repaired by Microsoft. And we said in our comments their policy is to continue repairing consoles up to four years after they are no longer selling those consoles. So some of what was said is inaccurate with respect to what Microsoft is currently offering with respect to console repair.

All of the console manufacturers also have pretty robust e-recycling efforts where people can, for free, get their consoles recycled to avoid e-waste and some of the other issues that were implicated there.

On peripherals, I don't recall in the record seeing anyone targeting video game consoles peripherals, but you can see in some of the websites that we provided that those peripherals are also repaired by console manufacturers in warranty and out of warranty. And so I'd need more specifics, I guess, to know the answer on any given device.

But my understanding is those can be repaired by the manufacturers, and I don't know that circumvention is always required with respect to peripherals. I do know some peripherals can inter-operate with other devices, as we discussed in the
disability-related exemption classes, without any need to circumvent. So I would need more specifics to answer that question.

MR. BARTELT: Thank you, Mr. Williams.

As I said, I'm going to turn now to some questions focused on medical device repair, so I know you've spoken a little bit to this earlier, but maybe I could get a little bit more insight about how TPMs are actually inhibiting access to repair devices.

I think what we saw in the written comments was that the opponents were saying that the original equipment manufacturers in this instance were providing access and servicing information as required by the FDA regulations, and that that was sufficient to perform basic maintenance and repair services.

So I guess to both Mr. McHargue and Mr. Kerwin, maybe you could both elaborate a little bit for us about what FDA-mandated access and servicing materials that OEMs are failing to provide and why what you're receiving is maybe inadequate or TPMs are preventing access to basic maintenance and repair activities.

I guess, Mr. Kerwin, I see your mike's off, so please go ahead, and then we'll turn to Mr. McHargue.
MR. KERWIN: Well, thank you for the opportunity to speak. We appreciate that. It would not simply be FDA that we would be speaking to. There are applicable regulations from the Center for Medicare and Medicaid Devices, particularly 42 C.F.R. 482, which requires that hospitals maintain adequate information on equipment to have an acceptable level of safety and quality.

But to speak to your point on AIAT FDA, first, that only pertains to radiation-emitting devices such as x-ray, and that has to do with information pertaining to assembly installation. And what we're seeing -- and let me just back up and say that at IAMERS what we're seeing is that independent servicers in the secondary market may well become like the watch repair people to the extent that they're adversely impacted by this exemption.

We treat rural and regional hospitals located everywhere from Eastern Appalachia in West Virginia to Kansas, and we are conducting a survey of some of these hospitals and, unfortunately, were not able to complete it, but what we do know is that all of them are having zero capital budgets and are unable to undertake only the basic work.

And in this connection, the independent
servicer, whose rates are substantially lower than the original equipment manufacturer, is a preferred model. In addition, the turn time when equipment breaks down is easier. So the AIAT is providing assembly information -- is also something, sadly, with a right but no remedy.

That is to say that the FDA has widely acknowledged that if there's non-compliance, there is no remedy for that. And we now see the DMCA and other federal and state causes of action being used to thwart the ability of independent and in-house diagnostic imaging services by claiming that the use of these manuals is a violation of the law, and I know there are several cases coming to trial this year.

And if there's an issue, retaliation is alive and well. That is to say, many of the members are fearful that if they speak as to these issues, they'll see a slowdown of parts. They potentially will have a refusal to deal, notwithstanding that some of these same manufacturers no longer own the machines, the equipment, that they are selling to hospitals, group medical practices, and to some independent servicers.

We have witnessed since the last hearing a massive consolidation in diagnostic imaging, with
three manufacturers occupying 70 percent of the
diagnostic imaging market, with manufacturers
controlling all but nine percent of the servicing of
equipment.

Few hospitals, group purchasing
arrangements, and rural hospitals possess the market
power to insist upon providing information to fix
their own equipment. Without this information, it is
difficult to conduct a root cause analysis of a
problem with equipment.

And as you may know, many of our members are
ISO 13485 qualified, and in the ecosystem of medical
device care you have many HDOs, health delivery
organizations, and they're well-established clinical
engineers in an oversight capacity. This is not an
area where fearmongering really should have a place.

And one can only look to the FDA MAUDE
reports, which are the manufacturer and user facility
reports which must be filed by the manufacturer or the
hospital where an adverse event to look at is found,
and you would see that under one percent adverse
events have been occurring with respect to this.

So the conduct that we're speaking of is
causing a problem for those who have lawful possession
of the equipment and those who would service it,
because the price differential can be $150 to $250 an hour for an independent servicer versus six to $800 an hour for a manufacturer with a minimum four-hour time cap.

So this exemption is causing adverse events, and we do feel that a new exemption needs to be undertaken. I should say this TPM. And we are asking to take this into account. I wish I could bring many members with me, but a number of them are just painfully worried that if they contribute to this conversation that they could potentially suffer a loss in delayed equipment or refusal to deal and other activities.

MR. BARTELT: Thanks, Mr. Kerwin.

MR. KERWIN: Let's make sure --

MR. BARTELT: Oh, and I'm sorry, I do want to give others enough opportunity. I know we don't have a tremendous amount of time today. I do appreciate your remarks here. And we may be able to circle back again yet.

But I just wanted to give Mr. McHargue, as I said, a chance, and then I believe Mr. Cheney has a question, and we can get to some of the other people with their hands raised. Thank you.

Mr. McHargue?
MR. McHARGUE: Thank you, Nicholas.

