UNITED STATES OF AMERICA

+ + + + +

LIBRARY OF CONGRESS

+ + + + +

COPYRIGHT OFFICE
SECTION 1201 ROUNDTABLE

+ + + + +

TUESDAY
APRIL 10, 2018

+ + + + +

The Section 1201 Roundtable met in the Mumford Room, James Madison Memorial Building, 101 Independence Avenue, SE, Washington, District of Columbia, at 9:00 a.m., Regan Smith, Deputy General Counsel of the U.S. Copyright Office, presiding.

PRESENT

REGAN SMITH, Deputy General Counsel of the U.S. Copyright Office
KEVIN AMER, U.S. Copyright Office
ANNA CHAUVET, U.S. Copyright Office
RAFI GOLDBERG, National Telecommunications and Information Administration
JULIE SALTMAN, U.S. Copyright Office
JASON SLOAN, U.S. Copyright Office

ALSO PRESENT

JONATHAN BAND, Owners' Rights Initiative
STEVE ENGLUND, Dominion Election Systems, Election Systems & Software, and Hart InterCivic ("Election System Providers")
JAY FREEMAN, SaurikIT
HARLEY GEIGER, Rapid7
J. ALEX HALDERMAN, University of Michigan Center for Computer Security and Society
JOSEPH LORENZO HALL, Center for Democracy & Technology
BRETT HILDEBRAND, Samuelson-Glushko Technology Law and Policy Clinic
ALEX KIMATA, Samuelson-Glushko Technology Law and Policy Clinic
MIKE KEALEY, Dorman Products, Inc.
AARON LOWE, Auto Care Association
CHRIS MOHR, Software & Information Industry Association
BLAKE REID, Samuelson-Glushko Technology Law and Policy Clinic
ANDREW SHORE, Association of Service and Computer Dealers International
DAVID J. TAYLOR, DVD CCA
CHRISTIAN TRONCOSO, BSA The Software Alliance
BRUCE TURNBULL, AACS LA
KIT WALSH, Electronic Frontier Foundation
J. MATTHEW WILLIAMS, Association of American Publishers, Entertainment Software Association, Motion Picture Association of America, Inc., and Recording Industry Association of America ("Joint Creators II")
JONATHAN ZUCK, ACT The App Association

CONTENTS

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

9:00 a.m.

MS. SMITH: Good morning, everyone. Thank you for coming.

My name is Regan Smith. I'm Deputy General Counsel at the Copyright Office, and I, along with my colleagues, will be presiding over this hearing, which is part of the section 1201 rulemaking.

First, let's introduce ourselves, starting from left to right.

MR. SLOAN: Jason Sloan in the Copyright Office.

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

MR. AMER: Kevin Amer, Senior Counsel in the Office of Policy and International Affairs.

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

MR. GOLDBERG: And I'm Rafi Goldberg from the National Telecommunications and Information Administration, which is a mouthful. So, we usually just call it the NTIA.

And we would just like to thank the Copyright Office for allowing us to participate in

these hearings once again. Thank you.

MS. SMITH: And we are again very grateful that NTIA is here and participating in this with us.

So, we are all excited to be here today and hear all of your evidence. I know some of you; I see some familiar faces, but also some new faces. So, I want to explain how the process will work.

As you probably realize, the goal of these hearings is to try to analyze and further develop in the record in relation to the proposed exemption to the anti-circumvention provisions in section 1201 of the Copyright Act. We are more interested in clarifying and developing the record rather than going over arguments which were already seen in the written comments. It's helpful if we can use this time to hone in on the issues, particularly disputed issues or areas where the record may be a little bit patchy.

And some rules of the road: make sure to speak into your microphones. Speak slowly because there is a court reporter and, also, this hearing is being live streamed.

I will be calling on people or others will be calling on people. So, if you would like

to speak or make a comment, just tip your placard up and we'll know that you want to speak. We'll try to call on people in turn as how they've raised their placard. But, either way, we'll make sure everyone gets a chance to speak.

I think no one has exhibits for this hearing, but for future panels, and looking at the audience, we will mark exhibits prior to that.

And in terms of audience members, we also have a sign-up sheet for audience participation which will be Thursday or Friday. So, if you're interested in speaking briefly on one of these subjects, you can fill out a request, so we can make sure to accommodate you in the time.

The microphones, we can only have four on at a time. And I believe if you have four, you might start to get some weird feedback. So, if you can, just try to press the button to turn off your microphone after you speak.

