LIBRARY OF CONGRESS

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

Pages: 851 through 966

Place: Washington, D.C.

Date: April 21, 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.

Wednesday,
April 21, 2021

The parties met remotely, pursuant to notice, at 10:32 a.m.

PARTICIPANTS:

Government Representatives:

REGAN SMITH, General Counsel of the U.S. Copyright Office
KEVIN AMER, U.S. Copyright Office
STACY CHENEY, National Telecommunications and Information Office
MARK GRAY, U.S. Copyright Office
BRAD GREENBERG, U.S. Copyright Office
MELINDA KERN, U.S. Copyright Office
LUIS ZAMBRANO RAMOS, National Telecommunications and Information Administration

Panelists:

MICHAEL AYERS, DVD CCA and AACS LA
JAY FREEMAN, SaurikIT
JONATHAN KAUFMAN, Stanford Law School Juelsgaard Intellectual Property and Innovation Clinic
PHIL MALONE, Stanford Law School Juelsgaard Intellectual Property and Innovation Clinic
MORGAN REED, ACT | The App Association
MITCH STOLTZ, Electronic Frontier Foundation
J. MATTHEW WILLIAMS, Joint Creators and Copyright Owners
AARON WILLIAMSON, Software Freedom Conservancy

Also Present:

BRANDON BUTLER
WILLIE CADE
GAY GORDON-BYRNE
SINA KHANIFAR
KEVIN O'REILLY
LETICIA REYNOLDS
PAUL ROBERTS
MARK SCHAFFER
JESSE SPIEGEL

P R O C E E D I N G S

(10:32 a.m.)

MS. SMITH: Good morning, everyone. We're going to get started. Can everyone who's a panelist please turn on your video. Do we have Mr. Ayers?

MR. AYERS: Hi.

MS. SMITH: Oh, yep, okay. I think we have everyone then. No. Mr. Reed?

MR. REED: Hello.

MS. SMITH: I feel like I'm watching the Hollywood Squares. Hello. Okay. Well, good morning, everyone. We're going to get started with the last day of the Section 1201 hearings. This is day seven, and we are looking at Class 11, which concerns proposed adjustments to exemptions in connection with uses of jailbreaking.

My name is Regan Smith, General Counsel for the Copyright Office. I think many who are participating or who are watching are familiar with our procedures, but I think we'll start by going over the rules just in case. So we are being recorded and we will be live-streamed and a written transcript will be made available of these proceedings. This session is going to be moderated by attorneys from the government, so we'll ask questions. And if you wish

to participate, you can use maybe the Zoom "Raise Hand" feature, we found has been the most reliable. But, if for some reason it's not working for you, you can raise your hand in real life. Anyone watching or participating can use the chat or Q&A function if there's technical difficulties, and someone from the Copyright Office will reach out to assist you.

At the end of today's hearing, which is 1:45 Eastern, we're going to have what we're calling an audience participation session. So there is still time to sign up if anyone wishes to contribute their thoughts to any of the classes in this rulemaking, and we're asking that you limit any comments to about three minutes. Again, someone from the Copyright Office will reach out if you put in a request and provide details with how to participate for that. Please try to mute yourself when you're not speaking. I know we are all pros at this by now, but that will help the court reporter, and making sure not to talk over others will also assist that.

So, to start, I'm going to ask my colleagues in the Copyright Office to introduce themselves, so Mr. Amer, Ms. Kern, and then Mr. Greenberg.

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

MS. KERN: Good morning. Melinda Kern, Ringer Fellow.

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

MS. SMITH: Thank you. Mr. Zambrano Ramos, could you please introduce yourself?

MR. ZAMBRANO RAMOS: Thank you. This is Luis Zambrano Ramos. I'm a policy analyst in NTIA's Office of Policy Analysis and Development within the Department of Commerce. Thank you.

MS. SMITH: Thank you. So now we'll go around and we'll introduce the panelists, first those who are supporting proposed adjustments. So, Mr. Freeman, Mr. Stoltz, and Mr. Williamson, if you could just introduce yourself and identify the organization that you are here representing if you are representing an organization.

MR. FREEMAN: My name is Jay Freeman. I am here for SaurikIT, which is my company. We developed Cydia, which is the alternative to the app store for Jailbrook and iWest devices, and have been here at years prior, so I recognize many of your charming faces today. I also am a member of the group Exploiteers, which developed the jailbreak for the Google TV. I did not myself participate in that work

directly, but I was with everyone as they were working on it, cheering them along, and saw the process of it. I also am now in charge of technology at a company called Orchid Labs, which is building a -- which raised, in fact, nearly $50 million to raise a private placement for the Internet built on top of the existing Internet that is free of censorship and surveillance and, therefore, has a strong interest in network routing devices.

MR. STOLTZ: Hi, I'm Mitch Stoltz. I am a senior staff attorney with the Electronic Frontier Foundation.

MS. SMITH: Mr. Williamson, it looks like you might be trying to unmute, but just in case -- all right. We'll come back then to Mr. Williamson, who is with the Software Freedom Conservancy. Are you able to unmute or no? All right. So maybe someone on -- we'll either come back to you, but if you need help, please message to the team.

So now there's three panelists who are participating in opposition to some of the proposed changes. So please, Mr. Ayers, Mr. Reed, and Mr. Williams, could you introduce yourself? Oh, now we have two Mr. Williamsons, so we'll go back to you at the end if we can.

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

MR. REED: And this is Morgan Reed and I'm the President of the App Association.

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

MS. SMITH: Okay, thank you. Mr. Williamson, do you want to see if that fixed the issues?

MR. WILLIAMSON: My apologies. Zoom froze at an inopportune time. My name is Aaron Williamson. I'm an independent attorney here representing the Software Freedom Conservancy.

MS. SMITH: Okay, great. So we have various questions teed up, but I wanted to start by making sure that we have the right scope of the two requests. So, as the Copyright Office understands it, the Software Freedom Conservancy is looking for an exemption to permit circumvention on firmware and routers and other networking devices to enable the installation of alternative firmware, is that correct,

Mr. Williamson?

MR. WILLIAMSON: That's correct.

MS. SMITH: Okay, thank you. And then, with respect to EFF, I think, Mr. Stoltz, I wanted to make sure I understand the scope of the request to modify the smart television exemption because it seems like the language changed a little bit from the petition to the reply, and some of the written comments, which we've all read, indicate that the exemption is not intending to encompass DVD players, Blu-ray players, or set-top boxes or gaming consoles. But, you know, do you want to in your own words just sort of describe what you're looking for and why it -- if there's anything you can say about the changes in the written submission from the initial to the reply comment.

MR. STOLTZ: Absolutely. We intended no change. The exemption is not meant to cover DVD or Blu-ray players or game consoles. The exemption as we conceived it was, you know, sort of built around the paradigmatic examples that we gave in our initial position, the Roku, the Amazon Fire devices, and the Apple TV and similar devices. So, in our reply, we discussed some sort of ways in which we might cabin that language a little bit more, but the intent is the same.

MS. SMITH: Okay. And, I mean, are you willing to cabin that language by excluding those devices that I mentioned? I think what I understood in the reply was that EFF was saying this encompasses video streaming devices, and so I think a corollary, if that's the right understanding, is whether that phrase is descriptive enough to keep in what you mean to keep in and keep out where some of the objections have been raised.

MR. STOLTZ: Yes, that is the intent. As we wrote in our reply, but I can mention it here, I think what we're -- the way we propose this is devices that run a variety of applications with a primary purpose of streaming video from the public Internet for display on a TV screen and not integrated into other types of devices, such as video disc players or game consoles.

MS. SMITH: Thank you. Do any -- does anyone else want to comment as to whether that clarification is helpful? Or -- Mr. Ayers?

MR. AYERS: Thank you. Yeah, I certainly appreciate the clarification that there's no intent to cover DVD players, Blu-ray players, and gaming consoles, which include DVD and Blu-ray drives. I'm still -- because, certainly, as originally proposed,

the language covered quite a -- even if not intended, kind of a very broad swath of devices, anything that provided a software application on a screen, which includes DVD and Blu-ray playback. Those are enabled by software on devices even if they're not doing Internet streaming.

I remain concerned, though, about the primary purpose test, especially in the context of devices with multiple functions, like a game console or like a Blu-ray player that has streaming ability, is what exactly is the primary purpose. How is that going to be determined? And what happens if that primary purpose arguably evolves over time? A device with physical playback capability may have been -- may sort of in the public mind be considered primarily for that physical media, but over time, as streaming becomes more popular in the public mind, depending on whose mind we're looking at here, it may be determined that this is a multifunction or it's a streaming device that just happens to play physical discs. So I do remain concerned about the primary purpose test.

MS. SMITH: Thank you. Do you have a sense whether that is likely to happen in the next three years, Mr. Amers -- Ayers, with respect to the devices you're here to discuss?

MR. AYERS: I don't know. We can certainly think about that and get back to you. I think we already have the situation where a lot of these devices are considered multipurpose. They're offered as entertainment devices, not necessarily specifically as a Blu-ray player. So I think we already have an element of that to consider today.

MS. SMITH: Okay, thank you. I see, Mr. Stoltz, that you've indicated you wanted to respond, but I think it might make sense to let Mr. Williams comment first and then you could respond too. Okay, go ahead, Mr. Williams.

MR. WILLIAMS: Thank you. Yeah, I have similar concerns to Mr. Ayers. It is quite helpful, of course, to acknowledge that consoles and Blu-ray players and cable and satellite set-top boxes should not be covered, but the language that's put forward in the reply just doesn't get there, even setting aside whether there's an issue with jailbreaking, so to speak, of these other plug-in-type streaming devices. I mean, for some users of a Blu-ray player, the primary reason they have it is they have an older television and they want to watch Netflix or they want to watch Hulu and they use the Blu-ray player to access those applications because they don't have a

smart TV. And so they may play Blu-rays as well, but their primary purpose for that device might be for streaming content.

And, for video game consoles, the language also doesn't work for me because, if you're talking about a switch, for example, it doesn't have a disc drive. There's no optical drive. The way the wording is put forward, it talks about a device that's designed to display applications on a screen, including streaming video. I mean, that it's -- the language is just too broad and could sweep in consoles.

And so it would be great, of course, to say in some regulation or in the recommendation these things are definitely not covered. That would give us some comfort. But, as the marketplace develops, as these exemptions get renewed over time or even within the next three years, the way things are progressing, the language has to be really precise. And I don't know how to fix it for them. I've thought about it, but I -- it's a hard line to draw and I don't think they've been able to draw it so far, and so we're still very uncomfortable with it.

MS. SMITH: Thank you, Mr. Williams. Mr. Stoltz, would you like to respond to those comments?

MR. STOLTZ: Yes. So these are three-year exemptions and they're based on the record before us and not the speculative record of what might happen in three years, which nobody has a crystal ball and nobody has proposed. What we have right now is really evident from looking at the website of any major electronics retailer, and all of them, the major ones that we've looked at, put streaming players or streaming boxes in their own category, separate from DVD and Blu-ray players, separate from game consoles. Now we have proposed to explicitly exclude those, regardless of the primary purpose of the device, to specifically exclude devices that are integrated with either a disc player or a game console. The -- Yeah, I'll leave it at there for now. I was just going to say the other -- no, I'll leave it there for now. Thank you.

MS. SMITH: Okay. Can I ask you one follow-up question, which is it seems like from the initial petition to the reply, the word "television" has been substituted for "screen" and could you address what was motivating that change? So the existing regulatory exemption was for a so-called smart television, you know, which was based on the record in 2015, and we want to understand what's motivating the

proposed language change here.

MR. STOLS: Just that it could be a computer monitor.

MS. SMITH: And in your understanding, the same type of devices would connect to the computer monitor as to the television, is that right, or --

MR. STOLS: Yes. Anything that basically could take an HDMI input.

MS. SMITH: Okay, thank you. Now I'm going to pass the questioning to my colleague, Mr. Amer.

MR. AMER: Thank you. So just to sort of continue on this line, I'm wondering -- I think I'll start with the opponents. So assuming it's possible to define the exemption in such a way that is clear that, you know, it excludes things like video game consoles and Blu-ray players, and I'm not saying it necessarily is possible to do that, but if it's possible to define an exemption that applies to -- that is limited to sort of video streaming devices of the type that the petitioners have described, do you have particular concerns about the effect on the market if the exemption were to cover those types of devices? Mr. Williams?

MR. WILLIAMS: Yeah, thank you. So we do still have concerns and I think they're substantial

concerns. Once these devices are altered, there's a lot of applications out there that infringe on my clients' works. And when the devices are tied to a store, let's say, of the provider of the device, that provider has some control, some ability to remove applications once there are problems identified, and once they are hacked, that might go away.

And so we do have concerns about that. We tried to lay them out in our comments. I recognize that they're similar to the concerns we've raised for multiple cycles with respect to other devices and that the Office has ultimately decided to grant those proposals. But we wanted to make sure it was clear we do have concerns and there's a lot of infringement out there. It's well documented in government documents, as well as court cases, and so we have a lot of concerns about it.

