UNITED STATES OF AMERICA

+ + + + +

LIBRARY OF CONGRESS

+ + + + +

U.S. COPYRIGHT OFFICE
SECTION 1201 ROUNDTABLE

+ + + + +

WEDNESDAY
APRIL 25, 2018

+ + + + +

The Section 1201 Roundtable met in the Room 1314, UCLA School of Law, 385 Charles E Young Drive East, Los Angeles, California 90095 at 9:00 a.m., Regan Smith, Deputy General Counsel of the U.S. Copyright Office, presiding.

PRESENT

REGAN SMITH, Deputy General Counsel, U.S. Copyright Office
ANNA CHAUVET, U.S. Copyright Office
STACY CHENEY, National Telecommunications and Information Administration
JOHN RILEY, U.S. Copyright Office
JULIE SALTMAN, U.S. Copyright Office

ALSO PRESENT

COREY DOCTOROW
JAY FREEMAN, SaurikIT
JOHANN GEORGE, OmniQ
KARIN GILFORD, Movies Anywhere
BRUCE JACKSON, Air Informatics LLC
SINA KHANIFAR, Electronic Frontier Foundation
ROBERT MIRANDA, SmarTeks
THOMAS MOONEY, Harman International
CYNTHIA REPLOGLE, iFixit
KIT WALSH, Electronic Frontier Foundation
KYLE WIENS, iFixit
J. MATTHEW WILLIAMS, Joint Creators II
MATTHEW ZIEMINSKI, Puls

CONTENTS

PROPOSED CLASS 7: Computer Programs - Repair 5

PROPOSED CLASS 11: Computer Programs - Avionics 123

Los Angeles Audience Participation 160

Adjourn 231

Exhibit No.		Page
3-C	Karin Gilford Presentation	161
3-D	Johann George Presentation	284

P-R-O-C-E-E-D-I-N-G-S

9:00 a.m.

MS. SMITH: All right, great. We're going to start. It's 9 o'clock, so thanks for being here.

This is the section 1201 hearings, and it's the last day. We're talking about Class 7, which is repair.

My name is Regan Smith. I'm Deputy General Counsel of the Copyright Office. And I see some familiar faces, some not familiar faces.

So, just quickly, we're going to be commenting and facilitating a discussion about whether or not to expand the contours of the current temporary exemption for a class of concerning repair of motor vehicles.

If you'd like to speak, tip your placard up and we'll call on you. And try to say your name for the court reporter.

And I think we'll start by -- we'll introduce ourselves. And then you can introduce yourselves.

MR. CHENEY: I'm Stacy Cheney, Senior Attorney-Advisor at NTIA, National Telecommunications and Information Administration. Good morning.

MR. RILEY: I'm John Riley, Attorney-Advisor, Copyright Office.

MS. SALTMAN: Julie Saltman, Assistant General Counsel at the Copyright Office.

MS. CHAUVET: Anna Chauvet, Assistant General Counsel at the Copyright Office.

MS. SMITH: Mr. Miranda?

MR. MIRANDA: Robert Miranda, founder and owner of SmarTeks.

MS. WALSH: Kit Walsh. I'm a Senior Staff Attorney at the Electronic Frontier Foundation here in support of the proposed exemption.

MR. WIENS: Kyle Wiens, founder of iFixit. I'm here in support.

MR. ZIEMINSKI: Matt Zieminski, logistics and quality at Puls. In support.

MR. WILLIAMS: Matt Williams from MSK representing AAP, ESA, MPAA, and RIAA.

MR. MOONEY: I'm Tom Mooney with Harmon. I lead our global public affairs shop.

MS. SMITH: Great. Thank you.

MS. SALTMAN: Okay. Good morning. Before we start, I just wanted to sort of let you know how we're planning to proceed, because there are a lot of issues at play in this particular

exemption.

So we sort of see that there are five different categories of -- or we sort of like divided the possible expansions into five categories. And we're going to go through each one in turn. So, I would appreciate it if you could sort of direct your comments to the issues that we're talking about at the time.

And also, because we have a lot to cover in just two hours, please keep your responses as sort of short and direct as possible.

So, I'd like to start with the EFF's request to expand the exemption to cover non-motorizing vehicle devices or other devices. And also address the modification or tinkering aspect that they raise. Then we'll talk about telematics and entertainment systems after that third-party repair. And then finally tools.

So, for -- wait, so I'm going to direct my first question to Ms. Walsh.

You've asked for an exemption for modification and repair of various types of devices including internet of things devices, appliances, computer peripherals, toys, are you limiting your request to consumer devices?

MS. WALSH: No. Just as with the

security research exemption, it's important that devices not necessarily intended for individual consumers be repaired.

So, for instance, power generator systems, control systems, computer systems are in a wide variety of devices. I think probably some of my colleagues could speak to more examples of the non-consumer devices as well.

MS. SALTMAN: And what evidence is there in the record that there's a need for an exemption for those type of devices?

MS. WALSH: So I think I'd like to ask my colleagues to address that.

MS. SMITH: Is there anything in the record yet? Or is this going to be new?

MR. WIENS: I mean, we -- under the --

MS. CHAUVET: I'm sorry to interrupt. For the court reporter, if you could please all say your name before you start speaking.

MR. WIENS: Sure.

MS. CHAUVET: Thank you.

MR. WIENS: Kyle Wiens. The Copyright Office found that there was standing for an exemption for repairing agricultural equipment. And I would refer to a lot of the discussions around that.

MS. SALTMAN: Okay. So, in terms of the devices discussed in your submissions, some of these devices are devices that -- where the TPM would control access to more expressive works. And some of the devices seem like they are less likely to control expressive works. How could the Office craft an exemption that is supported by the statutory analysis that covers both types of devices?

MS. WALSH: Mm-hmm. So a lot of the opposition to the class is oriented towards concerns about infringement. So you might have -- and we had opposition in regard to video game consoles and in regard to devices that entail entertainment products.

So there are two ways that the exemption as proposed is limited so that it doesn't speak to those products.

The first is, it's about access to software. So you're allowed to circumvent in order to -- the class of works is software.

The second is, the proposal is that the class will only cover non-infringing uses. So, to the extent that there's concern about infringement, that's still covered not only by ordinary copyright law, but also not subject to the proposed exemption.

MS. SALTMAN: So, in terms of -- well, let me start with video game consoles. How is expanding this exemption to video game consoles different than an exemption for jailbreaking video game consoles, which the Register has rejected twice out of concern for piracy and infringing uses that could follow from that.

MS. WALSH: So there are two components here. There's repair, which we've been using broadly for repair, diagnosis, maintenance of video game consoles.

Then there's modification. So, in regard to modification, it would include the ability to jailbreak a video game console.

MS. SMITH: So since we have decisively rejected that in multiple past rulemakings, why should we reconsider that conclusion?

MS. WALSH: You look like you're champing at the bit.

MR. WIENS: Well, I would encourage, maybe, Robert could explain a little bit of the situation on the ground. He runs a repair shop in Barstow that fixes games consoles.

MR. MIRANDA: Robert Miranda. Some of the -- so we are a general electronics repair company. If this may help. So, let's say a

consumer brings in a, let's say, a PS4, for example. And their drive isn't working where the disc inserts. If we wanted to replace that drive, we couldn't just pull out the drive and put a new part in as if it was a car. You can change the tire. You're good to go.

The new drive is software-locked to the motherboard which that plugs into. And it causes the device, the drive not to work at all.

So, essentially, what you have to do is you have to replace all the internals, which has the economical impact that the repair price is three, four hundred dollars more than what the device is even worth.

And it goes into other, you know, e-waste problems. Multiple problems like that. Essentially, not having that software lock between the devices would allow us to properly serve the community. Because there's no near service centers anywhere. It takes four weeks for someone to even get a device repaired if they had to send it out.

MS. SMITH: So you know they can send it out and get it repaired by the video game manufacturers?

MR. MIRANDA: Yeah. But it's not necessarily repaired. It's a console swap. They

would get something different. They wouldn't get their old console. They would lose a lot of saved data, content. So by us providing this service, we'd be able to reduce costs. We'd be able to prevent a lot of e-waste. We'd be able to, even as far as just having the consumer be able to fix it the same day versus waiting a long time for something simple.

MS. SALTMAN: And aren't those consoles generally covered by warranties, just in terms of the cost of repair?

MR. MIRANDA: So, some -- yeah, there's a one-year manufacture warranty on these devices. But there's a lot of consumers that we serve that don't have warranty, and they don't have any other option.

MS. SALTMAN: Mr. Williams?

MR. WILLIAMS: Thank you. Matt Williams. I wouldn't say they don't have any other option. I think we have submitted evidence, both in the 2015 proceeding and in this proceeding, that shows that the console manufacturers can do repairs.

There are one-year warranties. And then there are also extended warranties available as well. And then the pricing may vary depending

on what type of repair needs to be done. I don't think it's accurate to say that, in all instances of repair, all the content on the console would be lost. But I would need to speak directly to the console manufacturers about that.

But I don't think there's anything in the record to this point at all that speaks to the situation on the ground being any different than it was three years ago. So I don't think there's any grounds for making a different decision here.

MS. SALTMAN: Mr. Zieminski?

MR. ZIEMINSKI: Yeah. Matthew Zieminski. Our organization represents 2,000 technicians that are mobile that promise a service that can come to you and do a repair in 60 minutes or less.

And right now, with game consoles and certain smart phone repairs, we cannot guarantee that because there are software locks that tie components to each other that arbitrarily make it so that we cannot complete that repair.

And it maybe was not as big of a problem three years ago as it is now. But I think that the problem right now is that more and more consumers have these devices in places that these manufacturers don't have service facilities,

whereas our technicians are in places like Omaha or Lincoln, Nebraska, we can do that repair in a customer's home and get them set up that same day. Otherwise, they have to ship it out.

MS. SALTMAN: Does the lock on that you have to circumvent to repair like a physical piece, like the disc port or whatever, by circumventing that lock do you have access to creative content as well, to the actual games?

MR. ZIEMINSKI: No. The only thing when we do a repair that we are actually doing is taking a new component that -- you know, taking the old, broken component out, putting the new component in. And maybe firing it up, turning it on with the customer to verify that it works with them.

MS. SMITH: What types of devices are you repairing?

MR. ZIEMINSKI: As an organization, we repair iPhones, Google Pixel devices, Samsung devices. We're starting to do TV installations and smart home appliances. And we've, you know, done some odd jobs for game consoles as well.

MS. SMITH: And in what instances have you, you know, needed to undergo to circumvent TPMs or, you know, been prohibited because it would have

required circumventing a TPM?

MR. ZIEMINSKI: Sure. So, primarily we do smartphone repairs. And there's--- on an iPhone, for example, if you have a home button that has touch ID, that is digitally paired with the logic board.

It's very common, the way that these phones were designed, that like on the iPhone 5S for example, as soon as you open it up, you tear that cable. It's very easy if you open it up too far. Because we don't have access to certain things that would make that repair viable, we essentially cannot complete the repair if that cable is torn. You've now lost that capability of having your touch ID.

So what we have to do is either tell the customer, hey, you have to get a new device from the manufacturer, or we can replace it and you can just restore functionality of your basic home button.

This was an issue a couple of years ago in the news where it actually ended up shutting down devices entirely just for this lone reason. It was a solvable reason, but it happened.

MS. SMITH: Do you have any other examples?

MR. ZIEMINSKI: For us, specifically, no, not immediately.

MS. SMITH: Thank you. Mr. Williams?

MR. WILLIAMS: Thank you. Matt Williams. I think Mr. Zieminski referred to the locks as arbitrary. And I think the record's been established that, with video game consoles specifically, they are not arbitrary, they are integral to the overall design that's intended to protect the copyrighted content that's accessible through the consoles.

MS. SALTMAN: So, on that point, if an access control to repair some physical component of the console were circumvented, are you saying that could allow for access to creative content?

MR. WILLIAMS: Yes. My understanding is that most of the repairs that have been talked about would result in a jailbroken console.

MS. SALTMAN: And so then like a subsequent user, like not the repair person, but the user when they get the device back, would then have sort of like enhanced access to the creative content. Is that what you're saying?

MR. WILLIAMS: Yes. They could play unauthenticated copies of games. So, pirate copies of games.

MS. SALTMAN: Okay. Thank you. I didn't mean to cut you off if you had more.

MR. WILLIAMS: No. No, that was the main point that I wanted to make. Some of these other devices that are coming up kind of for the first time really in the record, it's hard to respond to whether each type of device would involve the same type of problems that I'm describing.

But I don't think that there's anything in the written record that establishes that really any kind of device can't be repaired through the same types of channels that video game consoles can be repaired.

And I think that when you are talking about devices that are designed to access expressive works, that the countervailing interest of preventing the unauthorized access outweighs the need to get to independent repair.

If you're dealing with motor vehicles, you've decided that's not the case. If you set aside entertainment systems, and maybe there's some other device that is more in that line that's not designed to access expressive material, but I don't think I've even seen an example like that in the record anywhere.

MS. SALTMAN: Mr. Wiens, if you have any

examples of what Mr. Williams was just describing?

MR. WIENS: Sure. Yeah. Kyle Wiens. I'd love to -- okay, we want to give the customer the device back in the exact state that they give it to us, which means the device absolutely should not be jailbroken, it should be locked down. There shouldn't be any additional ability to pirate content.

The goal is not to expand the functionality of the device in any way. The goal is to -- I have a physical optical drive that's broken. That's one of the most common things that fails. It's mechanical. It spins around. It's got a laser. It fails. We want to be able to replace that drive for people. Or repair the drive in place.

MS. CHAUVET: Well, would it be reasonable then to have a limitation in the exemption to that? Like basically having it be returned to the state that it was in before the repair was attempted to be made?

MR. WIENS: I believe EFF's language is in that vein, yes.

MS. WALSH: Well, I'd also stress the importance of modification. So, that includes many of the examples that we put into the record about

you need to modify to use competitive light bulbs, to use competitive cat litter, printer cartridges, et cetera. That sort of consumables market is one where modification is necessary in order to get the value out of the thing that you paid for and prevent unfair monopolies from being the result of leverage of DRM.

I see a question. There are other examples of enhanced functionality of drones and radios and other devices that we put in.

MS. SALTMAN: And just on the first point, relating to Ms. Chauvet's question, do you think the definition of repair in section 117(d) is consistent with what you're seeking with respect to repair? I understand it doesn't include modification.

MS. WALSH: So, section 117(d) sort of breaks-out the concepts of maintenance and repair. And the concept of repair that we're all talking about includes maintenance. It also includes a diagnosis component.

And it should be clear. I think under that definition it's clear. But it should be clear that if you're repairing a bug or a vulnerability or something in the original device, that that's repaired, even if it's not authorized by the

manufacturer.

MR. WIENS: I'd also note that this really comes down to the design of the device. We don't want repair of these devices to have to impinge on the copy protection mechanism.

It just so happens that the way that a couple of manufacturers decided to design their product meant that the component that was most likely to fail cannot be replaced without also replacing the most expensive part of the console.

And that was an explicit design decision that absolutely did not need to happen. It should be very possible to swap out the optical drive without compromising the authentication function.

MS. SMITH: What do you say to what Mr. Williams just said, which is that 1201 exists in part to encourage copyright owners to disseminate their works digitally? They've designed the lock in this way because I guess they've determined this is what they need to do in order to incentivize them making this available in the first place.

MR. WIENS: If you think about every person that has a failed console and has to go out and spend four hundred dollars on a new console, that's four hundred dollars that they aren't spending on games.

MS. SMITH: But I think we just established that it could be repaired under warranty, right? Is that not --

MR. WIENS: I mean, these consoles -- and this is credit to the manufacturers. I have an Xbox. I've had it for four years. The warranty only covered the first 25 percent of the time that I've had it.

So, the warranty -- usually these failures, particularly the optical drive, it's a wear component. It's a mechanical component. They don't generally fail within the first 12 months. They fail two, three, four years out.

MS. SMITH: Mr. Williams, did you want to respond?

MR. WILLIAMS: Thank you. I credit that Mr. Wiens doesn't necessarily want to enable any kind of infringement through engaging in the repair. But I don't think there's anything in the record to show that the consoles have been designed in the way that they are for any reason other than copyright protection and, you know, basic functionality of the consoles.

I don't think I've heard yet an affirmative representation that they can repair the consoles in all instances and put the copyright

protection scheme back in place to avoid returning a jailbroken console.

We did say in our comments that it would be far preferable if a repair exemption included the 117 language that requires you to get back to the original functionality.

Of course, this proposal goes way beyond that and goes even to modification and to jailbreaking. But, even if that was included in a repair exemption, I would have a lot of concern. And I know it's a separate bucket today, but when you get into the repair shop scenario, not everyone might be as well intentioned as Mr. Wiens.

And if you've got all these repair shops that are supposedly returning consoles back to their original functionality, trying to go out and police all of that would be very, very difficult. And I think it would be prone to a lot of abuse.

MS. SMITH: So if there were an exemption which was crafted around repair and maintenance in 117(d) more tightly, and not extending to third parties -- and now understand we're going to talk about other things after this. But what is the concern from the point of view of your clients in terms of the statutory factors?

MR. WILLIAMS: Sure. So, number one,

I'm not very confident that they can actually restore the copyright protection system that's on the consoles.

MS. SMITH: Maybe they can't. Maybe they can't make use of the exemption. But 117(d) says this is a non-infringing use if you can restore functionality.

MR. WILLIAMS: Well, 117(d) says that's a non-infringing use if you're an owner of the software. In this instance that would not be the case.

I understand that sometimes you've gone beyond that when you've determined that in specific instances the record justified it. But our position would be that 117 would not cover this activity because it's limited to owners of copies of software.

Setting that to the side, in the past, when you've looked at this issue, because of the potential harms involved, you've said that the activity involved with copying of the software is a different analysis under the fair use factors and under the 1201 factors. The potential harm that could be caused is much greater.

So, I just think they're a very different category of devices. I don't think

there's anything in the record to establish that they can restore these devices to their functionality. I think a lot of what we're hearing today we're hearing for the first time.

And if you're going to kind of go back on some of what you've decided in the past in this space, which is a very sensitive space, I feel like there should have been a much bigger record built and a much stronger attempt to prove up what they're now testifying to.

MS. SALTMAN: Ms. Walsh, could you speak to that? Because, you know, the record is pretty thin on the different types of devices mentioned in your comment. And the sort of fair use and statutory factor analysis is done sort of wholesale, not device specific. And I think that the -- could you speak to Mr. Williams' concern? And also how the Office could --- would have the authority to craft a broad exemption that includes, for example, both devices that do have access to creative content and devices that don't.

MS. WALSH: Sure. So, this is an area that's been subject to your prior rulemaking with regard to cars, subject to an extensive study by the Office that found that Congress should consider getting 1201 out of the way of repair activities.

We have a record that stretches back in that regard. And we introduced a variety of devices, you know, of different types, different uses that illustrate that this is not an issue that's restricted to any particular technology.

We have an opposition that says, well, we're concerned that this isn't appropriate for video game consoles or devices where there's a risk of copyright infringement. There's nothing in the record that proves that there's a risk of copyright infringement. So the idea that the record is thin --

MS. SMITH: Are you talking outside of Video game consoles? Or --

MS. WALSH: Mm-hmm. Right. In this class.

MS. SMITH: Okay. So, those video game consoles, put the consoles to the side.

MS. WALSH: Yep. So, we have devices from across the spectrum where we have examples of non-infringing uses. And we have a sort of narrow opposition. And I think the approach of -- you know, we think the entire exemption is warranted, that it's been demonstrated that there are likely to be adverse effects on these non-infringing uses over the next three years.

And to the extent that there's a desire to carve out a video game console or devices that are primarily about the playback of audiovisual works or sound recordings, that's something that we can talk about how to scope that so that it's limited.

But we're talking about balancing the right to make these non-infringing repairs and modifications that are in the record that are being described further here, against an unproven assertion that copyright infringement is going to result for a narrow category of those devices.

MS. SMITH: Well, I would like to discuss how to scope it so it's limited. Because this is something we asked questions about in the study and didn't get a tremendous amount of feedback. We also asked questions in the NPRM. For example, the study asked about language that the United Kingdom has for its own anti-circumvention law, which is, I think, somewhat similar to what the MPAA has suggested. I mean, can you build upon that now?

MS. WALSH: Come back to me. Give me a moment.

MS. SMITH: All right. Mr. Williams?

MR. WILLIAMS: Yeah. Thank you. I

don't think the record has established, especially with respect to modification, that there's a lot of non-infringing uses at issue here.

We talked some in Washington about, you know, wanting to modify a robotic dog. That's not a non-infringing use. Just because you wish that the copyright owner designed something differently doesn't give you the right to start redesigning it.

So, I don't think, especially with modification, that there's a lot of examples of non-infringing uses that are being impeded.

You know, I'm thankful to hear that they're open to carving out expressive works. I think that drafting is going to be very, very difficult to do. And I do think it's their burden to try to come up with a way to do it that doesn't put expressive works at risk. And I'm happy to engage in that exercise.

I do want to say, hopefully we can set video games to the side. But I want to say it's a little surprising how much time we spent talking about this, because I think the only example involving a video game console is jailbreaking it to run Linux on it. And that's just --- that's been dealt with previously. And so there's not anything about repairing consoles.

MS. SMITH: So, I appreciate that we're focusing on consoles because it was an item that the proponents set out. But if we set aside the consoles, are the concerns you articulated, I think, in response to the last question you were called upon about the record, are they there in these instances of, you know, consumer devices that might not in turn play a video game or music or audiovisual work? Or do you think that they're lessened in terms of the infringement risk or concerns you raised before?

MR. WILLIAMS: I mean, in terms of our interest, yes, I think they're lessened. I think, in some ways, EFF raised a good point by saying that there are devices that do more than just that, but that also do that, also access expressive works. And that when you're talking about modification especially, but also repair, you could put works at issue even if you're talking about a laptop, for example.

And I don't think there's any explanation in the record as to why you have to engage in circumvention to repair a laptop, why you can't go through the normal channels to repair. There's just an off reference to wishing to repair a personal computer. And so there's really no

record.

And so, you know, part of our participation every three years, while we are focused on, of course, trying to preserve our interests, is also to make sure we preserve the procedural kind of rules of the road here. Because once you do something in one area out of the desire to try to address a concern that's been raised, if you do that even though the record's not been built, that precedent gets set. And over time, the exceptions start to swallow the rule and the procedures don't have real meaning.

And so I do have that concern, that I don't feel the record's been built, even if you are going to exclude things that get to expressive materials. But that would greatly lessen our concern if you figured out a good way to do that.

MS. SMITH: Mr. Wiens, do you want to speak about that? And perhaps Mr. Williams' questioning of personal computers specifically and, I guess, his sense of the record has not been built.

MR. WIENS: Sure. I mean, we're looking at electronics moving into every possible product. And the ability to build a record across every single product that's out there being

repaired --

MS. SMITH: Well, but there's a difference, right, between building a record across every single product and building a record across a large amount of products. And the written submissions here were, honestly, quite short.

MR. WIENS: Sure. And I can -- I mean, I'm happy to share like the -- I was just looking at our Xbox 360 "red ring of death" repair. And we've had over a million people follow our instructions to repair that console. And there's a huge amount of interest out there in the public.

The challenge is that, frankly, the repair world are not also IP lawyers. And there's a very narrow bench to draw on of repair shops that can afford to -- I mean, Robert doesn't have a lawyer. Right? He's a small shop that's employing -- you've got three people that work for you? Five?

So he's up to five employees in Barstow. But, I mean, the repair industry is oftentimes holding on by our fingertips.

MS. SMITH: And we appreciate you all being here. So, since we do have the benefit of your presence, can you give us some specific examples?

MR. WIENS: Around game consoles? Or around other products?

MS. SMITH: Outside of consoles.

MR. WIENS: Sure. That have TPMs, you're looking for?

MS. SMITH: Mm-hmm.

MR. WIENS: Yeah. We're increasingly seeing, as you start seeing security threats, there was a casino that was hacked through a temperature sensor in a fish tank in the lobby.