I think, unless there's any questions, we'll start by asking the panelists to identify themselves and any affiliation or interest that you have. And then, we'll start by asking some broader questions to try to get at the issues.

So, Mr. Kealey?

MR. KEALEY: Mike Kealey, Dorman Products. I am Executive Vice President of Commercial. So, I have responsibility for all of our product development initiatives for both new and re-manufactured aftermarket auto parts.

MR. BAND: Jonathan Band. I'm here on behalf of the Owners' Rights Initiative.

MR. SHORE: Andrew Shore. I'm here for Joe Marion, the Association of Service and Computer Dealers International. And in full and fair disclosure, I'm also Executive Director of the Owners' Rights Initiative, and ASCDI is a member. So, you'll need a program to keep it all straight.

MS. SMITH: Thank you. We appreciate that.

MR. LOWE: Aaron Lowe, Senior Vice President for Regulatory and Government Affairs for the Auto Care Association.

MR. WILLIAMS: Matt Williams. I'm with Mitchell Silberberg & Knupp. I'm representing AAP, ESA, MPAA, and RIAA.

MR. TURNBULL: I'm Bruce Turnbull with the Turnbull Law Firm, representing, as it says, AACS LA, but also this morning the DVD Copy Control Association. We filed joint comments.

MS. SMITH: Okay. Thank you.

So, I think everyone knows that the Register of Copyrights has already determined that she can recommend renewal of the existing exemption for repair. So, here today, we are here to discuss potential expansions or modification of that current exemption.

And I think we would like to take it in pieces based on general issues. And the first pieces we would like to discuss are third-party assistance and manufacture and provision of tools.

And so, I guess my first question, pretty broad, is the Copyright Office has said in its study that Congress should consider legislative clarification to allow for third-party assistance. Would anyone like to explain why the proposed expansion would be within the scope of the Office's authority as opposed to abutting against the anti-trafficking provisions, or not within the Office's authority?

Mr. Williams? Just tip your placard up next time, so we're sure that you're trying to speak.

MR. WILLIAMS: Sure. Sorry about that.

So, I would take the side that it would not be within the Office's authority at this time.

I understand there is a proposed legislative amendment, but in the context of this rulemaking, I think the Office has been correct to say that it should not and cannot issue exemptions that are likely to be interpreted to encourage trafficking.

I think the focus of the proponents' arguments on this issue was that the statute refers to users of works, as opposed to owners of works or copies. But there's a number of ways to explain that without saying that Congress intended to mean that a service provider could get an exemption.

For example, section 117, you've dealt with that issue about whether an owner or a user/licensee could get an exemption. There are also people who access streaming media content who are not necessarily owners of copies, but are users of a work. And so, there are other reasons why Congress would make that choice, aside from allowing services exemptions.

MS. SMITH: Mr. Band?

MR. BAND: So, I think you have to look at section 1201 as a whole. And as you say, you have the anti-trafficking provision, but at the same time we do have this rulemaking. And if you looked at the anti-trafficking provision literally, it says

you can't make for traffic, right? You can't make or distribute a circumvented technology.

Now, certainly, anyone who is granted an exemption is going to have to make a circumvention device, right? Or have to come up with the software or do something that allows it. And so, arguably, already the statute is a null set, right, that you have a rulemaking that allows an activity, but, then, the anti-trafficking provision prohibits the development of the technology that allows you to engage in that activity.

Now you've taken care of that problem by saying, well, no, it can't possibly mean that, taken literally. And so, you have interpreted the trafficking provision in such a way that it is not in conflict with this rulemaking. Okay? Otherwise the rulemaking would be an absurdity.

MS. SMITH: Well --

MR. BAND: Well, let me just finish that thought.

But, given that, it seems that you can easily interpret the authority under the rulemaking to allow not only the person, not only the owner of the work to engage in the circumvention in order to get access to the work, but to allow someone,

a third party, to help them. Just like courts have found that the fair use privilege can apply to someone, not only to the person who is the ultimate end-user, but someone who is providing a service to that end-user.

MS. SMITH: So, you've brought up a couple of issues, including making it personal, too, how the Office has looked at that, as well as third-party assistant. Would it be, is it your understanding that the Copyright Office could just allow an exemption for someone to distribute a technology product, service, device, or component, a list of things prohibited in 1201(a)(2) or (b) under 1201(a)(1)?

MR. BAND: Well, I think it's a matter of how far you're willing to stretch the statute.

MS. SMITH: We're not looking generally to stretch the statute.