MR. AMER: Thank you. Mr. Stoltz?

MR. STOLTZ: Yeah, thank you. So I think we can all acknowledge right now that infringement exists, infringing applications exist. But I wanted to point out something else that's existed for 11 years now, and that's that we -- there have been exemptions covering jailbreaking of personal electronic devices for 11 years now, and they're

devices that are in many ways very similar to what we're proposing here. Most significantly, we've now had an exception for, I believe it's six years, for smart TVs. What we're proposing is a slightly expanded class, a narrow expansion that covers not only smart TVs where the hardware is integrated into the display but where the streaming hardware is separated out into a box or stick but otherwise functionally equivalent.

And here's what we know about those: They have not significantly contributed to infringement, as the Office has recognized in past cycles, and that's the relevant question, right? The relevant question is not, do there exist apps that assist infringements? We know that those exist. The question is, does granting this exception so that law-abiding people can add and remove functionality from the devices that they own contributes in any material way to infringement? And there is no evidence of that in the record.

MR. AMER: Thank you. Mr. Reed?

MR. REED: I think there are three parts of this. The first is that Mr. Stoltz was using the term "no significant increase in infringement." That's not the standard that the Copyright Office uses.

The second part of this that's worth noting is we're not in a situation where there isn't an alternative. There are plenty of alternatives. You can throw Linux on a USB stick and plug it into your TV and there's plenty of open source streaming capability that you can do without hacking a device that someone else has put copyrighted material on that they want to protect and profit off of. So the market hasn't failed. There is the availability of this technology widely available in other places.

And then the third point, and I think we've kind of danced around it, is, Kevin, you kind of got to it, which is, at a certain point, it's becoming indistinguishable. Anything with a USB port in it is essentially capable of running what would have amounted to a super computer 20 years ago. So the idea of transporting it from the TV to the stick is not a minor expansion. It's an enormous expansion because it's essentially the ability to change anything that plugs into your screen and jailbreak it.

So I think that basically that's not the standard. We haven't met -- it's a much broader expansion than to describe it as merely going from something installed to something not. And I think right now we're not limited in the market.

And just very quickly to go back to an earlier point, Mr. Stoltz was saying, well, they divide these Blu-ray players from boxes that stream. While he was talking, I just did a quick Google search. So the Sony S3700 is $78 with Wi-Fi and USB installed and its top picture that it shows is a Blu-ray player. You see the picture of the Blu-ray player. The next screen is Netflix. So Sony is marketing these products, and I've got a bunch of them up here, with they'll play your disc, but they'll stream your Netflix. So I think this idea that there's some bright wall of separation between the box that plays the disc and the box that streams your content is no longer the reality we live in. And you can buy it for 78 bucks. So it's not even a -- it's not even a price competition issue. Thank you.

MS. SMITH: Can I ask one question? It sounds like you're disagreeing, Mr. Reed, with Mr. Stoltz's characterization of the expansion to devices that are otherwise functionally equivalent to the current exemption for smart televisions, where the functionality is embedded in the television.

MR. REED: Right.

MS. SMITH: Can you just elaborate upon what you see as where those differences are from the

technological perspective or other functional perspectives based on how they define it?

MR. REED: Well, as I said, you hit on it earlier, Regan, when you were talking about screen versus TV and how do we define television. The reality is, is that anything with a screen that I can plug a USB port into or an HDMI -- HDMI has its own separate capabilities -- but, if I'm plugging a USB stick into it or have access to its display capabilities through that, I'm essentially, the world is my oyster. I can do almost anything I'd want to do.

So I think that limiting it or trying to create this artificial construct of its preponderance of its capability is to stream and we've moved it from inside the TV to a stick outside the TV, once you move it outside that TV and you've moved into that format, you've really opened the door to -- I can't even -- basically, it's the Internet of things, right? It's a door-opener for everything. So it's not limited because it's not just something that came inside of a TV and we're modifying it.

Earlier, Matt gave a great example where he said, you know, you have an older TV and you want to plug in your Blu-ray box and that's how you're going

to get your Netflix. So I think that if you think about what that capability is going on, now instead of a Blu-ray box, I'm doing a Kodi Box. I can do almost anything a computer would want to do in that case. So it isn't limited because, once I'm plugged in, I have access to pretty much everything I need, and it's much closer to plugging in a full computer. In fact, arguably, it is.

MR. STOLTZ: Could I? If I could respond to that?

MR. AMER: Sure, sure.

MR. STOLTZ: I think -- I would hope that we actually talk about the definition that we proposed and refined because it is not, in fact, that broad and it is also, as we've said, focused on the paradigmatic examples that we've given, the Amazon Fire devices, the Apple TV, the Roku. Beyond that, again -- so Mr. Reed mentioned Kodi. Kodi is a lawful product and one can already run Kodi while taking advantage of the existing exemptions on a smart phone, on a tablet, on various other devices. That's -- that is something to be encouraged.

MR. REED: If I could --

MR. AMER: Okay. Well, wait, let me just ask another question here and I think it relates to

the same themes. So you can hopefully address --

MR. REED: Yeah.

MR. AMER: -- your previous comments can address this. So I know that the opponents cited a number of cases, for example, where they talked about various enforcement actions that copyright owners have pursued against manufacturers of devices, some of which I guess allow -- involve Kodi, others I guess have pre-loaded content. I know the Joint Creators cited the Chip Box case and the Dragon Media case. I wonder if you could talk about how similar or different a jailbroken streaming device is compared to the devices in those cases. Is the dividing line -- is the relevant dividing line based on whether content is pre-loaded on the device, or should that not be as relevant?

MR. STOLTZ: The relevant dividing line comes from the law and that law says an open, fully configurable media player, which one can think of like a web browser is a lawful product. A player that is preconfigured to connect to infringing streams is a form of inducement of copyright infringement. So those cases that the MPA cited in their papers concerned, as I understand it, devices that were preconfigured to connect with infringing streams. A

jailbroken Fire Stick or Apple TV is not that. It is not that until software is added to it that has those characteristics. Again, the same thing applies on a cell phone, on a smart phone. The same thing applies on a tablet. But jailbreaking itself, but for the prohibition of Section 1201(a), is still a lawful product. That's the difference.

MR. AMER: Okay.

MR. REED: --

MR. AMER: Mr. Freeman, I know you've been waiting, so let me go to you first, and then we can come back to Mr. Reed.

MR. FREEMAN: Thank you. So there's a clarification that I think is important to make here and this is from the perspective of somebody who is maybe deeply integrated with the software stacks that we're using and saying the technology that we're actually working with here. So we often are using the term "jailbreaking." And we're using it fairly loosely. And we all come here every three years and we talk about jailbreak a lot. And we -- I think we all have a general idea of what it is. But there are specific nuances that are very important that related to the written comments from Mr. Reed, as well as the Joint Copyright, and now the spoken commentary, both

from Mr. Reed and from Mr. Stoltz, with relation to what functionality you would need to jailbreak a device for versus not.

And so I'm going to take one specific example that is kind of threaded through a lot of the different comments here and that is relating to Kodi and a Fire Stick. This is something that in Mr. Reed's comments, there's specific mention of there's a website you can find, troypoint.com, that talks about how you jailbreak a Fire Stick and you install Kodi on it. And there was even commentary here about some of the discussion even from Mr. Stoltz, talking about applications you might load onto a jailbroken device. The vast majority, if not, almost all of the devices that we're talking about in this class of devices that are designed to show applications on the screen are user extensible in the form of applications that they're allowed to run and, in fact, are user extensible by the end user of the applications they're allowed to run, and they are not designed to prevent people from writing an application, even one that is primarily designed to infringe and running it on the device without any circumvention of any technological measure.

In particular, I will pick on the Fire

Stick. That website, troypoint.com, has no clue what the term "jailbreak" means. They use the term "jailbreak" continually to mean taking a third-party application and loading it on the device using the supported feature of going into the settings panel and saying, I would like to be able to load a third-party application onto this device.

And so I feel like we need to really be focusing our attention on what is the actual infringement that we're talking about, what is the actual infringement that is possible. And I'm kind of under the maybe naive impression that the idea is that while there's copywritten music and movies that are moving to this device that people are going to jailbreak it and then rip that content off the device. And that is not what Kodi is doing and that's not what any of these other products are doing. I don't know if I've heard of anybody who are waiting on jailbreaks for these devices in order to get that content.

Now I see Mr. Reed shaking his head, and I just want to say that I think that the reason why I have that naive impression is that loading a -- and this now ties directly to what Mr. Stoltz had said, loading a third-party application onto a device to add functionality to it is not bypassing the technological

protection measure for purposes of accessing any of the content that is being protected by that technological protection measure and, therefore, seems outside of the scope of the statute that we're discussing. And so all of this discussion about loading third-party applications on the devices seems out of scope for so many reasons that I find that we always end up getting so stuck on this idea of, well, what could you do with the device theoretically, but it doesn't seem relevant. That doesn't come to light.

MR. REED: Right.

MR. AMER: Okay, thank you. So let's go to Mr. Reed and then Mr. Williams, oh, and then Mr. Stoltz quickly, and then I think we're going to move to the next topic.

MR. REED: Well, weirdly enough, I'm going to agree with Mr. Freeman almost entirely on almost all of that from the standpoint of developing a stack and the ability of third-party applications to run on products. That's what my members do. We write applications that run on products.

The difference that we're running into here -- and it was interesting with Mr. Stoltz saying that Kodi Box, the underpinning software, is legal and legitimate, also completely correct. The difference

is we don't have a market failure, number one, and number two, we're now getting wrapped around the axle on the whole platforms debate and discussion, right, so that the purveyors of these products that use TPMs to protect what third-party applications can be installed or how they're installed have some measure of control, and they use copyright appropriately to ensure some level of control over those platforms.

Now this would be a much more interesting discussion if there was literally no other way to put a plug-in device in, but we quite -- we have plenty of open-source USB sticks that are available. So the ability of my members to write applications that run on a Fire Stick, run Apple TV, part of the decision we're making from a market perspective is the advantages of that user interface and the safety and security that a user feels. So degrading it and having a world where the applications are less certain, less for sure -- and, look, Cydia, there's some great stuff on there, to Mr. Freeman's credit. That's a -- there are some wonderful things on that product. But, frankly, most of the users out there on the iPhone are looking for a different experience than is provided. I enjoy some of that stuff, but it's not for everyone.

So the problem that we're seeing, Mr. Amer, is we don't have a market failure, and the ability to load third-party applications are something that the holders of the TPMs want to have some modicum of control over. To Mr. Freeman's point, it's not 100 percent. To Mr. Stoltz's point earlier, bad things do slip through. But what we're talking about here is expanding that exemption when there isn't a clear-cut need for it, and the standard that the Copyright Office needs to use is one where you're needing to create an exemption to fill a hole where something is missing either in the market or the capability, and that's just not the situation that we're seeing. I certainly know my members love putting apps on wherever they can, but we also benefit from some of the platform advantages.

MR. AMER: Okay, thank you. Let's go to Mr. Freeman next, or was that your --

MR. FREEMAN: Sorry, I just had not lowered my hand from earlier.

MR. AMER: Oh, okay. That's fine. Let's go to Mr. Williams and then, Mr. Stoltz, you can respond to both.

MR. WILLIAMS: Thank you. So, on the Kodi Box cases and the similar cases about applications

that are involved in illegal streaming of video, I mean, I want to be clear that I am not personally litigating those cases, so I do want to make sure I'm clear on that because some of these details are important, of course. But my understanding is that in at least some of those cases, Amazon Content Services is a plaintiff. I also understand that at some point in time, because of its association with infringement, Amazon's app store stopped facilitating the downloads of the Kodi application. My understanding is also that Google stopped -- stopped prioritizing search results for Kodi because of its association with infringement. And if you look at the website for Kodi, I think you can kind of make up your own mind on how they market themselves. But there is a real problem there, and the cases are trying to address that problem, and it is only exacerbated by removing the ability of an app store to try to address infringement concerns.

The other point I just wanted to make is that what Mr. Freeman is saying about the ability to install third-party apps on these devices, if true, renders the need for this exemption zero because there are alternatives. And if consumers are looking to do this and they're proactive about it, then they can

already do it, if I'm understanding his point, and why undermine the kind of typical retail setting that most consumers experience by encouraging these devices to be hacked if people who actually are proactively interested in doing this can already do it?

MR. AMER: Okay.

MR. STOLTZ: May I respond?

MR. AMER: Mr. Stoltz, yeah, let's go to you next, and then I take it, Mr. Freeman, did you want to just quickly respond to that last point about -- okay. So, Mr. Stoltz.

MR. STOLTZ: Thank you. I think we should talk a little bit about what the need is. Again, this is in our papers, so I won't belabor it, but -- so one need is with Apple TV. That's a high-end device, a fairly expensive one that does not allow sideloading. People who want to add applications of their choice that were not pre-approved by Apple have to jailbreak, and that's very similar to other devices that run iOS. Other devices, Android-based devices and some other ones, Mr. Freeman is absolutely correct that those allow sideloading.