So relative to our ability to seek service and manuals, there has been, I would say, improvement --

MR. BARTELT: Oh, and I'm sorry, Mr. McHargue, could I jump in one -- I'm not sure if this is best directed to you, too, but maybe as part of your response, could you clarify -- you had just mentioned manuals, and I think -- are you seeking access not just to the computer programs but -- I wasn't sure if there were -- if the original equipment manufacturers were claiming copyright in works besides the programs themselves, but also in like the manuals or other literary works or ancillary materials?

If you have any insight there, we'd appreciate it, and then whatever else you want to comment on concerning the TPMs that are preventing access.

MR. McHARGUE: Yeah, I'd say in general, we have access to manuals for the most part, but now the manuals are digital. We're told that we can access all of them for a particular fee. What we're really bumping into is the fact that we are told by the original manufacturers that we can buy a service advisor or something that can help us get in,
potentially read the codes, read the errors. We can go and buy the parts to actually install, but the issue is once we install, we cannot get the last bit of software to have that vehicle, whether it be a tractor or a combine, recognize that new piece of equipment and actually make it functional.

So in the details of how this all works, again, I'm not a software engineer, but what I know for sure is that we can get all the way to the end, and if I have a combine sitting out to field, and the rain is coming, and my independent repair tech comes out, installs the part, gets it up, and says, "Well, that's as far as I can go. You're going to have to have a tech from the equipment manufacturer come out, finish that repair." And so from that aspect, that's not working for us.

And to be clear, agriculture is not seeking an additional exemption from the Copyright Office. We appreciate what was done in 2018. But those are some of the issues we're still dealing with, though, relative to -- since 2018.

MR. BARTELT: Okay. Thank you.

Mr. Cheney, you had a question? And then we'll move on.
MR. CHENEY: Yeah, thank you.

MR. BARTELT: Yeah.

MR. CHENEY: Oh, I appreciate it. Thank you for giving me a moment here. I just want to clarify one thing. I don't think it was very clear from part of your question. And then I want to ask an additional question.

The manuals that you're talking about, in order to access those, do you have to break a TPM to get access to those manuals? And how is that done? Can you describe that a little bit?

The other thing that I want folks to get into a little bit here and talk about is this system of what the opponents are calling unauthorized independent providers, and what that system looks like, and why would hospitals and clinics and others that have these devices be having those folks on staff? And what are the qualifications in order to do that?

Just a little bit more detail there, I think, and some of that may have come up in these Cal State Senate hearings, and some of that -- so whatever's relevant from those hearings that were happening last week that maybe, brought in, might be helpful, so including like ISOs qualified and some of
that kind of stuff I think I heard you mention. So I
hope that's helpful for this conversation. Thank you.

MR. BARTELT: Okay. Thanks, Mr. Cheney.

I realize I should have called on Mr.
Inacker earlier, and then maybe we'll go to Mr.
Inacker, Mr. Reed, Mr. Wiens, and Ms. Sheehan.

Go ahead, Mr. Inacker. Oh, I believe you're
still on mute. Very good.

MR. INACKER: Thank you for that. Just a
couple of quick points of clarification. So the TPMs
would not be removed by the exemption that we are
requesting. We just don't want to have the penalties
associated or the consequences associated with
circumventing. "Basic service" is defined by the OEM.
It's not defined by an independent service
organization. They define what you're allowed to have
access to.

"Basic service" is insufficient to do what
we need to do to get our customers -- hospitals, care
givers, imaging centers -- the type of service that
they need to have their equipment be fully functional.
"Basic service" is insufficient in order to do that.

That's why we have to be able to go around
the TPMs in order to make the equipment as functional
as possible, especially when it comes to removing and
replacing high-end pieces of equipment like glassware in imaging devices. It is essential for what we do as an organization.

And it's unconscionable to me as a consumer of health care, where we can provide a service that offers a 30 to 50 percent reduction in cost to what an OEM is capable of doing, that we're not all standing up and saying we need to have access in order to be able to do this.

MR. BARTELT: Thank you, Mr. Inacker.

Mr. Reed, I'm not sure if you want to continue in --

MR. REED: Yeah.

MR. BARTELT: -- speaking to this, go for it.

MR. REED: Yeah. So I think we heard a little bit of that old line, "lies, damn lies, and statistics." It was interesting to say that when Mr. Kerwin said, "Oh, well, it's only one percent." Well, that one percent, according to the FDA's MDR review from 2017, was 40 deaths, 294 serious injury, 38,500 patients and/or operators exposed to potential harm. So when one says, "One percent, oh, gee, it's not that many," it's actually a lot.

The second part of that's important. Again,
within the scope of what you're looking at, the FDA already has requirements called the Quality System Regulation, or QSR, that governs OEMs. So if you look at the section 710 of FDA's Reauthorization Act, we already have all of those things in effect.

The specific language is, "Quality systems help ensure that products consistently meet applicable requirements and specifications." So when Mr. Inacker says, "Well, we should be able to reduce cost," part of what he's trying to overcome is he doesn't want to pay for or do the necessary things to meet the FDA's requirements as a QSR.

So right now, we fully support and think it's a great idea if OEMs or others can provide service and support and meet the FDA's requirements for QSR. Then that's probably a way to go for it. Right now, the third-party servicers kind of don't have the same transparency or accountability, and don't necessarily submit adverse event reports in the same way that the others do.

So I think that it's a little glib to say, "Gee, we save you 30 percent," but if it results in 40 deaths, 294 serious injuries, and 38,500 patients and operators exposed, then I'm not sure it's something that we wave off with a hand.
So I would encourage the Copyright Office to be very cautious for over interpreting the cost reduction as something that should drive this forward, especially since the market exists.

MR. INACKER: May I please respond to Mr. Reed?

Mr. Reed, all of our organizations are ISO 13485 certified, the same certification as the OEMs. Your numbers -- if you look at how many of the OEM organizations have caused issues with imaging equipment because of their delays and lack of responsiveness, those numbers will be a heck of a lot higher than they are for the independent service organizations.