And so every single product, as electronics is added to it, it also is having some kind of security mechanism that's added to it. It turns out it's not sufficient to add WiFi to your fish tank monitor. Now you also need to add security to it.

And so you're going to see, across every product, some elements of security being added to it. LG, since the beginning of 2017, hasn't sold any appliances that aren't WiFi connected. And in LG's opposition they filed on the right to repair bill, they've said that they don't want people modifying and tinkering with or repairing their appliances because of the security implications.

So that shows that we're starting to see TPMs being added across every kind of product. Not necessarily to prevent repair, but to secure the product. But the side effect is that it really starts

to limit repair.

MS. SALTMAN: But for a lot of those products, like LG home appliances, I mean, those are generally covered by warranties and are -- there's not necessarily a need for circumvention outside of those channels.

MR. WIENS: So your typical warranty is 12 months. The anticipated life span of an appliance would be in the ten-year range.

A recent study by WRAP, a waste reduction agency, found that 70 percent of consumers were dissatisfied with the life span of their appliances.

If you take game consoles for an example, they've manufactured hundreds of millions of game consoles. If everyone is five, ten pounds, you're talking about literally over a billion pounds of e-waste is being generated.

This is massive amounts of raw material. A warranty is nice. It's a nice idea. But, overwhelmingly, products don't break within the first 12 months. They break after that. And that's where you need the repair ecosystem. Whether that's owners or -- you know, the manufacturers have a great repair mechanism, but it's insufficient. It's always going to be

insufficient.

The car manufacturers know that they can only perform about a quarter of the repairs that happen on cars themselves. The rest is performed by the independent repair industry.

MR. RILEY: So, why is it insufficient? Is it price? Is it something else?

MR. WIENS: Why is the warranty insufficient?

MR. RILEY: No. Why is LG's repair service insufficient?

MR. WIENS: Sure. Yeah, so let's talk about Apple's battery situation. So, Apple was slowing down phones with older batteries. People realized all of a sudden that your battery needs to be replaced.

Apple has manufactured around a billion iPhones. Of those billion iPhones, most of them are more than two years old and need a new battery. Apple has five --

MS. CHAUVET: But you don't need to circumvent to replace a battery. Or do you?

MR. WIENS: At the moment, no. But it's very possible that could -- well, actually -- actually, yes. So, Apple rolled out a new software tool that lets you monitor the battery's health.

Only Apple's genuine batteries will report battery health to the software. So we're going to have to find some way -- and there may be a TPM. We don't know. But it's very possible that --

MS. SMITH: That sounds a little speculative. There may be a TPM, but you don't know, and you can replace the battery without circumvention. I mean, can you come up with a concrete example of where you need to circumvent for repair?

MR. WIENS: Sure. Well, the home button situation. So, right now you have two iPhone 8s. You cannot swap the home buttons on the iPhone 8s without circumventing the TPM. And it's not the same TPM as jailbreaking the phone. It's a different one.

MS. SALTMAN: Mr. Zieminski, did you want to speak to cell phone?

MR. ZIEMINSKI: Yeah. I just wanted to comment that, you know, when we're doing these types of swaps with the home button or an optical drive, we're not even taking another, you know, a non-Sony or a non-Samsung or a non-Apple part.

We may in fact take from what we call a donor device, right, that's already broken for another reason and inoperable and we're just trying to transfer it over

to make a salvage, workable device, for a variety of reasons.

And what we find is that even using an OEM -- original equipment manufacturer -- part, it does not work. And that, you know, kind of causes major issues. So, even when we try to use original parts, we still find these roadblocks to performing successful repair for the consumer.

And then, further, the second point would just be that a lot of times these services are not even acknowledged, to a certain point.

So, with Apple and the home button, the error 53 issue, this was ignored, for, I believe, two years. It took, you know, Kyle writing a blog post. And then, a year later, it took, you know, a news outlet picking it up before, even a year after that when class action lawsuits were filed, that Apple said, "okay, this is an actual issue and we'll start to do service from our centers for this issue."

MS. SMITH: Do you ever reach out to Apple or Sony or any of these manufacturers and get permission for repair? Or do you understand that it's prohibited? Is it -- what's the relationship there like?

MR. ZIEMINSKI: Yeah. We do. I mean, we try. Obviously, we always try to work with them

rather than against them or alongside them. And in most cases --

MS. SMITH: Did you typically have success?

MR. ZIEMINSKI: What's that?

MS. SMITH: Is there typically success?

MR. ZIEMINSKI: Off and on. It depends on the manufacturer. So, our organization, for example, we work very closely with Google to do Pixel repairs, right? And as a result, we're able to do more repairs locally -- or regionally for the Google Pixel customers.

MS. SALTMAN: Mr. Williams?

MR. WILLIAMS: Just very quickly. I wanted to note again that there are extended warranty options as well. So it's not always a 12-month warranty. I think Microsoft, I think they call it the complete warranty. I think it's three years. And includes things like if you spill a drink on your console and it breaks. Things like that. So, I just wanted to say it's not always 12 months.

MS. SALTMAN: Ms. Walsh, could you also address, in your submission you argued that you didn't think 1201(f) was sufficient covered for the kind of modification that you're looking to do.

Could you expound on that argument a little bit? And explain why you think 1201(f) doesn't cover the kinds of modifications that you're seeing here.

MS. WALSH: Sure. So, first of all, I want to talk about why a modification generally can be expected to be a fair use in this context, the context that we've been talking about.

MS. SMITH: That would be helpful.

MS. WALSH: And one reason is that this is modification of the functionality of software in order to achieve new functional things. It's transformative. It's not using any expressive copyrightable elements of the software in an expressive -- MS. SMITH: How are we to know that? I mean, that seems like a broad assertion, that it's not using the software. Or it seems like you're --

MS. WALSH: No, no. It's --

MS. SMITH: -- talking about creating a derivative work.

MS. WALSH: Right. Well, what we're talking about -- all of these uses that we're talking about, we're doing the fair use analysis on a potential derivative work.

MS. SMITH: Right.

MS. WALSH: And so, in the sense that it is an alteration of the copyrighted work, then the copyrighted work is involved.

MS. SMITH: Right.

MS. WALSH: But these are copyrighted works that are primarily functional. So, both under the second factor, we're talking about things with a thin copyright whose significance is functional, that's no something you can get a monopoly on under copyright law.

The transformations that we're talking about are about adding new functionality or even new expression in the example of, you want the iVo to say the things that you want it to say, instead of the things that it's originally programed to say. That's not -- that's a transformative use. And it's even more clear when we're talking about, you know, light bulbs and other devices, where it's entirely about the functionality.

MS. SALTMAN: But it seems like the fourth factor is really sort of the most -- well, I mean, you know, generally it's the most probative one. And here there isn't, in your submissions, an analysis of the fourth factor with respect to these different types of devices.

MS. WALSH: So the fourth factor is

often in favor of a fair use in this case because you have software that's tied to a particular device. You can't upload just the firmware that runs the device and get the benefit of owning that device. There's a physical product that it's tied to.

So it's very unlikely that there's going to be market substitution as a result of these works where the work's utility and market value is connected to a physical device.

MR. WIENS: Right. There's nobody out there selling this firmware. We were talking about the cellular unlocking, and no one -- you're not seeing Broadcom concerned about piracy of the software that runs on their chips. So the commerciality of the firmware is purely tied to the functionality of the physical device.

MS. SMITH: Mr. Williams, did you want to --

MR. WILLIAMS: Yeah. Thank you. Matt Williams. I just disagree with the fair use analysis that Ms. Walsh presented. And I think, number one, it's impossible to do it as one big analysis that covers all modifications of all devices that include software. But even setting that to the side --

MS. SALTMAN: Well, can you tease that out a little bit?

MR. WILLIAMS: Sure.

MS. SALTMAN: So, why is it impossible to do it sort of in like a broad fair use analysis?

MR. WILLIAMS: Well, sure. So, okay, there's a few reasons. First, as you've acknowledged in previous rulemakings, game consoles, for example, it's a different analysis because of what's involved with modifying that software.

The modifications in that instance not only alter the firmware, but also decrease its value because it no longer can protect the copyrighted works that it was designed to protect. And that changed the way you viewed those types of modifications under the fourth factor, because the firmware value was harmed. In each device, things like that can come up.

The second part of it is, what is the modification you're trying to accomplish? I mentioned the robotic dogs. I don't think that that is a non-infringing use. I think that that is the ways that someone might modify a robotic dog are ways that the copyright owner might choose to market new versions of that dog in the future. And when

you do that you avoid paying the customary price for that potential modification that's going to come out in the future.

So, I think that it's very hard to just say blanket, across the board -- and this is what the 1201 study concluded as well -- all modifications are fair use.

And if you look at the Oracle opinion and the way that they analyzed the previous interoperability cases there, I mean, they say that even in those previous cases which involved the creation of entirely new works that didn't include any of the expressive elements of the preexisting software, that that was only a moderately transformative activity.

And, here, I think what's being described, in every instance, would not be the creation of entirely new work, that they're not just wanting to analyze the preexisting software and build an interoperable add-on to it. They're wanting to actually modify the existing software and create a derivative work, as you said.

And to make a blanket conclusion about that, in the abstract, I just don't think is possible.

MS. SMITH: Ms. Walsh?

MS. WALSH: Yeah. So, it's not abstract. There are a lot of examples that we've given to which the analysis applies. And the objections that we're hearing are, well, maybe it doesn't apply to video games and dogs. But we've demonstrated that it's likely that there are going to be adverse effects on non-infringing uses over the next three years.

And by creating an exemption that authorizes those uses, the non-infringing modifications for these devices, then you're doing your -- you're fulfilling the statutory mandate of creating space for these non-infringing activities to take place.

So the analysis that we've given, there aren't a lot of objections to applying that to the examples that are in the record.

Also, Oracle v. Google was wrongly decided. It's not the law anywhere. If we go by what the Federal Circuit says, then 1201 requires an access to infringement. It doesn't get the analysis of the factors right in terms of transformativeness or the nature of the work.

MS. SMITH: Would you say the most helpful case law to your position is Sega v. Accolade and the Sony v. Connectix case?

MS. WALSH: Mm-hmm.

MS. SMITH: Are there other cases you would point to?

MS. WALSH: We refer you to our record.

MS. SMITH: Okay. That's what I saw in there. Okay.

MS. SALTMAN: And can you address the 1201(f) question I asked earlier?

MS. WALSH: Yeah. Absolutely. So 1201(f) has, to my knowledge, never been successfully raised as a defense to anything because of limitations that are sort of well-known to the Copyright Office and have been briefed over and over.

In particular, a very significant limitation is that it's about making one piece of software interoperable with another piece of software. And we've been talking a lot about hardware interoperability. That's the closest sort of case to 1201(f). And it likely -- you know, a rightsholder would argue it gets knocked out because it's not just about software and software. So 1201(f) --

MS. SMITH: Can you cover the Gimbal example or the radio example from your submissions?

MS. WALSH: Mm-hmm. So, the --- both of

the -- the Gimbal example involves additional hardware.

MS. SMITH: If it also involves software, it might cover it, right?

MS. WALSH: Yeah, I think there's sufficient legal uncertainty, given this defense that's never been successfully applied, that people are chilled from engaging in these activities and relying on that exemption, as we've seen repeatedly for other exemptions over the rulemakings.

MS. SMITH: Do you have more information on what the circumvention activities -- I kind of want to walk through a lot of the examples, but the radio and the Gimbal examples to start with.

MS. WALSH: Yeah. So, we provided links to the descriptions that the technologists gave of their process, as well as a short summary. So, which example would you like to start with?

MS. SMITH: I just want to start with the winch.

MS. WALSH: The Cat?

MS. SMITH: Yes. The Cat.

MS. WALSH: The Cat tractor. So this is --

MS. SMITH: Because I didn't find the

explanation in the video of what the circumvention activity was. I thought maybe you could talk about that.

MS. WALSH: Okay. So, the step, the user had to brute force the encryption on a file from the firmware's RAM and decrypt the firmware blocks in order to achieve control over the Gimbal and reprogram the motors for any uses. So the description step would be the step where a TPM was most likely to be involved.

MS. SMITH: And what are the TPMs on the consumable examples that you gave?

MS. WALSH: So, let's see. So, we referred to ink, coffee, juice, a cat litter box, cleaning fluid.

I understand also that, since this has happened, there have been consumables for use with artificial pancreases. So, actually a medical device use where there is a technological restriction on making third party life-sustaining medicine work with the device that you've been given.

MR. WIENS: The cat litter DRM, I mean you can just use soapy water to refill your cat litter. But the DRM was -- I mean, it was very similar to what you see on the ink cartridge. It

was just a little -- it was just a little chip in the replacement.

MS. SMITH: Okay. So the Lexmark case concluded maybe that the TPM wasn't effectively protecting the copyrighted work. So that's part of why I'm asking this line of questions.

MS. WALSH: So, yeah --

MS. SMITH: Yeah, I mean, does it work like the Lexmark printer cartridges? Does it work differently?

MS. WALSH: So I think for all of these I would have to -- so you're saying that you took a look at the cited references and they didn't provide an answer to that information?

MS. SMITH: I'm just trying to understand more. Yeah.

MS. WALSH: Okay. So, for an ink cartridge, Lexmark is one example of how it worked. And that was contingent on the way that they had designed it then. So the company could decide that they're going to design it to include, you know, a poem in the chip as well, or something that is more, arguably, copyrightable. And create -- to add section 1201 as a legal barrier.

One of the obstacles is, you don't know what's in there until you bypass the TPM. So, from

the perspective of a user who wants to make their cat litter box work, they can't know beforehand if bypassing that TPM is going to lead to a section 1201 claim.

MR. WIENS: I pulled up the source code for the cat litter hack just to see. And it looks like there's an RFID chip on the cat litter module. And so I guess you could have probably cut out the RFID chip and put it on his new cartridge, but instead what he did was create a custom firmware. So he took the existing firmware, decompiled it, made modifications, and removed the chip. And then loaded it onto the cat litter robot.

So, it's almost more in the category of modification than repair, I would say.

MS. SALTMAN: Ms. Walsh, just to clarify, your initial submission limited modification -- so, not repair, modification -- to device owners. Is that your position, that that the class of people who are exempted for modification are the owners of the devices?

MS. WALSH: Well, I think it would be appropriate to use language like "users of the copyrighted work."

The third party issue has surfaced in the rulemaking. So, for the same reasons, it's not

necessarily just the device owner who would legitimately be making these modifications.

MS. SMITH: So, the current exemption was adopted, in part, upon a finding that 117 might provide a basis for non-infringing uses. And that would go away if it changed to user from owners, correct?

MS. WALSH: Section 117 requires that someone be the owner of the copyrighted work, but I believe that they can authorize someone else to do it. Is that -- let me double check that.

MS. SMITH: Yeah, you can make or authorize the making.

MS. WALSH: Yeah. So that would be my answer to that. But I would also say that the fair use analysis for activities that are aligned with section 117 is bolstered by the presence of section 117, even if you are not the owner of the copyrighted work.

And I'd also say that there isn't evidence in the record for most of the devices that we're talking about to counter the presumption that the person who purchased the device is the owner of that copy, of the copyrighted work.

MS. SMITH: Would you find that the authorization of the owner of the device might be

an important consideration in the analysis of whether these activities are likely to be non-infringing?

MS. WALSH: Can you give an example?

MS. SMITH: Well, as opposed to just the user. The authorization of an owner is language that's in 117. So, I'm wondering whether that would be --

MS. WALSH: Oh, I see. It provides an additional basis for finding that it's non-infringing. But it's also non-infringing as a fair use.

MS. SMITH: Mr. Williams, did you want to respond?

MR. WILLIAMS: Yeah, I just wanted to respond. Ms. Walsh said there's a presumption that everyone owns the copies of the software unless somehow in the record it's been proven otherwise.

And I don't know that there's any basis for such a presumption. I think the proponents have the burden of establishing that the consumers do own this software. And I don't think they've even tried to do that.

MS. WALSH: When you buy a device, unless there's some documentation that alters your legal status with regard to that device, then you're

the owner of that copy of the software that's in the device.

MR. WILLIAMS: This is Matt Williams. There's a multi-factor analysis depending on which court you look at. But in all instances that we've seen in the rulemaking, there are terms of service associated with acquisition of copies of software.

Sometimes people are the owners of them and sometimes they are not. But I don't think the burden shifts in this rulemaking to us under some kind of presumption that if we don't establish lack of ownership that they have successfully established ownership. I don't think they've introduced any of the terms of purchase or terms of use for any of the software in the record.

MS. WALSH: So it's absolutely not the case that all the examples of purchased products that have been subject to rulemaking come with the terms of service.

I don't know if that's what you intended to say, but that's not the case.

And the multi-factor analysis that Mr. Williams invoked comes after there's some document that purports to restrict the rights of the user.

It's also not an issue that needs to be deeply probed in the sense that fair use provides

a basis for finding these activities non-infringing without resort to section 117.

But section 117 bolsters that.

MS. SMITH: Mr. Williams?

MR. WILLIAMS: Yeah. Thank you. I understand that in certain instances the Copyright Office has concluded that it's going to go outside the boundaries of section 117.

But I think to just completely discard it and pretend that it's not there, would be an improper way to proceed in this proceeding.

Just because in some specific instances it might be non-infringing under fair use to copy or modify software, doesn't mean that in every instance it should be.

And to just say that it never matters whether you own the copy, would really be to ignore section 117. I don't think that that would be a proper way to proceed.

MS. SMITH: Do you think whether you're the owner of a device is relevant to the first factor or other factors in 107?

I think that was something we considered with the current exemption for motor vehicles.

MR. WILLIAMS: So whether you own the device, does that impact the nature of the use? I

think it could.

I think it might depend on what activity you're talking about. I think for example, if you clearly weren't the owner of a device and you went into someone else's computer system and started playing around with it that that could negatively impact you under the first factor.

MS. SMITH: Even if you had authorization?

MR. WILLIAMS: Well, if you had authorization by the owner of a device, then under 117, if they own the software as well, then you would be -- you would potentially be covered if you met all the other requirements of 117.

Under section 107 I again, think it would depend on the activity. And I think to say that in every instance, if the activity is repair, it is therefore fair use, would again read section 117 out of the statute.

MS. SALTMAN: Mr. Wiens, I know your placard was up. But I want to hear Ms. Walsh's response to that.

MS. WALSH: Sure. So, I'd add that under the appropriate analysis of section 117, even if there is a EULA in place, the person who owns the device is typically also the owner of that copy

of the software.

So, under Krause, you look at indicia like are they free to dispose of it, et cetera. And that is generally, you know, I don't think there's a counter example in the record of the way that users are -- exercise the indicia of ownership over that physical copy and ought to be considered for purposes of their 117 rights to be owners.

MS. SMITH: I think Mr. Williams must have questioned it in the context of video game consoles. And also just in general trying to understand the devices.

Do you see any merit to this position?

MS. WALSH: I'm sorry, what's the question?

MS. SMITH: What about video game consoles? Is that right, Mr. Williams? Did you question whether the owner of a video game console owns the software in that console?

MR. WILLIAMS: Yes. My understanding is that those are licensed copies of software.

And I think that under Vernor for example, the fact that the console manufacturers are providing ongoing support and repair services, and requiring that those avenues be used, actually weighs in favor of a conclusion that it's a licensed

copy of software.

Because one of the Vernor factors is that additional restrictions are placed on the use beyond just calling it a license. And with game console software, I think those additional restrictions are in place.

MS. WALSH: But you're free to resell your video game console. You're free to dispose of it. You don't return it to the manufacturer at the end.

For purposes of 117 you're the owner of the software that operates the video game console.

MS. SALTMAN: Mr. Wiens?

MR. WIENS: Yes. I wrote an article about this. Because in the last triennial, John Deere said that the farmer is not the owner of the copy of the software on the device.

And so I wrote an article explaining their position. And I got thousands of annoyed emails from farmers saying, of course I own the software.

The overwhelming expectation of consumers is that they own the copy of the software on the device. And we've seen this from the public reaction.

We see this in our discussion, I bought

my Xbox used. There was never any license agreement that I signed when I bought that Xbox.

So, the -- this is, as we see electronics move into more and more products, I would say the overwhelming majority of products have no license -- that have software in them, have no license agreement associated with them.

When I buy, you know, a flashlight that has software in it, there's no license agreement associated with that. I'm assuming that I'm buying the flashlight and all that's contained therein.

MS. SALTMAN: Ms. Walsh?

MS. WALSH: Yeah. So I wanted to refer back. I apologize. I wasn't able to find the language in the notice of proposed rulemaking that you were asking for comment on a while ago.

Could you point me to the specific language involving a UK definition?

MS. SMITH: That might have been specifically in the 1201 study. But it vaguely also in the NPRM raised a question of whether we should -- you can put all the devices on one hand, or certain types of devices that are more likely to fall within the category of adverse effect of non-infringing use for modification.

MS. SALTMAN: But that --

MS. SMITH: So I know that UK was specifically mentioned in the rulemaking impairment.

MS. WALSH: Okay.

MS. SALTMAN: I think we're just trying to figure out whether and to what extent the Office would have authority to grant, you know, a broad or a narrower exemption.

And based on what record evidence, is the fundamental question. Okay.

But maybe we should move on, because we have a lot to cover. So, let's talk about the telematics in entertainment systems in motorized land vehicles.

So, I have some technical questions. And we talked about these a little bit the other day in the unlocking context.

But, in most car systems, the submissions discuss telematic systems in cars. And also the entertainment systems in cars.

Does the same TPM control access to both of those systems? Are there layers of TPMs? Are there separate TPMs?

Can anyone talk about how that works technically?

MR. WIENS: Maybe I'll take a stab at it.

And then I'll let Mr. Mooney explain their perspective.

MS. SALTMAN: Mr. Mooney.

MR. WIENS: Yeah, so it was -- it's interesting. I mean, if you look at the way they describe it. They're describing it as the telematics and infotainment system.

And the way that many vehicles are designed right now, the telematics and infotainment systems are the same computer.

That's actually unfortunate, because telematics -- increasingly what's happening is, the diagnostics on vehicles used to come out through the OBD port, or the onboard diagnostic port.

It's right underneath your steering wheel. There's a little port you can plug a reader in. It's a standardized interface across most vehicles.

And that's been the primary interface historically for accessing all of the -- like I just fixed my wife's car last weekend. It was giving me error code PO715.

It turns out that's the transmission speed sensor. So I bought the sensor, fixes the car.

Now, as these things are getting more

sophisticated, we're moving from the diagnostic data coming out through the OBD port, and it's going over the wireless. And so that's the shift between diagnostics from a physical port to diagnostics over the air, over telemetry.

Unfortunately, the way that the manufacturers are deciding to do that is the same module that has the cellular connectivity say for downloading new maps or new videos, or streaming music, they're using that same modem for transmitting the telemetry data.

And so, it puts all of you in an unfortunate situation where the world of repair and the world of entertainment systems are like, colliding. Because of maybe, an accidental or a choice of efficiency of combining telematics and infotainment into the same unit.

MS. SALTMAN: So, the telematics data you're talking about, is that data that is needed to repair sort of other parts of the car? Or --

MR. WIENS: Yes.

MS. SALTMAN: Is circumvention just needed to repair the telematics system or that modem?

MS. WIENS: No. I mean, this is where you'd be getting access to diagnostics like, your

oil needs changing.

All of the diagnostic data from all of the -- and there might be 25 different computers in the car, are funneled through the telematics system.

MR. CHENEY: Can I ask just a -- I'm sorry to --

MS. SALTMAN: No. Go ahead.

MR. CHENEY: Can I ask just -- because normally with the port, right, you would just go into an auto repair store and they would plug in their device. And you would get that data out.

And then you could buy the part right there in any auto repair store.

MR. WIENS: Right.

MR. CHENEY: Now, with that change, where does that telematics go? And is that where the problem lies?

MR. WIENS: Right. Yeah, so this is the challenge. And it's -- so that same OnStar kind of signal. So the diagnostic data is going straight back to the manufacturer.

It's the same thing on tractors. The diagnostic data is going to John Deere. You log into your online John Deere account and then you can see the error code for your tractor.