But there's a few things that you don't get with sideloading. You don't get fundamental access to the device, which means you can't change -- which

means there are aspects of it that can't be changed, so, for example, wanting a different home screen, and that's really important because the manufacturers of these products steer the user towards their own video offerings or the video offerings of trusted partners, and one aspect of and one important reason why people want to have fundamental access to the devices that they own is to choose the video they want to see without being steered. So that's another example.

And I'll give a third, which is making devices compatible with other devices that people happen to own, so the ability to use game controllers that you may have with a streaming device that you have in a way that hasn't been implemented by the manufacturer. Connecting phones or other personal computing devices, allowing them to interact with the streaming device in ways that the manufacturer hasn't already implemented and isn't approved of in the app store.

And then very quickly, so this notion of, well, the app authors or platform maintainers having the ability to use TPMs. That's not what's at stake in this rulemaking. Nothing in Section 1201 affects a manufacturer's ability to use TPMs, particularly because most of -- most users don't jailbreak.

Jailbreaking is a significant minority of users who want expanded capabilities, who have these needs. Another one, by the way, is increasing privacy, say, by running a VPN to control where people's personal information goes. That's something else you can't necessarily do with sideloading. But --

MR. AMER: Let me just -- and I'm sorry to interrupt. Let me just jump in because I want to be mindful of time. So I want to give Mr. Freeman a chance to make his point, and then we do have to turn to the next topic. So, Mr. Freeman.

MR. FREEMAN: Yes. I just wanted to help draw this line that in some sense Mitch is describing here. So the list that Mitch has given is actually interestingly in the document from Joint Copyright. It is like, these uses include, and there's an entry one, adding a web browser to a streaming device, and then I provide a slight separation and then I say I'm selling different home screen saver, controllers, broadcast, TV tuner, a list that continues. And then, at the end of the paragraph, it is stating that these identified uses can be accomplished through devices without access controls with app installations that are readily available in the marketplace, talking the same discussion we're having here.

The line that I think is important to draw is, is that there is a supported set of functionality that applications are allowed to have on these different platforms, and then there is what you're able to do when you have jailbroken the device, and that separation is where we oftentimes talk about the restrictions that Apple has on their -- for example, on their app store, which include the Apple TV. But, ironically, the thing that everyone here is always concerned about, which is building applications like Kodi, is virtually never in the set of restricted things of the companies that are, you know, we talk about as having extremely restricted practices with relation to what you can install on your device. I'm sitting next to an Apple TV that is not jailbroken that's running Kodi. I can't run my Orchid Labs VPN software on it. I'm unable to -- it's got a screen saver that actually started making me feel seasick and I really want to change it. I can't change the screen saver. There's a lot of functionality in the device that I have no ability to change, but, ironically, the only thing that I am easily able to put on it here is I can install Kodi on it without issue because no one is restricting the ability to display things to the screen or use access on the network.

And I really feel like that line needs to be understood because I feel that without understanding that line, we end up in these discussions of thinking that these exemptions are going to enable some large amount of infringement, even ones that I feel are not related to the statute, but it, in fact, doesn't. Those infringement possibilities were always here. The thing that you're limiting us from being able to do is to get access to that extended functionality.

MS. SMITH: Thank you, Mr. Freeman. Does anyone disagree with that characterization of what the access controls are doing? Mr. Reed?

MR. REED: I would say I wouldn't disagree, but I'll give a codicil. So, in the terms of service with Apple, for example, one of the things that we are not permitted to do is use undocumented APIs. And so jailbreaking in part is, well, I want to mess with the guts of this product, I want to do something that isn't part of what Apple allows me to do. But here's the reality of it. We don't have a market failure in that there are other products that if you want to tweak, test, turn, and do other things, there are plenty of products available. And as Mr. Freeman noted, the reason that Kodi Box, the baseline software that runs Kodi is available on these app stores is

that the underpinning software itself does not necessarily mean that infringement's going to happen. The problem, as the Copyright Office has noted, is what becomes the primary or most regular use for it, and it doesn't take much of a web search to see that that's a primary purpose.

But, yeah, I mean, this is the natural poll intention that exists between somebody who wants to tinker and a company that wants to sell an experience. And Apple sells an experience. They want that Apple TV to have a certain experience and they built it into their pricing model and the way that they sell it to my developers about what we get out of being part of this platform. We get access to customers in a way that they're more willing to use our applications.

So the problem that he's outlining I don't think necessarily is a problem because the market has offered other solutions. You don't have to buy an Apple TV. They aren't the only product on the market. They are very highly restrictive. From a member's perspective, there are benefits to that. There are also tradeoffs. We don't have access to the full suite of APIs. But there are some significant economic benefits that go to third-party developers who participate on those platforms.

MR. AMER: Mr. Ayers, did you have something quickly?

MR. AYERS: Yeah, thank you. And acknowledging that if we actually are talking about expressly and explicitly carving out DVD, Blu-ray players, and game consoles, it may be less of an issue. But just to clarify, as I've mentioned in other elements of this hearing, of these hearings over the past couple weeks, the firmware of a device is not only protecting against -- or restricting the ability to install third-party software and not only protecting against malware and so forth, but it's also used to protect other elements of the device that are used in a content protection ecosystem, such as making sure that the applicable cryptographic elements, such as decryption keys, device keys are available and secure for the device to play protected content. So that's one of the elements that's protected by the firmware, in addition to all these other functionalities we've talked about.

MR. AMER: Okay, thank you. I believe my colleague, Ms. Kern, has a few follow-up questions to sort of drill down on this issue a little bit more, and then we will turn to SFC's petition regarding routers.

MS. KERN: Thank you, Mr. Amer. So I just had a couple questions on how the proposed exemption differs from the current jailbreaking exemption that's currently in place. So I just wanted to ask whether the TPMs used for non-integrated video streaming devices differ from those for integrated streaming devices, and if there is a difference, what are they, and do these different TPMs require different avenues of circumvention?

MR. STOLTZ: They do not. The smart TVs that are capable of running a wide variety of applications primarily use versions of Android, as do many of the non-integrated devices. For the most part, we're either talking about flavors of Android, including Amazon's versions of Android, or we're talking about versions of Apple's iOS, or we're talking about the manufacturer's proprietary operating systems, which do exist in both of these cases. But the types of TPMs and the methods of circumvention are essentially the same within each one of those sort of software platforms.

MS. KERN: Thank you. Mr. Freeman, I didn't mean to put you on the spot, but I saw you nodding your head, is that correct?

MR. FREEMAN: That is definitely correct.

MS. KERN: Thank you. Okay. And then moving to Mr. Williams, Joint Creators and Copyright Owners argued that the lack of functionalities that proponents seek to add on the devices protected by TPMs is a mere inconvenience and that these, I guess, uses can be accomplished through devices that are already available on the market. So, I guess, can you please provide specific examples of adequate alternatives to circumvention?

MR. WILLIAMS: Sure, and I think part of what we said was based on what they admit in their comments, which is a lot of this is just because people want to do it because they enjoy it and they think it's fun. And that's okay, but it's not really a justification for creating a regulation in the C.F.R. of this, you know, import. And so that's kind of why we said a lot of this is about convenience.

And then, on the alternatives side, I mean, one thing that Mr. Stoltz was talking about was using your video game console controller to operate one of these streaming stick devices, and you can just Google these streaming stick devices. I mean, they come with their own controller. You know it -- you don't need to use your video game console controller to control one of these devices. You've already got your own

controller if you want it and you want to use it. And so there's another question with that one also, which is does this exemption even enable that or would you also have to hack the video game console controller, which would not be covered, as I understand it, by this proposal.

So those are the kinds of issues that we were trying to point out, and we've discussed some of them today, that there's other ways of accomplishing the same goals without this exemption and that, if it really is a matter of people just wanting to have fun with some of these devices, I don't think that's grounds for an exemption.

MS. KERN: And, Mr. Stoltz, would you like to respond?

MR. STOLTZ: Yes. Mr. Williams' clients produce entertainment. So, if the question is wanting to have fun, that's kind of all we're talking about here. It isn't really because people can also use these devices to inform themselves and to communicate with others. So I think importance may be a little bit in the eye of the beholder. But, if the test is having fun, then there is an equivalency here.

Another point to some of the ways that Mr. Williams and Mr. Reed have presented evidence in this

hearing now, there are no rules of evidence in this proceeding, nor should there be. But I would offer that presenting "I just did a Google search and here are some of the undisclosed websites that I found" is not a very helpful method of adducing facts in this proposal. We can Google as well. We have cited our sources in our papers. So this notion of sort of what one might find out there, I guarantee you, you can find anything you want out there on the Internet.

And, finally, specifically about game controllers, the majority of them, in my understanding, do not have TPMs on them. And, again, the issue is equipment that you already own being able to use it in -- use them together. And this idea of, oh, well, you can go out and buy more equipment, there's not a rationale that the Copyright Office has ever credited with regard to jailbreaking exemptions. I mean, you can go buy another phone. You can use a PC instead of a phone. But this is -- the precedent is that that's not an operative concern with respect to jailbreaking. There's no reason why that should be an operative concern with respect to non-integrated steaming devices when it was not a concern with integrated streaming devices.

MS. KERN: Thank you. And then just one

more question, and I'll direct this to Mr. Stoltz. So, in past recommendations, jailbreaking was recommended because the exemptions sought to install alternative software. In some of your comments, you note that users want to jailbreak video streaming devices to install other absent programs, such as In Control and Air Magic, and then you mentioned a couple other things, such as, I believe it was increased privacy, devices compatible with others in the home, installing a different home screen, and possibly sideloading. So my question is basically, how are users adversely affected by their inability to install apps or programs or do some of the things that you had mentioned previously?

MR. STOLTZ: Well, all of those things require jailbreaking. And I realize that in this proceeding we've used the word, the term "jailbreaking" a bit loosely, and Mr. Freeman is correct about that. The term "jailbreaking" originally came from the iOS, sort of the Apple world. We use it a little bit more loosely here really to mean to gain fundamental access to the device for the purpose of adding or removing software. But all of those things are adding or removing software, and one cannot do them without circumventing access controls

on the device.

MS. KERN: Thank you. And then it looks like Mr. Zambrano Ramos has a question.

MR. ZAMBRANO RAMOS: Thank you, Ms. Kern. This would be for proponents. I'm curious if some of these uses have to do with accessibility, so, for example, using a game controller instead of the controller that came with the stick, and if you could talk a little bit more about those uses. Thank you.

MR. STOLTZ: Yes. Those can absolutely pertain to accessibility. Certainly, different forms of controllers have different forms of accessibility and different levels of accessibility. I believe it was called end controller, the idea there was sort of a universal control interface to a streaming device. In other words, one can use any sort of input device, basically anything that can simulate a mouse or keyboard to provide input to the device, which means whatever device is most accessible to the user. So that is absolutely a factor. Otherwise, you're sort of at the mercy of the manufacturer.

I should add that can also include manipulations of the screen. This is something again that you can't do with sideloading. So inverting the video to make the text more readable or altering the

colors that are displayed on the screen to make them more readable to people with certain visual disabilities, that's another feature that generally can't be done with sideloading and not at all on an Apple device without jailbreaking.

MR. AMER: Okay, great. I think we are going to have to move to the next topic, and so I want to turn to, Mr. Williamson, your petition regarding jailbreaking of routers and other networking devices. I just would like to start with you and invite you to sort of describe generally what the purpose of this exemption would be and to describe the types of activities that you're hoping to make possible.

MR. WILLIAMSON: Sure. Absolutely. And I appreciate the opportunity to testify here today. So my client, Software Freedom Conservancy, is a nonprofit organization that supports the development of free and open-source software and advocates for the rights of the users to use software in the way that's most suited to them. They are the fiscal sponsor for a project called OpenWrt, which is a project to produce an open-source, free and open-source software operating system that can be run on routers and other dedicated networking devices.

And as we pointed out in our petition,

OpenWrt allows users, number one, to secure their devices. It's regularly updated and, as we pointed out, research suggests updated far more frequently with security patches than the stock software that comes on routers. It gives users the opportunity to protect their privacy, for example, by installing DNS encryption and VPN software on the router itself. And it gives users the opportunity to run a host of free and open-source applications on the router that wouldn't necessarily be available without replacing the firmware on the router. And as we pointed out, it also supports several research efforts into development of new networking techniques that have directly fed into the development of networking standards and improved networking capabilities.

MR. AMER: Okay, great. Thank you. I wanted to invite the opponents to address this proposal. I know there were some concerns in the comments. In particular, there seemed to be a concern about -- similar to the other petition, about to what extent -- what devices this would cover and to what extent this might permit access to other types of copyrighted works. So, I know that Software Freedom Conservancy in its reply said that routers and other networking devices possess neither the video outputs

required to transmit content to televisions, nor the processing power to run video streaming applications. So I wonder if that addresses any of the concerns that the opponents have raised, if that sort of allays any of the concerns you had with this proposal. Mr. Ayers?