MR. REED: And, Steve, I'd be happy to go to the FDA and talk with you about some of those failures. The Copyright Office is not the place --

MR. INACKER: The FDA -- the FDA -- the FDA --

MR. REED: -- to have that discussion.

MR. INACKER: The FDA --

MR. REED: This is not --

MR. INACKER: -- clearly --

MR. BARTELT: I'm sorry, gentlemen, gentlemen, for the sake of the discussion --
MR. INACKER: The FDA clearly said in 2018 that --

MR. BARTELT: -- speaking over each other.

MR. INACKER: -- independent service organizations provide a valuable service to the health care providers, and no difference between what an OEM is doing and a qualified --

MR. BARTELT: Yeah, so again --

MS. SMITH: Just a moment.

MR. INACKER: servicer --

MS. SMITH: Just a moment. Just a moment. Just a moment. Just a moment. Thank you. Everyone is going to get an opportunity to speak, but we cannot have cross talk over this, and we cannot have going back and forth without the moderator. That will not work for the court reporter, and we want to make sure everyone gets a chance to speak.

So we're going to go a little bit over time because we know there's a lot of issues. We do want to cover them. But I have to ask you to respect my colleague who's moderating.

So I think, just to take some of the tension off of that issue, and also I think some of these issues might be going a little bit beyond, I want to make sure we're centered on the 1201 rulemaking. I
think let's give Ms. Sheehan a chance to weigh in.

Thank you.

MS. SHEEHAN: Thank you. I just wanted to respond really quickly to what Mr. Reed mentioned about the FDA, and I'll say that it's possible Mr. Reed is not familiar with the FDA's 2018 study reporting on the quality, safety, and effectiveness of servicing of medical devices.

In that study, the FDA issued a report which, in part, sought to determine how valid these concerns were about the quality of servicing provided by the original equipment manufacturers versus third-party independent entities. And the report found that the objective evidence indicates that many OEMs, original equipment manufacturers, and third-party entities provide high quality, safe, and effective servicing of medical devices, and in fact, that the continued availability of third-party entities, including independent service organizations, to service and repair medical devices is critical to the functioning of the U.S. health care system. So just to address some of those FDA concerns that Mr. Reed raised.

But moving on and refocusing on really the core inquiry here, if Mr. Reed would contain his
emotional responses, that would be delightful.

But also just this is a Copyright Office hearing. This isn't an FDA regulatory proceeding. And so the Copyright Office is concerned with whether or not there should be an exemption issued to section 1201 for the purpose of medical device repair.

And I'll say again, as I said throughout this hearing, that repair is a non-infringing activity. The absence of an exemption to permit repair on medical devices as well as other software-enabled devices causes real tangible harms. In medical devices, that's very prescient.

We have people who are left without a functioning wheelchair for months at a time, waiting for original equipment manufacturers to send out a qualified repair technician.

We have hospitals unable to repair rooms full of ventilators because they can't get access -- they have to wait months for manufacturer-branded repair services to come out and provide them with a special dongle which is needed in order to get access to the device to do the repair, or to provide the service keys -- again, another TPM -- that's used to lock out hospitals and technicians as well as independent service technicians and privilege
manufacturer technicians.

And as I said before, the Federal Circuit found in Chamberlain -- and this has not been -- this has not been disputed -- that 1201 doesn't give new exclusive rights to copyright holders. So that means that 1201 does not give a right to medical device manufacturers or medical device app manufacturers to control the market for repair or to exclude independent repair providers.

MR. BARTELT: Okay. Thank you, Ms. Sheehan. I do have a question about maybe how these TPMs would work and how the -- you know, just hypothesizing, that if the circumvent -- this is maybe directed to Mr. Wiens.

I don't know if you have any technical background that you could help with -- or maybe Mr. Kerwin -- that once the TPMs would be circumvented on these types of devices, would the copyrighted works -- would the software programs or the data remain on the machine afterwards? Would they need to be put onto another device?

I'm just curious about sort of the actual mechanics of circumventing on these medical devices. I think we've heard about a lot of other devices over the years. But I'm not sure, maybe you could provide
specific examples of how circumvention works in these instances and if it could be restored in such a way that it would be sort of to the original specifications.

First I'll let Mr. Wiens -- I see you've had your hand raised for a little while -- then maybe Mr. Kerwin.

And we can maybe come back to you, then, after that, Mr. Reed.

MR. WIENS: Sure. Thanks for the question. These are relatively -- oftentimes, like with the wheelchair, there is a service password that you need to enter, and so if you don't have the service password to get into additional menus, then you're out of luck.

So really, the goal is just to bypass the password so then you can get in. There are very common settings, like traction settings, that you might want to change on a wheelchair. And kind of the same thing with the ventilators and other equipment. You know, you plug the service dongle in.

So, no, the software should remain on the device. The data should remain on the device. The goal isn't to exfiltrate the firmware from the device. It's simply to bypass whatever check is there to see
if a branded manufacturer representative is sitting in
the chair.

In many cases, the larger hospitals have
been given these service passwords, and it's the
smaller hospitals that aren't given the passwords.
And I'll defer to Mr. Kerwin to share the situation on
the ground.

MR. BARTELT: Thank you, Mr. Wiens.

MR. KERWIN: I, I --

MR. BARTELT: Mr. Kerwin, go ahead.

MR. KERWIN: I quite agree. The CMS has
issued various bulletins consistent with the laws
cited that require you to keep your equipment in
accordance with the original equipment manufacturer
specifications or, for certain types of non-diagnosed
equipment, to maintain alternative maintenance
activities with a risk analysis.