MR. BAND: Right, right. No, no, no, but, look, let's be real. I mean, we're already or you've already sort of engaged in a creative interpretation to allow the people who get an exemption under 1201(a)(1) to make a circumvention technology, right? Because they can't just sort of -- it doesn't appear, it doesn't come down from

the sky.

MS. SMITH: Correct.

MR. BAND: I suppose we could say, yes, well, it does. I mean, usually, you can --

MS. SMITH: We said it was implicit in the statute.

MR. BAND: Right, exactly.

MS. SMITH: So, while we've endorsed creativity generally, that was not our goal, ergo, we should just read the statute plainly.

Did you have a question?

MR. AMER: Yes. Could I just follow up on that?

So, I mean, I think we said in construing the term "manufacture," we read it in light of the term "trafficking". And we said that the term "trafficking" as a matter of general definitional meaning, generally refers to commercial activity. And so, if you're talking about manufacturing a tool for self-help, we think that manufacturing wouldn't cover that if you were a beneficiary of an exemption.

I think that the challenge for us here is, if we're talking about providing a service, and if you're talking about a third-party service provider, for example, that is likely to be a

commercial entity. And so, the distinction that we drew in the context of manufacturing doesn't really help for purposes of allowing commercial third parties to provide assistance. So, I think that's kind of what we're talking about.

MR. BAND: Well, I guess I would respond that the term "manufacture," you could construe it to say, well, if a repair shop -- well, just like you're saying, a user, if he manufactures it for his own purposes, it's not a manufacturer, I think you could certainly also say that, if a repair shop develops the circumvention technology, but it's not selling it, meaning it just develops the technology for itself --

MS. SMITH: How is the repair shop making money if it's not selling its services?

MR. BAND: It's selling its services, but it's not selling the device.

MS. SMITH: Okay. Mr. Turnbull?

MR. TURNBULL: We've tried to find where a fine line might exist. And in our view, the term "user" can be interpreted to be an expert repair person. Where we draw the line, however, is we would object to and think the Office would not have the authority to grant an exemption for somebody

rendering assistance. So, if the product is physically brought to a repair facility, and the repair facility has the physical product in its possession, and is, then, using the physical product, that literally, in our view, would be acceptable under the statute. Whereas, if the repair person is rendering assistance in some other manner, then you probably are over the line.

And this is one where we're mindful that our interests with DVD and Blu-Ray players, you know, it may be a little different from some of the situations presented by farm equipment or autos, and that sort of thing. And while we have no position on those exemptions per se, in looking at the commentary, our view has been that you can read the word "user" in the way that the study report suggested that you might, particularly if you, then, take the further view that "manufacturer" can be read in the context of the trafficking word as well.

MS. SALTMAN: So, just to clarify, Mr. Turnbull, do you understand that a third-party repair person providing assistance, as you described, as a user, would they be able to provide both repair assistance and repair to add improvements to a device? Or do you think that a

user just has the ability to repair?

MR. TURNBULL: We are very concerned about the possibility of improvements. And in fact, in our comments -- and I am mindful of not repeating -- but in our comments we did make the point that modifications that would actually enable certain kinds of functions that have been the subject of previous requests for exemptions, you know, that certainly should not be allowed. Now where you could draw the line, I don't know, but we would for sure say that, for example, adding functionality that, for example, a DVD player or a Blu-Ray player would not allow access for certain purposes, and modification to allow access for those purposes should not be provided.

MS. SMITH: So, assuming something was non-infringing under a section 117 or 107 -- and we can later discuss whether modification is always or sometimes or never within those bounds -- AACS believes that, if a service shop or an independent repair shop provides services, would it be at the direction of a user, or what would the statutory advantage be?

MR. TURNBULL: Our line is that, if the repair person is, in fact, using the product, not

providing services in support of the owner of the product, but if they have physical possession of the product, then they are the user of the product.

MS. SMITH: So, if I take my car to a dealership and I say, "I want you to fix the lights on the fritz," or whatever, they are both using my product and providing a service to me. So, how would that work in practice?

MR. TURNBULL: At that point, if they're within the terms of the exemption --

MS. SMITH: That's what I'm asking you: would they be?

MR. TURNBULL: No. Well, but if what they're doing -- I mean, in other words, if you gave an exemption to the user of the product to repair the lights, just to take a --

MS. SMITH: Well, I think what we're talking about is whether or not -- currently, it says you can engage in repair, diagnosis, maintenance --

MR. TURNBULL: Right.