MR. AYERS: Thank you. Again, this is sort of like this is a situation where the explanation is helpful certainly, but I'm not sure it exactly matches with the proposal as currently drafted, and so I'm assuming there's a way to get to there from here. My concern is with the text "other networking devices," where that could actually be a very broad term, and I would want to make sure that -- I don't think this is the intention. My understanding of the explanation is that this is not the intention, but, as currently drafted, "other networking devices" could arguably sweep in anything with Wi-Fi, and so we'd want to make sure that we're not doing that.

Or even taking it just a slight step further, many devices now generate their own local area networks, their own SSIDs, in order to make it easy for a consumer to make a network connection with that device and to use a remote device to adjust other settings. I'd want to make sure that those sorts of

devices, for instance, a game console that generates its own SSID in order to allow easy setup, is not swept into the category of "other networking devices" simply for that reason.

MR. AMER: Thank you. Mr. Williamson?

MR. WILLIAMSON: Yeah, I understand that concern, and that's obvious or that's absolutely not the intention to sweep in just any device that has networking capabilities. So I think that we would support an exemption that extended to dedicated networking devices, including routers, switches, hubs, bridges, gateways, modems, repeaters, and access points, and that that would be effectively those dedicated devices would be a pretty comprehensive list of the devices that we're concerned with.

MR. AMER: Thank you. Mr. Williams?

MR. WILLIAMS: Yeah, thanks. I agree with Mr. Ayers, and the narrowing is helpful. We definitely want to make sure things like VR headsets, other devices that can connect directly are not swept in to this proposal and that it's really focused on the types of uses that Mr. Williamson has identified, things like upgrading the security protections on the router, et cetera.

There was some comment in I think the

opening comments that basically said these routers are the equivalent of general purpose computers. And so drawing the line the way you did, Mr. Amer, that says, well, then they're not -- they're somehow not capable of running streaming applications, you know, I'm not sure that those two things work together. So I think the line-drawing here is going to be the most important part. And I think adding also the limiting language that you included in the voice assistant exemption last cycle but is not in some of the preexisting exemptions, we would support doing that or even language that's even more limiting.

MR. AMER: Okay. That's helpful. Mr. Reed, do you have a similar position to Mr. Williams in that it sounds like there may be some openness to the substance of this proposal if there is appropriate limiting language, is that accurate?

MR. REED: Yeah, that's correct.

MR. AMER: Okay.

MR. REED: And I have a personal fondness for OpenWrt. I think there still may be some code in there that I wrote back in the days. But the question I had for Aaron Williamson very quickly was, how are we envisioning Mesh networks? So, for example, let's say a Blu-ray player, we're going to start seeing it

on Mesh. Do you see this extension -- if one of Mr. Ayers' clients' Blu-ray player is now an extender, a range extender or is part of -- now that we've jumped to some of the new standards onto a Mesh network, do you think that -- you want to keep it limited enough that, no, it doesn't mean you can open up the Blu-ray player? But we can get to say the baseline Lynksys router and make a modification there or do software updates, but not necessarily break into the Blu-ray player, even though it might be part of a Mesh network? That's my interpretation of your limiting and that sounds fine. I mean, that sounds reasonable to solve Mr. Ayers' problem and Mr. Williams's points of view on the general purpose computer.

MR. WILLIAMSON: Yeah. Maybe my client will rap my knuckles, but I do -- I'm not aware of any plans to put OpenWrt on Blu-ray devices, nor is that what's contemplated by our client.

MR. REED: In which case then I think the limiting language is helpful. But I agree with Mr. -- Matt Williams's points on just be careful that we don't turn it into an exemption that gets Mr. Ayers' clients wrapped around the axle. So, yes, thank you for the limiting explanation, Mr. Williamson.

MR. AMER: Mr. Zambrano?

MR. ZAMBRANO RAMOS: Yes, thank you, Mr. Amer. Just a couple of questions for proponents. I just want to make clear, would this include the modem/router combos that are sometimes leased by Internet access providers?

And then the second question, I was curious if you could drill down a little bit on the TPMs at issue. I notice there were different kinds of TPMs and different methods of circumvention, and at one point, I think your comment mentioned that the TPMs protect the stock operating systems of the networking devices. I'm curious if you could talk a little bit more about how that protection works. Does it control access to stock firmware? Does it just prevent you from loading a different firmware? Does it do both, or does it do something else? Thank you.

MR. WILLIAMSON: Sure. Thank you. So, you know, I guess I don't think that there is any intention here to enable the installation of alternative software on a device you don't otherwise have the right to install software on, right? So a leased router, I think, would properly fall outside the scope of the proposed exemption.

And, sorry, apologies, quick reminder of the second half of your question.

MR. ZAMBRANO RAMOS: How do the TPMs at issue work? What exactly do they protect?

MR. WILLIAMSON: Yeah, absolutely.

MR. ZAMBRANO RAMOS: Do they protect access to the firmware software? Do they just prevent you from loading different firmware?

MR. WILLIAMSON: They primarily prevent, as I understand it, yo know, many of the routers or the examples that we cited in our comment involve firmware encryption schemes that basically check to see whether the firmware you're loading is consistent with the firmware encryption scheme that they want to see on a new firmware for installation. So it's necessary to circumvent or reverse-engineer that encryption scheme in order to produce a firmware that is encrypted according to the right sort of protocol. There are also definitely examples out there, you know, of firmwares that are encrypted on the device and then sort of loaded into the memory decrypted, I believe, and there are also your typical access controls, user name and password, that sometimes is necessary to circumvent those to get root access to the device. Those are the ones I'm primarily familiar with.

MR. ZAMBRANO RAMOS: And, sorry, just a follow-up. And do you think that all of those TPMs

you mentioned constitute TPMs under the statute?

MR. WILLIAMSON: Well, unfortunately, this is -- I advise clients on the scope of Section 1201 regularly, and the language is very broad, right, and so it's difficult to say with certainty which of those TPMs would be considered to effectively control access to a copyrighted work or protect the right of a copyright owner. So, certainly, they're all measures that I think could be interpreted that way.

MS. SMITH: I wanted to check and see, Mr. Zambrano Ramos, do you have any more questions?

MR. ZAMBRANO RAMOS: No, thank you, Ms. Smith.

MS. SMITH: Thank you. So I think that we are done with our questions, but we wanted to give any of the panelists an opportunity, you know, sort of a last call, if there's anything you think that we should know before we conclude this hearing. We might -- we'll probably wrap up a little bit early. So I don't know, Mr. Williams, if your hand is still raised or newly raised. Let me know, Mr. Williamson. And if not, I see Mr. Stoltz had raised his hand. Okay, Mr. Stoltz?

MR. STOLTZ: Thanks. I just -- and, again, thank you for this opportunity. I just wanted to

reiterate that and point out that there is, you know, a very small difference between the existing exemption, which has been in place for six years, and what we've proposed here with regard to non-integrated streaming devices, and what you won't find in the record is any meaningful distinction. So opponents have not offered up any meaningful distinction. In fact, I think Mr. Williams said that, you know, his objections are the same objections that he has raised in previous cycles and that the Copyright Office has not credited. So I'll leave you with that and thank you again.

MS. SMITH: Thank you, Mr. Stoltz. Mr. Freeman?

MR. FREEMAN: This is one very minor clarification that I'll be kicking myself forever if I don't quickly add.

So I separated out in the joint copyright list of uses the adding a web browser versus all of the other ones. And the reason why I separate that one out is that's a use case where you might ostensibly believe that, well, you can build a web browser if you're given merely the same access you would need in order to print things to the screen, such as with Kodi, my description with that. But, in

fact, web browser engines, because of their third-party code-loading security requirements, in addition to a lot of their intricate performance requirements, actually require more access to the system than is oftentimes given to third-party application developers.

And so I just wanted to kind of throw in there that this subtle line between the things that are allowed, which weirdly include Kodi, and the things that are not allowed, which include all of these things that we would like to be able to do, is extremely subtle.

MS. SMITH: Thank you, Mr. Freeman, for the clarification. Mr. Williams?

MR. WILLIAMS: Yeah, thank you. Just a couple of clarification points about what Mr. Stoltz just said. I tried at the beginning to articulate that we have kind of multiple grounds for objecting in opposing this proposal. The first one and the most important one for us does not relate to the objections that we've put forward in the past that the Office has disagreed with us on, and that's the one we focused on first during the hearing, which is how do you define this class in a way that doesn't sweep in the devices that Mr. Stoltz says he doesn't want to cover.

And the language they've put forward, I would submit, doesn't succeed in that. Whether it's integrated or not integrated into a device, it doesn't address the concerns that I raised about the fact that some video game consoles don't even have disc drives. They certainly run applications. They certainly stream video to a screen. And so that's our primary objection.

The point I was trying to make about past decisions and the Office's kind of disagreement with where I come out on things was more about the fact that we do think that these exemptions over time cause harm and result in infringement, and the evidence that I've put forward about that in this discussion during this cycle is similar to things we've put forward in the past and that have not, in the Office's view, been enough to deny exemptions. So I just wanted to be up front about that from the beginning, but I didn't want it to get confused here at the end that I was saying everything that I've put forward has been rejected in the past. I don't think that's the case.

Mr. Freeman keeps referring to our list from our comments. I mean, what we tried to do was just summarize what EFF put in their comments. So this is not our list. It's just a list of things that Mitch

put in his comments that we were trying to respond to.

And then the last thing I guess I'll say in the spirit of fun that Mitch was raising earlier is touche on that one. We do want people having fun, and our clients love that people enjoy their products. And so, you know, congrats, you made a good point there.

MS. SMITH: Thank you, Mr. Williams. Mr. Williamson?

MR. WILLIAMSON: I just want to take a moment to express my appreciation to Mr. Reed for his contributions to OpenWrt and to the Copyright Office and the NTIA. I know that this proceeding is a long one and potentially grueling at times, and so I want to thank you for your dedication and professionalism throughout this process.

MS. SMITH: Thank you. I think we all appreciate the time that it takes for participants as well and appreciate you coming forward and sharing your thoughts. I noticed this proceeding was not mentioned as particularly fun, but we appreciate you showing up and think it is important to the process.

We're going to stop 14 minutes early and then we will start at 12 Eastern with Class 10, which is -- I'm sorry, 1 p.m. Eastern, which is Class 10,

unlocking. And so, if anyone is in the attendee or anyone else wishes to sign up for the audience participation session, that will be -- that will conclude these hearings, so this is sort of last chance to sign up if anyone wants to contribute anything else for our discussion. Okay, thank you.

(Whereupon, at 11:46 a.m., the hearing in the above-entitled matter recessed, to reconvene at 1:00 p.m. this same day, Wednesday, April 21, 2021.)

//

//

//

//

//

//

//

//

//

//

//

//

//

A F T E R N O O N S E S S I O N

(1:01 p.m.)

MS. SMITH: All right, everyone, we're going to get started. So can all the panelists please turn on their video? Great. So this is the last scheduled panel for the Copyright Office's Section 1201 rulemaking hearing. This is Class 10, unlocking. And before we dive into that discussion, which we're looking forward to, I wanted to just flag sort of the last call opportunity for any members who are listening who wish to join the audience participation session, which is going to commence immediately after this session at 1:45 Eastern. There is a link being provided in the chat for those who wish to sign up, and I think we'll keep it open for about 15 more minutes just to let us know if you wish to contribute.

What that means is any of the proposed categories or subjects for discussion in the rulemaking we're opening up to hear from members of the public. We're asking that you do try to limit your comments to around three minutes. I think then we'll be able to accommodate everyone who does sign up for the hour session we have so long as we keep the comments pretty much contained that way. But please, we encourage, we like to hear from you, so sign up

through the link in the chat if that's something that is of interest to you.

So turning to this session, I think everyone is pretty familiar with living our lives on Zoom by now, as well as these hearings. But just to go over, we have a court reporter who is transcribing the proceedings. The video will be live-streamed and will be made available on the Copyright Office's YouTube channel. So please wait for someone from the government to pose a question so we don't step on each other speaking. This is a sort of shorter, smaller panel, so we may not need to use the "Raise Hand" function on Zoom, but we have found that to be generally effective otherwise.

And to get started, I think we'll have those from the Copyright Office introduce themselves. I'm Regan Smith, the General Counsel. So, Mr. Amer and Mr. Gray?

MR. AMER: Kevin Amer, Deputy General Counsel.

MR. GRAY: Hi, everyone. I'm Mark Gray. I'm an attorney-advisor here in the Office of General Counsel.

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

MR. CHENEY: Sure, thank you. I'm Stacy Cheney. I'm a senior attorney-advisor at the Office of Chief Counsel at NTIA in the Department of Commerce.

MS. SMITH: Thank you. And then, Professor Malone and Mr. Kaufman, could you please introduce yourself and the organization you're representing today?

MR. MALONE: Good morning. I'm Phil Malone. I'm the Director of the Stanford Juelsgaard IP and Innovation Clinic. Jonathan?

MR. KAUFMAN: Hi. I'm Jonathan Kaufman. I'm a student in the Juelsgaard Intellectual Property and Innovation Clinic at Stanford, and we are representing the Institute of Scrap Recycling Industries, or ISRI.