So that information will stay with the
hospital and is expected to be there because, as we
know, the Joint Commission has oversight of these
hospitals and is the delegated authority for many of
the states.

And in addition to your earlier point about
vendor management, unauthorized independent providers,
the hospitals will undertake their own vendor
management programs. Some have formalized departments. Some are much smaller. And they do like to see members ISO 13485 qualified, which is the ISO standard.

So the risk is minimal, and I also affirm the other speaker's reference to the 2018 report, which I believe addresses some of the concerns raised.

MR. BARTELT: Okay. Thank you, Mr. Kerwin.

Mr. Reed, I had a specific -- well, two specific questions to you, maybe that you could -- and then any other things that you needed to respond to.

One was to what extent are the existing other types of laws that -- maybe the Computer Fraud and Abuse Act, HIPAA, FDA regulations, other existing things -- alleviate any sort of safety concerns here?

And the second was -- I don't know how much particular insight you have as you're not directly representing -- one of the opposition comments that we had received was a lot of -- some of the examples that were cited were -- seemed to relate to physical issues rather than issues resulting from circumvention of a TPM.

I was curious if you have any examples or maybe I can't --

MR. REED: Yeah.
MR. BARTELT: Where circumvention of TPMs has led to the types of instances that you've referred to. But go ahead.

MR. REED: Right. I think the long and the short of it is, interestingly enough, I think all of this talk about the FDA and Ms. Sheehan's comment directed at me kind of points to the reality. The FDA actually has structures in place to do this the right way. The Copyright Office and the 1201 proceeding is not the right place to do so.

By the way, HIPAA doesn't apply in any of these instances. Just so you all understand, HIPAA actually deals with portability of electronic information. The section that you might be referring to is the privacy rule, which came separately. HIPAA actually only covers what are called covered entities, and covered entities are organizations that file electronic insurance claims or their business associates.

So HIPAA doesn't actually have any constrains around this. OCR, the Office of Civil Rights, doesn't have any oversight over this space at all, unless a covered entity is engaging in a practice that exposes someone's PHI. So it's really, really separate.
But you hit the nail on the head. The agency that does have oversight over this is the FDA, and I'm very familiar with the 2018 report. I actually think that the work that's being done in this conference on this call right now is kind of misdirected.

Our efforts should really be at how do we ensure that the FDA and its Quality Systems Regulation moves forward in a way that appropriately allows for repairs in a way that actually keeps patients safe. I'm not sure why we're talking about medical devices at a 1201 hearing which was more around protecting people's movies and music. So I think that --

MR. AMER: Well --

MR. REED: -- part of the problem we're running into is --

MS. SMITH: Well, Mr. --

MR. REED: But -- sorry, Regan. Did I --

MS. SMITH: I bet Mr. Amer and I have the same question, which is does that also cut the other way, which is if we're looking at whether the copyright law should be playing a role in this field --

MR. REED: Yeah.

MS. SMITH: -- where what we're looking at
is whether it's likely to be a non-infringing use, and we don't -- we haven't really necessarily seen, I think, a reliant interest from the FDA on the copyright law for the discussion.

MR. REED: Yeah. I think that's a great question. It was exactly where I was going. So you heard a little hint about it, about on the manuals part of it. The reality is the manuals are protected intellectual property, and so if breaching TPMs is a way to have access to the manual, the manual is copyrighted material.

So there are some instances where copyright does come into play, and I do know that has been an area of significant dispute, which is access to the manuals, which is copyrighted material. So where the tools are -- where the infringing tools are -- or I'm sorry, the tools are intended to allow access to the manual, it is intended to allow access to material that the owner of the copyright doesn't want to provide access to, and that the use would be infringing in terms of the purpose of what their product is.

But I think those are kind of two separate questions, so the first question that I was asked was, "Is this the right venue?" My argument is no, FDA has
these things in place. Let's look there. Your second question was, "Are there infringing or potential infringing uses?" And I would say you hit it earlier when we heard the discussion about manuals and access to the IP.

So I think that's a place that is, in fact, in dispute, and there are conflicts about access to the IP.

MR. BARTELT: Thank you, Mr. Reed.

MR. AMER: Well, what is the --

MR. BARTELT: Go ahead, Mr. Amer.

MR. AMER: Is the concern about access to the manuals a copyright-related concern? I mean, it doesn't seem to me that you're concerned about people getting access to the manuals so they can read them in the way that movie manufacturers or makers are worried about people seeing a movie without paying for it. I mean --

MR. REED: I -- the --

MR. AMER: -- are you worried about people copying of the manuals that --

MR. REED: Well, yeah, and --

MR. AMER: -- seems like a --

MR. REED: Yes. Yeah. I don't want to stick up for the manual manufacturers, but what I do
know is, yeah, manuals actually contain an enormous amount of very specific proprietary information. They may include information about pin-outs. They may include information about access to specific information.

Now, there are questions that we all have to answer about whether or not that limits repair, but the reality is yes, absolutely, manuals contain information that is protected, proprietary, and, in fact, again, not speaking for that industry, it's my understanding that that's part of what they provide to licensed OEM repair shops, is they license access to all of that copyrighted material to enable the repairs to take place, and that's part of their license agreement with those third-party repair shops.

So I think it's considered a valuable resource to them. It's adjacent to my industry. I don't represent -- you know, they're not part of my membership. But yeah, I do know that they definitely license access to those repair manuals, and that's a key part of their control and income stream and value for the IP that they're creating.

MR. AMER: Okay.

So I think we're going to go to Mr. Inacker and Ms. Sheehan, and then I think we're going to have
to move on to vehicles.