MR. CHENEY: So you can't go to the auto repair store now and have them plug into that port.

MR. WIENS: Right.

MR. CHENEY: And get that data out.

MR. WIENS: Right.

MR. CHENEY: That's no longer available as a service?

MR. WIENS: And this is why AAA feels so threatened by the shift to telemetry. Because it's cutting out the independent repair world.

And it moves -- by virtue of this TPM, it moves all of the control over who can access all that diagnostic information to being in control of the manufacturer and not third parties.

MS. SALTMAN: But does the consumer have control? Like you said, the consumer could log into his John Deere account and see the telematics data.

So could, I mean, could a consumer log in, get the data, give it to a repair person who could then do the repair?

MR. WIENS: Unfortunately that's not the way most of them are designed. John Deere's system maybe is a little bit friendlier with other cars like a Tesla for example.

You don't see independent repair shops

fixing Teslas. Because they don't have access to that information, just the Tesla service.

So what you'd want to do is go into the telematics chip and say, hey, this server that you're sending all the data to, send it to my personal server instead. Or send it to AAA instead.

That would be the kind of modification the user would want to do. It might be as simple as changing an IP address.

MS. SALTMAN: Mr. Mooney?

MR. MOONEY: Yeah. I was about to say, I can't speak to what's unfortunate or not. I feel like that's pretty speculative.

You know, I think there were some statements about the unfortunate design versus what was done in the past. And I can't speak to that and say that's --- that adds any kind of weight to this discussion.

The other piece there is the OBD-II port is certainly very much still in effect. That has not been removed from vehicles.

That is still an option for all repair.

MS. SALTMAN: And that's -- you can get the same telematics data off the OBD?

MR. MOONEY: Yeah. So, the difference in -- the difference between an OBD-II, depending

on what the functionality is, versus some sort of a wireless or over the air option is that the OBD-II has to kind of physically plug in.

When you're talking about a wireless system, it's more in a real time manner. But the same data exists.

MS. SALTMAN: And is there -- do you need to circumvent any kind of access control to use the OBD-II as an unauthorized repair?

MR. MOONEY: Yes. I mean, you know, there -- and this starts to wade into a different discussion.

But, I mean, right now there are options for owners of the vehicle to plug in things like a Progressive dongle that kind of tracks how you drive in order kind of -- you reap the benefits of safe driving on your insurance premiums. Right?

So there's ways to access it now. It's not physically protected in any way where you would have to go to the manufacturer.

Again, that's not Harman's domain. I just want to be very clear about that. That's the OEM, the automakers' onus there.

We simply provide the system that enables certain functionality.

MS. SMITH: Do you know if this

diagnostics data -- maybe someone else does, if you don't. If it were obtained after circumvention, is it coming in a structured or an unstructured way?

I'm trying to determine if it's a factual -- you know, if you're just getting facts, or if it's likely to be a copyrightable compilation of data.

MR. MOONEY: Yeah. So, I think the point there is that -- and it was made, that there's this blending. Right?

And that's the infotainment, when you talk about infotainment, we're talking about the entertainment and the telematic system kind of blended together.

There's a whole host of, you know, when you're looking at that there's PII involved. There's also, in terms of position, navigation, and timing. States have different statutes around what that means.

But then there's also the copyrightable works that are in existence on the system. Or in effect, the system is enabling the streaming of the transmission, the viewing on that entertainment system.

Some things come preloaded --

MS. SALTMAN: Aren't those works

covered by other TPMs as well? Like for example, wouldn't you have to like log into your Spotify account to stream it on your car?

MR. MOONEY: Correct. It depends on what's preloaded and what's -- you know, so yes. There are ways that you can log in and access those things.

However, some things do come preloaded. Like a Waze, or a Sirius XM, where they are kind of part and parcel with the infotainment system.

MS. SALTMAN: Ms. Walsh?

MS. WALSH: Yeah. So, I just want to remind us all that one of the big harms here is a lack of competition.

And so when we think about like well, isn't there an authorized repair service that you can go to? Sure.

There could be the monopolist that you can go to and get higher prices and lower quality of service than if you had a competitive market.

MR. CHENEY: Ms. Walsh, I just want to push back a little bit though. Mr. Mooney just indicated that that port still is available.

That means I can go to any repair shop. If that's the case, I can go to any repair shop and they can plug in their authorized device and give

me the code that I need to fix it.

If that's the case, then this monopoly argument doesn't work. So tell me, if that port is actually still working, then tell me how this is an issue.

MS. WALSH: Sure. So, I'm going to answer that question and then also, on the other vehicle-specific stuff, defer to folks that looked like they were excited about it.

But, last time around we talked about the market for the creation of those diagnostic tools. And so maybe you move the monopoly to, you know, if there's something that can be achieved over OBD, you move the monopoly to the market for providing diagnostic tools.

So you mentioned, it's an authorized diagnostic tool. This is something that we talked about last cycle with regard to cars is the need for competition so that someone can make a diagnostic tool that's better or more affordable than the one that the manufacturer authorizes.

It's about preventing an illegitimate monopoly at any step in the road. So the reason I raise this point is not necessarily to make a vehicle-specific point.

But just to talk about as we say well,

you know, isn't there -- isn't there service from the original manufacturer?

That's not addressing the harm to competition that's created by a barrier to repair or modification.

MS. SALTMAN: Mr. Wiens?

MR. WIENS: Yeah. The OBD port does not provide all the same information that happens over the telematics data feed.

It used to be that was where you got all the information. Increasingly, there's less and less available on those OBD ports.

Effectively, what they make available --

MS. SALTMAN: I'm sorry, can you -- yeah, can you specifically ---

MR. WIENS: Sure.

MS. SALTMAN: --- talk about what's available ---

MR. WIENS: Yeah. So the car manufacturers are behaving in a regulated environment.

So, the information that they provide over OBD is the minimum that's legally required that they provide. And the requirement that they provide the information actually goes back to the

Clean Air Act, which said that vehicle manufacturers have to provide information relating to the emission system of the vehicles, so that independents can maintain the emission system of the vehicle.

So you have Tesla, the Tesla Model S has an OBD port. And if you plug into it, it gives you almost no information.

Because the Tesla doesn't do anything with regard to emissions. And so like the transmission speed sensor error that I was talking about on my wife's car, Tesla doesn't have an automatic transmission. And so any information relating to how to repair the various subsystems on a Tesla are almost not coming -- there's almost no information on the OBD port and instead it's all coming over the telemetry data that's encrypted.

MS. SMITH: So if you circumvent the Tesla and get the telemetry data, does it come to you as -- in a structured manner or an unstructured manner?

MR. WIENS: Yeah. That's a great question. That goes over my skill level.

MS. SALTMAN: Ms. Walsh, do you know?

MS. WALSH: Well, I have a comment about compilations, which doesn't directly answer that

question.

But it is, the Ford v. Autel lawsuit involved an assertion under section 1201 that the set of diagnostic codes and what they meant was a protected copyrightable compilation. And that circumvention of encryption on that was an issue in that case.

That's what I have to add on the compilation discussion.

MS. SALTMAN: Mr. Mooney?

MR. MOONEY: Yeah. I'd just like -- oh, this is Tom Mooney. I'd just like to add that -- so I think we're sort of inferring with this, you know, speculative lack of information that's coming out of the OBD-II port, is that there's some sort of one-way communication.

There are sensors on that vehicle that kind of talk to the user in real time. And back to the manufacturer. And back to third parties. I mean, there's a lot of communication going on in that vehicle. The manufacturer wants you to know if there is an issue on that vehicle.

So the fact that, you know, there's a statement here that you're sort of blinded by what is going on in the vehicle because you can't access telematics data, I think isn't correct.

The other piece is, you know, when you think about what telematics data is, I mean, and you think about fair use, the consumer can already sort of do what they need to do with the data.

I mean, there's nothing that stops you from say, plugging into Waze and using that position navigation and timing of your vehicle. There's a -- the use case is very small for why you would be circumventing security controls around a very complex system on telematics and infotainment.

MS. SALTMAN: So you're saying that sort of without having to circumvent anything, consumers have access to most of the telematics data?

MR. MOONEY: Well, I mean, in terms of how, you know, if you -- this isn't an Xbox, right? And it's not a cell phone.

It's a vehicle moving at 70 miles an hour down the road. There are safety implications around that, but I'm just going to try to kind of stay away from that.

But, it's a different beast. And what you would be using telematics data for in terms of fair use can already sort of be accomplished without circumventing any kind of system or security controls.

MS. SALTMAN: And earlier you mentioned that some of this data is PII. And that this implicates various state laws.

Can you give a concrete example of that?

MR. MOONEY: Give me one second. It might not be concrete, but I know -- so I know when you start to corroborate information in terms of users' location, where they're going, their home address and all of that, it becomes a personally identical -- identifiable information issue.

And it weighs into privacy.

MS. SALTMAN: But, I guess I mean, doesn't -- if it's data about the person who's accessing -- if the person is accessing data about themselves, is that still a PII issue?

And if it is, like under what state law?

MR. MOONEY: No. I don't -- you know, if it's again, fair use for the vehicle, I think -- I don't think it's a PII issue.

I mean, if you're saying that you need to access this information or allowing a third party software, like a Waze for example to access it, or Sirius XM for example to access it, that in turn in my mind is fair use.

MS. SMITH: So you suggested that there's a small use case of where you need to

circumvent something. And you give an example of Waze.

But Mr. Wiens suggested that you need to circumvent, I guess, the same log in order to get diagnostics about the oil system. Is that your example Mr. Wiens?

MR. WIENS: Sure.

MS. SMITH: I mean, do you agree with him or disagree with him?

MR. MOONEY: Well, but what I -- I question why you would need to do that. I mean, that is -- well, not why but why it's not already available to you via the warning systems on the vehicle.

Again, this is OEM territory. But, in my mind when I think about this, there are display options across your dash, infotainment screen that tell you that things are happening.

And that you should go seek a licensed provider for service and repair.

MS. SMITH: Mr. Wiens?

MR. WIENS: Sure. I can give you an example. I was in Dallas the other day, rented a car, it was 2:00 a.m. Got out on the freeway, I was driving five miles down the freeway. And got a warning that flashed up, your engine is

overheating, shutting off.

I pull off to the side of the road and I realize that this particular Toyota vehicle actually did not have any readout on the dashboard at all to tell you the coolant temperature.

Which is like, it's one of the fundamental dials that's been on vehicles. And I went through the manual, I went through everything.

And it turns out that this car, the manufacturers decided that the user should not know the coolant temperature. That's an example of the kind of thing that I as an owner would like to know.

It might have given me -- it was certainly a safety issue. I couldn't believe they shut the car off on the highway without giving me any advanced notice. The engine just shut off.

So, that would be one example where I would like to be able to know that information.

MR. MOONEY: Yeah. Again, this is -- again. I feel like this is where you're getting into, but, this is OEM territory.

MR. WIENS: Sure.

MR. MOONEY: And I'm not an automaker. But what I can say, is if you pop -- in most vehicles, when you pop the hood, there's something that tells you the temperature of coolants and other liquids

inside the engine compartment.

MR. WIENS: No, I mean, you can open it and have steam come up. And that will tell you. But there's no -- if it doesn't have a physical dial, you're out of luck.

Let me give you an example of another fair use. There's a company called Comma.ai that was started by one of the founders of the iPhone jailbreaking ecosystem.

And it's an aftermarket add-on to your vehicle that makes it autonomous. And he's -- it plugs into the CAN bus.

He pulls in as much information as he possibly can from the vehicle to add on and make the car autonomous, which is a pretty cool extension of a vehicle.

And it's building on top of all the software. He -- the more sensors that that system has access to, the safer it will be.

And so by being able to tap into additional telemetry, additional sensor data, you're going to take this from a system that is reasonably safe to very safe.

MS. SALTMAN: Can you address the point that Harman raised in their submissions that allowing people to access telematics data creates

a security concern, and that for example, a fleet of Jeeps was hacked by security research through -- researchers through the telematics TPM?

MR. WIENS: Sure. And that was Charlie Miller who testified in the last triennial. And I think he was actually in this room.

And he told us that he had a circumvention for a major motor vehicle manufacturer. But he was afraid to talk about it because of the concerns of being prosecuted under 1201.

And so it turns out he responsibly disclosed the vulnerability. This is a -- you have -- the moment that you add a wireless interface to anything, you're adding a security implication.

And this is a challenge. Unfortunately, we also need access to these systems to repair, and this shows the tension between, as we continue to secure these devices and add TPMs, we also need to be able to get in to perform repairs.

It's very possible, we've seen this with a number of abandoned devices, we see this with appliances all the time where the manufacturer adds wireless to a device, abandons it, stops running security updates. The user has to come and break through their TPM to just turn the wireless off so

that they can secure their device.

And certainly that would be, if I was buying a modern vehicle, Matt has a brand-new Subaru with a Harman system. The first thing that I would do is go into the telematics system and turn off every wireless interface.

But, I think I would -- that would be -- I would be violating 1201 to do that, but I don't want a car with any wireless signal in it whatsoever. Because I don't trust it.

So, it would be a way that I would secure a vehicle. Because I understand Mr. Mooney has a lot of very talented security engineers that work for you. But, I don't trust them with my life.

MR. MOONEY: And again -- this is Tom. I don't understand how that's relevant to -- what was just stated, I don't know if it's relevant to what we're kind of getting at here in the heart of copyrighted works.

There -- so yes, there are safety implications and security implications, most definitely. And that is our concern.

Yes, Charlie Miller and Chris Valasek performed some research. And it -- the jury's still out on how responsibly it was disclosed at the end of the day.

However, that is our concern is that there are safety issues. I mean, it is when you start to weigh it outside of the Copyright Office's purview.

When you start talking about privacy and vehicle safety, which would, you know, fall under NTSA for example. But again, the scope of that challenge is so large.

And it is so complex and so hard that you sort of don't want to leave it to -- and the systems that are on the vehicle that do touch a Harman system potentially or a Panasonic system potentially, or an LG system potentially, interface with the rest of the vehicle.

And in some instances it's a safety critical functionality of the vehicle. Steering, throttle, and breaking.

When you start to circumvent things willy nilly, it becomes an issue yes, for safety. I wholeheartedly agree.

And it's a challenge that faces the entire industry, in a step above the entire internet of things, business.

MS. SALTMAN: Thank you. So Mr. Williams, I wanted to ask you a question that we sort of discussed in the D.C. hearing on repair,

because I wanted to hear responses from these proponents.

And it relates to my question, the question I asked Mr. Mooney, I mean in terms of the expressive works that are contained in entertainment systems, are those protected by their own TPMs, so that privacy really isn't a concern if people are just circumventing the modem TPM to repair -- to get telematics information to repair the car?

MR. WILLIAMS: So, I can't speak across the board for every type of service, because I don't know the technical specs for every type of service.

But, yes. My understanding is they are frequently protected by their own, at least a separate log-in. Although I think Mr. Mooney just referenced that sometimes that might not be the case. If a service is kind of built in from the purchase date of the car, you never necessarily have to go and log in until your temporary subscription runs out. And then you get a communication saying, do you want to pay to stay and keep continuing.

We introduced the statement from Chris Bell about some of the ways that we're concerned opening up the TPMs on the entertainment systems could expose those types of services to

unauthorized access, even if they do require a log-in.

And one of those ways is spoofing. And so if you had multiple vehicles within a family for example, if you can get into the system, as Mr. Bell described it, you could potentially get access to the code that identifies the authorized vehicle and spoof it into other vehicles.

That's just one example. He was also concerned, and we discussed this in the Class 6 panel as well, about whether you could attach a peripheral device and start downloading copies of content that you only have subscription access to.

I don't -- I can't speak to whether the telematics data is sometimes --- that you have to, you know, hack the same TPM to get to the telematics data as you would to the entertainment system.

Mr. Mooney can speak better to that than I could.

MS. SMITH: I actually had the same question for Mr. Mooney, is that you referred to the Harman system or the Panasonic system.

Are those protected by their own TPMs, or is that not the right way to think of it?

MR. MOONEY: Yes, so that comes down from the OEM. That is based on requirements.

So, just to kind of put it in perspective, we don't go out and design, you know, say an infotainment system that would go into a Chevy Volt or a Tesla Model S on our own. Right?

Those things are designed in advance at the manufacturer level and pushed down to the supply chain. Harman, being at the top of that supply chain, would then source out and just, you know, build that system based on those requirements.

MS. SALTMAN: Mr. Mooney, in your submissions you refer to an FCC rule mandating the lockdown of various parameters controlling radio frequency devices.

Do you have more information on what the FCC rule is? Like what is the cite for that rule?

And how exactly does it -- is it implicated by this?

MR. MOONEY: Can you give me one second?

MS. SALTMAN: Yeah. Sure. Mr. Wiens?

MR. WIENS: Sure. And maybe I can answer that too. I think that the best way to think of these infotainment systems is, it's a general purpose computer that's running lots of apps on it.

And one of the apps might be the Sirius XM app. On my PC I have the Spotify app. Just because my PC is jailbroken, I have root level access

to the PC, does not mean that I have access to the Spotify app.

The Spotify app itself has its own TPMs. And it's protected. And I think that you can think of these infotainment systems the same way.

Just being able to --

MS. SMITH: I'm sorry. Are you thinking of it as the app? Or are you thinking of it as the operating system of the PC?

MR. WIENS: The infotainment system is effectively an operating system. It's a computer running an operating system.

On top of that operating system you have various apps. And so one of those apps would be Sirius. And so each of these entertainment apps are running on top of that common infotainment substrate.

But just being able to access the infotainment system does not mean that I can immediately break into the app and get access to the copyrighted content.

And I think that thinking of these systems as general purpose computers is probably a better framework as we move into more and more sophisticated vehicles than thinking of it as once you get into the locked box that is the infotainment

system, all of a sudden you're going to be able to pull off Taylor Swift, and ---

MS. SMITH: Well, what do you think about Mr. Bell's submission, which was a little bit more specific in terms of how you might be able to exceed the bounds of a subscription, whether it is for permanent downloads or, you know, I guess have it on more vehicles then would have been permitted. Because you can get the authorized code, I think is what Mr. Williams just said.

MR. WIENS: Right.

MS. SMITH: I don't want to paraphrase incorrectly, but ---

MR. WIENS: Yeah, and I don't recall the exact specifics of that. I would say, just like I have on my computer, I can have Spotify. I can save some of those offline.

It's still encrypting those offline -- that offline media. So, I would just leave the protection of that copyrighted work to -- in the control of that app that should be designed to protect the media.

And we don't want access to be able to go in and break the Spotify DRM on the infotainment system. We just want to get into the system so we can read the telemetry data.

MS. SALTMAN: Do you want to respond, Mr. Williams?

MR. WILLIAMS: Sure. I'm not a technologist. I think the way I understand it from talking to Mr. Bell and from Mr. Hughes who testified on Class 6, is that there are additional protections in place on a PC that are not necessarily in place on a voice assistant or an entertainment system in a vehicle.

And that they believe that Mr. Wiens was referring to the way Spotify intends you to access copies, which is to temporarily download them while you have a subscription and to no longer retain them when you do not have a subscription.

I don't know that that would actually be enabled in a vehicle entertainment system. I've never tried to do it with my Spotify account.

But, I do know that Mr. Bell believed that once you got root access to the entertainment system, you could likely extract, and actually at a rapid pace, copies of your playlist essentially from Spotify.

MS. SALTMAN: Ms. Walsh?

MS. WALSH: I think what we just heard from Mr. Wiens is that if you could do that, that would be circumvention of another TPM.

So, this exemption does not grant the ability to do that.

MR. WILLIAMS: That's not my understanding from Mr. Bell's statement.

MS. CHAUVET: Mr. Mooney?

MR. MOONEY: Well, yeah. I'd just like to say that I can't -- I mean, I can't make that assertion broadly across every system and every manufacturer.

In the life cycle of a vehicle the -- you know, how these systems are designed from a security perspective or an architecture perspective changes.

You know, when you go through the quarters of, let's say of a calendar. And you look at on the surface what looks the same to you and I, is the same Volkswagen Passat rolling out over the course of that year has actually changed, you know, for lack of a better term, the brains or the guts of that vehicle has switched from providers to suppliers, depending on costs and other issues that kind of weigh into how that vehicle is manufactured.

I can't say blanketly that, you know, because of this then that when it comes to protection and security.

MS. SMITH: Do you think that knowledge is in the hands of the OEMs? Or who would have that knowledge?

MR. MOONEY: Yeah. At the end of the day the OEMs are the ones who are designing it and setting those requirements.

MS. SMITH: Ms. Walsh?

MS. WALSH: There are a couple of points. So, like Tesla for instance uses a variant of Ubuntu, which is a general purpose test operating system for general purpose computers.

Microsoft is the provider of technology for a lot of these things. There's not a technical reason why, if indeed there's not a layer of TPM on these apps, why they couldn't be designed to include it.

That's in the hands of the manufacturers. So, it's up to them how they design their software with or without that second layer of TPM.

What -- we've heard sort of conflicting information about whether it's there now or not. But there's no reason they couldn't include it.

MS. SMITH: Okay. I'm not sure that's helpful to you. Because if they designed it so that the first layer of the TPM is what's supposed to

protect the entertainment content, then that would seem to go -- be a negative in terms of granting this exemption.

MS. WALSH: If it's -- well, let's say that it's entirely within their power to design it one way or the other, that would create a pretty perverse incentive to have fewer layers of protection for your content so you can sweep up less sensitive information like software.

MR. WIENS: If I was to design these systems, and I was responsible for protecting the IP that was given to me by the movie studios, I absolutely would be wanting to design that well and not rely on the thin protection of relatively weak TPM on that infotainment system. I'd use my industrial strength standard encryption that we've been hearing about from AACS over the last few days.

MS. SALTMAN: Do you mean the protection would come from -- like do you mean the sublayer of protection?

MR. WIENS: Right. I would build it into the movie player app that's running on the Ubuntu Tesla player.

I'd build it into the Spotify app or the -- again, I wouldn't trust the overall system. I would want any given media player to have its own

protection.

MS. SMITH: Mr. Williams, do you want to respond? And in particular thinking about Mr. Hughes, I can't frankly exactly recall whether the RIAA felt like it was within their control or not.

Do you -- what do you think about what Ms. Walsh and Mr. Wiens were saying?

MR. WILLIAMS: Sure. Just let me note quickly so I don't forget what I wanted to get back to. And then I'll respond to that.

So, I mean, without getting into the individual commercial contracts between any individual label and any individual service provider or device manufacturer, I think the general picture that Mr. Hughes described is that the record companies make efforts when they negotiate with service providers to try to ensure themselves a certain level of protection.

Sometimes they might actually be involved in discussions about the specs of how a TPM will be implemented. Sometimes they may not have that leverage.

So not every negotiation is the same. But it is true that in any negotiation related to a subscription service, they are going to be asking for some representations that protections are going

to be in place because the entire design of the service, if it's not advertising-supported, is that you only get a certain level of access depending on how much you pay.

And even if it's advertising-supported, if you're not intended to make copies, then there are TPMs that are supposed to be in place for that.

But they don't have control over every aspect of the design. And they don't necessarily have control over the agreement between the service provider and whatever device manufacturer the service provider chooses to allow the service to run on, assuming there is an agreement there.

So, I think they do make best efforts to try to protect their content. They have every motivation to do so. But they can't completely control the entire design of every system. I think -- just two more quick points.

I think you're right to question the notion that, well, my client's members should be required to have 16 layers of protection in place. They do have probably that many in some instances for different types of choices the consumers are allowed to make within a service.

But, each one of those things is important. And Mr. Bell's statement speaks to the

fact that from his point of view, the lock on the firmware is part of that overall system.

And that it's not that every single piece of the pie falls apart if you get through that lock, but that -- in his view some pieces of the pie become exposed.

And so, it is still a danger. And I think when you compare what we're discussing with what's in the record with respect to the need to repair or modify entertainment systems, there's virtually nothing.

I think the one thing that I can recall is a suggestion that someone should be able to turn their entertainment system into a storage unit. I don't even understand if that's to store the content that someone wants to record off of a subscription service, or whether it's to port content from outside the vehicle into the system. But that's the only thing I can recall.