MS. SMITH: -- by the owner of a lawfully-acquired device. And if we said "by the user who has lawfully acquired a device," in this instance of an independent repair shop, do you

believe that's an exemption that the Office could do that would still remain within the statutory mandates of 1201(a) or do you think it would go beyond that because it would be condoning anti-trafficking?

MR. TURNBULL: I think, read literally, it's within your authority.

MS. SMITH: Okay. Mr. Shore?

MR. SHORE: Thank you.

Just quickly, I guess -- and I look at these cameras right in front of us, for instance -- I don't think that there's anybody in this room who, if they owned this camera, could repair it. Given the advances in modern technology and the complexity of the things that we own, third-party repair is totally necessary.

And so, if you didn't read the statute to allow third-party repair shops to engage in services for goods that the individual owns and brings to them, then why even have the rulemaking? And there are, to be fair, there are cars from the '60s still around that people can repair themselves, but even my 2010 has technology that I wouldn't even start. I lost the key, and I couldn't unlock my car because of the complexity of the technology.

MS. SMITH: So, the Copyright Office has acknowledged sort of these policy-driven issues --

MR. SHORE: Yes.

MS. SMITH: -- in our 1201 study. And I think, right now, I'm trying to just nail down our statutory basis, our regulatory authority, how far it might extend. Because we recognize that this may be something of use. So, I think that's what we're trying to focus on in this part.

So, maybe Mr. Williams and, then, Mr. Kealey?

MR. WILLIAMS: Thank you.

Although I almost always agree with Bruce, on this issue I don't think I can, if I'm understanding his position correctly. In that scenario that you were discussing with him, as I understand it, the repair shop would have somehow acquired the tool, not necessarily manufactured it. And then, they would, for money, offer the service of using the tool to circumvent and repair products. And while I'm not here to specifically address automobile-related issues, my understanding of that scenario is that it would always require circumvention in order to get to making the repair.

And in that instance, if you look at the

language of the anti-trafficking provisions, that would be providing a service for the purpose of engaging in circumvention. And I don't think that your statutory authority goes that far that you can grant exemptions under 1201(a) that, as you've said before, are very likely to result in people going out and engaging in trafficking.

I think you hit the nail on the head a second ago when you said you've done your work in the policy arena, you've provided the report to Congress. Something may or may not come out of that. But I don't think the fact that you reached one conclusion in that arena should change your regulatory authority in the proceeding.

MR. AMER: Well, so that's helpful. I mean, I think the argument that we've heard sometimes from the other side is that, if you're talking about something like a repair shop, is that a service that is primarily designed or produced for the purpose of circumventing? Now, as I understand your position, I think you would say, well, circumvention is never the ultimate goal of a service. And so, even if you are circumventing for the purpose of allowing piracy to take place, that service should be understood to be primarily

designed for the purpose of circumvention.

But what about that concern? I mean, even thinking about the concern Mr. Shore raised, just sort of the practical need in many cases for third-party assistance, doesn't the statute suggest that there are some types of services that should be understood as not primarily designed for circumvention, but that, nevertheless, sort of incidentally involve circumvention?

MR. WILLIAMS: Yes, I think to say otherwise, you would have to read that language out of the statute, which you can't do. On the other hand, as I was trying to say, my understanding is that, in the auto repair arena, and in many of the arenas that we would care about, pretty much every act involved in that service would result in an act of circumvention. And so, it's not that they're engaging in a service that occasionally happens to involve circumvention. It's that, by definition, it involves circumvention. So, in that scenario, and probably others, but at least in that one, I think it would violate the trafficking provisions.

And I also again think that the Office has been correct to say that it's not just let's read strictly the trafficking provisions, and,

then, if there's some argument that maybe something doesn't fit within them, you grant the exemption. I think it's the other side of the coin, which is that, if it looks like trafficking, you're supposed to stay clear of it and not encourage something that is possibly going to lead to trafficking.

MR. AMER: Yes, but, I mean, you're agreeing that there is some class of services that incidentally involve circumvention that wouldn't fall within the trafficking. So, I think what we're struggling with is trying to figure out how to draw that line.

It seems to me that -- I don't know -- one could argue that if you're circumventing for purposes of fixing a car and, then, you put back the TPM, for example, you know, you unlock the product, I mean, is that a way to distinguish services that are primarily designed for circumvention compared to those that only incidentally involve circumvention towards some other end?

MR. WILLIAMS: I think that would be the defining line for what's primarily designed for circumvention, although we did say that, if you ultimately decide to grant some kind of broader

repair exemption, that the 117(d) factors for defining repair would be more helpful than some less bounded definition of repair.