MR. INACKER: All right, thank you. And I just wanted to answer Mr. Bartelt's question directly. So for a medical device, after TPM circumvention, the data remains on the device. The software remains intact. The device is left in its original state after the repair is complete. This is all about fair and equitable access.

MR. AMER: Thank you.

Ms. Sheehan?

MS. SHEEHAN: So first off, I want to say I'm kind of unaware of the circumstance where a TPM would protect access to the service manual, but in the case where it would, I just wanted to address Mr. Reed's claims that that would be infringement. I would say that if the purpose is repair, and the use of the manual -- again, the purpose is repair -- this is a non-infringing purpose.

Also if you have a license to use the machine and the manual, you have a license to use it, to read it, to use the instructions.

And then I also want to address just one of the fair use factors here, weighing in on whether that would be infringing, whether the use of a manual in this case would be infringing, and just say that the
nature of the copyrighted work at issue with a manual is highly functional, right?

So copyright will protect the expressive content in that manual, but it's not going to protect the instructions, the set of steps, the information contained within that manual, and so we're not talking here about a movie or a novel. Most service manuals are, indeed, a set of instructions.

Refocusing on kind of what we're really concerned with her, which is technological protection measures that keep certified biomedical engineers that work in hospitals or that work with independent service organizations, independent repair people, or people who own take-home medical devices -- encountering TPMs that prevent them from repairing their device.

And most often, we see those occurring through the existence of passwords, or security keys that someone has to use to get into the service terminal for those devices, or to authorize a replacement part, or to calibrate with a new part, or kind of dongle-based security mechanisms. And so --

MR. AMER: Okay, thank you.

MS. SHEEHAN: -- beyond the manual it's --

MR. AMER: I'm sorry, could I just --
MS. SHEEHAN: -- largely irrelevant here.

We're really focused on the TPMs that are obstructing repair of the medical device itself. Thank you.

MR. AMER: Could I just stop you there? And I'm sorry to interrupt.

And, Mr. Kerwin, I see your hand up, so I don't want to leave you out, but if you could be brief, and then we're going to turn to our last topic.

And thanks for everybody's patience.

MR. KERWIN: Well, thank you. And could I just, on behalf of IAMERS, thank you. What I was going to say is that relative to the cyber issue that was inquired about, the FDA has issued its own guidances, and those of us who are participatory in the joint public-private partnership of HSCC with 600 members are working on quality and white papers.

But the HHS, the Health and Human Services, is where people record in the civil rights division when a cyber issue has happened, and I urge you to look to see that there is very few that are related to servicing, if any at all. So it's important to realize that the FDA is not in the business of intellectual property. They have publicly indicated such. And it's entirely appropriate to have it here today. Thank you.
MR. BARTELT: Thank you, Mr. Kerwin.

As Mr. Amer said, we're going to turn to our last topic, which is vehicles. We heard briefly from Mr. McHargue and Mr. Rosenbaum earlier. I think we are going to -- I have just basically one question for you each, maybe a little bit more.

First, Mr. McHargue, you had mentioned earlier issues with access to tools, but my question is going to be a little bit different. It's under the current existing exemption for vehicles, there's a few different limitations, one that it not violate other laws. There was a comment about gaining access to vehicle user data.

I'm just wondering, under the existing exemption, how repairers or potential users of the exemption are being inhibited from making necessary repairs. If you have examples that you could provide us, or where the existing language you would suggest be modified in order to accommodate those users.

MR. McHARGUE: Well, I appreciate that question and I probably can't get into, again, the technical side. Probably where I think the need for additional repair people in our area -- there's been a proliferation of expert third-party repairs groups in the ag equipment sector, and so I think possibly
because of the 2018 ruling, I think that has given credence to allowing that possibility.

What, again, has been difficult is even the third-party experts can't get access to -- if I'm the owner, have access to, say, a service advisor from John Deere, they're having difficulty getting access to that same software that I could use to repair, but yet I can infer that to my expert, and they're having difficulty getting the same amount of tech that, say, an OEM can provide.

And even if they could do that, there's still these issues relative to the final repair that was mentioned, whether it be the dongle or the payload, that's needed. So again, I don't know if that's technically within the copyright part. I think there are other laws. When it comes to EPA, safety, some of those things are probably outside this conversation.

But just from on the ground, that's kind of what's going on in the equipment repair side of the equation. I don't know if I answered your question.

MR. BARTELT: Okay, sure. No, thank you.

I do see that we have a few other hands raised that may be able to -- that may be responsive to this question, so I'm going to turn to Mr. Wiens,
Ms. Sheehan. I see Mr. Cheney has a question.

And then, Mr. Rosenbaum, I have a question for you, too that we'll get back to after those comments.

So, Mr. Wiens first?

MR. WIENS: Sure, and just to share the specific challenge that the farmers are having, if you are familiar with the case Dorman v. G.M., the part that you get from the factory -- let's say you get a new transmission or a new ECU. It comes without firmware, and so you need to move your copy of the firmware from your existing ECU onto the new part.

And in the ag industry, these are called payload files. The payloads are the firmware. And a circumvention would be exactly what Dorman did in the G.M. case, where you basically move your copy onto the new one.

What the branded kind of the John Deere reps are doing is they're downloading from John Deere's servers a copy of that firmware and loading it onto the device, so just to clarify the farm situation.

Did you --

MR. BARTELT: Oh, no, I just wanted to see -- I was going to turn to Ms. Sheehan, but if you had one more point you wanted to make, we can do that, and
then --

MR. WIENS: Sure.

MR. BARTELT: move on.

MR. WIENS: Well, yeah, and real fast to talk about the auto industry and what's different, because things have changed so much in the last three years in the car world. Three years ago, when we were talking about circumventing -- or the telematic system and the infotainment system, the state was new cars were coming with Blu-ray drives, right?