And I don't think that's enough to justify risking the harm that you identified three years ago and that caused you to design the current exemption.

MS. SALTMAN: I mean, I think what I'm understanding, and correct me if I'm wrong, from the proponents is that the TPM for the infotainment

-- the entertainment system is linked to the system for telematics and so that TPM has to be circumvented just to get telematics data to repair the car.

And I think there is evidence of that in the record.

MR. WILLIAMS: I think, if I understood Mr. Wiens, he said that there are instances of that. I don't think he said that that was universally true.

But he can correct me if I'm wrong.

MS. SMITH: Can one of the proponents speak to -- are there times when, to your knowledge, someone tried to make use of the current temporary exemption and was unable to do so to repair the vehicle or engage in diagnostic lawful modification, et cetera, because it would have involved the telematic system sort of unintentionally? Or as a side effect, if that makes sense?

MR. WIENS: Yeah. I don't have any specific example of that. I can just say the trend, the shift, I think that's a better question for Dorman. Because I think in D.C. they did provide some examples of that.

Increasingly what they're seeing is that there are -- there are significant challenges. I'd refer you to the current case, Dorman -- or GM

v. Dorman, where they're suing them for 1201 infringement. Clearly GM does not feel that the current exemption is covering what they're doing.

MS. SALTMAN: Since we're running low on our time, let's move onto third party repair. The Office in its 1201 study said that Congress should consider a legislative clarification to allow for third party assistance.

Can one of you proponents address why a proposed expansion to allow for third party repair would not violate or at least sort of trigger the anti-trafficking provisions in section 1201?

MS. WALSH: Sure. So --

MS. SALTMAN: Ms. Walsh. The court reporter.

MS. WALSH: So, there are two reasons. So the Office doesn't need to write limiting language into the exemption about, you know, the type of user.

The question is whether people who are users of the copyrighted work are adversely affected in their ability to make non-infringing uses.

So, sort of off the bat, the exemption doesn't need to say you need to be this kind of user or another kind of user. When we get to the

trafficking, there is a specific list of requirements for what kinds of activities rise to the level of unlawful trafficking so that primarily circumvention services are marketed in that way or having limited commercial significance other than for circumvention.

And for repair services, they are primarily repair services. They're not circumvention services.

They're not -- or at least there is a universe of repair services that don't rise to that level. You can imagine one that is marketed in that way.

But, there's clearly space between, you know, there's clearly space in the universe of repair services for things that don't necessarily fall under any of those three categories for prohibited trafficking.

So, the exemption shouldn't foreclose people who are in that space. Where they're offering a service that doesn't rise to the level of trafficking, the exemption shouldn't foreclose them from engaging in that legitimate activity. And it shouldn't foreclose courts from figuring out where that line is precisely.

So, if someone, you know, offers a

service where it's in the gray area, then in order to get the full scope of what the trafficking is supposed to allow people to do, it shouldn't be foreclosed by denying them an exemption under 1201(a)(1), because doing -- that person, their activities potentially implicate both.

So, an exemption under 1201(a)(1) gets it out of the way so that the scope that's not prohibited under (a)(2) can be explored in the market.

MS. SMITH: What would you say to the Joint Creators' concern that, I guess, I don't know, it's certainly a slippery-slope concern that it's something -- that active circumvention is always for another purpose.

And so it's difficult to say whether something is primarily designed for circumvention or primarily designed for repair.

MS. WALSH: Well, I think we could look at -- we could -- so the statute suggests that's sort of the way that it's marketed or the commercial significance are ways of getting at that.

So, if you're offering a service, and the only way that it's commercially significant is the circumvention aspect of it, then that's something that might be excluded.

But, if you're offering a service and the primary significance of it is, I can get your device to work, then that's an example of something that would not be.

So, I'm not sure that that's such a, you know, unsolvable conundrum.

MS. SALTMAN: With respect to, you mentioned the question that the Office raised in its study regarding whether the word user in section 1201 can be interpreted to include third party repair people.

So can you talk a little bit more about whether the Office would have authority to use that interpretation?

And particularly, wouldn't that implicate the -- I mean, to the extent that you're relying on 117, because it would be a user and not an owner who is doing the repair.

And wouldn't that implicate your ability to rely on 117 to cover the repair services?

MS. WALSH: So, user is a broader category than owner. So owners are a type of user.

So in that sense, you know, the statute contemplates users. Some of those users will have the benefit of section 117, both for repairs and modifications since 117(a)(1) does permit

modifications.

So, it's a question again of --

MS. SMITH: But 117(a)(1)'s modification is just sort of like in the service of repair going back to the intended functionality, right? That's what the CONTU report said.

Do you disagree with that? I mean, I appreciate that you're asking us to go beyond 117.

MS. WALSH: Um-hum.

MS. SMITH: But, just in terms what 117(a) itself is directed at, I think it is a bit narrower.

MS. WALSH: Well, the CONTU report said that you should be able to add new functionality to it. So, it's not limited to just making it work the way it originally worked.

If you want to make it work with a new machine for instance, then that's permitted under 117(a)(1). So, Krauss and the CONTU report did that.

MS. SALTMAN: I have sort of a practical question for Mr. Wiens. With respect to agricultural vehicles, there's a lot of discussion in the submissions about the need for third party repair.

Could you talk about, like what's

happening now? Because, you know, I read that there were a lot of farmers who lived, you know, miles away from a service facility.

MR. WIENS: Mm-hmm.

MS. SALTMAN: And who, you know, were told that it would take four months or whatever, to get their vehicle repaired. And they had a harvest that needed to happen within the next couple of days.

So, what are those farmers doing now in a situation like that?

MR. WIENS: Right. Good question. I mean, they do the best they can. Part of this is, the farmers are realizing that they need to tool up and learn the code.

So, there's a bit of a reeducation happening. It's interesting being here in California. Farmers in California are actually a fair ways behind farmers in the Midwest in that regard.

Because the farmers in the Midwest don't farm all year. And so they have a couple of months in the winter to learn the code.

So, services like Codecademy and I mean, you're seeing, it's interesting, you go into the tractor forums, which I spend a lot of time on, I

imagine you don't. And there is increasing technical discussion.

There's a lot more comfort around getting in and diving in and understanding things now then there was before there was the exemption.

You're also seeing the universities starting to help out. So my alma mater is Cal Poly. It's both an engineering and an ag university.

And there is a group of students that has been working with -- there's a group of computer engineering students that's been working with the agriculture department.

Where the ag department has given them access to their tractors. And they have been reverse engineering the tractors under the exemption and starting to post some of the diagnostic information.

And I can -- I don't think this is in the record, because it got posted afterwards. But it's -- the website is tractorhacking.github.io and it has the results of some of their initial research. And they're working on documenting interfaces with the goal of building an alternative diagnostic tool that's the equivalent of John Deere's diagnostic laptop software. Their hope is to build an open source diagnostic software.

But these are complex machines. The Society of Automotive Engineering Standard that the heavy equipment industry is using is complex. And then there's a lot of propriety John Deere work on top of it.

So, it's going to be, I think, many years before we have anywhere near the kind of alternative -- an alternative that's as functional as John Deere's diagnostic software.

MS. SALTMAN: Mr. Mooney?

MR. MOONEY: Yeah, Tom Mooney. I would just caution that, you know, we're talking about tractors here versus millions and millions and millions of light duty vehicles on the road all falling into the same class.

So when we think about the needs of the few outweighing the safety and security of millions of folks who are driving on the roadways every day, I think it's just something that I'd like to consider up against a very specific use case when it comes to agriculture.

MS. SMITH: Well, I mean, there is a temporary exemption that the Register has determined she can recommend renewal of for motorized vehicles, both light and heavy duty.

And I think we're questioning whether

in the heavy duty context, whether there is difficulty and the intended beneficiaries being able to actually make use of that.

MR. MOONEY: Okay. Yeah. That's fine. I just wanted to clarify. Yeah.

MR. WIENS: The other thing that I would add is that the third party limitation is really a challenge.

We're seeing increasingly some of these independent, you know, local -- there's more of these independent local machinery operators.

Or sometimes you have a farmer where he's good at fixing his equipment, so he fixes it for his neighbors too and now he's a third party. And so that's -- if you think about the, you know, years of investment that you're going to want to put into learning how to do this, developing your own tools or your own equipment.

Certainly the more equipment that you can work on, the more incentive there is going to be to invest in that technical knowledge.

MS. SALTMAN: Mr. Zieminski?

MR. ZIEMINSKI: Yeah. I just wanted to point out that similarly to Mr. Mooney's comment, the needs of the millions far outweigh what the capacity of the original equipment manufacturers

can do and what the owners can reasonably do on their own.

We need to dissemination that information as far as possible, as broad as possible so that we can get, you know, devices serviced quicker and more efficiently.

And if you use the Apple iPhone battery fiasco, all of, you know, doing the math and we can recite to you the numbers. But it would effectively take Apple 2.7 years just to catch up with the backlog in the United States to be able to do that if you relied strictly on Apple Geniuses.

If you extended that then to the implications because iPhones are not limited to the United States, they are all over the world, it becomes a greater problem.

Contrarily, independent repair shops in the iFixit network, there are almost 20 thousand independent shops just in that network. There are not near that many dealerships or places you can go for authorized service right now.

MS. SALTMAN: Mr. Mooney?

MR. MOONEY: Yeah. I just want to clarify that we're in no way against, you know, the repair of vehicles.

You know, we're talking about a very

specific and the ability for the consumer to do so on their own, we're talking about a very specific, you know, circumventing security controls around very specific systems that house copyrighted or enable copyrighted works.

Or in instances, data that has acc -- or systems that have access to safety critical information on the vehicle itself. So, --

MS. SALTMAN: So, what's your specific opposition to allowing an exemption for third-party repair people?

MR. MOONEY: Well, so I think there's a number of ways -- there's a number of ways that these vehicles can be serviced as is.

We're saying that there are specific concerns around copyrighted works on these systems that we would like to protect. That uphold, you know, our ability to compete in the market and be a trusted systems provider to the OEMs.

MS. SALTMAN: Mr. Williams?

MR. WILLIAMS: Thank you. We made our full case in our written submission and in Washington. So, I won't repeat all of it.

But, you know, I just want to say the associations I'm here representing don't really have a position as a matter of policy on whether

it's a good or bad idea to have automobile repair shops be able to do some of the things that are being discussed, setting aside entertainment systems in the vehicles.

But, I don't see a legal path for you to create an exemption for those repair shops under the statutory authority that you've been given.

And so you refer to it as a bit of a slippery slope argument. And in a way maybe it is as a matter of policy that the big concern is this spreads to other areas.

But also as a matter of actual statutory authority. I don't think that the term user was intended to say that you could create an exemption that applies to repair shops who are engaged in trafficking.

I think that was probably intended to apply to people who for example, don't own a piece of software, but maybe you're able to find a way to grant them an exemption in certain circumstances.

Or people who have access to a piece of content through a subscription service. And not permanent access. But they want to make a clip.

There's other types of users who are not owners of copies that could be contemplated by that

word. And I think you've been right to say that you don't have the authority to grant an exemption that even implies that trafficking is covered in any shape or form.

MS. SALTMAN: What about if we were to grant an exemption that circumvention is exempted when it's a necessary step undertaken by -- or at the direction of the owner of the vehicle?

MR. WILLIAMS: Yes. I don't -- I think there may be some circumstance where that would not involve trafficking.

But I think in most cases it would. As I understand the automobile market, and I'm not here representing the OEMs, and so I might be incorrect about this.

But, as I understand it from reading the record, pretty much every instance involves circumvention. And a business where every instance involves circumvention, I think is going to be involved in trafficking.

There's also the issue of marketing under the third prong of trafficking. And if you read that too narrowly, I think it would really read it out of the statute.

Because for example, you could say well, I'm not marketing the circumvention if I advertise

free access to movies. I'm not, you know, but the circumvention is required to get you to the access.

So, I --

MS. SMITH: Well, if I paraphrase your position to Ms. Walsh. I'll paraphrase her position to you.

MR. WILLIAMS: Yes.

MS. SMITH: She's saying the commercially significant purpose of an independent car repair shop is to fix the car.

MR. WILLIAMS: Mm-hmm.

MS. SMITH: It's not to engage in circumvention. It's to fix the oil light or whatever has gone wrong with it.

MR. WILLIAMS: And the commercially significant purpose is only one of three possible trafficking violations. I'm not sure -- well, actually, I don't think I agree with your interpretation.

But even if you do, it could still be primarily designed for the purpose of circumvention or marketed in a way that informs consumers that they can achieve something that required circumvention.

And I don't think that kind of marketing should have to include the words, we will circumvent

your access controls. That's too, you know, that's never going to be the way that something is marketed.

MR. CHENEY: Mr. Williams, can I just probe a little bit more on this? And just sort of flip the argument a little bit.

What if you were to say that by granting the 1201 exemptions, but then no one could use it, doesn't that really make 1201(a) ineffective if there's no one that's able to ever use it?

In other words, the only time you can go and have some of this work done would be to go to somebody that knows how to make that repair on that John Deere tractor for example, right?

You have -- you've bought this fifty thousand dollar tractor.

MR. WILLIAMS: Right.

MR. CHENEY: You've got some problems with it. You've figured out kind of what the problem is, but the only way to fix it would be to go to a John Deere that may take you two or three months.

You've got two or three days, you've got crops in the field, they're going to go bad.

You've got a neighbor that can fix it. You go to him. He fixes it. Wouldn't that action, if that action becomes trafficking, doesn't that

make 1201(a) a null and void?

In other words, you kind of gut the first one if you say the second one is so -- can only be narrowly applied in only these handful of things, if you really read those that narrow.

Does that make sense?

MR. WILLIAMS: If I'm understanding you, I think you're asking, does it kind of take the umph out of this proceeding, basically.

MR. CHENEY: Yep.

MR. WILLIAMS: Because an exemption won't practically be able to be used in specific circumstances.

I won't adopt all of the factual things included in that hypothetical as a scenario that would actually happen exactly in that way. But I understand what you're getting at, I think.

And I think from our point of view, you're raising a good policy question. And it's an important policy question.

And it's something dealt with in the 1201 study. It's not something that the statute currently enables the Librarian to address through an exemption.

The one specific instance where Congress did bless that type of a provision was in

relation to phone unlocking. And there was a very specific bill passed in the legislative history.

It very clearly says this doesn't imply any authority to do this in other circumstances. And in fact the Register previously read that statutory enactment to imply that you need that kind of activity in order to create those kinds of exemptions.

So, as a matter of policy, whether ultimately that's something Congress should take up or not, I think is a question the Office has already dealt with.

But it doesn't change the authority that's been given to the Office in this procedure.

MS. WALSH: Well, this is Ms. Walsh from Electronic Frontier Foundation. What we're talking about now is how to interpret the statutory language that's there.

And Mr. Cheney raises the important point that if you interpret it in an overly restrictive way, you defeat the intent of Congress to continue to allow for non-infringing uses.

And in creating this rulemaking to have presumably a meaningful impact on vindicating people's right to take advantage of the freedoms that they enjoyed prior to the enactment of the DMCA

with regard to these non-infringing uses.

So, it's legitimate to consider how interpreting it in a really restrictive way would defeat the purpose of the regime.

MS. SMITH: Did you want to speak to Mr. Williams' citation or reference to the unlocking act?

MS. WALSH: I think it may be a suggestion that Congress in the many years between the enactment of the DMCA and the unlocking act has recognized that it's important to be more explicit about the importance of third party rights.

I don't think it suggests that. I don't think it undermines the idea that it's implicit in the original statute.

But seeing how the statute has been interpreted, it would make sense as a lawmaker to be really clear that, no, the ability of third parties to help individuals make use of the exemptions is important.

MR. WILLIAMS: Thank you. Matt Williams. I just wanted to clarify and make sure I wasn't unclear on this point.

That there are exemptions where people are exercising them. And they're not going to service providers.

So it's not that I'm saying the whole proceeding in every individualized proposed class of works involves this policy question in the same way. But, I understand that with respect to motor vehicles, there is this policy question presented.

And there's kind of negotiations that have gone on with the independent repair shops and the OEMs. And I'm not here to speak on whether that solved that policy question properly or not.

But I think each proposed class is different. And I don't think that issue is presented with respect to every type of proposed class.

MS. SALTMAN: Let's move on quickly to tools. I want to pose a similar question that I just had on third party repair.

How -- what authority does the Office have in light of the anti-trafficking provisions to include an exemption for tools, for unauthorized tools?

MS. WALSH: Well, I would give the same answer to that. That well, I think it might be -- I'd give the same answer that not all tools are, you know, meet the requirements to be prohibited under (a)(2).

But I'm curious if what kinds of tools

are in the question.

MS. SALTMAN: So, I mean, you know, currently people can develop their own tools. The owner of the vehicle can develop their own tools for repair.

And under the MOU that repair shops have with the car manufactures, there are authorized tools that can be licensed. So, is there a need for other tools to provide repair services to consumers?

MS. WALSH: Yeah. So, this is something that we discussed extensively in the context of cars. And touched on a little bit earlier today in regard to the market for providing diagnostic tools.

So the way that an exemption interacts with that is in order to develop the diagnostic tool, you need to do circumvention to understand the system and what's necessary to do diagnosis and repair.

The tool itself is not a circumvention tool. It's a tool that is built using the knowledge you have gleaned about how the system works. So, it doesn't need to circumvent in order to do the diagnosis. It's reading the data that gets sent out by the car.

But in order to build that tool, someone needs to have circumvented in order to do the reverse engineering of the device. So that you understand what the codes coming out of it are.

If there are undocumented ways of interacting with the software that will let you do repairs that otherwise aren't transparent to independent repair folks and so on.

And so that is a tool whose existence is enabled by an exemption that lets you get in and look at it. But it's not a circumvention tool, because it doesn't do any circumvention.

MS. SMITH: So that sounds to me like a tool that is enabled by 1201(f). Do you disagree?

If so, how?

MS. WALSH: So there's a space where it, again, involves enabling interoperability of hardware. Because when you replace a physical component, you need to change the software in the device like a car to get it to work correctly with that car.

MS. SMITH: Sure, separately. And that specific example you gave of the diagnostic tool has software, right?

MS. WALSH: So that diagnostic tool, you're trying to understand functional elements of

-- I -- certainly if the developer of that tool were sued, then 1201(f) would be raised as a defense.

I would expect the other side to argue that it's not interoperability with software, but instead it's a device that is just taking advantage of some kind of information. Not necessarily software interoperability.

MS. SALTMAN: Is there any legal basis or any authority that the Office -- I mean, some of the proponents have asked for the ability to distribute or disseminate these tools.

But that seems to run up against the anti-trafficking provisions. Do you have any argument that the Office has the authority to exempt that behavior?

MS. WALSH: So in the context of making sense of the way that the exemption allows an individual to take advantage, they have interpreted, you have interpreted the verbs that are prohibited in the trafficking provision in light of the whole provision.

And found us a commercial scale requirement. So, I think that there's room to look at whether noncommercial or personal are.

Otherwise, something that's not commercial trafficking is lawful. And would help

people take advantage of the exemption.

Now a lot of the things that we're talking about that are really important are commercial repair services. So, that would not be a complete, you know, panacea.

MS. SALTMAN: Mr. Wiens, in the agricultural context, can you just talk about like what role do these types of tools play in the repair needs?

MR. WIENS: Sure. I mean, this is -- developing the diagnostic software, I mean, the hope is that we'll be able to use the circumvention to develop this diagnostic tool.

So I can plug it in. And maybe at some point use the circumvention to identify what the error code was. But now we can understand the signals that are coming off the CAN bus.

The agriculture equipment is relatively unsophisticated compared to the automotive vehicles that have infotainment systems. They're simpler. There's fewer TPMs overall.

And so I think what Ms. Walsh is referring to, where you can use the circumvention to develop the tool. And then that tool does not do any circumvention itself, is very viable.

From everything that I understand so far

from our investigation of how John Deere's technology works in particular.

MS. SALTMAN: Mr. Mooney?

MR. MOONEY: Hey, sorry. So can I just clarify? So what we're talking about?

So are you in essence talking about like a sniffer? Essentially you're saying that it is reading data that is coming off of a product.

But that data is benign in some way? I'm just curious. Or it can only be used for good?

MR. WIENS: I mean, the intent would be benevolent. There are things that you do over in standard CAN like resetting an error codes where it's not purely reading data coming off the line.

You're communicating. You're acting as a device on the network.

MR. MOONEY: Right. So, I just think that's important to clarify. It's like there is this benign data that's coming out.

So when you're reading -- you have the ability to read, there's all kinds of sensitive information flowing back and forth.

MS. SALTMAN: This is the telematics, right?

MR. MOONEY: Yeah. But it's just like the hack of what, you know, of sniffing data,

spoofing data.

It's the fact that you were able to access and see it.

MS. SALTMAN: I see.

MR. MOONEY: Which has safety implications from a telematics perspective. If you were able to -- so a vehicle is communicating through a number of other systems that its positions, its navigation, where it's going, and the timing of that.

If you were able to alter that by a millisecond, that has potentially grave implications for the user. So, it's not just this -- and I get where you're coming from.

But there's more to it when you get to -- when you're talking about data flow on and off of a vehicle moving down the highway.

MR. WIENS: Well, and who owns that data?

MR. MOONEY: We don't.

MS. WIENS: I do, right? It's my car. It's my data.

MR. MOONEY: So, I think how it goes now is that the manufacturer, the OEM owns that data. Or whoever, whatever agreements they have with other providers.

In most cases, Harmon is simply a data enabler. And now we provide a system that provides functionality in some way.

MS. SALTMAN: What's the support -- so in terms of who owns the data, is there -- is that sort of under the terms of the agreement with the owner of the car?

Like how -- what determines who owns the data?

MR. MOONEY: I can't speak to that.

MS. SALTMAN: Okay. Okay. Thank you. That's all helpful.

Mr. Wiens, if there were an exemption that allowed for the kind of tools you're talking about, but didn't allow for distribution of those tools, would that fill the need that there is for these kind of tools?

MR. WIENS: I mean, the distribution is a challenge. We've seen -- it's interesting, as I've been looking, the companies who distribute diagnostic tools for heavy equipment for long-haul trucks, I found almost all of them are in Canada and the UK, and none of them are in the U.S.

And so it really seems like there is a stifling that's happening around -- where the software companies that are developing and selling

and distributing these tools, are trying to stay outside of the United States.

So, I would see a benefit to, I mean, I think most of the market benefit will come from being able to distribute these tools, but.

MS. WALSH: Yeah. Can we be clear about what kind?

MS. SMITH: Yeah. I think that would be helpful.

MS. WALSH: This is Ms. Walsh from EFF. Can we be clear about what kinds of tools we're talking about restricting?

Because the diagnostic tools that I've described are not circumvention devices. So, I don't know what the basis for restricting their dissemination would be.

MS. SMITH: I don't think we're suggesting there is if it's not something prohibited by 1201(b)(2) or 1201(2).

So, I actually was also confused about that.

MS. SALTMAN: Okay. Sorry for not being clear. But, I mean, the proponents have asked for circumvention tools as well.

MS. SMITH: But I mean, I wonder if Mr. Wiens can explain if something is only in Canada,

why 1201 is the cause of that?

MR. WIENS: Well, those are potentially tools, -- I mean, different classes of tools that you could develop.

So those probably are tools that involve circumventions.

MS. CHAUVET: So what type of tools would those be if they're not for diagnosis?

MR. WIENS: Well, so --

MS. WALSH: For repair.

MR. WIENS: Yeah. I mean, some of the existing repair tools. I mean, there's different classes of things that you can do.

Some of the tools would require a circumvention in the rule. And some of the tools would not.

So, you have various levels of how deep you can go.

MS. WALSH: So, Ms. Walsh again from EFF. If you have a prohibition on doing the reverse engineering that allows you to develop the tool, then it makes sense that you don't get that tool in the jurisdiction that has the prohibition.

MS. SMITH: But right now there is an exemption but for repair. And we have said that the ability to develop or make use, self-help to find

your own tool would be encompassed within that.

So, I'm not --

MS. WALSH: Mm-hmm.