I think that, because the statute refers to primarily designed, you have to assume that, theoretically, there is such a service. I couldn't tell you one, sitting here today, and I don't think I've seen any in the record. I think you very accurately described our view, which is that circumvention is almost always going to be for the purpose of achieving some other goal. So, no one is really going to be in the business of circumventing just to show people they can circumvent. And so, if you define it in a way that says, well, really my goal is repair or my goal is some other activity, that that's not enough, in our view, to take you outside of the trafficking provisions.

MS. SMITH: I wonder if maybe Mr. Kealey could speak to that, because I see (a)(2) also says there's only a limited commercially-significant purpose. I'm wondering if you know, especially in the vehicular context, if the tools for circumvention are more connected towards diagnosing what's wrong with the car or repairing

something, or if circumvention is one act and, then, the acts of maybe more traditional auto repair or diagnostics are separated from that?

MR. KEALEY: There are a couple of things in there. So, I'll try to deal with each of them.

So, if I could just go back real quick, you had asked the question as to whether or not it was in the Copyright Office's jurisdiction to sort of extend the exemption. And one of the things that's concerning to us is the existing exemption as it references vehicle repair and extends the exemption to the motor vehicle owner.

And we would sort of agree with the report to the Register of Copyrights from June of 2017, page 4 in the Executive Summary. "In cases where beneficiaries cannot themselves make use of an exemption, the Office believes it is important to allow users to seek assistance in making use of that exemption."

So, with respect to automotive repair, modern vehicles today have somewhere between 50 and 70 complex computing devices on them. They perform all sorts of functions, from rolling your window up and down to the braking system on the vehicle.

And if one of those computing devices goes bad, the motor vehicle owner does not have the tools or aptitude to be able to fix the hardware failure in one of those devices, put that device back onto the vehicle, and then, put the software that was on that device back onto the repaired module. There's just no practical way for them to go about doing that.

So, without being able to extend that exemption to a third-party repair facility that can perform that repair on their behalf, the exemption is effectively useless. And so, for us, one of the things that we would like to see clarified in the exemption is that that right can be extended to a third-party repair provider or for the exemption to remain silent with respect to the motor vehicle owner.

MR. AMER: So, that's helpful. I think the challenge for us is to -- I mean, we're, obviously, not granting or recommending exemptions for purposes of the trafficking, where that's clearly outside our authority; everybody agrees with that. But I think, nevertheless, if we were to sort of recommend an exemption that might allow for some third-party assistance, we would need to have some theory about the trafficking provisions

and how they should be interpreted and some way to differentiate, you know, services that are provided by a third party that are not trafficking versus those that are.

And so, I think your points are well-taken from a policy standpoint, but I think, from our perspective, we're trying to understand what your theory would be or what you're suggesting that we do in terms of interpreting the trafficking provisions.

MR. KEALEY: With respect to automotive repair and diagnostics, I think the software that we're talking about is effectively useless outside of the device that controls the vehicle on said vehicle. I can't think of a situation where somebody would want to traffic in vehicular software, especially with respect to specific computing devices on the car.

If the exemption was limited to repair and remanufacture of specific devices and repair of the vehicle, I don't know if that doesn't sort of put a bow around the issue.

MS. SMITH: Okay. Thank you.

So, Mr. Band, I would like to let you chime in, but I also have a question for you about

Mr. Kealey's comments. He said, without third-party assistance, this exemption would be fairly useless, which I was surprised at because the last rulemaking, in Owners' Rights Initiative comments there's a lot of emphasis over both the personal American tradition of souping up or fixing one's car as in self-improvement, as well as this is listed as a basis under 107 for personal education, to engage in taking apart the software and playing with it. So, do you want to speak about whether you agree with him or disagree that individuals can make use of the car exemption or an exemption for repair?

MR. BAND: Well, let me, I'll first answer --

MS. SMITH: I know that's sort of two questions.

MR. BAND: Yes. All right. So, first, let me respond to that.

I guess the answer is, it depends. It depends on the car. It depends on the individual. Certain people, obviously, are better equipped at doing these things by themselves than others.

And also, we're interested in broadening the exemption beyond the automotive

sector. I mean, our focus has been on a much broader exemption, that if you're talking about embedded software, which was not what anyone intended when 1201 was drafted, that that's the kind of thing that people should be able to circumvent or get assistance.