I was looking this morning. I couldn't find a single new 2021 model year car that comes with a Blu-ray drive. I think that kind of -- like that has passed. And instead, the media is played from your phone, so I take my phone, and I use Apple CarPlay or I use Android Auto, and so the media -- any sort of concern that we have about piracy is centered around these mobile devices and not actually the car itself. So media has moved off of cars.

And then in the other direction, all of the data that you need for repair has moved into the telematic system, has moved into telematics. And that's where you've seen the most recent Massachusetts auto Right to Repair bill, which was introduced because of all of the problems that the mechanics are
having because the data, instead of being passed to
the service technician via the wired port, it's coming
wirelessly.

And as we talked about three years ago, that
wireless telematic system and the infotainment system
on the car is one and the same. It's the same ECU.

MR. BARTELT: Okay. Thank you, Mr. Wiens.

Ms. Sheehan?

MS. SHEEHAN: I'd like to reiterate what
Kyle said. So in 2018, the Register passed on the
opportunity to recommend an exemption for vehicle
telematic systems. But as we're seeing these
telematic systems are increasingly ubiquitous.

If I have a Tesla right now, and I need to
repair it, the current exemption from 2018 doesn't
cover my repair because my mechanic would need access
to the telematic system in order to complete that
repair.

And again, as Kyle said the politics are
changing around this, and we've seen a ballot
initiative pass in Massachusetts with over 75 percent
of people who are recognizing the need to access these
wireless telematic systems and the need for their
independent repair providers to be able to access
those wireless telematic systems. So that's one area
where we'd like to see this exemption expanded.

In addition, we'd like to see the removal of
the kind of duplicate liability for violating another
law. So to the extent that the current language of
the exemption imposes an obligation to follow other
laws, we think that compounds liability in a way that
really doesn't add any extra deterrent effect and is
just kind of hammering on, and adding complexity and
risk of litigation, to people using the exemption.

We'd be open to phrasing that in a different
way that, again clarified that the exemption is not
authorizing or making lawful any activity that
violates another law, but this compounding of
liability we think is an extra burden on the people
who benefit from the exemption that should be trimmed.

MR. BARTELT: Okay. Thank you, Ms. Sheehan, and I'm actually going to ask Mr. Rosenbaum about that
in a second, but I wanted to turn to Mr. Cheney first, because he had his hand raised.

Please go ahead, Mr. Cheney.

MR. CHENEY: Thank you.

And my line of questions actually followed
the same line of reasoning here, because you brought
that up originally, and so I just wanted to pivot just
a little bit on what Ms. Sheehan said.
And so this has come up a little bit in other exemption discussions. In Class 13, Rapid7 proposed some language, and this language has been talked about in other exceptions, possibly to replace "this does not violate any other applicable law."

So let me read what they proposed, and this has been endorsed in that space, good faith security research, by the Department of Justice and others, so let me read what they propose here and just sort of substitute the words in.

In this case, it says, "Good faith security research that qualifies for the exemption under Paragraph A," whatever we write there, "may nevertheless incur liability under other applicable laws, including, without limitation," and in this case, they list Computer Fraud and Abuse Act, et cetera.

So would that be acceptable modification language, Ms. Sheehan and others, both opponents and proponents, in sort of finding a middle ground on that change? Just if you think.

MS. SHEEHAN: I think that would absolutely be acceptable.

MR. BARTELT: Okay. And, Mr. Rosenbaum, go ahead.

Heritage Reporting Corporation
(202) 628-4888
MS. SMITH: Can I --

MR. BARTELT: Oh, go ahead, Regan.

MS. SMITH: Just a second, Mr. Bartelt.

Yeah. I might have missed it, but either I need to clarify for myself what was said, or we need to clarify the record.

I think in 2018, the Register recommended removing the limitation that excluded access to telematics and made it when it is necessary for repair, so I think I'm still a little confused as to what the proposed scope of the change is, because it seems like some of what you're saying about modern cars is already being addressed. If I'm missing something, let --

MS. SHEEHAN: Sorry, Ms. Smith. You said the 2018 exemption covers access to wireless telematic systems for the purpose of repair?

MS. SMITH: That's right. We considered that, and we granted that adjustment and removed the limitation that had been put in place in 2015. So it's broader. That was a change made in 2018. That is --

MS. SHEEHAN: Then I must --

MS. SMITH: -- we are recommending renewal for. That's fine. I just -- glad that we just --
we're making progress and getting things clear. Okay.

Mr. Bartelt?

MR. BARTELT: Sure.

I wanted to -- I guess that my question was similar to Mr. Cheney's, so I was going to ask Mr. Rosenbaum about this sort of -- the removal of the language concerning -- or modification of the language concerning that the exemption not violate any other applicable law and any concerns that he might have about that. And he may have wanted to respond to some of the other comments that were made.

Please go ahead, Mr. Rosenbaum.

MR. ROSENBAUM: Yeah, thank you. Thank you very much. I'll start with what I call the illegality limitation, which is the limitation in the existing vehicle exemption that circumvention does not constitute a violation of applicable law. We would not support any relaxation of that. That is a critical limitation.

The 2015 record was replete with information on automotive vehicle software which controls complex aspects of motor vehicle performance and ensures that vehicles meet stringent regulatory standards for safety, fuel efficiency, and emissions control.

You know, the Copyright Office rightly
recognized this in crafting the vehicle exemption in
the 2015 rulemaking, that the automotive industry is
highly regulated, and so they took into account --
rejecting arguments that these risks were unrelated to
copyright concerns, finding that these were of
overriding importance, basing it on letters received
from the EPA, the Department of Transportation, and
California's Air Resources Board finding the
illegality limitation was necessary.