MR. WIENS: But if you think about the -- if I'm going to a venture capitalist and asking for money. And I want to create a software company and start developing these tools, and the exemption might go away in two years, it's going to be very hard for me to get funding.

MS. SMITH: Well, we are not in the position of adopting any permanent exemptions. That's some legislative matter.

So, I'm --

MR. WIENS: No. I totally understand. I'm just saying that might be another reason that you see these happening overseas.

MS. SMITH: Mr. Williams?

MR. WILLIAMS: Yeah, just quickly. I think you understand this. And that's why you're asking the questions.

But I think this topic is something you've got to be really careful with if you're trying to design it in a way that enables certain tool generation by beneficiaries of exemptions without getting into the trafficking provisions.

And I think there are instances where

an individual who has an exemption and wants to exercise their rights under that exemption, could create a tool for that purpose. That type of personal use.

I think you would need to look at, is the manufacturer of the tool or the importation of the tool for the purpose of exercising one of these three prohibited activities?

And if you decide that a repair shop is prohibited under those three prongs from doing what it does, then the manufacture of the tool by that shop becomes something that there shouldn't be an exemption for.

So, I think that's a hard line to draw. Hopefully I'm being clear.

But I just -- I do think there are times when people can make a tool that doesn't quality as trafficking. And I do think this is about trafficking. Because it says otherwise traffic.

But, just drawing that line would require a lot of care.

MS. SALTMAN: Thank you. That's helpful.

MS. CHAUVET: Just a quick question about the MOU, just to clarify the record. So, under the MOU is it that tools for diagnosis are

available?

Or are we talking about tools for repair? And in either case are those sort of basically allowed tools from the manufacturers, but that actually circumvent when they either diagnose or repair?

MR. WIENS: Sure. Yeah, if you have the tool from the manufacturer with the key in it, then there's no circumvention. Because you're basically authorized by the manufacturer to do that.

So that's what the MOU says. Is that the manufacturer would have to make available those tools.

Unfortunately the tools under the MOU are only your standard, like cam bus level tools. They are not telemetry, telematics level tools.

And so, you know, you have levels of repair. It's allowing certain, -- you know, you can do a certain set of repairs under the MOU.

But over time as these vehicles get more sophisticated, there are other repairs that are not allowed. And I think Aaron Lowe referred to, you know, ongoing discussions.

They're finding that the MOU is insufficient. And they're looking for additional

remedies on top of that.

MS. CHAUVET: So I guess a follow up question for Mr. Mooney. So, if these tools under the MOU are essentially circumventing, it sounds like in some cases.

Why is it okay for these repair shops to use those tools to circumvent? But then not like have someone -- because you're talking about like security and everything else.

So, I want to know like how the tools offered under the MOU meet your security concerns? Presumably they do.

MR. MOONEY: Well again, you know, a lot of this falls within the manufacturer who is selling to a dealer. Who then, you know, is working with authorized repair service providers.

There is a handshake of sorts that goes on between the manufacturer at the dealer level or at the repair level, to ask to be able to get keys or codes or tools to access systems within that vehicle.

And I think that's a -- and to me that's okay. I mean, if there's some sort of process by which that takes place, and which it does already, then there's no objection on that to my, you know, to my end.

MS. SMITH: So do you have something else?

MS. WALSH: It's a different topic.

MS. SMITH: Did you have something else to say on this class?

MS. WALSH: Yes.

MS. SMITH: Okay. Go ahead. What else?

MS. WALSH: So I just want to point out, as you think about, you'd asked a couple of questions about scoping the devices that are involved.

So, we think that the record demonstrates that the need is not limited to a particular kind of device. And point out that section 117 is not restricted in terms of what machines are contemplated. It doesn't exclude entertainment devices.

I would say to the extent that you are persuaded that the speculative concern about potential copyright infringement justifies narrowing the class.

I'll throw out alternative language to consider. Such as excluding a device that is primarily a media playback device for audiovisual works and sound recordings.

Again, just to reiterate, don't think

that such an exclusion is warranted.

MS. SMITH: Mr. Mooney? I think this is sort of last call for anyone on this Class before I turn it over then.

MR. MOONEY: Yeah. So, nothing additional. I just wanted to make an important note here before I think we close out.

Is that Harmon is a wholly owned, and this is more for the record, we're a wholly owned independent subsidiary of Samsung.

However, any comment that was made here today, or any position or opinion, is of Harmon, not of Samsung.

MS. SMITH: Thank you. Understood. Mr. Williams?

MR. WILLIAMS: Just very quickly. I appreciate Ms. Walsh's attempt to offer some limiting language.

And although I can't endorse what she offered, I'd be happy to work with you on any language that you want to try to craft.

MS. SMITH: Thank you. Mr. Wiens?

MR. WIENS: I'd just like to thank you for considering this topic. The environmental implications of the decision that you make will be far sweeping and potentially have greater

implications then a lot of the decisions that some of your colleagues at the EPA maybe making right now. This is a very big deal.

And the tools and ideas and techniques that are developed in the repair industry in the United States, reverberate throughout the world. This is really important and I appreciate your time and dedication on this.

MS. SMITH: Thank you. We appreciate everyone's participation in this. We're going to adjourn shortly for a break.

But, start again as scheduled at 11:30 to discuss Class 11. And I'll just remind anyone in the audience, if they wish to sign up for audience participation that's going to start at 1:30 on this sheet that's on the table.

Thank you.

(Whereupon, the above-entitled matter went off the record at 11:08 a.m. and resumed at 11:30 a.m.)

MS. SMITH: All right, I think we're going to get started with our last hearing for the triennial section 1201, rulemaking. This is Class 11, which is a request to circumvent TPMs protecting computer programs that capture avionics data.

My name is Regan Smith, I'm Deputy

General Counsel of the Copyright Office and I think we on this side will introduce ourselves and then the panelists can introduce themselves.

MR. CHENEY: I'm Stacy Cheney, Senior Attorney-Advisor at NTIA, National Telecommunications and Information Administration.

MR. RILEY: John Riley, Copyright Office.

MS. SALTMAN: Julie Saltman, Assistant General Counsel of the Copyright Office.

MS. CHAUVET: Anna Chauvet, Assistant General Counsel of the Copyright Office.

INTRODUCTIONS - PANELISTS

MR. JACKSON: Thank you and good morning. My name is Bruce Jackson, and with Air Informatics.

I filed the request for the exemption for avionics or information off of the current generation of aircraft. Any aircraft. But the concerns are the current generation being digital, software intensive, data intensive and connected.

Now, I can start with a bit of background of who I am and why I come to this point, if you wish.

MS. SMITH: I think it may be helpful briefly. Now in general we have received --

MR. JACKSON: Can you speak up a little bit.

MS. SMITH: Here, I'll move the microphone closer. So we've reviewed the written comments carefully and I think the point of this hearing for us is to probe where we're trying to understand better the evidentiary basis for the requested exemption, as well as connect it to the legal standards of the Copyright Office and NTIA are looking at in determining whether to recommend that an exemption be granted.

So I think if you wanted to briefly summarize what brings you here, that would be a helpful starting point. And then we'll sort of drill down on questions that are probably geared at what is happening in the Copyright Act and what we're supposed to look at --

MR. JACKSON: Right.

MS. SMITH: -- in determining whether the exemption might be appropriate to recommend.

MR. JACKSON: So shall I just wait for your questions or --

MS. SMITH: Why don't you briefly summarize what you're seeking to do.

MR. JACKSON: Can you speak up, I --

MS. SMITH: Can you briefly summarize

what -- why this exemption is necessary in your view.

MR. JACKSON: Okay. The current generation of aircraft, the aircraft such as the A350, the Boeing 787, the Gulfstream G650, these generation of larger business jets and commercial airliners are digital as I was saying.

They are basically computer controlled, at this point. And the avionics systems on board generate large quantities of data on a normal operational basis. That information is used for a variety of purposes. And those purposes can be for flight operations quality assurance, how well the airplane is being flown, how well the pilot is flying the aircraft, is he doing so in a safe manner in a way unto which the airline has their airline standards.

There is information regarding to maintenance and other activities on the aircraft. And there is, today with these aircraft, there are security concerns. The FAA has evaluated these new generation of aircraft and determined special conditions. Meaning that the design the airplane taking into account information technology, the certification rules to which they have been -- which have been reviewed, do not account for the digital nature of these aircraft.

And the fact that there can be digital threats, cybersecurity threats, to the aircraft itself. The FAA has identified -- well they have a database and the last time I looked, about 24 different aircraft, that have been identified as having security concerns.

And in that, they have also published regulations and actions to which the airlines must -- the airlines and the operators, because it could be a private operator for that matter, who has a business jet, that they must comply with and maintain to keep the security of the airplane in the air worthiness of the aircraft itself.

The aircraft is controlled and basically broken down to the three domains. The passenger domain, which has little concerns of actions in it. There is an information domain to which is controlled. And then a control domain which is the actual net operation of the aircraft. And each of those has the control domain and the information domain has a concern and a potential risk. And so part of the regulation is to develop security protocols for maintaining this aircraft and part of that protocol is to review the data.

Now the FAA and the airlines and the operators have had an ever increasing improved

safety record because of the activities they have done to oversee and provide quality assurance for the maintenance support and operation of the aircraft.

And so, with the digital nature of the airplane itself, there is an increased interest in the control of that information even though there is a requirement now for the airlines to review that data. So we're in a bit of an interesting area at this point.

MS. SMITH: So is your company looking to make like an aftermarket data analytic product or what is your interest in circumventing a TPM on an aircraft?

MR. JACKSON: Air Informatics, my company, is really looking at the information, the communications, the analytics, the connectivity, and the cybersecurity for the airplane. So it's in essence, how do we collect the information because they are vastly wireless, but there is also wired means to collect the data, what they call sneaking out, running out to the airplane with a USB drive.

But it's about the connectivity, the analytics, understanding what's going on in the airplane and the cybersecurity.

MS. SMITH: So are you already

collecting this data or is there data that you would like to collect that is being hampered by an access control.

MR. JACKSON: I'm sorry I'm having a hard time hearing. I've probably been around too many airplanes. But --

MS. SMITH: Are you already collecting this data or is the collection of the data that you're seeking to get hampered by an access control?

MR. JACKSON: It is both really. In a sense of the work that I've done and the work that we've done have dealt with airplane health management for Gulfstream, cybersecurity for Box and penetration testing for the airline, or the operator, or for the manufacture of the component box that would go on the airplane. And for assessments of the security of the airlines infrastructure to support the airplane. And the development of the airplane network security program.

The drive for the request of the exemption has been really the situations have occurred where a manufacturer has chosen to encrypt data and not provide access to it. Or to act -- to prohibit the access to that data and prevent companies from doing the analysis. Now we do the

analysis as a contract to an operator or an owner because we are in contract to those parties.

MS. SMITH: So is the aircraft operator or owner allowed access to that data and then they pass it on to you? Or are they having a hard time getting that data also?

MR. JACKSON: A combination of all of the above. In the sense of we can do the analysis because it can be complex and it had can be novel and interesting in the sense that their not well-versed in the space and they've gone to third parties.

MS. SMITH: But can the aircraft operator or owner get the data that you're seeking to get? Right you're trying to circumvent something in order to get data is what I understand in essence what your request is. And I'm trying to figure out who -- whether or not the aircraft owner already has access to it.

MR. JACKSON: The aircraft owner, we work in conjunction with the owner or the operator. And I say owner or operator because you could have leased aircraft.

MS. SMITH: Right.

MR. JACKSON: And you could have owned aircraft. And there is a fine line difference

between that and a difference in interest. But we fundamentally work for the operator because they are the ones that have the requirement to maintain a safe and secure aircraft. So the FAA regulations go fall on the operator of the aircraft itself. And so we work for them typically in this case.

We could work in the sense of a leasing company may say I want that data because we have to have that data when the lease gets turned over in order to meet requirements of the FAA. We want to make sure we have it up-front instead of trying to collect afterwards.

And they have concerns of failures of the airline and inability to get that data would have a significant impact on them in the end.

MS. SALTMAN: Does -- is it the manufacturer of the airplane who controls access -- who would give access to the data or the manufacturer of sub components within the airplane. How does that work?

MR. JACKSON: You buy the airplane, you buy all the systems in it. You pay for the gas, you hire the flight crew, you fly the airplane. The owner's requirement to maintain in a safe condition is --

MS. SALTMAN: Yes, but --

MR. JACKSON: Is on the operator.

MS. SALTMAN: But so who has access to the data that you are trying to access? If that's protected by an access control, like who has the password to get to that data? Is it the manufacturer of the component, or --

MR. JACKSON: No, it's a responsibility of the airline to collect that data. The standard, or how that data might be formatted is by an industry-based standard. In the sense there is a committee or group called ARINC, we were originally called Aeronautical Radio.

That was formed by the airlines themselves going back to the '20's to create standards so they can have interchangeability of components or parts or the like. And they've defined a format standard to which the manufacturers build to.

But the software itself may both be -- may be developed by the box owner but the information we're collecting relates directly to how that aircraft is being operated, how it's being flown, how it's being maintained in itself.

MS. SALTMAN: I guess what I'm trying to get at is, in order to get to the information, I mean, is it possible to go to the manufacturer of

the box or the airplane and seek permission or get a license to access that data?

MR. JACKSON: Well, they are trying to exert the position, some, that you can't deal with the data unless you get our permission. But the airlines believe, and historically, this information has been the airlines considered their airline information. And it could be anything from -- any type of information.

MS. SMITH: Do the airlines already have access to this data that you're seeking access to.

MR. JACKSON: They have -- yes, because they're responsible for -- example: there is a wireless access point on the top of the airplane. In what's called the electronics bay or in a compartment of the airplane itself, which holds all the computers, there are file servers. The airplane information is collected in that file server, in essence the hard drive. Then on landing, that data is streamed out directly from the airline to a corresponding access port at an airport or at that their hangar to go directly into their possession.

MS. CHAUVET: I'm sorry, to go into whose possession -- to go, when you say the data

is going to the hangar or whatever and it goes into their possession. When you say their possession, who do you mean, specifically.

MR. JACKSON: I missed the last part.

MS. CHAUVET: When you are saying their possession, whose possession are you referring to?

MR. JACKSON: The data from the airplane after a flight goes, you know, they have the responsibility and they have setup systems so it goes back to the airline. And so it can go directly when they land and pull into the hangar or to the terminal and it goes directly back to their servers.

MR. RILEY: When you say the airline, do you mean the owner or the operator?

MR. JACKSON: The owner or operator, really yes, that's the best way to do it. And that's what I'm saying.

MS. SMITH: I guess I had thought that you were looking at the airlines or the operator as a potential client but it sounds now like you may be trying to access data that is proprietary to the airline that they do not wish to share.

MR. JACKSON: We do not do anything without the airline's request and on contract. So we're not listening in and going back to them because

that data belongs to the airlines.

MS. SMITH: So now I'm confused why the exemption is necessary if the airline already has the data. Can't they just give it to you?

MR. JACKSON: Again, I apologize.

MS. SMITH: Can the airline just give you the data if they already have the data and it's their data?

MR. JACKSON: I'm not sure I understand.

MR. CHENEY: So let me maybe restate the question slightly different. So in what process are you interrupting that data flow? You said that the airplane pulls up, it then is transported or transmitted to a server at the hangar --

MR. JACKSON: Right.

MR. CHENEY: And at what point are you interrupting that? Are you getting it after it's already stored by the operator or are you getting it in between that, is that when you're getting it?

MR. JACKSON: It can be either in the sense that we have and can set up an access point and manage that access point. And so the data comes from the airplane and we can do things where we manage the delivery. We oversee the delivery from the airplane. We can capture the information as a

service that then delivers it to the airline.

MR. CHENEY: So then can --

MR. JACKSON: So that doesn't mean we do an analysis of it, we just do a connectivity and delivery. We can do, on contract, the analysis of the data.

MR. CHENEY: So let me probe a little bit more on that. In order to do so, you're saying that you have permission of the operator to interrupt that flow?

MR. JACKSON: Yes.

MR. CHENEY: And so it's curious to me why they wouldn't give you that after it already was loaded onto their server rather than interrupting that. Is there some reason why you have to interrupt that data flow in order to get the data? Is it because the format of the data is the problem?

MR. JACKSON: No. It's in the sense of it's not in their business model to do wireless and information management at that side and they may find that it is not cost effective as their own systems. And so it's a matter of economics. It's not that they can't, they may not be good at it or they may not find it economically -- they may find it economically better that we do it, then they do

it. So it's a matter of just a business model, I think is how I'm answering.

MS. SMITH: I'm not sure that that is his question. I think he's saying maybe, Mr. Cheney, correct me if I'm wrong, but if you're getting the data at one part of the process are you just seeking to circumvent to make it more convenient to get it at a different part of the process? Or is there something else going on?

MR. JACKSON: It's a matter of their business choice. We can deliver the data, capture it and make sure, manage that collection process. And delivering it to their servers to look at. Or we can deliver it to their servers for somebody else to look at. But it's their data, if I'm understanding what you're saying, is to their data and frankly, you may have an operator that is small. Two airplanes. And that's just not something they're good at or want to be good at. And so they're going to say help us get that data.

And that's part of the business, to do the connectivity piece and the management piece and part of it would be a report to say so much was delivered as of this date but I don't know what's in the ones and zeros.

The business model could also say do the

analysis of the data. It's the analysis of the data that -- because the data that we manage may be encrypted and we can't see it and that's fine. But the data in a case that's encrypted, the airlines or the owner or the operator, may then say we would like you to review and analyze that data as well. But if it's encrypted, we have -- that's a means of protection that we have to then overcome.

MS. SMITH: Can they give you the airline's permission to decrypt the data in that example?

MR. JACKSON: Yes, if they have it and yes, if they're given that decryption code. That has not always been the case. There have been cases where the original plan was a standard VPN from the two ends of the end point, you know, from the delivery to the receipt of the data on the ground or at a hangar. And then they chose to encrypt it. And so --

MS. SMITH: Who is they?

MR. JACKSON: We can be the VPN end point but they chose to encrypt it as well.

MR. CHENEY: Who's encrypting it in that example?

MR. JACKSON: Well, it would be the manufacturer of the airplane.

MR. CHENEY: And so by -- what you're suggesting is, I think, in this process, let's see if we're teasing this out and we understand that. I think that's what we're trying to get at here, right? Is that -- is you're working -- your client is primarily the operator of the airlines.

MR. JACKSON: Yes.

MR. CHENEY: Whoever's operating the airplane. This data is being encrypted or coming from the manufacturer of the airplane or the manufacturer of the part or whatever, and they're the one that's imposing the encryption on it and you want to decrypt it at some point in that process. Is that what we're getting at?

MR. JACKSON: Yes. If it's on contract with the owner or operator. There have been cases that didn't happen with us but a manufacturer of the airplane -- the operator, owner or operator, has data. They have collected it. And now they want to give it to a third party company to do analysis of it because they didn't have the expertise or the staff or economically, they thought it would be better to contract it out.

MR. RILEY: And this is the encrypted data?

MR. JACKSON: It could be encrypted or

it could be decrypted --

MS. SMITH: Well, if it's decrypted you don't --

MR. JACKSON: In case it could be encrypted.

MS. SMITH: If it's decrypted 1201 is not hindering your ability, I think, to analyze that data. So we're more focused on when there's encrypted data.

MR. JACKSON: Encrypted data. And then the OEM, the manufacturer, steps in the middle and says no, you can't give that to them. We're not giving you the code and that became a business challenge, it became a regulatory challenge. In this particular case, the company that was doing the analysis was purchased by another large well known company and the OEM said well, we withdraw our -- if you're going to go with that company to do, now that they're owned by this other, we don't have a problem with that. And so, it got very complicated in that sense.

MS. SMITH: Do you --

MR. JACKSON: So there --

MS. SMITH: Have you received threats of legal action based on section 1201?

MR. JACKSON: I'm not sure that --

MS. SMITH: So in that example, it sounded like the situation was resolved. So I'm wondering about, again, the need for this exemption. Has your company or your clients received refusals to decrypt the data or cease-and-desist letters invoking section 1201, or something suggesting that this prohibition on circumvention is an obstacle to what you want to do?

MR. JACKSON: I really apologize, I'm not hearing you properly.

MR. RILEY: Has anyone told you that you cannot decrypt the data, that you've been presented with a cease-and-desist letter, or --

MR. JACKSON: We have never received a cease-and-desist letter.

MR. RILEY: Have you asked for permission and been told no?

MR. JACKSON: We have been told that we would not be given permission.

MR. RILEY: So when the -- let me just clarify some things you've been saying. It sounds like the aircraft owner or operator can get the encrypted data off of the airplane without a problem. But the problem is decrypting it.

MR. JACKSON: Correct. And the actual

access to the data. And they have even gone to the point where even the data was not encrypted or they refused -- they basically have threatened that you have to pay a license to review that data.

MS. CHAUVET: Do you know of any circumstances where someone has asked for a license to the encrypted data and the license has been refused?

MR. JACKSON: The data has not been requested -- not, we have not been told that you can get a license for this data.

MS. SMITH: I thought you said just a few minutes ago that someone could be offered a license to the encrypted data. So that's what I'm asking about.

MR. JACKSON: It was another company, that is how it's happened. And the situation that I described of the OEM stepping in between and saying you can't have access to that data without a license to it, was not with my company, but it was with a company that I was working with. And we couldn't go forward, even with discussions.

MS. SMITH: But that implies you can get a license to the encrypted data.

MR. JACKSON: They --

MS. SMITH: So I'm asking --

MR. JACKSON: Yes.

MS. SMITH: For any examples where a license to the data has been requested but then has been refused.

MR. JACKSON: In this particular case, I was managing, we were managing, a certain part of that chain. A certain part. And I was managing the security -- development of the security protocols.

In that we were pointing out and determining what type of analysis would be required and how to manage the requirement to analyze the data. The particular -- our owner operator had a long standing agreement with that owner operator that data would be managed.

The OEM stepped in and says you can't allow them that data.

MS. SMITH: You said earlier though it is the aircraft's operator's data, so how can the OEM prevent them from sharing their own data?

MR. JACKSON: That is a question that I can't -- that is a question I cannot directly answer because I am of the belief, the owner operator was of the belief that they owned that data.

Because, again, it was a box that they purchased, came with the airplane. The format was

commonly known and was not proprietary. And they, the manufacturer of the airplane was saying you can't do that. In the end, they removed their objection when the third party company that was doing the analysis was acquired by a major partner.

MS. SMITH: Do the owner operators, which it involves their data, do they support your request for an exemption. Do you know?

MR. JACKSON: For them to do the analysis?

MS. SMITH: For you -- this exemption, there was only two comments, maybe three comments, filed and we didn't receive any from the airlines. Do you know whether your clients support your request for this exemption?

MR. JACKSON: Again, I'm not exactly sure I'm hearing you properly.

MS. SMITH: You seem to be seeking an exemption to circumvent an access control to get at data owned by the airlines.

MR. JACKSON: Yes.

MS. SMITH: Do the airlines support your request, do you know?

MR. JACKSON: Yes, I believe they would in this case. If they --

MS. SMITH: Have you asked them?

MR. JACKSON: We have engaged in that with airlines and it's an ongoing discussion and it's something we've had with other airlines globally. That, of course, doesn't impact this decision because it's not a U.S. airline.

MS. SMITH: But the airlines may be in a position to give you this data.

MR. JACKSON: Yes and no. If the data has already been encrypted -- has been decrypted and they have the codes, yes they can. It is their data, it is their right to manage it any way they wish. That is their position, that is our position.

There have been cases where they have not been given that information to decrypt that data.

MS. SMITH: Does this data, it comes through in bulk form. Would you call it unstructured data?

MR. JACKSON: It is in bulk form, it's raw files, it's un-interpreted. It requires a degree of interpretation and it comes not as ones and zeros but in some form of, how can I put it, formatted data but it's not in a easy to understand fashion. It's a combination of codes and text characters with certain meanings.

The meaning of this data, and it could

be altitude, pressure, temperature, speed, how the airplane is flown, control service inputs, things like this, that the industry has defined definitions of this and formats of it saying this is the order of the data and you can take it from this x-y-z to an intelligent text stream of speed, altitude, pressure.