MS. SMITH: Great, thank you. We appreciate you coming today. And I think Mr. Gray is going to be directing the proceeding. Go ahead, Mr. Gray.

MR. GRAY: Great. Hi, everyone. So, like Regan mentioned, in the past, in some of our past hearings, we've done "Raise Hand" because we've had a lot of participants. Today is pretty small, so I'm hoping this can be a little bit more of just a dialogue and a back and forth.

So, with that said, I wanted to start off asking a few questions about the request to expand the unlocking exemption, Class 10, to Chromebooks. So, in the proposed regulatory language ISRI provided, you propose adding a line that says "all purpose laptop computers (including Chromebooks)." Could you discuss more why, in your view, it's necessary to specifically include a brand name for Chromebooks and what purpose that's serving beyond just keeping language for all purpose laptops?

MR. KAUFMAN: Sure. We included that in a parenthetical for the avoidance of doubt. Typically, when you think of laptops, you think of PC laptops that run on Windows. And since Chrome has their own operating system, we want to just be very clear that the laptops definition that we included is not just PCs that run on Windows but also Chromebooks that run on a separate operating system. That's the only reason that that was singled out.

MR. GRAY: So one of the reasons I ask that is I think the way Google uses that brand name is sort of anything using Chrome OS, and that includes some of their tablet form factors where it may not necessarily be a clamshell laptop, but it has maybe a traditional laptop screen and then an optional detachable

keyboard. So, given that we already have the tablet exemption in Class 10 or in the current unlocking exemption, one of the questions I had was just sort of whether that was going to add more ambiguity and confusion rather than just saying laptops are a prong and then tablets are a prong.

MR. KAUFMAN: Yes. So, as far as whether or not it would create any ambiguity, I would agree that the line between tablets and laptops is getting increasingly blurry. There are two-in-ones. In my view, a laptop is just a tablet with an attached keyboard. So the fact that they are currently treated differently, one being exempted and the other isn't, doesn't make a whole lot of sense from a copyright law point of view. So, if it would be helpful to include laptops in the same prong as tablets by adding tablet or laptop computers that includes both the hybrid cases and the ones where you have a laptop that doesn't have a touchscreen and has that attached keyboard, we're fine with that. Really, we have no position about creating a fifth category for laptops or modifying the tablet language to make sure it includes laptops and Chromebooks. If they can be both a tablet or a laptop or both, I think that might help address that concern.

MR. GRAY: Great. Well, that actually answers the next question I was going to ask about potentially combining those two.

So turning to the adverse effect on non-infringing use analysis, I know, in your initial comment, you mentioned that ISRI members are beginning to obtain wireless laptops and it sounds kind of maybe between the lines that a lot of these are Chromebooks. Could you talk more about sort of the scale, like, the quantity of laptops that are coming in to recyclers, but particularly how many of those are specifically locked to a wireless carrier, as opposed to just generally being a laptop?

MR. KAUFMAN: Sure. So we don't have any specific numbers to speak to the scale, but I can speak to the prevalence of locked 4G LTE laptops on the market. So, in our submission, we mentioned a few examples. By my count, there are three laptops, I believe, that are locked to T-Mobile, there are six that are locked to Verizon that are on the market, and there's one that's locked to AT&T. I can give the names of each of those, but a very significant percentage of these laptops are locked to carriers.

And then, to the first point about the number of laptops that ISRI members are receiving, we

think that the only reason why these laptops have not been received in the quantities of phones or tablets in past cases is that the market for these laptops is kind of new as of the last two or three years and there's not been a lot to trade up to. So, in a more robust market with lots of options, you would, in theory, after a year or two end up selling your laptop, usually trading up to another model. There hasn't been a lot of 5G models to trade up to. The 4G models are more or less the same. So we expect that as 5G laptops enter the market, the number of these 4G first-generation laptops will increase accordingly.

MR. GRAY: And so maybe to build off of that, obviously, 4G is not sort of the first cellular technology. Have there just not been a lot of 3G laptops that needed to come and get included in this proceeding before? Why -- I mean, I understand that maybe there's not a lot to trade up to on the cellular connectivity side, but laptops and processors get faster ever year too. So I'm trying to figure out, why have we not seen issues with locking cellular-enabled laptops until now?

MR. KAUFMAN: Sure. So the first cellular-enabled laptop that I am aware of was a single model, I believe it was the HP Chromebook 11 released on

Verizon in 2014. There wasn't a whole lot else on the market after that. And then, in the last three years, we have seen an emergence of these cellular-enabled laptops. So, just from the span of 2019 to 2021, the number of 4G LTE laptops that are commercially available has doubled. And there is some lag time from the point in time that someone buys a cellular-enabled laptop. The average life span for any laptop is around three to five years. Of course, at some point along that way, the original owner may move on to another laptop. That doesn't spell the end for that laptop per se.

But, in the last proceeding, the reason why laptops was not its own category was the number of laptops on the market paled in comparison to what we're seeing now. And I really think we're in a situation where, yes, we have not seen it at the scale that the recyclers received phones and laptops in -- phones and tablets, I'm sorry, in the past, but we have every reason to believe that they will either this year and even more in next year and the following year.

MR. GRAY: And that's partially a result of just increasing adoption and availability of 5G specifically?

MR. KAUFMAN: Yeah, I would say that the adoption of 5G is a major factor in people being willing to sort of move on to a better and improved cellular laptop.

MR. GRAY: Great. How --

MR. CHENEY: Mark, if I could jump in?

MR. GRAY: Oh, sorry. Please, go ahead.

MR. CHENEY: Yeah, sorry, I didn't want to interrupt you there, but, Mr. Kaufman, if you could sort of speak to, and perhaps you alluded to this a little bit in your document, about how perhaps not just the confluence of 5G being deployed more nationwide and being more available in the last year, but also the pandemic and the use of laptop increase and the need for that to include cellular technology as part of that, rather than just a Wi-Fi connection? Can you talk about maybe that sort of scenario as well in this discussion?

MR. KAUFMAN: Sure. So, obviously, in the last 13 months, where people work and how they work has changed dramatically. We've seen that some people are able to work from home, where they may have Wi-Fi. Others have to find a place maybe in a park or elsewhere to do their work, and that always connected feature of cellular-enabled laptops, I think, has

become increasingly appealing, especially as there's a lot more remote learning, a lot more people working remotely. And so the flexibility to not be beholden to getting a stable Wi-Fi connection wherever you are and being able to rely as a backup on these cellular networks, I think that use case in the last year, on top of everything else I have mentioned, certainly strengthens the case for more people turning to cellular-enabled laptops not only in the past year but in the coming years.

MR. GRAY: Great. And so I have a few more questions about sort of some of the specific evidence that you provided about the prevalence and quantity of locked laptops. So, in the initial comment, you mentioned that Verizon has a locking policy where devices are locked for at least 60 days after purchase. And the URL you provided for that site, in the locking FAQ, one of the questions is what devices are locked under this policy, and the Verizon answer is it's all Verizon smart phones that they sell either at a main Verizon store or a retail partner. And so that page seems to suggest that most of that locking is happening on the phone device side, as opposed to laptops. So are there other areas in your submission that can speak maybe more specifically to the kind of

carrier-issued policies about locking non-phone devices?

MR. KAUFMAN: Sure. So I think just as an initial matter, in the past, the Copyright Office has looked to alternatives to an exemption in the form of voluntary unlocking policies as being an option. I think the fact that that policy is sort of silent on laptops was important evidence.

As far as whether or not they are indeed being locked, there are people who have received and purchased that Lenovo Flex 5G laptop, which was the one exclusive to Verizon, who have encountered, tried using a different SIM card and have been unable to. And I think the crucial feature here with any locked laptop and especially these 5G laptops is the fact that from a technical perspective, the underlying modem supports all carriers, and that's something that we alluded to but didn't fully flesh out in our submissions. The modem that goes in that Verizon exclusive laptop does indeed support Verizon, T-Mobile, AT&T, and really any other carrier. So the only barrier in that case is the locking of that laptop.

Other 5G laptops that we're aware of that are locked, there's a Dell laptop that was sold

exclusively through T-Mobile, and T-Mobile's website says that for all devices that are sold through T-Mobile, they are locked as a consequence -- for fear of theft or fraud. That policy, I do not see limiting it to smart phones, and it suggested that if you're buying through T-Mobile, we're going to lock it regardless of what it is. But I think the crucial point is that it's that lock which is the barrier, not any technical limitation.

MR. GRAY: All right. And so you talk about the Lenovo Flex 5G, and so I read through those reviews you pointed to. The language sounded a little bit more like it was being sold exclusively through the Verizon sort of network or through Verizon as a company. There was actually another review from a Neowin, I think, where they were able to get it technically working on other carriers. So it was a little unclear whether there was a software limitation there or whether they just hadn't maybe put the drivers in or something like that for that laptop. Are you aware of any other sort of reviews or public statements about the Flex 5G specifically that make clear it's a software limitation rather than something else?

MR. KAUFMAN: Our understanding was that it

is a software limitation, that the folks at Neowin in that article which we did come across were somehow able to make it work. But the folks who did receive the laptop maybe didn't have the technical sophistication of the experts at Neowin, I believe have encountered a PIN lock that looks like it is the same TPM that would be present on the same modem that is in phones and that same modem is just being put into a laptop.

MR. GRAY: And maybe just to clarify for the audience and for the record, when you say PIN lock, you mean you have to enter some sort of PIN or numerical code to actually have the software allow you to use it with maybe a SIM card from a different network or somehow otherwise identify yourself to a different network?

MR. KAUFMAN: Yes. So just to expand on it, the thing that prevents any device from being used on a carrier is a setting in the cellular modem itself. Last cycle, it was referred to as the baseband processor. That is synonymous with the modem. Then you are able to modify that setting by circumventing a TPM that basically modifies whatever bits of code to allow it to communicate with other carriers. And so that hardware, and that's the firmware associated with

that hardware that was designed by Qualcomm, that same modem that's being put in a tablet or a laptop with an attached keyboard, we have every reason to believe that that same TPM is going to be there. It was developed in one case for phones and tablets, but no reason to modify or think that the associated TPM would be any different when you put it in a device that just happens to have an attached keyboard.

MR. GRAY: And that modem, is that the X55, or is that just sort of specific to the Flex 5G?

MR. KAUFMAN: So that X55 modem, which is the first 5G modem and the most widely adopted one by Qualcomm, was first in phones, and every 5G laptop that we cited to and that has been announced will be using that same exact modem.

MR. GRAY: And you have no reason to believe that the firmware would be -- that there's, like, custom firmware for the modem across different device categories?

MR. KAUFMAN: No, because, when we were looking at this for phones and for tablets and seeing that the same parts were being used, there was nothing in the record to suggest that when Qualcomm is just making these silicon chips, that they are having the foresight, oh, where is this chip going to end up.

For their purpose, it's much easier to have one set of firmware associated with that one piece of hardware, and wherever it goes, that firmware would still be there.

MR. GRAY: All right, great. Do you have any questions, Mr. Cheney, before we move on from laptops?

MR. CHENEY: No. I think you covered what we're interested in. I just wanted to make sure too that the language that we have in the proposed alternate -- well, you talked about 5G and 4G LTE. You really didn't want to limit the exemption to that language. It was sort of talked about throughout and then somehow and someways proposed in other places, but it looks like the actual language does not include that limitation, is that correct?

MR. KAUFMAN: I believe our language is 5G, 4G LTE, or any other cellular connection capability.

MR. CHENEY: Well, I'm reading your text. It doesn't include 4G LTE and 5G. So I was just wondering if you're just indicating wireless telecommunications network rather than specifically naming the type of technology that's going to be used there, to keep it more broad.

MR. KAUFMAN: Oh, yeah, yeah. I'm sure,

yeah. I thought that the qualifier we had put in lapsed. Yeah, there's, I think, no reason to narrow it to the existing technologies. The wireless telecommunications network I think is sufficiently forward-looking and works for us.

MR. CHENEY: Okay, thank you.

MR. GRAY: Great. And, actually, maybe one more question before we move on. So one of the things that the Office has to do in this proceeding is both sort of look at the current state of the market and what is likely to happen in the next three years. How, if at all, should the Office think about the broad history of carrier locking devices in predicting what is likely or not likely to happen in the next three years?

MR. KAUFMAN: Yeah. So I think that what we have seen in the past is locking of phones, tablets, really any device that connects to a carrier, it's in the carrier's interest to lock you in. And as the number of form factors expands, whether it be laptops or anything else in our all devices category, there's simply no reason to believe that that practice is going to end and so nothing to suggest that carrier locking is a thing of the past. It's very much a thing of the present and the future.

MR. GRAY: And do you have any additional commentary you want to add beyond the written submission on the significance of the Department of Justice's Antitrust Division letter to GSMA?