There's nothing in this record that would
mitigate anything that was provided in 2015.
Expanding the exemption would risk public safety and
cause environmental harms, potentially. So again, we
would not support any relaxation of the illegality
limitation.

Sort of getting to the -- you know, I don't
want to get too much into telematics, since, as Regan
pointed out, that was at issue in 2018.

You can see from our 2018 filing that
telematics, all -- again, back to the MOU, but not
just the MOU, state and federal regulations going back
to 2002 requires automobile manufacturers to provide
repair and diagnostic tools and information to
independent repair shops to the same extent as
dealers.
And whether that information is in telematics or not, that information needs to be provided to the independent repair shops. So it's just simply not an issue. And our view here is that the existing language of the exemption does not cover third-party repair, commercial repair, shops.

And to the extent that there's any suggestion that there should be some affirmative language that would cover them, we would oppose that, and we don't believe there's anything in this record that would support that.

You know, as we've said, and you can look at our filing, again, the MOU obviates any need for that sort of thing. Anyone who needs their car repaired is able to get it repaired. There's nothing on the record suggesting otherwise. And of course, the statutory framework doesn't permit it. So I don't want to get -- I could go into depth on each of those things, even further.

I guess one thing that was a reply -- and this might be my only opportunity to reply to this -- there was a reply from the Auto Care Association on the MOU that was extremely misleading, suggesting that it does not apply to all users and to all independent repair shops. In fact, it does. You know, under the
MOU, manufacturers make the tools and information available to everyone.

And also, there's a provision in the MOU requiring standardized tools so it's not -- the suggestion was that independent repair shops are forced to buy tools from the manufacturer. That is not the case.

And finally the issue of whether they're prohibitively expensive, which we've heard -- the MOU includes provisions that these tools and information are provided on fair and reasonable terms, and this language goes back to regulatory language back to 2002.

There's never been any dispute brought under either regulation or the MOU suggesting that these are not being provided on fair and reasonable terms. You know, and this just simply isn't the forum to litigate that. You know, there should be the MOU. There are other places if there's a dispute.

So with that I appreciate the opportunity to say my piece. Thank you.

MS. SMITH: Thank you, Mr. Rosenbaum. And thank you for your patience, because I understand on the road map, this came to the end, so we're glad you're here, and we know this is a tremendous amount
of issues. We've got the benefit of your briefing.

We also went a little bit over. I think
this is sort of last call for comments, and people
could try to keep it a little bit short, because we've
got a lot here.

But, Ms. Gagliano?

MS. GAGLIANO: Sure. So first, I wanted to
share one quick point in response to what Mr.
Rosenbaum was saying about the safety and emissions
regulations.

EFF actually sent FOIA requests to the EPA
and Department of Transportation, and their responses
confirmed that they have never actually used 1201 or
relied on it in any way to help enforce these
standards.

They aren't actually making use of it, which
I think reinforces Ms. Sheehan's point that it's
really superfluous, second layer, and draw attention
to the distinction only the Copyright Office can grant
exemptions. FDA and then --

MS. SMITH: Can I ask you --

MS. GAGLIANO: Okay.

MS. SMITH: -- is that response in the
record? It might be, but have you provided that to
us?

Heritage Reporting Corporation
(202) 628-4888
MS. GAGLIANO: I don't think that we have.

MS. SMITH: Okay. Thanks.

MS. GAGLIANO: Probably not. And then in terms of just --

MS. SMITH: Okay, thank you.

MS. GAGLIANO: -- the closing comment quickly is that on modification, which was really the focus of our request, especially want to reiterate that the question is not whether there are infringing modifications that are prevented by TPMs in 1201, but that the question is whether there are non-infringing modifications that are being adversely affected and prevented by 1201. And we have shown that there are.

And these include modifications that promote the creation of new copyrighted works, including new photographic works by modifying digital cameras, new software works by building on what's come before. And I think the recent decision in Google v. Oracle really reinforces the importance and transformative nature of that purpose, the purpose of expanding the utility of software. So I think that is the point that I wanted to leave you all with.

MS. SMITH: Thank you.

Mr. McHargue?

MR. McHARGUE: Well, I appreciate this
conversation. Unfortunately, the ag exemption isn't quite the same as the auto sector, because we do not have a national MOU, and so we still are constrained by a lot of necessary tools having to go back to the original OEM to get that service.

And we desperately need access to those third-party experts on a broad scale, because, again, we don't have an MOU nationally that is kind of putting in place these standards, nor do we have a dispute arena that we can go back and we can say, "We need to be playing together in a certain form or fashion."

But again, thank you for allowing me to be here. I appreciate the work of the Office.

MS. SMITH: Thank you. We appreciate you coming and bringing your perspective, too.

Ms. Sheehan, I saw you sort of nodding during the last comment. If you wanted at all to comment on -- obviously, this rulemaking is limited to the anti-circumvention provision and not the anti-trafficking provision. But that was a question that just sparked me about the ag market.

MS. SHEEHAN: Absolutely. We completely agree with the Office's interpretation of the statute, that Congress, in using the term "user," deliberately
chose not to use the term "owner." And therefore, the exemption is not limited to the owner of the device. It's to anyone who is using the device, including potentially a third-party provider of repair services. And so we fully endorse that, and we would request that permission for third-party assistance extend to all exempted categories.

I just wanted to say a couple of things, one in response to Mr. Rosenbaum and one kind of wrapping up our testimony as a whole, and just say that Mr. Rosenbaum put a lot of weight on the existence of alternatives and the existence of branded repair services.