MS. SMITH: So the format is dictated by industry standards or FAA regulations. Is that correct?

MR. JACKSON: The document -- the development of that standard is done by committees, by the operators themselves -- that are composed of the operator staff. It was originally done over at the company called ARINC. ARINC in its structure has been recently sold. There's a history to that, ARINC was formed in the '20's by the airlines themselves. Everybody had a piece of the company, a percentage of the company. And they still have committees that define standards for the development of the box, the format of data in this particular case.

Now as it turns out, during the beginning of the recession, the airlines wanted to get rid of the ownership of the company and they sold it to a private equity firm Carlyle. Carlyle

then sold it to Rockwell Collins. Rockwell Collins then diverse, you know, sold off the Standards Group to SAE, which is Society of Automotive Engineers. They are maintaining this in the same way they have before.

MS. SMITH: They're maintaining a standard?

MR. JACKSON: The standards and developing new standards.

MS. SMITH: How do the operators comply with the FAA regulations currently if there is encrypted data they are having trouble getting access to?

MR. JACKSON: I'm not again --

MS. SALTMAN: Well, can I ask -- because the FAA regulations mandate that the airlines have to analyze this data and collect it. If a manufacturer of a box or a component refuses access to the data, isn't there some way you can point to these regulations? Is there an enforcement mechanism where the manufacturer has to comply to allow the airline to comply with the FAA regulations?

MR. JACKSON: That action has not been taken. The FAA does not seem to be interested in taking that action. They don't care how you get the

data, as long as the analysis, I shouldn't say data, I should say the analysis, is done, as long as it's done. And so they don't care if you pay a license or do it yourself. They just say it has to be done.

MR. CHENEY: Are you saying that in some instances, that it's not being done today? Is that why your service is being offered? Is there a gap?

MR. JACKSON: There are, I know very specifically of cases, where it's not being done.

MR. CHENEY: And it's done because they can't interpret the data because it's encrypted and it can't be read, except by some third party provider like yourself?

MR. JACKSON: It's a host of reasons. Manpower, knowledge, experience. I don't think there's one definitive reason that they are not doing it.

MR. CHENEY: So it's not necessarily primarily that there's encryption on the data that is not the reason that they're not providing it.

MR. JACKSON: That is one of the reasons.

MR. CHENEY: It is one, okay.

MR. JACKSON: It is certainly one of the reasons. I mean, there have been cases where they -- goes back -- they have not managed to create a

consistent connection to the airplane. And so they were unable to get it for periods of time.

Could be weeks or months. And though the regulations say that you need to do this on a periodic basis, it was not done. And there are cases where the encryption, and they didn't do it because they didn't have the skill, they didn't have the encryption codes and it's not being reported.

I know on some manufacturers, one manufacturer, and airplanes, they are not distributing the encryption codes and to comply with the regulations you have to go to their designated company. And that's just the way they did it.

MS. SALTMAN: What happens if an airline doesn't comply with these regulations? Does the FAA impose a fine on the airline? Are they grounded? What happens?

MR. JACKSON: They -- if there is an audit of the regulation, there can be some form of penalty, which is typically a fine. The fines vary, depends on the severity of the issues. But audits are not that common.

MS. SALTMAN: And do you cite the exact regulation you are referring to you in your comment? Or do you have that?

MR. JACKSON: I can give you those regulations.

MS. SALTMAN: Okay.

MR. JACKSON: I can give you, those I can give you copies of because they're public. There's AC -- and I can rattle some of them off right now.

MS. SALTMAN: Sure, that would be helpful.

MR. JACKSON: AC 119-01, OpSpec D301, FAA 8900.168 -- what did I have. I thought I did have a list, but I can give you that digitally. AC 119 which I mentioned. FAA 8900.1 Volume 3, Chapter 61, which is the aircraft network security program. I mentioned OpSpec D301, which is in N8900.189 and that's aircraft network security as well. N8900.358, dealing with aircraft electronics systems security special conditions. Those are the primary ones that are in place right now.

MS. CHAUVET: Given that there are so many current regulations, why would it not be more appropriate for the FAA to address the issues of manufacturers not providing --

MR. JACKSON: They --

MS. CHAUVET: --- decrypted data.

MR. JACKSON: Well it may be, and I can't say whether it is or is not, they are not getting

them -- they tend not to get involved in something relating to this.

MS. CHAUVET: Have there been direct efforts or have you tried to --

MR. JACKSON: I had --

MS. CHAUVET: --- affect the FAA regulations or any other regulations to require manufacturers to provide encrypted --

MR. JACKSON: I've had conversations with those individuals to understand why it's not being done and what their position is and the answer has been it's not our position to do that.

MR. RILEY: If you were able to get the encrypted code, how would you decrypt it?

MR. JACKSON: Well, the encryption code is like anything else, it's like any other encrypted data, you just apply the code and it will --

MR. RILEY: But assuming you don't have the code?

MR. JACKSON: Well --

MR. RILEY: Let's assume you have the encrypted data but not the encrypted code, what happens next?

MR. JACKSON: Right. If I don't have the decryption key.

MR. RILEY: Right.

MR. JACKSON: Now you could go through a variety of algorithms to try to find a way to go -- to find that code and go do it. That's the standard process of procedures. But it's not one that I choose to do. That, in my opinion, gets a little bit dicey even if we have the permission to do it. But you can technically do that. It depends on the strength of the code and how they've chosen to encrypt it, the algorithms they've used.

MR. RILEY: How strong is the code?

MR. JACKSON: It varies. It's up to whoever's setting up the encryption algorithm.

MR. RILEY: What's typical? 16 bit? 32 bit?

MR. JACKSON: It's typically, I hate to say this, I've seen some pretty weak encryption codes. They are not current to NIST standards or recommendations. Historically, they just have not.

One manufacturer only, I don't know if it was late last year or the beginning of this year, changed digital certificates from SHA1 to SHA2 and that's been recommended to be changed 10 years ago by NIST. But they just hadn't.

These are not necessarily the most, well -- I've seen various levels of encryption. From

very weak that could probably be decoded in a short period of time.

MR. RILEY: Is there any concern that if you were to decrypt the code it would somehow become corrupted?

MR. JACKSON: Well you have standard methods to make sure the data is not corrupted. That's built in to the information. There is means to which the data can be authenticated, validated, and can with CRC and other forms of digital means to make sure that the data, the integrity of the data, remains.

That's key to what has been done and that's a fundamental principle in developing the data stream and the delivery of data.

MS. SMITH: So you're --

MR. JACKSON: So that's not necessarily related to decrypting it or not. And you would be able to tell whether it was, you know, corrupted in one manner or another.

That's critical in a couple of ways. One, you're dealing with very specific information with a format that, output format, that is within the expected norms. Corrupted data from going from 600 knots per hour, 600 miles per hour to 601 miles per hour is, you would detect that from a CRC but

the type of errors you would have is you're suddenly doing 60,000 miles per hour, which is obviously in error.

But there are means to digitally determine that the authenticity, the non-repudiation, all these components are in it to make sure that what is sent is what is received. And that's independent of encryption.

MS. SMITH: So you have said in your writing that the circumvention would be conducted in a controlled setting such as an office or data management environment. And that the data would not be exposed in any real time flight operations setting. Can you explain a little bit more how that would work?

MR. JACKSON: Well you're dealing with standard methods, tools, process and procedures to guarantee that you're not losing any data loss. You're not going to have any data loss or data --

MS. SMITH: But I think my question is you're not taking the data while the plane is in the air? Right? I mean, what does that mean, the data would not be exposed in any real time flight operations setting? That's your statement, so I'm just trying to understand what is behind that?

MR. JACKSON: I'm not. You're saying

that how do I prevent the data being lost and being --

MS. CHAUVET: No, I think she's talking more about safety concerns. So like you say you're going to be analyzing the data in a controlled environment not when the plane is in the air.

MR. JACKSON: Oh!

MS. CHAUVET: And I think she just wanted some more information about that statement that you made in your written submission.

MR. JACKSON: This is just being done in industry standard practice and services and environments. That's fundamental with everything you do. And the data does not directly impact any air worthiness or provide any flight risks. The data is to see that the airplane is being flown properly, maintained properly. Probably the most real time concerns is the cyber security side to make sure that you can look at the data at some close interval to determine that nothing -- no one has touched the airplane with an intentional means to harm or to corrupt or in any way to affect the air worthiness of the airplane or the flight.

MS. CHAUVET: Once you have access to the data, particularly in the cyber security area, which you're just referencing, does that give you

control of any kind over any of the software in the plane or information about being able to access the software in other parts of the airplane?

MR. JACKSON: The data that is received, again, is in all cases advisory. In the sense that it does not -- I mean the data is always advisory in the sense you can look at it to determine how well the airplane is being flown.

Whether certain maintenance actions have actually occurred. Maintenance actions have been done properly. In the cyber security side it would be to make sure that nobody has touched the airplane. That you can see no malicious act that would impact the airplane itself.

MR. CHENEY: I think part of the question here is is that misuse of this data in some way, does this data give you the sort of information that would -- were it be published on the internet, for example, that it would allow some cyber security incidents or allows you that sort of access that you would be able to have some malicious access to the aircraft or be able to --

MR. JACKSON: Access to the aircraft -- I'm trying to think of the best way to answer that. The data itself should not or would not impact the operation of the aircraft itself if it was revealed

to someone. It might reveal someone's flying capabilities. It might reveal a maintenance fault. It does not impact some software being changed or reloaded or, you know, counterfeit software to be delivered to the airplane.

MR. CHENEY: So, I think -- if we can restate what you're saying just to make the point is that this data is given to you at some point by the airline.

MR. JACKSON: Yes.

MR. CHENEY: After the plane is on the ground.

MR. JACKSON: Yes.

MR. CHENEY: All of this data is given to you to analyze what the plane has just done.

MR. JACKSON: Yes.

MR. CHENEY: And then to give it back to the airline to say this is what's wrong. It's not to access anything while the plane is in the air or to affect its next flight.

See that might be one of the issues is, does that data give you an opportunity or, whomever might get access to this data, some information that allows them to do something with the plane as it takes off for the next flight.

MR. JACKSON: The -- in any of this you

may look at a case where somebody is flying erratically and it might be flagged to the airline that something dramatically is wrong with how this airplane is being flown. There could be something that could determine they made a maintenance error and the anti-lock brakes, you know, are mis-wired. That requires a very quick analysis which is not being done now. Most of this is trend related information. The most important real time or near real time analysis would be the security of the airplane itself. To look at the data and to see that there was no unauthorized access to the airplane. There is the equivalent of a firewall and that no one attempted to go through the firewall.

Or there's an access point. And you can see there was no unauthorized, repeated attempts to log into the airplane from -- at some airport, that was unauthorized. That's the type of thing the FAA is most concerned with that would raise a red flag that says hey, we have to look at something. Because all of a sudden at x-y-z airport someone tried to connect into an access point on the top of the airplane a hundred times. And the airplane didn't respond or the airplane responded.

Did someone maliciously try to upload something to the airplane? Try to connect through

something? Those are the type of things that are most important in a real time basis. That, I think, is what you're looking at, the answer, the type of thing you're looking for with that question.

MR. CHENEY: Well, actually I was looking for the sensitivity of the data itself that you're getting. Can that data be misused?

MR. JACKSON: Yes, and the misuse --

MR. CHENEY: Not the mix.

MR. JACKSON: No, it should not be in the sense in that sense.

MR. CHENEY: So my question is then why is the manufacturer encrypting the data? What's the --

MR. JACKSON: Well, there's economic value to data. There is a belief, and I have been told by a vice president in charge of one aircraft program, that it is their intent to own everything on that -- all the data off of that airplane, because it impacted their business opportunities for global services.

So that they could offer certain maintenance operations and they wanted to be solely responsible for that. That was specifically told to me by a vice president of an aircraft program at a well-known manufacturer. So, it's similar to

what I had said with the airline being told by a manufacturer that no you're not authorized to give the data captured from your airplane on how you're operating it or how the pilots are flying the airplane to a third party company to do the analysis.

MS. SMITH: All right thank you, Mr. Jackson, very much. I don't think we have any more questions for you. So that will wrap up Class 11 and we will back at 1:30 for our very last session.

MR. JACKSON: All right, thank you very much.

MS. SMITH: Thank you.

MR. JACKSON: I appreciate it.

(Whereupon, the above-entitled matter went off the record at 12:21 p.m. and resumed at 1:30 p.m.)

MS. SMITH: All right, we are going to get started for the last session for the section 1201 rulemaking, this we've termed the audience participation section. We have seven people who have signed up. And so the first person, however, is someone we were not able to accommodate for our Class 3 panel which was held in D.C. so we're going to give her a little bit more time, which is similar to what we did for the people in D.C. who were unable to come to L.A. So I think first we will introduce

ourselves and then perhaps, Ms. Gilford, you can introduce yourself.

So my name is Regan Smith, I'm Deputy General Counsel of the Copyright Office.

MR. CHENEY: I'm Stacy Cheney, Senior Attorney-Advisor at NTIA, National Telecommunications and Information Administration.

MR. RILEY: John Riley, Attorney-Advisor, Copyright Office.

MS. SALTMAN: Julie Saltman, Assistant General Counsel at the Copyright Office.

MS. CHAUVET: Anna Chauvet, Assistant General Counsel at the U.S. Copyright Office.

INTRODUCTION - AUDIENCE PARTICIPANTS

MS. GILFORD: Thanks, nice to meet you. Karen Gilford, I'm the General Manager of Movies Anywhere.

MS. SMITH: Thank you and you would like to offer comments in respect to Class 3, which concerns space shifting. Is that right?

MS. GILFORD: Yes.

MS. SMITH: And I understand you have a presentation for us.

MS. GILFORD: Yes, I do.

MS. SMITH: Okay, you can go to the

podium and present that. We will call that Exhibit 3C and that along with the rest of the exhibits will eventually shortly be posted to copyright.gov.

(Whereupon, the above-referred to presentation was marked as Exhibit 3C for identification.)

MS. GILFORD: Okay. I have a presentation, also a short video that I'll lead with. The video that I'm going to present is actually a piece of advertising, a 30 second spot, that describes our product. This is how we communicate the value propositions to consumers in the marketplace. I thought it would be helpful to start with this.

(Video plays.)

MS. GILFORD: I'm a Mac person, so excuse me. Thank you.

So I'll walk through a quick presentation to give you an overview of Movies Anywhere. As you can see from my video, Movies Anywhere, as its name speaks to, is a product that's focused on feature films. Where we feel very lucky to work on our product because we know that consumers love feature films, which is really the product that

streams through Movies Anywhere.

The other thing that we see happening today, and one of the reasons why Movies Anywhere was sort of brought to bear by the studio partners that power it, is folks have an amazing experience in their homes right now to watch movies in the living room with broadband speeds increasing, screen sizes increasing, and a proliferation of devices in the living room now that really make it seamless to access content with a couple of clicks.

We know that people now really enjoy watching premium content in their home. But one thing that has emerged in the space over the past few years with the proliferation of broadband and devices is a little bit of consumer confusion about if I buy something here, can I watch it over there? And so the studios came together to fund and power Movies Anywhere to solve that and create what we call interoperability between different services.

So the mission statement of Movies Anywhere is it's an app, as you saw, also web-based and it brings your purchased movies together so you can watch them whenever you want, when and where you want. So regardless of where you purchased them, you can link your accounts to Movies Anywhere, as you saw in the video, we will bring the collection

together. And then we'll also bring that consolidated collection back out to your retailer end point so you have a choice where you want to experience that consolidated library.

This is a slide that shows an overview of our ecosystem at this moment in time. So the interoperability feature really brings together three main cohorts. The first one is our studio partners. We currently have five of the major studios in our service. Sony Pictures, Fox, Universal, Disney and Warner Brothers. So those are the five video partners. There are about 7,500 titles in the service. We have retailers integrated, iTunes, Vudu, Google Play, Amazon and Fandango Now. That constitutes approximately between 75 and 80 percent of the U.S. market share for electronic home video licenses that are sold.

And then on the lower left hand side you see all the platforms where consumers can download the service or navigate to the service on the web. We are on all the Apple platforms, Android platforms, Amazon platforms, Roku, and those smart TVs and other end points that are powered by operating systems like Android TV where consumers can access the Google Store and download our app.

This is just some quick stats on the app.

Our tag line is Your Movies Together At Last. We do focus on feature films. As I mentioned, there are 7,500 titles available in the service. And what that means is that the 7,500 titles which are a combination of titles from the five studios are available for this interoperability feature. Meaning that Movies Anywhere has taken them in and mapped them to all the retailers which facilitates the movies being able to flow across the platforms.

We launched on October 12th of last year. The app is free for consumers to download --

MS. SMITH: Can you explain the difference between this Movies -- there was a previous product, was it Disney Movies Anywhere, or what's the difference?

MS. GILFORD: Sure. Disney Movies Anywhere was only Walt Disney Company feature films. So it was limited to a catalog of about 500. So Movies Anywhere expands the offering, utilizing some of the sort of backbone technology that was developed for DMA but brings four more studios into the mix.

MS. SMITH: Thank you.

MS. GILFORD: We are an English language supported app although the content does support -- the actual films are available in other

languages and right now this is a service that is only available in the United States.

The next few slides will just give you a little bit more of an in-depth product walk through. If you have the app you may have seen some of these. The first screens just show you our welcome and sign up process. When somebody navigates to the app, they're just greeted with a few quick screens that they can get past if they would like but it just kind of gives it a little bit more of an explanation of what the app does so that we're very clear about the service that we're bringing.

You can sign up for the service using an email and password of your choosing. You can also sign up using Google or Facebook. The first page you are greeted with when you download the app or navigate up to our website is what we call our Explore page. This is the home screen. We do try to personalize it for each user profile. And really the purpose of this page is to let consumers know sort of what the newest releases are out in the marketplace that are available in the service. Any special features or promotions. Seasonal things, offers that we may have or that our studio partners may have, things that we think that the consumer

would be interested in knowing about.

The next screenshot and area we are showing here is really the bread and butter of the service, which is our retailer account linking screen. So this is where consumers will go to create the linkage between Movies Anywhere and their preferred retailer. So they can navigate to the retailers where they purchased films, hit that connect button. It's a pretty seamless integration where you would also then sign into Vudu or iTunes, or Amazon, Fandango or Google. It sends you back to Movies Anywhere. It gives you a very clear signal that you are connected and your movies are starting to flow in and then flow to the other retailers. So there is a feedback loop as this functionality is happening.

And then you can also set on the screen the retailer that you would like to be your default. So then screens will show in a minute, when you go to buy a movie, then that would be your retailer of choice. If you haven't set one, you'll be presented with all the options available to purchase on that platform.

The next page is our redeem page. This is where consumers who have purchased a physical DVD that has a redemption code in the pack and it

gives them an opportunity to also enjoy a digital copy, would come and enter the code that comes in an insert in that pack. Here and then we fulfill the title right in Movies Anywhere. It gives them feedback that the title has been successfully redeemed and drops into their locker.

MS. SMITH: Can I ask a question. What if you've lost the code?

MS. GILFORD: If you lost the code, there are ways we have some forgiveness through customer care but it is the same -- but it does operate similarly to losing a coupon or a gift card or something like that. But there are some remedies that we can -- that happen in the customer care channel occasionally.

MS. SMITH: And you can redeem this through -- for Blu-Ray or DVD's? Are there any other physical media?

MS. GILFORD: It's for the titles that have the code. It's clearly marked on the physical packaging if the unit you are buying has a code in there or not. They are generally referred to as combo packs because they give in pack the consumer a couple of different format options to watch the movies. So typically that could be an SD disk, a Blu-Ray disc and then a code. Now you might see one

with 4K and different options, but generally it's called a combo pack because the user is getting more than one option on how to consume it.

MS. SMITH: And this is a rollout starting in October 2017 or was it previously available -- I guess if the service didn't exist --

MS. GILFORD: There were other options to redeem those codes on other services and those still exist today. So for instance, in Disney Movies Anywhere you could've redeemed Disney codes.

On some of the retail partners, like iTunes, if you really navigate there is an area where certain studios may allow consumers to redeem codes directly on iTunes or in a service like Vudu you can redeem codes. That's decided on a studio by studio basis in their individual agreements with the retail partners.

MS. SMITH: So in terms of the studio agreements for Movies Anywhere, can they take those codes they may have had for Disney Movies Anywhere or something else through Vudu or Walmart or whatever and use that into this Movies Anywhere?

MS. GILFORD: Yes. We honor codes sort of like backwards compatible, if you will --

MS. SMITH: I think that's right, yes.

MS. GILFORD: So if the code redemption opportunity doesn't start just for codes generated after we launched, we go all the way back in index codes that are out in the marketplace.

MS. CHAUVET: And then besides the redeem codes and then I saw Vudu up there, are there any other methods to convert, I'll just say convert, generically like a hard media into a digital form?

MS. GILFORD: In our app, code redemption is the only method that we power and service. But you mentioned Vudu, who's one of our partners, they have a program that you may be familiar with called Disc to Digital for some eligible titles with certain parameters that they could probably speak to better, you are able to convert a physical disc to a digital copy. And if you do do that on Vudu and then link your Vudu account to Movies Anywhere, those copies would come into our service and then also flow out to the other retailers that you are connected to. And they're treated just like any other digital movie.

MS. CHAUVET: That's actually really helpful. And then besides Vudu are you partnered with any other third party that has a similar offering?

MS. GILFORD: No, just because our

other retail partners that we've integrated so far don't offer that. But Vudu just happens to be the only one that I know of that has that service right now and also has an integration with us.

MS. SMITH: So I'm trying to understand if there's a way if Movies Anywhere is a useful service for sort of back catalog media that consumers may have. Do they need to see whether disc to digital is offered by Vudu or do they need to buy a new copy that would have a code or what? Or is it just doesn't speak to someone who may have bought a DVD or Blu-Ray five or ten years ago.

MS. GILFORD: I mean, it depends, just on how that title is -- what unit you bought, and then how -- what studios have done that disc to digital license. I can tell you personally that I did disc to digital with titles that I bought 10 years ago and it worked perfectly fine. It didn't work for every title I bought 10 years ago, but it did work for some of them.

The My Movies tab, which is the center navigational item on the app, is what it says. That's where a consumer's movie library is stored. That's their digital movie collection. They can sort it, they can access playback from there and

that's where we also save any maybe viewership of a movie that may be stopped partially through so you can pick it back up.

And then the last page I think I'm showing is our movies detail page. So this is really the backbone of the system. There's a page like this for all of the titles in our system. It gives the basics that you may find on other sites that offer information about feature films. And this is where consumers would hit the buy button and be presented with retailer choice of where they may want to purchase the movie.

Movies Anywhere does not sell directly, we're just a hub. When, if you went off to purchase on iTunes or Amazon, you complete the purchase there, then be sent back to Movies Anywhere. That movie, once you have the linkage accomplished, when you need to buy something, it would automatically flow within it happens within seconds back to Movies Anywhere and then out to the connected retailers.

MS. SMITH: So if I were to use the Movies Anywhere app to buy a movie on Amazon, for example, the places where I could watch that, like the number of devices, that would all just be determined by Amazon. Movies Anywhere wouldn't alter the scope of that purchase in any way. Is that

right?

MS. GILFORD: Yes, we do alter the scope of that.

MS. SMITH: Oh, okay in what way?

MS. GILFORD: So let me give you an example. I'm going to use Apple as my example. If you buy a movie on iTunes and you are linked to Movies Anywhere and you're also linked to Google Play or Amazon or Vudu, you would be able to watch that movie that you purchased on iTunes on your Apple TV and your IOS devices which is part of their more closed ecosystem but that movie will also flow to Movies Anywhere and you will be able to watch it anywhere our app is available.

Like, for instance, a Roku device, an Android device, an Amazon device. So Movies Anywhere expands the ecosystem of the places where you can watch the movie that you purchased on iTunes, or Amazon, or Android, or any of our retailers. So it's exponential because you can watch your movie back not only on the platforms where Movies Anywhere is installed. You can watch it on any of the platforms that Amazon is installed on, Vudu's installed on, Google Play is installed on, iTunes are installed on, Fandango Now is installed on.