But, certainly, with cars, that's probably on the more complicated end of the spectrum, but some of the devices that we're interested in and that have software in them are much simpler, and, conceivably, an individual on his own or after watching a YouTube video, would be able to figure out how to fix by themselves. So, I think it depends. Certainly, cars are probably on the high end of the spectrum, but there's a wide range of spectrum of devices that have embedded software.

But, turning back to what Mr. Amer and Mr. Williams were talking about, and so forth, it seems clear, when you look at the statute, the trafficking provision talks about a service that is primarily designed, right, or it has a limited commercial purpose other than -- I mean, it's talking about a circumvention service. That's the service.

And to the extent you can say, well, no one is only going to just circumvent and do nothing, well, right, the point is to circumvent and, then, get engaged in infringing activity. That's what it was all about, right? Remember, this is about infringement. That's what the statute is designed -- and if not infringement directly, then circumventing to get access to something you haven't paid for, right?

To the extent that when 1201 was broadened beyond what was 1201(b) to include 1201(a) and get into access control, it's like getting cable without -- you know, sort of like tapping into a cable signal or tapping into a satellite signal without paying for it, getting something you weren't entitled to pay. That's what it was intended.

And I think, as you are interpreting the statute, you need to say, okay, what was this really all about; what was the intent? And it was intended to, let's say, deal with a service where someone would come out and circumvent the cable box, so that you could get HBO for free. That's the kind of service you're not allowed to engage in. That's a trafficking or that's the kind of service that 1201(a), the trafficking provision of 1201(a), was

designed to get at.

Here we're not talking about getting access to something you would pay for. You paid your $50,000 for your car. And now, you want to get it fixed because the --

MS. SMITH: Do you think the same would be true if it's like a rental car? I mean, just foreshadowing, you've requested to expand this to other devices where it's less -- maybe the ownership indicia is less clear. Does that make a difference in your analysis of whether these activities are likely to be non-infringing?

MR. BAND: Well, if it's a rental car, you go back to Hertz and say --

MS. SMITH: Hopefully.

MR. BAND: -- "Give me my money back." Right?

MS. SMITH: Yes.

MR. BAND: But, certainly, in the typical context where you're the owner of a device, you've paid your money for it, and you don't want to go back to the dealer who's going to charge you three times as much to repair. You know, once you're out of warranty, right, the dealer is going to charge you two or three times as much for every

repair. But this is your car; you should be able to fix it. And this was not what Congress intended, and you should interpret the statutes in a manner that would allow a person to exercise their ownership rights.

MS. SMITH: Thank you.

Mr. Lowe, I'll just sort of bundle the question to you also. Your comment has asked to add in language regarding the provision of tools. And I'm just curious what you think adding that language in, what it would allow people to do that they can't currently do.

Because the Copyright Office has said individuals should be able to make use of a tool in order to effectuate an exemption. And then, separately, we have raised these questions about regulatory authority for third-party assistance.

So, my question is, if we added in language allowing for provision of a tool, is that in a commercial way of selling it or is that just to clarify that a user can use a tool when they're engaging in the circumvention? I'm not sure what would change.

MR. LOWE: I was looking, I guess we were looking at the development of a tool, so that the

technicians have the tools they need to work on the car.

I want to go back to the comment. When people are repairing cars, the whole goal is to get that car workable again. There seems to be an assumption that they would be trafficking for illegal use. The assumption should be that they're going to be using it for legal use because there's little to be gained from any other use of this, of the circumvention issue.

So, we think that there are people that work on their own cars still. There is an active industry, and it's regulated in California and nationwide, where people receive executive orders to produce parts that are different than the original equipment part, but also are legal because they don't create problems for emissions.

So, there are a lot of legal uses that have already been developed, and a system that has been developed to allow for do-it-yourselfers, for modifications, and for getting those cars repaired. So, it should be, you know, the assumption that, if there's any trafficking, that that can be taken on an individual basis, but that, for the most part and in nearly all cases, it's being done for legal

purposes.

As far as the tools go, if the shops or the individuals don't have the availability of the tools to work on these sophisticated systems, and that the parts can be tested and the tools can be tested, it's going to be very difficult for individuals or repair shops to do the work.

And I guess I would differ in that I think the answer is both, that if you take the exemption -- if you don't expand the exemption, that is going to create a lot of problems for a lot of motorists. But there are also car owners. It's both. Car owners also work on their cars. Now it's a smaller percentage than it used to be, but it's still there and it's still a vibrant industry.

MS. SMITH: Thank you.