But this office has never found the existence of alternatives sufficient to defeat an exemption where adverse impact exists. And to do so in this case would, as I've said before in this hearing, give copyright holders a new right that they don't have under the Copyright Act, that they don't have under section 106, which is the right to control the market for repair services.

And you know, we know from Chamberlain that that right does not exist. And so I would argue that even though there might be alternatives, in some cases those alternatives are going to be inadequate. In
some cases, they might not exist at all. But even
when they are there, that itself is not determinative.

And then I just want to close by just
summing up whether we're talking about medical
devices, or tractors, or cars, or software-enabled
litter boxes, we're essentially talking about the same
functional software, the same copyright analysis, the
same purpose of the use.

And so in our perspective, the proper scope
for an exemption here is an exemption for the repair
of all software-enabled devices. We just want to fix
stuff.

MS. SMITH: Thank you.

Mr. Wiens?

MR. WIENS: Thank you. One thing I thought
that I would mention is -- you think about how to
craft this -- is John Deere's Service ADVISOR is a
subscription repair service. And in the existing
rule, you separated out subscription services. I
think that it was thinking of Spotify or SiriusXM, or
something.

But imagine a world where like OnStar, you
may be paying the manufacturer for a repair service,
and that may implicate whatever decision that you
make. Thank you very much.
MS. SMITH: Okay. Thank you.

And, Mr. Williams, I think you're usually the last to be introduced as a "W," so it's kind of fitting for you to get the last word so go ahead.

MR. WILLIAMS: Yeah, thank you. Just quickly, on the question that's mostly been related to medical devices and vehicles but is coming up as a general proposition of how far the Office should go with respect to third-party services, I just wanted to reemphasize that it's extremely important to my clients that the Office remain cognizant of that line between trafficking and 1201(a)(1). And so I just wanted to reiterate that.

And then a couple of points that Ms. Sheehan made a couple of times that I did want to respond to. One is that she said "alternatives to circumvention has never been a basis to deny a proposal." That's not correct. It's consistently been a basis to deny proposals. And where there are alternatives to circumvention, exemptions should not be granted.

Another point was just that -- and I know the Office staff is aware of this, but I wanted to get it on the record, because it came up a few times. I believe she said that Chamberlain has never been challenged. Chamberlain is wrong. The Office has
said it's wrong. MDY says it's wrong. Chamberlain is not good law at this point, in my view, and we shouldn't be granting exemptions -- or you should not be, excuse me, based on the reasoning in Chamberlain.

There is a new exclusive right. It's the right of access. It's in 1201(a)(1). And it's a good thing. Thank you.

MS. SMITH: All right.

Thank you, everybody. Thank you for your patience and willingness to go over as we help develop the record through this discussion. If we think we need anything further, we'll be issuing letters for post-hearing comments. And there will also be opportunity to participate through ex parte meetings subject to transparency disclosures once we initiate that.

So thanks again, and then tomorrow will be our last day of hearings, in which we will address proposed classes for jail-breaking and unlocking. Thank you. Bye bye.

(Whereupon, at 1:08 p.m., the meeting in the above-entitled matter was adjourned, to reconvene at 10:30 a.m. April 21, 2021, the following day.)

//

//

Heritage Reporting Corporation
(202) 628-4888
REPORTER'S CERTIFICATE

CASE TITLE: Copyright Office Section 1201 Hearing
HEARING DATE: April 20, 2021
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 Library of Congress.

Date: April 20, 2021

John Gillen
Official Reporter
Heritage Reporting Corporation
Suite 206
1220 L Street, N.W.
Washington, D.C. 20005-4018
Section 1201 Rulemaking Hearing
April 20, 2021

1. **Section 1201 Rulemaking Hearing**
   - **April 20, 2021**

2. **Citation**
   - **27 USC § 761:24**
   - **761:29**
   - **761:21**
   - **761:20**
   - **761:19**
   - **761:18**
   - **761:17**
   - **761:16**
   - **761:15**
   - **761:13**
   - **761:12**
   - **761:11**
   - **761:10**

3. **Key Words**
   - **causation**
   - **certification**
   - **challenges**
   - **change**
   - **careful**
   - **centered**
   - **carving**
   - **cars**
   - **carry**
   - **care**
   - **chance**
   - **Chief**
   - **China**
   - **chip**
   - **choose**
   - **circle**
   - **Circuit**
   - **circumstances**
   - **circumvent**
   - **crow**
   - **Cathy**
   - **causal**
   - **causation**
   - **circuit**
   - **certain**
   - **centered**
   - **centers**
   - **Central**

4. **Table of Contents**
   - **I.** Introduction
   - **II.** Background
   - **III.** Issues
   - **IV.** Analysis
   - **V.** Conclusion

5. **I. Introduction**
   - **A.** Overview of Section 1201
   - **B.** Purpose of the Rulemaking
   - **C.** Significance of the Rule

6. **II. Background**
   - **A.** Historical Context
   - **B.** Regulatory Framework
   - **C.** Related Legal Principles

7. **III. Issues**
   - **A.** Key Points
   - **B.** Arguments for and Against
   - **C.** Evidence Presented

8. **IV. Analysis**
   - **A.** Analysis of Key Points
   - **B.** Comparative Analysis
   - **C.** Conclusion

9. **V. Conclusion**
   - **A.** Summary
   - **B.** Implications for Future
   - **C.** Recommendations

10. **Appendix**
    - **A.** Supporting Documents
    - **B.** Additional Resources

---

**Heritage Reporting Corporation**
(202) 628-4888

Sheet 3 cards - constrained
Section 1201 Rulemaking Hearing
April 20, 2021

Heritage Reporting Corporation
(202) 628-4888