MS. SMITH: So does it affect the, I

guess, number of devices you can watch it on at the same time? Or is that a different subscription?

MS. GILFORD: Yes, there are, as most, it's any service that's doing streaming, there is -- I don't know the exact number, but it's pretty much on par with other similarly situated services that, you know, devices and simultaneous streaming. We don't look like outliers on any of our parameters.

MR. CHENEY: Would that be on per title or per access to your service? In other words, if you bought a household service for your home, would that access be limited to four or five instances of playing, and it might be four or five different movies at the same time, or would it be four of five instances of the same movie playing at the same time? Is that, what is the limitation?

MS. GILFORD: It's on an account basis, that's usually how it's managed. So you can download the app for free, but it's a one-to-one relationship. So one Movies Anywhere account can connect to one iTunes account can connect to one Amazon account, not multiple.

And then you have an opportunity, so for instance, me, I can set up a sub-account for my husband, a sub-account for my child, a sub-account for my second child. And so that would be, I think

you could do that up to six times. So you could set it up for four users and, theoretically then, we could all be enjoying the service at once, right.

So you're able to set up profiles that can access the same consolidated library. For children, you could set the, a limit on the MPAA rating so they're not exposed to perhaps R-rated content you have.

But that's kind of how it works. It's a one-to-one relationship between MA and each retailer, one account per, but then you can set up sub-accounts for your family to access, sort of the, if you will, family movie collection.

MR. CHENEY: How, you said you could download the app for free. Is there a monthly subscription service charge here? Or is it just the whole thing is free?

MS. GILFORD: The app is free to download, but the only thing that a consumer is able to play back are the movies that they have purchased at retailers.

MR. CHENEY: So the use of your app is free as long as they've purchased the video in one of these other services?

MS. GILFORD: Exactly. It's, it sort of adds more value, you could argue, to the purchase

of the film because now you are able to enjoy it in many, many more places of your choice.

So you don't have to worry, so to speak, if you bought a movie and you changed, decided to change device from Android to Apple, or vice versa, or buy a Roku in the living room, you can make your own device.

The intent is you can choose the device you want when you go into a Best Buy or Costco or wherever, and hook it up and know that the, your assets, the movies you purchased, are going to be able to be played back there.

So it's sort of, almost like a utility, if you will, that's kind of helping consumers be able to watch the movies they bought wherever they want.

MS. SALTMAN: Can you watch rented movies, rented through Netflix or Amazon? I guess not Netflix, but I know you can rent movies on Amazon. Can you rent a movie and then watch it in the app? And then also, do the same expiration parameters apply that would apply in Amazon?

MS. GILFORD: Right now we do not service rental or VOD. It's solely limited to a transactional model.

MS. CHAUVET: And then these uses, or

maybe all of them, go to personal use? Are there any restrictions on a public performance? And I'm thinking specifically, like, a teacher in a classroom being able to show a class a movie that maybe the teacher purchased through one of your partners.

MS. GILFORD: That's covered in the terms of use. It's available, but all those parameters are outlined in the terms of use. I honestly don't have it memorized to know about that specific.

MS. CHAUVET: And do you know if any of the, so say someone -- like for Netflix generally, I think even 100 percent captions its movies. So if something is captioned when it's, or at least the availability of captioning is available on whatever medium they purchased it, and they decide to watch it through your app, is that captioning still available?

And then I guess a second question would be, if they purchase something where captioning was not originally available, do you guys make that available through your service?

MS. GILFORD: I, we have, we are in complete compliance with all of the ADA captioning and all of that.

And we have our own files, if you will. We store all of the 7,500 and so movies we have. And so we will give the best available experience based on what we have. And even if one of our retailers for some reason or not has, sort of, a lesser experience, we will have -- when you -- you will get the better experience, if you will, in Movies Anywhere.

So we're sort of, our intention is almost to set the bar in that when you come in our service we'll have adhered to all of that and you will enjoy it with all of that.

So we're, you know, so we, since we're studio-powered, we want to have almost a gold standard situation there so consumers always know that they can go to this place and have, kind of, the best experience for that film.

So another example unrelated that probably is more clear is a lot of home entertainment purchases come with an extra benefit of bonus content, which a lot of fans enjoy.

So you could go to different retailers and see different incarnations of that bonus content. Some blow it out awesome and it's all there. Some choose not to host it, so you buy it and you just see the movie.

We have all of the bonus. So since we're studio-powered we're like, hey, this is the place where no matter where you bought it, you know if somebody tells you about a piece of bonus and you're like, wait, I didn't see that on retailer x, they didn't give it to me, you know, well, let me go check Movies Anywhere, and you'll still have access to sort of the ultimate package that you paid for regardless of your, where you bought it from.

MS. CHAUVET: And I know you're talking about captioning specifically, but I guess I also wanted to ask about audio description. For example, Hulu is involved in litigation right now because it does not currently offer audio description.

So I don't know if that's something that Movies Anywhere is also considering offering, or if its partners offer that service?

MS. GILFORD: I'll probably have to follow up on audio description. We just launched in October. And it has been discussed, but let me, if it would be okay to follow up because I don't have a clear answer. But the intent is that we would be the bar raiser for all that sort of stuff.

MR. CHENEY: In addition, do you have all the languages that might be available on the

original source video as well?

MS. GILFORD: Yes for, we are, we're, we, again, whatever was sort of available in the United States, so Spanish tracks are prevalent, some movies have multi-language tracks where, because of the creativity of the film, there could be French or something else.

So we're sort of, you know, we're adhering to all of whatever was distributed in the United States. So if the film was offered in the home entertainment window in the U.S. with multi-language, then we'll also have those languages.

MS. SMITH: Thank you. Continue please.

MR. CHENEY: Think that was her last slide.

MS. SMITH: All right, great. So thank you, that was very informative. With respect to Class 3, is it your view -- I guess I'm trying to understand how you would like us to think about this in terms of the relevance to the proposed class.

Are you suggesting that it could provide an alternative such that the exemption isn't necessary? Or are you seeing that the exemption might pose a harm to this business model? Can you

sort of talk about what has brought you here today in connection to the 1201 proceeding?

MS. GILFORD: Yes, I mean I, I mean my perspective on what we -- the main feature that I highlighted, which we call interoperability, is that's what it's intended to do, is to facilitate, sort of, consumer choice.

So for instance, you don't have to feel locked into one platform, one retailer, a physical device because of where you -- your movie purchase originated from. So you should be able to, the intent is to add more retailers over time, add more platforms, add more content so this robust system exists.

And that's in an effort to respond to consumer needs and advancements in technology that have kind of happened in parallel to the home entertainment industry.

Look, I would argue that the alternative would be, it would have a major impact on the revenue. Movies Anywhere would certainly go away. This is invested in by the studios almost as a cost center.

I'm not necessarily -- I'm not generating revenue. Although I have buy buttons, it goes out to the retailers. I'd like to hope that

we will be able to influence revenue over time. But it's, I'm not measured on a revenue goal, for instance.

So I think the studios would no longer invest in this service. And that would have a significant impact on the digital marketplace I would think for sure, and could have a major impact on just the transactional window overall.

I think it would drive up the prices of transactions or could eliminate the ability for consumers to buy movies over time because everything would resolve perhaps to a subscription service then where you could pay a fee and access it.

And I don't know, we see evidence that consumers do like to buy movies just based on the volume in the marketplace.

MS. SMITH: Can you alter any of the movies that, once you've loaded them onto Movies Anywhere? Maybe that's the wrong terminology, but I know we heard testimony about ClearPlay, for example, that might allow you to take out some content.

And we also, in connection with Class 1, heard from people who wanted to cue up specific clips. Is any of that, those features available

through your app?

MS. GILFORD: Not right -- so it's DRM protected so there, there's, you can't go in and extract clips and have them as a separate video file.

We, we're six months out of the gate. It was a very complicated launch. But in the future could I see us putting pointers in for specific scenes where, hey, here's that really funny scene, and you could maybe put a bookmark there to access it.

That could be a future feature on our roadmap that we could add. But it's just a matter of figuring out when that would fit in.

MS. SMITH: Does it import, sort of, the existing bookmarks? Like, the chapter selections you might have --

MS. GILFORD: Yes, absolutely, but they're the ones that are, the ---

MS. SMITH: In the physical copy.

MS. GILFORD: Yes, that are on the physical copy, yes, yes. So all the chaptering is there. And there's still images just as, that kind of represent each chapter.

So as you're sort of scrolling it's really easy to see where you are in the movie and kind of land on, perhaps, the exact moment that

you're trying to find in the movie.

MS. SMITH: All right, thank you very much.

MS. GILFORD: You're welcome.

MR. CHENEY: Thank you.

MS. CHAUVET: All right, our next panelist is Mr. Johann George. He also has a presentation which is going to be entered into the record as Exhibit 3D.

(Whereupon, the above-referred to document was marked as Exhibit 3D for identification.)

MS. SMITH: So we're still focused on Class 3 instead of shifting?

MS. CHAUVET: Yes, that's right.

MS. SMITH: So if you could start by introducing yourself and your affiliation and then proceed with your presentation.

MR. GEORGE: Absolutely.

MS. SMITH: Thank you.

MR. GEORGE: So my name's Johann George, and I am following up with a presentation that my colleague, John Mitchell, gave in the Washington portion of this panel.

I want to thank you for allowing me to

come and present. And my main purpose here is really to follow up on some questions of a technology nature that came up at the last meeting.

So this slide is really just to say that I'm not an attorney, I'm a technologist. And so I'm probably not going to be very good at those --

MS. SMITH: We will hold our legal questions.

MR. GEORGE: Exactly. Okay, so I'll just give a very quick recap to refresh your memory.

So what we are trying to do is to allow consumers who've actually bought DVDs, Blu-Rays, content in one way, and allow them to watch it anywhere, in some sense. Watch it on their phones. I think something similar to what Movies Anywhere seems to be wanting to do. One -- or does, I guess, already.

One, here what's true is that there's a lot of movies out there. There's, I mean, over a hundred thousands of domestic, mainstream-ish movies, not counting the large number of educational videos, all of those other kinds of things.

And people, you can, obviously people have purchased them, but it's not very convenient to only be able to watch them on a DVD. Or maybe

they bought it on a DVD some time ago. Maybe the current version is even not in print. They'd like to be able to move it into some place that is more readily watchable.

And of course, we know that there are many people out there who just go and make a copy and watch it on their favorite device. What we'd like to do is provide an alternative that's legal and that's well protected.

So the idea is that we allow you to transfer your -- transfer data from whatever media you have to an -- some other different media, typically electronic, and only one fixation of that data is kept at any one time.

So for example, if it gets transferred from a DVD to, electronically to your phone or something like that, the DVD no longer exists. And we are very careful to make sure that at no time a copy ever exists.

MS. SMITH: Do you have some slides sort of explaining that process? Because I think since we did hear from your colleague, the more you can focus on the technical aspects of what OmniQ is trying to do, that will be most helpful to us.

MR. GEORGE: Yes.

MS. SMITH: But I don't mean to rush you.

MR. GEORGE: Absolutely. So again, it's encrypted using multiple 2048 bit keys. At all time we, again, continue to respect the intent of CSS and AACS. And I think my colleague probably explained the exemption. So let me go to the next slide which talks about the encryption.

So I think two questions came up, and I'll answer those, and you might have more as I explain it. But the question was how we encrypt and how strong is the encryption.

So the data is actually broken up into chunks, probably about a megabyte in size. Each chunk is encrypted with its own 2048 bit key. So again, we think that that's better protection than the content scrambling system, CSS, which uses 40 bit keys or AACS, which uses 128 bit keys.

As you probably know, with every bit you add, it increases the security level by a factor of two. So it's, makes a pretty big difference.

Something else that's true is unlike CSS and AACS which use a single key for all the data and typically for one given movie -- they're all encrypted, every copy of that movie is encrypted with that same key. Every single, if you have a movie, every megabyte chunk is encrypted with its own 2048 bit key.

So if you take a 4 gigabyte DVD, typically there's probably 4,000 of these 2048 bit keys that are all unique. What's true is also if someone else has the same movie and they'd encrypted it themselves, that would be a complete different set of keys that's used.

So again, we think that the protection is pretty strong. The algorithm, I know that came up in Washington. That gets used and it's a stream cipher, which is similar to CSS and AACS. And again, each time the data is moved, new keys are generated limiting the lifetime of each key.

Another question that came up in Washington was transitory duration, which is sort of how long -- the transfer process -- for example, we're taking data from the DVD to stow it on a hard drive.

How long does that data and its copy of, so the megabyte is stored in volatile memory. And then it's destroyed on the DVD, and then it still runs in the hard drive and volatile memory is destroyed.

And the one question that came up is how long is it actually in the volatile memory. And again, it's less than a second.

MS. SMITH: Does that assume you have a

fast network? Does it depend on the speed of your network?

MR. GEORGE: It would depend on the speed of your network. So what's true is you sort of look at the speed of average networks in the U.S. or going even across the U.S., actually even past that, latencies are about 50 milliseconds. And the average transfer speed is about 50 megabits a second.

So a megabyte of data is typically transmitted in about 250 milliseconds. But it could turn out that your network is a little slower, it could take a little longer. But the point is it's well under this duration.

Something else that's true is if your network is slow you could -- we could just limit the process and say the network's too slow at the moment, when the network speeds up we'll allow that to take place.

MS. SMITH: Does both the decryption and the re-encryption, does that also occur in volatile memory?

MR. GEORGE: Yes, everything occurs in volatile memory. So yes, when it all, when it adds up, all adds up, it's well under half a second, well under a second.

And I think those are the questions that were mentioned in Washington. But if there's any other questions I'd be happy to take them.

MS. SMITH: I don't think so. Thank you.

MS. CHAUVET: Thank you very much.

MR. GEORGE: Great, thank you.

MS. CHAUVET: All right, next on the list we have Cory, and I apologize I'm going to not pronounce your name correctly.

MR. DOCTOROW: Doctorow.

MS. CHAUVET: Doctorow. So for each panelist who comes up, if you could please sit down, just introduce yourselves, your affiliation, and then which classes you wish to refer to in your testimony.

MR. DOCTOROW: Refresh my mind on the numbers of the classes.

MS. CHAUVET: You said Class 1 and Class 7.

MR. DOCTOROW: Seven, thank you. Hi, I'm Cory Doctorow. Thank you so much for entertaining my comments. I'm going to speak in a personal capacity.

I am a consultant to the Electronic Frontier Foundation, but really I'm speaking in my

capacity as a dystopian science fiction writer.

After a few days of listening to the hearings, I wanted to weigh in specifically in that capacity. I'm a bestselling novelist. I write for Macmillan's Tor, the largest science fiction publisher in the world. I'm published by Random House and Harper Collins in the UK.

And I'm deeply embedded in the entertainment industry. And I have a real interest in copyright being held in some regard by my customers.

I feel like we have now entered an era in which getting people to pay for works is an act of moral suasion. That as we've seen, virtually everything that people want to take for free they can, despite our tender ministrations.

I mean, I think it's pretty telling that we just watched a presentation about an anti-piracy technology that was played back on VLC, which violates DC -- CSS, and which is distributed from Hungary because it's the last territory that will tolerate their servers.

I mean, here it is having been trafficked into UCLA Law School by some technician in violation of section 1201, potentially criminal violation if they got paid for it.

And I think that in both of the areas that I'm commenting on today we heard a lot of talk about the idea that bypassing a TPM, even with no nexus with copyright infringement, should be viewed with great skepticism if it frustrated a business model.

And this is where my background as a dystopian science fiction writer comes in because it really is the stuff of a Black Mirror episode, where designing a technology such that bypassing a TPM is necessary to use it to benefit you, instead of its manufacturer shareholders, gives you the power to invoke the state's might to prevent your customers from thwarting your commercial desires.

And I feel like it does bring this framework that's supposed to regulate my relationship with my supply chain. As a working creator who depends on copyright to extract my living, it brings it into disrepute. It makes people think that copyright is a nonsense.

And I wanted to intervene in this normative way, and ask you as you deliberate on this, to consider that as you narrow the exceptions that have been asked for in the service of defending a business model, rather than in the service of preventing infringement, that you create the

situation in which people think that copyright is not something that they can or should bother to understand or give any real, serious consideration to.

And that if you were to be as liberal as possible in allowing people the traditional enjoyment of their own property, regardless of the impact on shareholders of the firms that manufactured that property before they exhausted their interest in it by selling it to a member of the public, that you would go far to bringing copyright back into repute in the digital age and to helping creators like me. So that's really all I had to say.

MS. SMITH: Thank you. We appreciate it.

MR. DOCTOROW: Thank you.

MS. SMITH: Appreciate your comments.

MS. CHAUVET: All right, our next panelist for the audience participation is Cynthia Replogle. I'm sorry if I mispronounced your name.

MS. REPLOGLE: No, it's Replogle. Hi, I'm Cynthia Replogle. I'm the intellectual property attorney for iFixit, and I deal mainly with trademarks and patents so I'm not a copyright expert at all.

MS. SMITH: Are you here to talk about Class 7 or a specific class?

MS. CHAUVET: Class 7 was repair.

MS. REPLOGLE: Yes, I guess that's the class it most applies to. I just wanted to take a higher level view and remind everyone of the purpose of copyright law.

In the Constitution it says, to promote the progress of science and useful arts by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries.

And on copyright.gov, it says, copyright protects original works of authorship, including literary, dramatic, musical and artistic work such as poetry, novels, movies, songs, computer software and architecture.

As I watched these hearings over the last few days, it's become clear to me that companies are misusing and abusing copyright by improperly asserting it as a cover for protecting other interests, often to the detriment of society, by conscious design decisions that impinge people's rights in their own property.

So I'd like to ask you to please keep in mind the purpose of copyright in considering

these exemptions.

I also volunteer for Surfrider, which is an environmental group dedicated to the protection and enjoyment of our oceans, waves and beaches. And I'm heavily involved with plastic pollution issues.

I've seen that society is divorced from experiencing and seeing the consequences of our disposable products. Plastics are derived from fossil fuels with all that entails, and many items like your plastic water bottles are used only once.

And you may put them in the blue bin, but the truth is that less than 10 percent of plastics are actually recycled, and the rest of them end up in our environment.

We have to realize that there is no away when we throw something away. We only have one planet, and it's important to consider what we do with our waste, and whether we create it in the first place.

Many electronics, consumer electronics, are similar in some ways. On the front end, the devices contain rare earth metals which are a limited resource. As well as sourcing them new by mining can be harmful to the environment and human health.

They're designed often to be used for just a few years and then discarded for the next new thing. They may have a battery that wears out and it's not easy to replace, or the screen is cracked or there's some other malfunction.

And even if someone wants to repair, copyright law is used to impede repair. And this results in mountains of e-waste. Repair.org says, Americans alone generate about 3.4 million tons of end-of-life electronics per year.

If you put every blue whale alive today, and there's 10,000 to 25,000 of them, on one side of a scale and one year of U.S. end-of-life electronic products on the other, the end-of-life electronic products would be heavier.

Those products contain toxins and heavy metals, things like arsenic, lead, cadmium, mercury, and dioxins, as well as explosive elements. And unsafe processing, such as burning, in developing countries, exposes people to health hazards, as well as polluting the water, air, and soil.

In the environmental community, we often talk about the four Rs, Reduce, Reuse, Repair, and Recycle. Many so-called end-of-life devices could be repaired, reused, or recycled but for

companies' misuse of copyright law.

So I would ask that you please consider the environmental and human health impacts of your decisions, as well as the purpose of copyright, and act for the greater societal good. Thank you.

MS. CHAUVET: Thank you very much. Our next speaker is Sina Khanifar.

MR. KHANIFAR: So I'd like to start off by thanking you for coming and listening to the comments. I wish I'd been here for all three days. Unfortunately, I was only able to join today.

So I have kind of a long story with the DMCA and unlocking that goes back far into my life to when I was a college student.

MS. SMITH: And are you here in connection with any other interest group?

MR. KHANIFAR: I am a tech fellow at EFF, but I actually haven't done anything really related to DMCA work at EFF. It's kind of mostly unrelated.

MS. SMITH: Thank you.

MR. KHANIFAR: Yes. So when I was in college and I was, at that point I was a green card holder, so I had moved to the U.S. and moved back to the UK. And I took a phone with me from the U.S. to the UK that I unlocked.

And it was a bit of an arduous process.

At that point, this was the time of flip phones, right. The Razer was just coming out. And I took, and it wasn't a Razer that I initially took. It was a phone that used to belong to my mom.

Cell phones were pretty early days then. And I, it took me a really long time when I got there to be able to actually use the phone in the UK.

And it was, I remember it was, very clearly, it was the summer of my first year in college that I had a couple of weeks extra, and I spent the whole time basically tinkering with this phone trying to get it to work.

And I've always been kind of an electronic software person, so there's a good amount of tinkering involved. And eventually I got there and I unlocked the phone and realized hey, if this is so painful for me, there are probably other people who are in a similar situation and want to unlock their phones.

So I actually ended up, by the end of the, kind of, process I'd hired multiple programmers who were helping me. We wrote a piece of software to kind of commercialize this and to enable people to unlock Motorola phones.

And it went well. I kind of got a little bit lucky. It was right before the Razer came out,

and the Razer was probably the most popular phone ever at the time that it was released.

And the software did quite well until at one point I got a, well I mean, this is how the news was broken to me. Someone, my mom called, and she received a cease and desist letter from Motorola very specifically highlighting DMCA section 1201, fines of up to, I can't remember, $250,000 per incident.

And I'd unlocked a lot of phones so that's a lot of incidents, right. And, yes, my mom called me. She was very, very worried as you can imagine, right, about what I'd been up to in college.

So, and I as a student, particularly as someone who was a green card holder, not quite in the bucket of being a citizen yet, was -- I was really worried about it. I mean, I shut down the service immediately, and was like, shoot, I guess I'm stuck, right.

And so there was a pretty big chilling effect on my business. And it took me over the course of a few months, I ended up being connected to, via various law clinics, to Jennifer Granick, who then had, I believe, published an article on it and then pushed for the original unlocking exemption to be added.

And that exemption, I believe, was in place for six years, right. So through two, kind of, three year processes, and then was removed.

And at that point I just happened to have finished -- I carried on doing entrepreneurial work, and I just happened to have left my last company, that last exemption was removed. And so I hopped on whitehouse.gov and created a petition asking the powers that be to make unlocking legal again.

Not so much because I personally do that much unlocking at this point. I've completely moved on from that industry. But because I do fundamentally believe in this right of users, once they purchase equipment, to be able to do what they want with it, right. And particularly, if they bought a cell phone, to be able to use it on another network.

So we put, kind of, it was a bit of a long battle. I went to Congress a bunch of times. And, obviously, the Unlocking Act as well as the FCC's kind of new rules around unlocking were put into place.

Now I know this year, I think for unlocking, no one's really challenged it in any meaningful, there's no real opposition, which is

great. I wish Congress had made it a permanent exemption.

But there are kind of related issues that I think are worth talking about. So one of the things that's started happening recently is that instead of controlling devices by locking them and preventing access to the wireless network itself, the carriers are instead preventing users from using, kind of, over the top services.

And some, ironically, those services are the very traditional thing that you buy a cell phone for, voice service. So voice service today is moving away from being, it's definitely not analog and it hasn't been for quite some time. But it used to be a specialized network, so CDMA2000 for some devices, et cetera. It's moving to all being voice over LTE, which is really just a variant of voice over IP.

And today, if you buy a phone that -- iPhones happen to be okay because Apple kind of pushes the carriers on this. But if you buy an Android phone on, let's say, a Verizon or T-Mobile or anywhere, and you try and take it to AT&T, you can unlock your phone, right.

Verizon sells its phones unlocked because of FCC rules. T-Mobile doesn't, but you can

unlock them, get them, to get them across for the most part.

But you can't get HD voice. And at this point, the carriers are almost entirely moving towards HD voice. No one's deploying older, typical voice services anymore, right. And you can't use HD voice on AT&T.