And I have one more question on a slightly different topic. You've asked to list out vehicles beyond motorized land vehicles to talk about light, medium, heavy-duty trucks and construction machinery. Do you think that's not permitted under the current temporary exemption? Or why would that regulatory change be advisable? I mean, it says "motorized land vehicles". Doesn't that include a truck?

MR. LOWE: Yes, I think just to make sure that -- those are mostly done by repair shops that work on those cars. They're not done by the actual owner of the motorized --

MS. SMITH: But that's currently permitted? You wouldn't say it's currently permitted under the temporary exemption?

MR. LOWE: I think we just want to make sure it's covered.

MS. SMITH: Okay.

MS. SALTMAN: Mr. Lowe, I just wanted to clarify, regarding tools for independent repair shops, my understanding is that, under the Memorandum of Understanding that is part of the rulemaking record, that independent repair shops do have access to the tools that they need. What evidence in the record or what evidence is there that they need additional tools that would not be licensed from dealers or from -- I'm sorry -- manufacturers?

MR. LOWE: Well, I think right now you're saying that the only place they can get those tools are from the manufacturer under the MOU. And that availability is there, but there's no competition. And so, I think the vast majority of

shops get their tools really from outside, other sources. The MOU is to make sure that, because the cars are becoming more sophisticated, that there would be the choice that they could go to the car manufacturer's tool and obtain it.

Right now, you're asking like for software updates. When you have to replace the software on a part because it's all, you know, it's almost all software-driven now, they buy the software when they buy the car, but, then, they have to go and buy the software again when they buy a part to put on there from the manufacturer. So, it should be that there is competitive availability of both parts and tools for the independent, and that's what keeps consumer choice and what makes repair affordable for Americans.

MS. SALTMAN: And I guess, just to clarify, you said that repair shops are getting tools both from the manufacturers and from other sources. So, what tools are currently prohibited by the exemption that you think should be included in the scope of the exemption?

MR. LOWE: Well, I think any tool -- I think the biggest problem is in the reprogramming and recalibration area, where you have to buy it

from the manufacturer. And the manufacturers have tightened up the rules in a lot of cases to get that recalibration.

GM just released a new requirement that you have to pay per VIN number for each calibration. They used to do it on, you could get it for a month for any GM car. Now the owner or the shop who's trying to recalibrate now has to pay per VIN number for that calibration. So, there's a huge profit center now for the manufacturers in just being the only source of being able to download a program onto that replacement part.

Recalibration is when a program, when you replace a part, the part has software on it with the program. They come with a blank chip on it, so that it's programmed to work with the rest of the parts on that car. So, you have to download that program onto the part again after you've replaced it. It's basically the same program in most cases.

MS. CHAUVET: So, just to clarify, Mr. Lowe, are you saying that repair shops can get the tools from manufacturers, but that it's just too expensive for them to get it that way? And then, I guess the other kind of second part of that question would be, well, wouldn't that expense just

be paid by whoever is having their car fixed?

MR. LOWE: Well, you know, they're all competing. I think you could say that the car owner benefits from the fact that there are competitive sources for both parts and tools. And because they can get the same repair done at an independent using an independent tool or an independent part, that would benefit in having that competitive advantage.

If you're making a commodity where you get the same service, then the car owner is going to pay a higher price all the way across the line. So, yes, I guess you could say they could get that repair done, but at what price? And you're taking away that ability to compete.

MS. SMITH: I'm not sure who is next. Maybe, Mr. Williams, you're being pointed out.

MR. WILLIAMS: Yes, I was going to get back to something Jonathan said about things that go beyond automobiles. So, if you want to stay on autos for a while, I can wait.

MS. SMITH: If we can stay on autos a little bit --

MR. WILLIAMS: Sure.

MS. SMITH: -- I think maybe this may be the last call on third-party assistance issues, and

then, moving onto the telematics and entertainment issues. And then, we'll get to broader devices.

So, Mr. Shore, did you want to contribute?

MR. SHORE: Just a last word on third party, and I wanted to go back to your original question about looking for a theory that could harmonize this and give you the authority. Why not read it against the First Sale Doctrine? Because the idea that you can't, with such complicated technology, again not on autos -- I'll keep pointing at the camera because it looks so complicated, and it's looking right at me.

MS. SMITH: I think someone is going to try to repair this camera after this session. You've kind of thrown down the gauntlet.

(Laughter.)

MR. SHORE: Right. So, if I owned that camera and I couldn't use a third-party maintenance provider to repair it, then it negates my rights under First Sale. I think that's one way to look at it.

And then, we end up just winnowing down what you can transfer under the First Sale Doctrine. Ultimately, nothing that has any sort of complex

embedded software.