MR. KAUFMAN: Yeah. I'm happy to elaborate on that a bit. When eSIM, which is basically a virtual SIM card rather than a physical SIM card that goes into phones, the promise of that technology was going to be that it was going to be easier for people to switch carriers. Unfortunately, that has not proven to be the case, and on many phones and other devices that have eSIM, the practice of locking persists, and that DOJ investigation ended up ending in sort of a voluntary agreement from the trade association representing the mobile carriers that they were going to play by the rules, but we have not seen that, as the adoption of eSIM has become more prevalent, that there's any reduction in the number of devices that a carrier locks. So we cited to that just to show that industry practice, even with the evolution from a physical SIM card to a virtual one, has not reduced the amount or prevalence of carrier locking.

MR. GRAY: Great. So now I'd like to move on to discuss the broader expansion, which is to allow

unlocking of any category of devices. So there was discussion of this during the last round in 2018, and I think, as we're all aware, the Office usually avoids broad use based exemptions, kind of like an all devices exemption here. In 2018, the Office actually did recommend an exemption for all devices, specifically in the context of the security research exemption. And so there, in the Register's recommendation, she pointed out that the proponents there had offered "substantial evidence of a legitimate need" to access the TPM protected software on a broad range of additional devices and systems.

So this is more of a two-part question perhaps, but (a) to what extent should the Office be considering that analysis in this request for Class 10, and (b) compared to the extent that you're familiar with that record, can you compare and analogize the record we have for unlocking wireless devices to the security research of all devices and how that record compares and contrasts?

MR. KAUFMAN: Yeah. I'm more than happy to. So, on the first question, I think that that security research exemption that eliminated the device limitation is directly on point and very much similar to what we are asking for here. When the exemption

was granted for security research, the reasoning was that the use in all cases regardless of the device was tailored to a specific purpose. And, here, in the unlocking context, it's the same thing.

The only purpose of the unlocking exemption is to allow the owner or recycler of a device to switch wireless carriers and to circumvent a TPM for that and that's it. This is not an exemption that allows for anything else. It's very narrowly tailored just like the security research exemption. So, for that reason, given that we also have tailored it to a specific purpose, the fact that the purpose in all cases is non-infringing, we think that that is very strong evidence that helps our case for a broader exemption here.

MR. GRAY: Well, so maybe to dig into a little bit of that, you offered some, I think maybe we can call them illustrative examples of devices in this category. So there was mention of smart TVs, of drones, of augmented virtual reality, and then certain Internet of things. So, to go kind of through those, on the smart TV point, it seems like the material and the evidence you provided are really talking about future looking trends. There was an article about a potential partnership in South Korea between Samsung

and SK Telecom, but that article talks about the North American broadcast over 5G being "years away." I know there's the 5G.co website that's a UK website and seems to be hedging a little bit on when 5G broadcasts are going to be widespread. So what kind of record evidence do we have that in the United States specifically, which is where this proceeding is covering, there are or are likely to be both 5G enabled televisions sold on the market but specifically 5G enabled televisions that are in some way locked to a particular 5G provider?

MR. KAUFMAN: Sure. I wanted to answer that question directly, but I just want to reiterate that those were illustrative examples, and I don't know how helpful it will be to talk about each one specifically. If you wouldn't mind, I just want to talk about the broad features of these devices that allow us to sort of analyze all four at the same time.

The starting point for that analysis and really the barrier in 2018 was with these specific examples we proposed, the Register said that these were likely to be fair use for the same reasons, but what we did not fully establish is that it was technically feasible for any of these devices to be used on other wireless carriers.

With that in mind, I just want to go back to our example of that X55 modem that I mentioned was in all 5G laptops, that same modem is being deployed in a wide range of use cases, including IoT, including drones, including virtual reality headsets. And the way of sort of thinking about this that I think is most helpful to the Copyright Office is that chip -- there's really only a few people making the chips that have 5G capabilities and that chip is what -- there is the setting that locks you to a carrier. And so just like for phones and tablets, when you reuse the chip, the analysis for the TPM was pretty likely going to be the same because there's really no reason that the firmware associated with a given piece of hardware is going to be different.

So, in this all device category, while we give those specific examples, I think what is more helpful is to look at tracking where that chip is going. And what we're seeing is that that X55 modem ends up getting packaged into some module that is sold by various IoT providers, and that module that has that modem then can be deployed for all of the different use cases that we mentioned. So, as just one example, Sierra Wireless is one of these providers that sells these modules with that X55 modem. They

say that it's applicable to a wide range of IoT applications, such as industrial routers, home gateways, industrial and consumer laptops, video surveillance, and digital signage.

There are other providers that I could point to, but, really, the factor that is consistent across each and that is most important is what is the copyrighted work and what is the TPM protecting it. The record in all of the past cycles is that it is on the baseband processor or the modem itself, and that modem, if it's being deployed in all of these cases, in virtual reality, in TVs, in IoT, then going through it one by one seems to not be the most efficient use of time.

MR. GRAY: Okay. So maybe to kind of quickly summarize the argument then, that basically your argument is we have these baseband processors. It's just a hardware unit. You can put it in any kind of device you want. That might be a phone. That might be a tablet. That might be a laptop. That might be a smart toothbrush for some reason for people who want that. And in all the same instances, we're talking about the same firmware, which would have the same TPM to the extent that TPM is embedded in the firmware and not a different layer of the stack. And

so, from your perspective, that sort of means the analysis can flow across these devices because the actual widget where the analysis is being impacted is the chip that is communicating to the network and not ancillary aspects of the thing it is embedded in, is that right?

MR. KAUFMAN: That's, yeah, exactly right. So the -- yeah, nothing to add beyond that.

MR. GRAY: Okay, great. So I understand the argument and I appreciate it. But to maybe come back to the point on the last round, one way -- the concern that there is not evidence that the devices could, in fact, be used on another network is in some ways another way of asking is there an actual non-infringing use that could be made but for the 1201(a) exemption ban.

And so a related question to that is how many of these devices are, in fact, being manufactured with that modem. And so, in the smart TV example, the evidence that we seem to have is more about, in the future, people will want to put this modem in because it is cheap to acquire and it could have benefits in case you have bad Wi-Fi at home or something like that. And for drones, I think the evidence was more that Verizon had purchased a drone company and less so

that DJI or one of the other big drone manufacturers is actually currently using these modems. My understanding, and this is maybe a little bit more of a layperson understanding, but my understanding is that a lot of times that's using Wi-Fi Direct or some sort of Wi-Fi protocol rather than a cellular protocol.

And so, really, to stay on this question, the question for us is how many of these devices are specifically being manufactured or are likely to be manufactured with this modem, with this chip, and what is the evidence that the Office could look to if we needed to have a record to feel comfortable recommending an exemption that would be broad enough to cover all those devices either because we're doing an all wireless devices exemption or simply because we're expanding to a broader category or group of categories of devices?

MR. KAUFMAN: Sure, okay. There is an organization, the GSA, the Global Mobile Suppliers Association, that tracks all devices that have 5G capabilities and they do this on a monthly basis. In 2019, there were 33 devices that were announced or commercially available with 5G in seven different form factors; in 2020, a year later, there were 253 5G

devices in 16 form factors; and in 2021, a year after that, the number was up to 703 devices in 22 form factors. So we've seen in just a span of two years the number of form factors increasing from seven to 22. And included in those 22 form factors are laptops, cameras, TVs, drones, and, like I said, this includes both announced and commercially available. So that's just a lay of the land of the number of devices.

What's also important to note is that as the number of devices explodes and the number of form factors, there's still really only two or three people that make these chipsets: Qualcomm, a company called MediaTech, and then a few companies in Asia. But, really, in the U.S., Qualcomm is the dominant one. And then, if you track where that specific X55 modem is going, we did not have this information in the record and we did our best to get this, but we have subsequently learned a lot and are happy to provide that to the Office in post-hearing questions or whatever is most useful.

But, if you just look at where that X55 5G modem is, which we know is capable on all three carriers and which we know at least in certain contexts has been locked, all you have to do is just

look at the modules that incorporate it. So you have companies like Sierra Wireless, which deploys their modules across all sorts of IoT devices, you have a company called Telit and Quectel, these are big players in the IoT space and they give sort of the circuit that allows a given company to tailor it to bridges or whatever the application. But the module is device-agnostic, and all of these modules that we have seen are using the X55 5G modem.

So, yes, the record on TVs and drones did not establish that, but we do have that evidence and are happy to supply that to the Office.

MR. GRAY: All right. So, for example, the GSA reports you're mentioning, those are not in the written comments?

MR. KAUFMAN: Yes.

MR. GRAY: And do those subdivide by regions where things are sold, or is it just literally global suppliers?

MR. KAUFMAN: They are based in the UK, so it's global. But, yeah, it includes the U.S.

MR. GRAY: Okay.

MR. KAUFMAN: Yeah.

MR. CHENEY: Can I ask a question here --

MR. GRAY: Please.

MR. CHENEY: -- Mark, if I might?

MR. GRAY: Please.

MR. CHENEY: Mr. Kaufman, this has been very interesting and thank you for that last little bit. I think it might be helpful to sort of step back just a little bit and think about -- you've listed these possible 22 form factors, 16 form factors and so forth. So let's think about somebody goes and purchases one of these form factors, right, they're going to have to contact the carrier. They're going to have to connect to the carrier. At what point will that be locked? Is it locked when they buy the device or is it locked when they connect to the carrier?

We had some indication in some of the comments that somebody -- they bought a phone, it was unlocked, and then they took it to a carrier, and they flashed it and locked it, right. So can you describe that process? So, if somebody were to buy something with one of these chips, it doesn't necessarily mean that it's locked at the time, but go through that for me a little bit.

MR. KAUFMAN: Sure, okay. So say that you're purchasing the module directly from Sierra Wireless. At the time that you're purchasing the module, because part of the module I suppose is a slot

for the SIM card, they ask you, do you want us to put in an AT&T card, a T-Mobile card, or a Verizon card. And then that module is given to whatever company wants to create an IoT solution for some specific vertical, whether it be in industrial or healthcare, and they're going to get those devices. It's going to have that SIM card. And given the policies that we have seen from the different carriers, that SIM card just at the beginning as just a general matter appears to be locked. And the lock, remember, is in the baseband. The SIM card is talking to the baseband, but the baseband, without changing that setting, is not going to be able to communicate to other carriers. That's one case.

The other that's maybe a little more helpful, you can buy these modules directly through T-Mobile or AT&T or Verizon. So, if you're buying, say, one of those Quectel IoT modules from T-Mobile, it's going to have a T-Mobile SIM card. There's no ifs, ands, or buts about that. And T-Mobile's policy is, if you buy something from us, as a first order matter, it's going to be locked.

Last little point, AT&T sells IoT starter kits just like this, and we have heard that those devices come with the AT&T SIM card, and when someone

tries to use a different SIM card, they run into that barrier.

MR. CHENEY: Thank you. I think that was helpful. Mark?

MR. GRAY: Great. We're starting to run out of time, so I'm going to just ask one last question, which is, in the past, when we've done the non-infringement analysis, there has been a role for the facts and the nuances of the specific device, and I'm thinking particularly here about the discussion we had in 2018 about unlocking used devices. And there were a lot of considerations in 2015, in 2018 about the substitution effects and the market harms and which market harms are cognizable and which ones aren't. And so can you just explain why, in your view, that is not a barrier to having a single unifying non-infringement analysis for all wireless devices when the use is unlocking those devices?

MR. KAUFMAN: Sure. So we're talking about the copyrighted work here, software in the form of firmware. Firmware only has value when it's attached to a device. So what we have seen in the phone context and in tablets, in wearables is there's been no emergence or no market substitute of software via this exemption because it only has value when it's

attached to a specific device. So, under that fourth fair use factor about the effect on the market or value of the copyright work, we think that that effect is really negligible because we've never seen the emergence of a market for just the wireless device software itself.

In the phone context, why would that emerge in the context of firmware for -- really, it's the same firmware we're talking about, so that's one thing. And unlocking actually, we think, increases the value of these devices both to recyclers, who can get more value, and to consumers, who can switch carriers and prolong the life span of these devices. So that analysis, when we went through it device-by-device in 2015 and then in 2018, that never has changed because there's never been any evidence of a market for just the firmware itself.

MR. GRAY: Okay. Well, in that case, I think I'm going to give it over to Regan to close out. But thank you very much. This has been very helpful.

MS. SMITH: Thank you. I just wanted to check with Mr. Cheney and see does NTIA have any further questions? No?

MR. CHENEY: No further questions.

MS. SMITH: All right. Well, thank you and

thank you especially to Mr. Kaufman. I think you have the record for sort of bearing more questions than any other participant. And I think, on behalf of me and my colleagues, we want to thank you for your thoughtful and substantive contribution. It was very helpful. Thank you.

MR. KAUFMAN: Thank you for the opportunity. I really appreciate it.

MS. SMITH: Yeah, thank you. I think that is a wrap for this panel. So we -- you can turn off your video if you're done because we're going to segue directly into our audience participation segment. We've had a fair amount of people sign up for that, which is great. So, again, we're going to ask that comments please be limited to about three minutes, if you can, and to identify which topic or proposed class that you wish to comment on.