Similarly, you can't even buy an unlocked phone, a phone that was unlocked originally and move it across to AT&T and use that service either. But it's one of the ways that they're kind of, the carriers are choosing to maintain control over the device ecosystem that's allowed on their services.

So that's one thing that I wanted to highlight as kind of an issue, and I think a real reason for not just renewing the unlocking exemption, but also perhaps broadening it to take these facts into consideration. Because the only way to really get around this problem, and this is what a majority of users do, is jailbreaking your phone and basically changing the firmware to make it seem to the carriers as if this is an approved device that has HD voice capabilities, right.

So I think it's a reason why jailbreaking and unlocking are now becoming a lot

closer in the way that they work. And the other part, I'm still in telecom so I'm cofounder of a company called OpenSignal and, as well as Staircase 3.

And telecoms are really moving to internet of things, right. I mean, we've heard a lot today about cars and repair.

I mean, this unlocking of your, the modem in your vehicle, right, if you've purchased the vehicle and, let's say, T-Mobile and Sprint are merging. And T-Mobile's shutting down its 2G network at the moment. You may well want to unlock your vehicle at some point in the future to change the modem and connect to a different network.

And as those telematic systems are becoming more and more integrated that may well mean unlocking the actual operating system of the vehicle in order to be able to do that, right.

But it's not just vehicles, I mean, internet of things is going to spread more and more, so. And we're seeing it also in the telecoms industry in the devices that you use to connect to the network.

So it used to be the case that everything came from the cell tower outside. Today a lot of connectivity happens indoors via femtocells,

software defined radios that basically generate a carrier's cell signal inside your home.

There hasn't been, I wish I'd had the, had thought about it to push for this particular class of exemption, but customers buy these femtocells. If you're an enterprise, you're often paying $5,000 or more to buy these devices. And they use the, your internet connection to generate, on licensed frequencies, a network that your users can then connect to, right.

But in a very similar way to, it's a, two ends of your cell phone, right. Your cell phone is communicating with the tower, the tower's communicating back. Those devices are now also locked, right, and only will broadcast on the carrier that you purchased them from.

And I mean, I guess it's going to go the next triennial and we'll see if maybe I have the energy, or someone has the energy to push for the ability to reverse engineer and change those devices.

But I think that's, it's in this larger class of things that people don't do because the, there is, in my view of these, a pretty strong chilling effect from 1201 in terms of trying to reverse engineer these devices.

And I think it's going to become, particularly with 5G -- 5G doesn't make it inside buildings, right, it's high frequencies. And they're about to do an auction on this, but 25 gigahertz, 35 gigahertz, those frequencies don't make it inside buildings.

So you're -- it's not just going to be your cell phones. You're almost always going to have to have a device inside the building similar to a WiFi router that provides service.

So I mean, I think this is a trend that -- that's only going to kind of continue. And the range of devices that the proponents and the nonprofit organizations and the companies come and petition for is only going to grow.

And to me, that's just the, generally a bit of a worrying trend, right, that, you know, each time they have to make a de novo case for these different exemptions, I know from the folks at EFF who work on this that, I mean, it's a huge burden of energy that could be going towards other equally, if not more, important work, right.

And I think it's a shame that -- when -- when I was pushing Congress to pass the Unlocking Act, this is something I pushed them on pretty hard on, right. And I think, you know, the original

intent of the DMCA and 1201 was to prevent piracy.

I actually think it hasn't had a huge impact in reducing piracy. I'd be really interested in meaningful studies that would look at that and how much of, and how much of piracy was stopped due to preventing DCSS and that kind of thing, and how much of it was actually due to the copyright notices that Cox and whoever else, and Time Warner and Spectrum and whoever else were sending to their users, right.

So generally, I was reading through the report that you guys sent back in June of 2017. And I feel like one of the things that wasn't really questioned in, you know, in that document was what is the real utility today that having these protections really enables?

And the particular part that worried me, and this was true of unlocking, and I brought it up with the folks at Goodlatte's office and everyone else's office who I chatted with, was that the tools and services are just absolutely critical, right.

No one is able to unlock their own cell phone, right. Like so I did it in college, the technology was way simpler then than it is now, right. But it's literally out of access for 99 percent of people.

And I grabbed a little screenshot here. You know, there was this argument made in the, in that document that perhaps the primary value of anti-trafficking provisions has been to prevent the development of mainstream business models based around the production and sale of circumvention tools. Permitting the distribution of such tools could significantly erode that important benefit.

And I think there's two problems with that argument. One of them is that it's just like your standard slippery slope argument, right.

If we enable tools and services for these very specific classes of devices, no DRM is ever going to work again, right. Or even that DRM isn't going to have its intended purpose, which I don't think is the case, as we talked about the car repair, pieces of it.

You know the copyright impacts of allowing people to repair their cars are really minimal. No one's going to take a Toyota's firmware and copy it onto a Honda's, a Honda, right. It's just not a real world issue.

And so, to me, I think those, that argument around allowing for those tools is just really, really strong, and I didn't see that really reflected in that document.

MS. SMITH: So we do -- I just, here we're focused on the rulemaking. And in that policy study and in that instance we were looking at legislative proposals, including we recommended Congress may consider one for this, services and third party assistance.

So while we do appreciate everything you're saying, if there's ways you can --

MR. KHANIFAR: Taylor it to the exemptions?

MS. SMITH: -- focus on what we're -- right, we're just interested in, under the current sandbox that we've been instructed, and taken up this rulemaking in, what we can do and how we should look at it.

MR. KHANIFAR: Sure. Yeah, so I think on that front, unlocking is probably the one that I'm most qualified to talk about. And I think those examples of unlocking becoming a bigger issue both for handsets and for the equipment being used to generate that signal, is really, really important.

I would express support for some of the other exemptions that have been mentioned. I don't think there's any that I can specifically talk about. Perfect, thank you.

MS. CHAUVET: Okay, thank you very

much.

MS. SALTMAN: Great, thank you. All right, next we have Kyle Wiens, who will be talking about Class 4.

MR. WIENS: Hello.

MS. SMITH: Hello.

MR. WIENS: Yesterday, it was discussed that potentially there was no one in the room that would be able to build the HDMI device that we were discussing. And I just wanted to say that I probably could.

MS. SMITH: Thank you.

MR. WIENS: That's all I got.

MS. SMITH: We'll take your word for it.

MS. CHAUVET: Short and sweet. All right, lastly, we have Jay Freeman.

MR. FREEMAN: Hello. So I'll be speaking on Class 4, then I'll make a comment on Class 8, I believe is the number, video game preservation. And then I will make a comment which is related to both and is also kind of related to everything in interpretation.

So first of all, for Class 4, which was HDCP/HDMI, so one of -- I always end up coming up here and saying that, another hat that I wear. And so another hat that I end up wearing is this, in

the county of Santa Barbara, I end up doing a lot of video recording of a lot of different public meetings.

And one of the things that I think we've always considered very important is that public meetings are very well documented. I mean, these meetings here are extremely well documented, which is something that I actually, I love so much about the Copyright Office.

MS. SMITH: Great, thank you.

MR. FREEMAN: And it is, and the process of recording a public meeting oftentimes involves trying to record all the different types of things that people end up bringing. And you have very little control over what people end up bringing.

And they end up bringing laptops that end up requiring things like HDCP strippers, which is something that, you know, when I entered, tried to, recorded that, I'm not supposed to do that, right. I'm actually up here saying that because I'm pretty certain that there's no one who's actually going to try to catch me on it.

But the problem is that I don't -- I don't have good access to that tooling and I'm actually, it technically is illegal for me to do that.

And so I'm in this awkward position whereby in order to adequately record the public meeting, sometimes which I'm a part of, because I know the exemption on government entities is only for security purposes, information security. It is not for general government.

Even, when the meetings I'm a part of, or the meetings I'm not a part of, I'm in this awkward problem where in order to actually keep an accurate recording of the meeting, is effectively impossible to do it under -- under the law, unless I request people have special hardware that they don't have.

MS. CHAUVET: I guess I'm --- I'm still puzzled why you need to, stripper, like to strip it for that purpose.

MR. FREEMAN: Yes. So actually, just last night, we had a meeting at the Isla Vista Community Services District. And the problem that we run into is that Mac laptops, which many people have, just default to having HDCP. And they output the monitor output through, using HDCP.

Part of this is because -- and it depends on the laptop you have. But the, it, but again, it's essentially it's like somebody is going to come with their, with the laptop that they own and all the presentation materials that they have and the

meeting needs to be recorded. And so the --

MS. SMITH: Well I mean, we're undergoing modernization of course at the Copyright Office.

MR. FREEMAN: Yes.

MS. SMITH: But in the meantime we've just asked people to bring a USB drive. I mean, can you do that?

MR. FREEMAN: So it depends on the kind of presentation. Sometimes the presentation requires specialized software that they have. So it's not, for example, a PDF file. It's not a PowerPoint presentation.

But it is, in fact, some kind of demonstration that they're performing. It is a format that uses a piece of software that runs on their computer but doesn't run on the computers that are available.

In some cases it is the, essentially, the audio visual setup of the room makes it very convenient for them to not have to constantly be switching back and forth between different systems.

And where it's like, so they can bring their single presentation machine, and then they can be doing everything from their presentation machine rather than having it, for example, during, parts of the presentation being run off of a USB

device from a console computer, which is sometimes embedded inside the lectern.

It's something that I've just, I've run into so many times. And it's actually something where, I mean, there are conferences that I work with. And the conferences have just gotten to the point to where they've just bought an entire box of HDCP strippers.

And -- and they sit there and they just make certain that every single room has one set up such that they can record whatever device is brought for that conference's purpose.

It is, I find it to be such a drastic and common need that I, and weirdly such an easily doable one because HDCP strippers are commonly available on the market despite 1201 because they're just produced in other countries and you can buy them online.

But the problem is is that importing that and utilizing it is still technically illegal. And it is an adverse effect on the ability for not only like these conferences to be able to organize their event and record it for the people's educational usage, it's an adverse effect on academia in order to be able to record the work that's being done by professors in order to show

to other people.

And it's an adverse effect on government agencies who are, actually have a mandate in order to be publicly accessible and to have the information that's presented available later. So that's my commentary on number 4.

MS. CHAUVET: Okay, Class 8 then?

MR. FREEMAN: Okay. Class 8, which was video game preservation. So a hat that I used to wear that I don't wear anymore, I spent four years working as a game developer on a massively multiplayer online game.

So now, this class is specified to be three, it's listed with three, actually it's supposed to read separate first.

It's listed with three separate types of games, one of which is massively multiplayer online games, one of which is video games with a multiplayer component, and then the third one is -- I'm sorry, video games with online multiplayer features.

And then the third one is just multiplayer online games.

Now so, during the discussion on this a couple days ago, there's a lot of discussion about just how incredibly complicated it is in order to

perform these types of modifications.

And I actually started to become, as somebody who wants this exemption to happen, I have actually started becoming a little bit concerned because it starts to make it feel like that, well even if you had this exemption, are you actually going to succeed in doing this very often?

And there were some comments from the opponents stating that, well in order to actually pull this off, the servers are sufficiently complicated that you would have to re-implement the entire world and, which would involve, which involve actually distributing or copying a lot of copyrighted material.

And I would like to point out that while that is true for some games, and that is true oftentimes when in relation to massive multiplayer online games, this class is covering multiplayer games, games with online multiplayer features.

The vast majority of games that are multiplayer actually have a very simple server. The very simple server's goal is to just deal with network address translation issues between all the clients.

If I try to have my computer talk directly to your computer, I'm on a cable modem at

home, you're on a cable modem, we can't talk directly.

But instead, there will be some simple server that was written by the developers that just coordinates access. It provides an online matchmaking service that allows you to find other players. It then provides forwarding service for those packets.

These are, as specified in, by the -- by the proponents, very particular to the individual games. It is very seldom that you'll find one that works on multiple games.

But it is something that, if you are able to reverse engineer the tooling of the game and then figure out how these online server components work, you can re-implement it without re-implementing, without, with essentially, you've cleanroomed it.

You aren't re-implementing any of the copyrighted material of the game. You aren't redistributing any of the art assets of the game. But you now are able to make these multiplayer online games, video games with non-linkable player features, and some massively multiplayer online games begin, work again for the purposes of video game archival.

MS. CHAUVET: Is circumvention required?

MR. FREEMAN: So circumvention is sometimes required for that. And the reason why is that the games themselves are oftentimes, the code for them has been obfuscated.

And the obfuscation, which is a form of technological protection measure, and is actually, it is the basis, obfuscation is the basis of many technological prevention measures across all these classes, including for example, the FairPlay encryption used on the iPhone to encrypt applications and to encrypt audio works.

That FairPlay, that, so the, that encryption mechanism, for example, that is protecting that application that, makes it so that I actually have to bypass that TPM.

I have to, I have to build some, I have to like sit around and reverse-engineer, actually. I almost said build tool, but that's actually the same confusion that was brought up by the developer last time is that you're building something for that one-off purpose in order to remove that obfuscation from that one thing, and then you usually just crumple it up, throw it away once you're done with it.

But I have to sit around and do a lot of work in order to understand what that application was doing, when it was talking to the server, to find out what information the server would have to return back in order to make it work.

And that's something that is eminently doable, but it is something that does require developers to actually sit down, break a TPM for that individual application and then do the work of doing that writing. And that is something that is currently illegal without an exemption under the 1201.

MR. RILEY: So there is an existing exemption. And this was a question --

MR. FREEMAN: Correct.

MR. RILEY: -- that we asked about yesterday, whether you can do that on, under the existing exemptions on PCs or to use a console as a type of listen server. And do you think that there's some of that that preservationists can do already?

MR. FREEMAN: So this is just, I, maybe I'm misunderstanding what the thing that is -- so my understanding exactly that we're intending to expand the exemption to include a different class of games. And so since the class of games would not

have been covered before, I'm not certain how --

MR. RILEY: Well, the preservationists can play, can engage in circumvention to play multiplayer games as long as it's done locally.

MR. FREEMAN: Correct. Yes, so that's different. So the idea is, so there are local multiplayer games. And local multiplayer games are typically, like you'll have a PlayStation with four controllers. And then people can sit down at that game and then, and work with it.

The difference here is, is that this is a, these are games that have an online -- online component. And so these are games that had previously been built in order to have an online matchmaking service that then allows you to do the across the internet communication.

And that's why they got expanded to further include multiplayer online games. It's possible, of course, I mean, I was just an audience member. It's possible that I misunderstood the class expansion, but.

MR. RILEY: So I guess the question was, you know, other proponents said that, they directed their comments toward local area networks in terms of the games that already have that option available.

And so the question is can you use the, as an example, the fact that preservationists can jailbreak consoles, and this is one of the rare circumstances that we allow this to happen, can you add that functionality by doing so and not have to have an additional exemption for some of these multiplayer games?

MR. FREEMAN: So if you're, local area network games, so that was another, that was another like era of multiplayer gaming whereby you, essentially, broadcast on the local area network information about who else is on that network. And then you'd be able to establish the multiplayer setup.

It's very different from the online matchmaking services that you end up seeing which I --

MR. RILEY: I completely understand that, but what we're asking about is can you recreate some of those online games but not on a connected network that goes outside of the building, but in a different sort of network that you create on your own to play those games, those online games -- I'm using online in quotes -- in a, not on a pre-setup local area network. But can you set up some sort of other network using the current exemption?

MR. FREEMAN: Because it is the class of work that is being expanded, I would have thought no, because it's, I mean -- so for this class of work, which is for the massively multiplayer online game, you could, like when you end up constructing an alternative server for it, you can run that server anywhere, including locally inside of a room, and you can make it so that no one outside of the room connects to it. You could call that a LAN.

But the, I guess the question that I have back to you, is do you consider that all of these categories that are currently listed here as the class expansion were covered by the previous exemption?

MR. RILEY: So I think that's a different question.

MR. FREEMAN: I think it's a different question as well, which is why I feel like the argument that is being made here is that in order to, is that we're attempting to expand the class.

And so we're attempting to expand what kinds of works we're allowed to do the circumvention on to include games that were not designed for LAN multiplayer, but were designed for online multiplayer, and designed for even massively multiplayer.

MR. RILEY: Yeah, and my question --

MR. FREEMAN: Okay.

MR. RILEY: -- is can you do any of that already under the current exemption?

MR. FREEMAN: No, because the exemption is tied to a class which is not massively multiplayer but is instead the more limited multiplayer.

MS. SMITH: So right now you can circumvent and you can jailbreak the console if you're one of these institutions. And then you can set up a LAN that, you know enables the matchmaking. And I'm not going pretend to know as much about some of the different types of games as some of the panelists, and perhaps yourself. But it needs to be a complete game.

A complete game means a video game that can be played by users without accessing or reproducing copyrightable content stored or previously stored on an external computer server. And so we're being asked to expand the definition of complete games.

But I think when you started discussing that there's some games where you don't need to reproduce copyrightable material on the external server, you just need to facilitate the matchmaking functions.

I think what Mr. Riley is asking is whether you could do that on a LAN that you create and it's part of this preservation activity.

MR. RILEY: Yes.

MR. FREEMAN: So two things. The description you just read I believe is actually subtly different in the sense that that was that, so there, the case of a matchmaking service, the matchmaking server code is copyrighted. You are reliant upon the copyrighted work that is running on that server.

The question is if you were to write a new one, is it a derivative work. And I believe that the answer has usually been no, unless you have, if you have never been able to see the original.

MS. SMITH: Well, if there's a video game that can be played, and I guess if you're doing your own matchmaking on this LAN, you can still play the game and be this, that becomes on the hood of the pin, whether you can still play the game if you've matchmade it in a different way you've set up on this LAN.

But I think that's what he's getting at, whether some of these games you're talking about can fall under the current definition of complete game.

MR. FREEMAN: And the definition of complete game you described?

MS. SMITH: Yes, I can read it again. It's video games that can be played by users, so it's focused, I think, on the playability.

MR. FREEMAN: Correct.

MS. SMITH: Without accessing or reproducing copyrightable content stored or previously stored on an external computer server.

MR. FREEMAN: And the class expansion, and the expansion that we're looking to do is for games where that, where it is required to reproduce copy -- okay.

Yeah, I just, I probably just misunderstand a lot of the context of the class expansions as an audience member. So the, I mean, the cases where I'm describing do require, essentially, reproducing something, but not copying something. Like, it's not really, I mean, it's not legal reproduction, it is instead a refaximile, like a --

MS SMITH: Kind of like reverse engineering?

MR. FREEMAN: Essentially, yes, so.

MR. RILEY: Can I ask what MMO you worked on?

MR. FREEMAN: It was, you wouldn't have heard of it. It was called Eschaton Chain of Command. It was something that was very similar to EVE Online that came out later. But we did not finish it. Turns out that no one at our company knew how to make anything that was fun. We only knew how to make things that were like fast.

So all right, so the final comment that I wanted to make is that, so the, when you look at what the goal of this process is, the goal of this process as defined in the law, was to find people who had non-infringing uses that were adversely affected. And then to figure how to continue, allow them to continue doing that.

The actual, like the statements in the law multiple times state that the goal of the, like the goal of the rulemaking process is to find and list the non-infringing uses that have been adversely impacted by the scope of this law.

It then lists criteria by which the Copyright Office is supposed to use to determine what an adverse impact is. But it is for what it, determining what an adverse impact is.

It's not, it does not seem to be like about whether or not the rule should happen, but about determining the criteria by which we can

measure adverse impact.

The, there is a criteria which is the marketability and value of the copyrighted work, which is listed at the very end of that list.

And I find that the, when I sit here and listen to these arguments, I sit here and argue against people, in person even with them, right, that the argument oftentimes ends up hinging on some idea that by providing an exemption for this class that that will decimate the market that is for that -- for that area.

And they're some places where the Copyright Office has explicitly looked into it and explicitly found things that they were very concerned by.

An example of that might be video game consoles, which tend to be a relatively specialized piece of hardware where a video game is designed specifically for that piece of hardware.

But we see that same argument somehow being utilized for things like online streaming media, for things like Spotify and things like Pandora. For things like Netflix and things like Amazon Prime.

And yet these are situations where the media is in a very general format that is playable

anywhere. These are cases where the software that is available to play it is available on every platform, both weak platforms and strong platforms.

We see this argument being applied to devices such as smart speakers all the way through to devices such as iPhones. And in some of these cases the argument is just, I will just say, almost absurd on the face of it, because on that very device you don't actually need to have done the circumvention.

So as an example of this, there was an argument that was made in the written comments about, from the App Association about -- oh wait, no. It might have been -- I'm sorry, it was either the App Association or it was the ESA that was about a game from one of their members which had been, which they found on the Google Play store.

They found another copy of that game that had the same art and the same name. But in order to reproduce a game that has the same art, that has the same name, you do not need to have a jailbroken device.

You do not need to have circumvented anything. You simply need to have screenshotted the art assets and then published a game that looks the same that has the same, that has the same name.

Very similarly, if you would like to publish, if you would like to have on a smart speaker, you would want to have audio being able to play through it that's pirated, well you can copy that audio off of any device, and then play it through your smart speaker.

If you would like to be able to watch a pirated movie, well if anyone in the world had managed to obtain a DMCA stripper just once, then you can stream that, you can, sorry, you can download a copy of that movie and play it on any of these devices without the user doing any circumvention.

Now the question is, is whether the person who is doing the copying specifically, but we know that that person was doing something illegal.

That person, and so the problem I run into is that the act of allowing, for example, a user to circumvent their device in order to disable the touchpad that is glitchy, the, to allow a user to circumvent a device in order to do security research that is not solely for the purpose of good faith research, to allow a user to circumvent a device in order to determine if there is, in order to get the timecode information from a DVD or to be able to get, or do screen readers, or any of these

use cases, this, stopping those people from doing that doesn't actually effect that market of pirated work.

And I feel like it, the Copyright Office for video game consoles I, I'll even admit as somebody who, I really hate admitting, I really hate admitting it. But I'll even admit that you make some arguments that move me at times.

But I just have never felt the argument for Spotify, Pandora, Netflix, Amazon Prime, any of these movie or music services because the content is so generally available.

I have not felt that argument for applications that can be used on general purpose computers with operating systems like Android that are available on all sorts of different hardware platforms.

MS. SMITH: I mean, I'm sorry, are you saying because there's a lot of pirated music that we should just allow circumvention to Spotify? Is that what it's classed into?

MR. FREEMAN: So what I'm trying to say is that we're throwing out the baby with the bath water. By saying that technically I can, technically, I can circumvent Spotify, even though what we're actually trying to get is circumventions

for purposes of protecting people, circumventions for allowing disabled people to be able to utilize work, circumventions that allow people to do things that were creatively not possible before, that because -- but people will say, but technically that car is capable of running Spotify so you shouldn't be able to jailbreak anything on that car.

And it's like, okay, but you know I really didn't buy a car in order to steal music from Spotify. That just doesn't make any sense to me. I mean, I was able to do that on my computer.

The reason, none of us are sitting around trying to -- and the pirates aren't doing this on cars. There's no pirate who is sitting around in their garage in a car trying to steal music from Spotify. They're doing it on all these other devices.

And so the idea to me that these circumventions that are, that circumventions are being argued as, they should be disallowed because of theoretical potential use cases that are copyright-ridden that are already able to be done everywhere else is just very strange to me.

And I feel like that should be more strongly realized when looking at that criteria, that there is an adverse impact. That adverse

impact has been shown. The adverse impact sometimes nearly feels devastating.

And the question is then, does that circumvention in that case, does the ability for the, does the copyright owner coming and claiming that theoretically the car can do Spotify -- I feel like they should really be on the hook to show that people actually are going to sit around in their garage with their car using these techniques in order to be able to circumvent that music before the Copyright Office does not grant that exemption.

So that's the, kind of, cross cutting concern comment that I wanted to make.

MS. SMITH: All right, thank you.

MR. FREEMAN: Thank you so much.

MS. CHAUVET: All right, well that concludes, that's everyone.

MS. SMITH: We are done with the hearings for the 1201 rulemaking. Thanks everyone.

(Whereupon, the above-entitled matter went off the record at 2:53 p.m.)