So I think what I'll do, participants have been notified about the -- provided a link to the audience participation session. But, to get started, it will be Willie Cade, then Jesse Spiegel, and then Brandon Butler, and I'll try to signal in advance as we get to who is next. So, Mr. Cade or maybe Ms. Cade, could you please turn on your video if you're there? Hello? You are muted, Mr. Cade, but when

you're ready, if you unmute, the floor will be yours.

MR. CADE: Thank you. I'm in Class 12, computer programs for repair. My name is Willie Cade. I'm a proud member of the Nebraska Farm Bureau. I'm speaking today in support of a continued exemption for agricultural equipment repair. Physical and logical -- or computer control, transformation of agricultural equipment has continued its rapid advancements since the last review. I believe it's fair to say that the previously recognized frustration by farmers of the lack of access to tools or skills to make use of the exemptions has significantly increased.

Producers' fleets of equipment is a substantial factor of their profitability. Given the high cost and necessarily long utilization of agricultural equipment, those fleets are now transforming to the point where realizing the intent of the exemption is essential. Indeed, the unusually high demand and record prices for used equipment can be partly attributed to the ease of repair with less computerization. As noted in this year's submission from the American Farm Bureau, AFBF, access to software tools for repair does not diminish the value to rights holders.

I'm heartened that the Registrar has

identified a legitimate concern for the exemption benefits engaged in activities such as automobile repair that simply do not implicate copyright in the analog world. Additionally, the change to the exemption from users to such items that were lawfully acquired is helpful. I'm struggling with the issue of necessary tools and how to maintain the integrity of the Act while simultaneously allowing for complete repair. Producers would greatly appreciate your guidance on how to thread this needle. Because software may need to be repaired and because repair may need to change software, I urge the Library to continue to grant the exemption for repairs both in agricultural and generally. Thank you.

MS. SMITH: Thank you, Mr. Cade. That was very helpful. We appreciate your testimony. If there's no questions, I guess we will go to the next person, which is Mr. Spiegel. If Mr. Spiegel can be promoted to a panelist and turn video on. Then we will have Mr. Butler and Mr. Khanifar will be next. Okay. Mr. Spiegel, if you can -- great, I can see you. Go ahead.

MR. SPIEGEL: Good afternoon. I'm going to be talking about Class 1. My name is Jesse Spiegel. I'm a student-attorney in the Glushko-Samuelson

Intellectual Property Clinic at the American University, Washington College of Law, and we have worked with the Joint Educators for many years in this proceeding.

Our society relies on video for everything. We communicate through video. We Facetime, we send gifts, younger people send Snapchat videos, and these often completely replace even speaking at all. So, when we want to learn how to do something, let's say, like, cooking a meal or fixing an electronic, most people don't open a recipe book anymore or an instruction manual, we go on YouTube. And, of course, now we've grown accustomed to working, socializing, and learning online using videos. So, clearly, effective education must also use more videos than ever to match how we now function in society.

And using clips from movies and television shows are a part of how we use videos to learn. The value of these clips can bring is recognized through the already granted exemptions, but the current exemptions include only a sliver of the educational experiences we are having online. We should be expanding access to education and not limiting it. And there are clear distinctions from the online learning platforms covered under the Joint Educators'

petition versus social media sites or entertainment platforms, where users are using or conceivably would use short clips.

Like TikTok, for example, is a platform where users are using clips to teach all kinds of ideas, but TikTok is not an online learning platform. Online learning platforms in our coalition have registered learners that enroll in courses to advance marketable and lifelong skills. They employ sophisticated digital protection measures, limit access to materials to students currently enrolled in courses, and make transformative uses of the clips constituting fair use. The Joint Educators' online learning platforms are not designed to entertain but instead operate for the purpose of providing educational instruction to enhance its users' skill sets. In other words, these platforms respect the goals of the DMCA.

And so we're aware of quality and access to education is a serious problem in America that implicates racial, class, gender, and age disparities that have long been identified but not remedied. So, thankfully, the chance to promote better equity in access to high-quality education through the ability to use the Internet to offer courses at all times and

in all settings, matching individual needs and goals has been gifted to us through technologies that allow platforms like LinkedIn Learning or Osmosis and Muser Media to provide educational opportunities we previously could only receive in the traditional four corners of a classroom that is accessible only to some, virtual or not.

So it's my view that we should celebrate this expansion of educational access, this very real opportunity in front of us to address inequities that exist in our educational system. Even by simply chipping away at them through this exemption and provide learners outside the box of K through 12 and accredited schooling needs to have the same chance of commentary and critical thinking skills that comes from analysis of short clips from movies and TV shows. Thank you.

MS. SMITH: Thank you, Mr. Spiegel. Can I ask a question about how you would conceive an online learning platform if TikTok, for example, would not be one? You know, how would you treat YouTube, for example? Because I know Khan Academy has a lot of videos on YouTube which I think are ways you can experience the teachings of Khan Academy. Where would you put that?

MR. SPIEGEL: Sure. I think YouTube is completely different from the platforms for several reasons. Users on YouTube rely on the viralability of their videos. They want as many people as they can possibly have to view their videos. That's how they make their money. And the platforms that we're advocating for, it's the opposite. They control the access to their information and their educational materials through a variety of means. Like, you have to enroll, you have to be currently enrolled in a course to access the materials, and once your enrollment ends, your access to those materials also ends, whereas on YouTube, things stay on in perpetuity and they want as many eyeballs, regardless of if you're a registered learner or not, to come and view those materials.

Also, anybody can upload something to YouTube regardless of if you're a sophisticated educator or not, whereas the platforms we are advocating for, they're run by educators with serious credentials and as well they're employing digital protection measures and really making sure that the content that they're using is only used for the educational purposes that they're advocating for, whereas Youtube is what I would call an entertainment

platform.

MS. SMITH: Okay. So I take it that your position is that if you are, for example, Khan Academy, you would have to sort of treat your use of the same content different depending upon what platform it is presented on with respect to 1201 and potentially an exception or limitation that they may be relying upon, is that correct?

MR. SPIEGEL: I would say so, yes, definitely.

MS. SMITH: Okay. Thank you. So, if we have no more questions for Mr. Spiegel, I think -- thank you. Thank you very much. We appreciate you sharing your thoughts. And now we are looking for Mr. Butler to turn on his video. Hello.

MR. BUTLER: Hello. Hi, everyone. Good afternoon. Thanks for letting me join you briefly here. So I'm joining on behalf of the Software Preservation Network and just wanted to add a little gloss to some of the modifications that we proposed in our reply comments. So I was able to watch our team on Monday and they did a wonderful job, and I think they actually were able to communicate this, but, on reflection, it really seemed to me that there was a lot of concern, both from the Office and from some of

the industry folks, about the notion of a public -- you know, a publicly accessible arcade, that anyone who finds -- who stumbles upon the collection could play online unmediated. And so I just wanted to reiterate that it's our view that the new concessions in our reply comments sort of add up to a situation where that shouldn't be covered by the exemption. So the requirements for being eligible that we adapted from the sort of revised 108 discussion document include that final requirement that reasonable digital security measures as appropriate to the activities be in place. And then we also suggested that, again, if this is a real concern, public access unmediated is a real concern, then also the language from 108 about, you know, having no prior notice or no notice that the requestor intends to use the material for any reason other than private study, scholarship, or research.

Given those two things together, it seems that, you know, an open -- a wide open unmediated kind of online arcade situation would be a situation where at least arguably the security systems in place are not adequate given that the purpose is to provide access only to people with, you know, that sort of private study type of an intent, right. We would be kind of on constructive notice that some people who

stumble across this stuff would not have that purpose and we wouldn't be doing enough to prevent those folks from having access if we just created a wide open online arcade.

So, if the rule that you're trying to craft is one that precludes that sort of wide open unmediated arcade, we think this rule is it. And we just wanted -- we thought that might be helpful to you because we could feel the angst in the virtual room over that possibility. And so one way to do that, if you're worried that that is not clear in the text of the rule, we'd also be open to kind of, I suppose, the equivalent of legislative history, right. In the Register's recommendation, you could explain that it is the Office's view, you know, that is the Office's interpretation of those two provisions in combination. And folks like us who try to give advice and guidance would take note of that and tell our clients and our institutions.

MS. SMITH: Thank you. Yes, we do consider the Register's recommendation, as well as the preamble to the final rule to be administrative guidance provided by the Office or the Library. Do either of my colleagues have questions?

(No response.)

MS. SMITH: Okay, thank you, Mr. Butler. So our next speaker will be Leticia Reynolds. If Ms. Reynolds could turn on her video? And then I just wanted to make sure those who are next are aware, so Sina Khanifar, if you're here, could you raise your hand so you can be promoted to a panelist? Then we also are looking for Kevin O'Reilly and Dennis Rigdon. All right. And here is Ms. Reynolds. Great. I can see you're here, but if you could please turn your video on if you would like to have video?

MS. REYNOLDS: So I'm not 100 percent sure my video is on. You just can't see me.

MS. SMITH: Okay, well, we can hear you, but you're a black square. So if you would like to -- that's fine if you would like to go ahead. It might be a camera issue, but if you'd like, we can hang for a second if you would like to figure it out. Let me know.

MS. REYNOLDS: I don't want to take everyone's time, so I'll go ahead. It's a new computer, so maybe I haven't figured out all the kinks of it yet.

MS. SMITH: Sure.

MS. REYNOLDS: So my name is Leticia Reynolds. I'm the President of the Colorado

Association of Biomedical Equipment Technicians, and I am -- sorry, I've never done this before -- so I am coming to try to persuade that we look at service materials needed for medical equipment repair is exempted from some of the copyright rules. I'm talking about, like, service keys or programs that are used to do maintenance.

Medical device manufacturers are hiding kind of the essential repair information and tools behind the Digital Millennium Copyright Act. This has made it where biomeds across the country are unable to support and maintain devices that maybe they have within their facilities. In a time like the pandemic that we have suffered last year, it made it where critical devices, unfortunately, we weren't able to maintain without relying totally on the manufacturers, which could lead into a delay of patient care and expensive repair costs, having to send them out or wait on vendors. So I encourage you to exempt service -- tools needed from some of the copyright regulations.

MS. SMITH: Thank you, Ms. Reynolds. Does anyone have any further questions?

MR. CHENEY: Maybe just a clarification there. When you say that they are making those not

available, what do you mean? Are they locked on the device itself? Are they behind a pay wall that you have to pay extra money to get those? Can you describe just a little bit how -- why is it that you're not able to access those repair materials or manuals?

MS. REYNOLDS: Sometimes manufacturers will not even -- even if you've been to school, they won't provide those materials. Other ones, you have to go to school even if their device is your own -- that maybe a hospital or facility owns. And so, unless you pay extra additional money or a subscription fee, you don't have access to those materials.

And that can go with service literature as well. I've seen examples. I work on anesthesia units and I went to school, but those manufacturers wouldn't give you access unless you paid for a tool or software to get access to those manuals. And so then you're very limited on your ability to repair medical devices without tools maybe for maintenance, routine maintenance or even service events.

MR. CHENEY: Okay. That's helpful for me. Thanks.

MS. REYNOLDS: Thank you.

MS. SMITH: Yes, thank you. So next we have

Kevin O'Reilly. And then just to preview who will be up next, Dennis Rigdon, Gay Gordon-Byrne, and Paul Roberts, if you can raise your hand if you're an attendee so we can get ready to bring you up. And, Mr. O'Reilly, if you could turn on your video, we are ready to hear from you.

MR. O'REILLY: Great, thank you so much. My name is Kevin O'Reilly. I am a right-to-repair advocate with U.S. PIRG. Again, I'm here to talk about Class 12 and the repair of electronic devices, also particularly about medical equipment.

So the problem that exists today, as Leticia just touched on, is that qualified biomedical repair technicians, also known as biomeds, are often locked out from being able to fix essential medical equipment, things like ventilators, imaging equipment, anesthesia machines, and all sorts of devices throughout the hospital. This has been a problem for a long time, but it's especially come under the microscope during the pandemic at a moment when manufacturers and biomeds that work for the hospital or even independent service organizations all should have been working together. Many in-hospital and independent biomeds continue to be locked out from servicing equipment, leading to delays of days, to

weeks, to sometimes over a month.

When you need -- a patient comes in and needs a ventilator or needs an MRI machine, there's no time to wait for an authorized or a really branded technician to come out and make the fix. So these software keys and software locks are a common way that it happens, and what we're really hoping is that we can remove the kind of fact that they're hiding behind the DMCA to shield this branded repair in order to deliver the benefit to patient care.

One thing that is worth noting is the FDA has looked into this and looked at whether or not there should be any regulation as far as in-house and independent biomeds go, and since 1996, they have decided not to undertake rulemaking on this account. So the FDA has purposely not taken any action on this. So we hope that by, you know, allowing for this circumvention that we won't allow the manufacturers to go further than what the FDA has called for.

MS. SMITH: Thank you, Mr. O'Reilly. I have a couple questions and my colleagues may too. Do you have any -- when you say the FDA has looked at this, can you provide any, I don't know, citation or any reference to that that is public?

MR. O'REILLY: Absolutely. So the FDA

issued a report in 2018. I can look up the name of it or also provide -- hold on, I've got it right here. So the report is called the FDA Report on the Quality, Safety, and Effectiveness of Servicing of Medical Devices. And then I can also follow up with the exact page number where they go into the specifics on the decision as far as rulemaking goes.

MS. SMITH: Okay, thank you. I think, you know, I think we have your contact information, and if we are going to be issuing a post-hearing letter, we would include you in the set of people who commented on this class that could receive one. But in your -- do you have knowledge as to whether that report addresses copyright or the DMCA or software locks at all in the consideration?

MR. O'REILLY: So it doesn't look into software locks. It more looks at the decision of whether or not the FDA would impose the regulations that it imposes on medical device manufacturers on the basically third-party repairers, whether that's folks that work for the hospital, folks who work for independent repair organizations.

MS. SMITH: Right. So, in the determination not to commence a rulemaking, it doesn't seem to your knowledge that the FDA was imputing a reliance

interest upon the copyright laws in separately regulating third-party actions?

MR. O'REILLY: Yeah, to my knowledge, that wasn't the case.

MS. SMITH: Okay. But is it to your knowledge that it is the DMCA right now that is sort of serving as a but-for cause that is precluding this repair that you would like to see enabled?

MR. O'REILLY: Yeah, that's my understanding. We've seen cases where independent service organizations have found ways to break those service locks that exist and they have been pursued for litigation by the manufacturer themselves citing this. So we're worried about that and think that that shouldn't be the case because, ultimately, the ability of folks to do that allows for better patient care.

MS. SMITH: Thank you. Anyone else have any questions?

(No response.)

MS. SMITH: No? All right.

MR. O'REILLY: Okay.

MS. SMITH: Thank you.

MR. O'REILLY: Thank you very much.

MS. SMITH: Thank you. I think next we're looking for Ms. Gordon-Byrne, and then Paul Roberts,

Mark Schaffer, get ready. Raise your hand, please. But, Ms. Gordon-Byrne, if you could turn on your video. Okay, please go ahead.

MS. GORDON-BYRNE: Okay. Hello. My name is Gay Gordon-Byrne. I'm the Executive Director of the Repair Association. I'm here to talk about the exemptions for anything with embedded software in Class 12. And what I'd like to try to get across is that repair doesn't create piracy. It just returns equipment to function. And from the repair community perspective, the only really interesting thing that we need to do is be able to restore the equipment according to whatever it is, the tools that are provided by the manufacturer that are not made up. These are tools that are made for that purpose and they are being withheld, and that means that no matter what somebody wants to do, whether it's fixing a ventilator, a tractor, a cell phone, a refrigerator, they are limited.

And I don't see that there's -- I believe there should be a very strong standard for blocking repair and I think it should be associated with actual evidence of piracy because, absent piracy, there's no -- I don't see why we can't all fix our stuff. So games can't be played on a broken device. It means

that the owner can't use the games that they've lawfully acquired. It probably also drives that game station owner to go buy a new console to be able to play the games they've already purchased. And I think that that is a consequence that shouldn't be something that the Copyright Office creates. Same thing with being able to repair any other thing with an embedded device.

I looked back at the Napster experience because I was a parent of teenagers in that time, and Napster did go after their customers and they chose a couple of teenagers and they went after them and parents like me said, uh-uh, not doing that, take that stuff off, take that stuff away, and Napster went away. So I'm curious as to what the content providers are doing in terms of enforcement because it strikes me that they're really being kind of lazy. They could be building things that can be repaired without any kind of piracy. They could be authenticating in different ways if it's really happening. And if it's not really happening, especially with the technology that came out of the '80s and '90s, why are we blocking legal repair? Are we really making a difference? Is this something that should be done? And I just urge you to take a look at some of those

things, that it's very, very distortion to a legal repair market, and that's what we're trying to expand and not make more difficult. So thank you.

MS. SMITH: Thank you. Does anyone have any questions for Ms. Gordon-Byrne?

(No response.)

MS. SMITH: No? We appreciate your testimony. Thank you.

MS. GORDON-BYRNE: Thank you.

MS. SMITH: I think next we will have Paul Roberts. And then I just want to call out again the three people who have signed up that we've not been able to locate. In case you're -- if you become here raise your hand, but Sina Khanifar, Dennis Rigdon, and Mark Schaffer. But, Mr. Roberts, we're happy to see you and please go ahead.

MR. ROBERTS: Hi, everybody, can you hear me okay? Okay. Thank you very much for inviting me to speak. My name is Paul Roberts and I'm the founder of securepairs.org. We're a volunteer group of more than 200 of the world's top information security and information technology professionals who support the right to repair, and I'm here today to argue in favor of the Class 12 exemption for repair of all software-enabled devices.

So the first thing I want to do is to offer my group to you as a resource on questions or concerns you may have about the intersection between technical protection mechanisms, TPMs, and cybersecurity. Our members in securepairs include experts and academics and independent security researchers in areas like hardware and software security, including some of the top researchers in areas like embedded device security, the security of medical devices, and more. And we are here really for you as a resource. You have my contact information, and I would be happy to connect you with any of our experts to answer, to do one-on-one sessions or Zoom sessions to field questions that you might have on these issues because I understand they are complex, you guys aren't cybersecurity natives, and so these can be challenging and confusing issues to contend with. And I really appreciate that, and I really welcome your efforts.

Let me just say briefly I think it's really important for all of you to understand, you know, kind of the nature of cybersecurity problems with embedded devices, connected devices, including, you know, let's say, medical devices or Internet of Things devices, smart home devices. The attacks and threats facing these devices have nothing to do with data stored or

secured by TPMs, data needed to access a device and repair it, replace a part and get that part to be recognized by the device, right.

Attacks on connected devices have to do with poor security and poor design or poor deployment of the device itself. For example, in 2015, TrapX, a security company, wrote a report called MedJack about a string of attacks on hospitals that targeted specifically -- the malware targeted connected medical devices. The problem there was that many of these medical devices -- this was in 2015 -- were running an operating system, Windows operating system that was almost 10 years old, and that's incredibly common in the medical device space and in other spaces.

So I think you need to understand that companies that are mature and healthy and robust in terms of information security have certain practices that they have enacted, internal security reviews, software security by design, default, and deployment. They have bounty programs where they reach out to independent security researchers and invite them in to test the security of their products.

They don't practice what many of these device makers are trying to push on you, which is security through obscurity, that if we just prevent

people from accessing our platform or understanding at all how it works, then we can keep it secure. And the reason that doesn't work is very simple, which is cyber criminals, whether those are nation state actors, like Russia and China, or just motivated criminals, for-profit type of criminal groups, are very resourceful and they're very determined and they, frankly, really don't care what the Library of Congress or the FTC or anybody else says the rules are. They're going to do what they need to do to get access to the systems that they want to access.

Who it disadvantages are white hat independent security researchers, repair technicians and professionals who want to access these devices for pro-social reasons, to extend their useful life, to conduct above-board security research into the cybersecurity, the device itself, so that the company can be aware of a cybersecurity flaw and issue a patch for it and improve the overall security of the entire connected device ecosystem.

So I just want to make really clear that the types of information that we're talking about that is -- that we need to -- that repair professionals and technicians need to get access to to replace parts, service problems, update software is not the type that

hackers are after or malicious actors or ransomware groups to carry out attacks, steal information, and so on. We know that there is a link between repair and these types of attacks because we already have an epidemic of these attacks, in healthcare, in smart home, in obviously critical infrastructure sectors as well, and this is happening independently of any broadly written right to repair.

So I really would encourage you to grant this exemption for repair and allow the very important work of repair professionals and technicians to go ahead and not to get suckered in to this kind of security through obscurity argument. Thank you.

MS. SMITH: Thank you, Mr. Roberts. Do we have any questions for him?

(No response.)

MS. SMITH: We appreciate your contributions today. Thank you.

MR. ROBERTS: Please do feel free to reach out if you want to connect with any of our experts. It's an excellent resource for you on some of these questions.

MS. SMITH: Okay, thanks. We appreciate it. At this point, our sort of solicitation of information is nearing conclusion, so if we issue post-hearing

letters, we'll include you on the class and we will also institute at the Copyright Office a process for ex parte communications where you can come and talk to us, but you need to disclose what you've said so that everyone who is interested in the area can follow along. Yep.

MR. ROBERTS: Great.

MS. SMITH: Okay, thank you.

MR. ROBERTS: Thank you.

MS. SMITH: All right. So I think the last person we've been able to locate is Mark Schaffer. If we can bring him up, please. And then I'm just noting two sign-ups, Dennis Rigdon and Sina Khanifar, if you are here, end up being here, raise your hand. Otherwise, I think Mr. Schaffer will be our last speaker. Hello, Mr. Schaffer, we're interested in hearing your contribution.

MR. SCHAFFER: Sure. Sorry about that. I was on double secret mute. It does happen. My apologies. So, yeah, thank you for hearing from me today. I know you've heard from several of us already and I just wanted to reiterate I think the need for making sure that owners of their products, either phones, laptops, tablets, whatever, they have the right to repair their products if there are software

issues or other issues that are preventing them from having the choices to be able to pick where they want to take their products to be repaired and to have their products repaired. So I don't -- I think, from a consumer standpoint, I'm speaking as a consumer of many of these products, I would love to be able to, hey, if my battery is dead or my screen is broken, that I have the choice to do that, that I don't necessarily have to send it back to the OEM or I am encouraged more along the lines of having to buy a new device. I think, from an environmental perspective, you don't want to have to go buy a new device when most of, 80, 90 percent of your device is still functioning.

So you need to have the ability to have those choices as the consumer, and I just think I'd like to see more support for that. I want to make sure that there isn't the ability to use DMCA and other legal, I guess, I wouldn't say loopholes necessarily, but legal issues around why I can't do that as a consumer. And I just would like to support seeing more support for repair and preventing hiding in some of these technical things that are available to some of the manufacturers today so that we can actually extend the life of our products and bring the

consumers more into the front, because it's very hard -- I engage in many standards and other things to try to improve these products, but it's very hard for the voice of the consumer to be heard.

So I do strongly appreciate your time today to hear sort of the voice of one of the consumers that loves his electronics but also gets a little frustrated with some of the limitations that are put upon them in making sure I can extend the life of those products. So thank you so much. I appreciate your time.

MS. SMITH: Thank you. The consumer perspective is certainly valuable. Thank you for coming today.

MR. SCHAFFER: Thank you. Sorry I'm late.

MS. SMITH: No worries. And I think we have found the next panelist too, so certainly no worries at all. Thank you, Mr. Schaffer. And if we can promote Mr. Khanifar. And I might not be saying that right. Hello.

MR. KHANIFAR: Hello there. Hi, everyone. First of all, I want to thank you all for the proceedings. I've been dipping in and out during my workday over the last few days, and I really appreciate the process that's being run and the care

and attention that's put in, been put into this.

My name is Sina Khanifar. I'm CEO of a company called Waveform. Honestly, historically, the part that I've been most interested in is on the unlocking side, but I missed most of the hearings this morning on that front. One thing I did want to kind of add there is it's just -- you know, I think with the rollout of 5G, we see computers like Apple building their own 5G chip sets and I really think that that integration is going to become broader and broader and that the need for unlocking in different types of devices is going to become greater and greater. So I think, as a consumer and as a technologist, I really encourage broadening those unlocking rules to apply to more types of devices.

And then secondarily, kind of reflecting on yesterday's hearings on the repair side of things, I run a company that sells wireless devices to consumers to help rural customers improve cell phone reception, and one of the biggest problems that we run into as a reseller is that our vendors don't take returns very often for the products that they sell us. And so we need to be able to repair those devices in order for them -- in order to not have to throw them away.

And the degree to which these software

devices are becoming basically pure technology, one of the most popular devices that we actually sell is this ray. It's an ASIC with custom firmware and custom software. It's very little of what we used to sell a decade ago, which was a ceramic-based filter that would amplify your cell signal. It's all software. And being able to repair those types of devices for us is just critical to honestly running a profitable business because these devices break on the regular. And so expanding, I think, the repair provisions or exemptions to all kinds of devices is really, really important for companies like mine. That's all.

MS. SMITH: Thank you. Any questions?

(No questions.)

MS. SMITH: Okay. Well, thank you for speaking today. It was very helpful.

MR. KHANIFAR: Thank you so much.

MS. SMITH: I think that then concludes the hearing for the 1201 rulemaking. And I think I mentioned a couple times, but the Office may issue post-hearing letters to participants in a particular class and then we will continue our analysis. We've appreciated -- got a lot of good information, I think, through these hearings. So we will continue analyzing and consulting with NTIA, and then the rulemaking is

on track to be completed in October of this year.

Thank you very much.

(Whereupon, at 2:28 p.m., the hearing in the above-entitled matter concluded.)

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

REPORTER'S CERTIFICATE

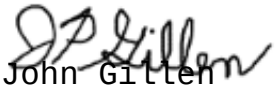
CASE TITLE: Section 1201 Rulemaking Hearing

HEARING DATE: April 21, 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 21, 2021



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

B

C

D

P

Q

R

S