Thank you.

MR. AMER: Well, but could I just say, I mean, the First Sale Doctrine is a limitation on the distribution right. It doesn't allow you to make an adaptation of something that you may own in a physical object. So, I don't know that that would really provide a theory for us to conclude that all of the activity that you're talking about is going to necessarily be non-infringing.

MR. SHORE: Well, but my point is that the First Sale Doctrine is totally negated. I mean, if you're looking for a way to -- you asked the question, how do you harmonize this, right? And why even have a First Sale Doctrine then, if you can't circumvent technology using third-party maintenance, as we, I think, generally agree that most technology would require third-party maintenance? All you're doing, then, is selling a brick. You don't really own that thing if it has no value because you can't repair it.

MR. GOLDBERG: So, let me actually ask you about what you think about an alternate theory, as well as others. So, section 117 says it's not an infringement for an owner or a lessee of a machine

to make or authorize the making of a copy in order to do a machine, you know, a repair.

So, I guess my question is, if a mechanic is making a non-infringing use under 117, and they have to circumvent an access control in order to make that use, do we think that there's still potentially a trafficking in a circumvention service or are they just the non-infringing user of the software, you know, undertaking circumvention? Which is it?

MR. BAND: No, I agree. I mean, I think that that's a perfectly viable basis for interpreting the trafficking provision, that it should be done in light of the other provisions of the Copyright Act like First Sale or 117. It certainly informs what should be seen as the scope of what's being prohibited. And it certainly makes sense, if you're going to be circumventing -- if the service that's being provided is a repair service and you incidentally have to circumvent in order to provide the repair service that is clearly lawful under section 117, then the trafficking provision should not be interpreted in a manner that would prevent that. Or, certainly, the rulemaking, given that, again, Congress decided that there

should be a rulemaking, that there should be exemptions, it should all be interpreted, so that it all fits together.

MR. GOLDBERG: Mr. Williams?

MR. WILLIAMS: Yes. So, I think that that's a very good question. But I would say the courts have been pretty consistent about saying a defense to copyright infringement is not a defense to a section 1201 violation or a 1201(a)(2) trafficking violation. So, I don't think that the argument that 117 would apply as a copyright affirmative defense means that the Office can go and grant an exemption that's likely to encourage trafficking under 1201(a)(2).

The other thing that I would note, although we wouldn't support an exemption that did this, is, for 117 to apply, they would have to restore the product to the original state of operation under 117(d), which is something the Office has proposed in its policy study. And so, that would be a wrinkle there as well.

MR. GOLDBERG: Sure. I guess just to sort of put a -- and I know we have been talking about this for a while. But, if my check engine light is on, and I take it into a mechanic, and in

order to make the repair, to restore it to the way it was working before, he has to circumvent an access control, is he trafficking or is he just a user?

MR. WILLIAMS: Yes, I believe, as I was saying earlier, that it would involve trafficking for a repair shop to sell the service of accessing a work by circumvention in order to engage in some further activity that the user is asking them to engage in.

As I've said, we're not primarily focused on automobiles. My clients are not, but this has effects in other areas as well. And as I was discussing with Mr. Amer earlier, if the goal is ultimately to say, get an unencrypted copy of a movie, and the argument is, well, the circumvention is just peripheral to that, it's not really my goal, that would cause significant harm. And it's basically the same theory that's being offered for some of these trafficking exemptions.

So, I think I'm worried about a slippery slope here, and that's the primary focus of our opposition to this.

MS. SMITH: Thank you.

So, just to be mindful of time, I do want to move on to the next topic. So, Mr. Kealey, I'll

call on you first, but if you can transition what you're going to talk to, maybe respond to Mr. Williams, if you desire. But the question to you is about the request to allow circumvention of the telematics or entertainment ECUs. And I want to know whether the current exemption precludes that? And is that preventing repair, diagnostics, or lawful modification of the vehicles as opposed to perhaps entertainment content accessed on the vehicles?

MR. KEALEY: So, I think that, to me, the telematics modules or the infotainment units on the vehicle are no different than a brake control module in terms of --

MS. SMITH: Are they separate modules?

MR. KEALEY: They are separate modules, but in terms of how they need to be repaired on the vehicle. So, if the vehicle owner has a failed infotainment module, they just want a repaired infotainment module that's in the same working condition as their current infotainment module had been to be replaced into their vehicle. No different than they would want a repaired brake control module to be placed into their vehicle.

MS. SMITH: So, it sounds to me like, in

a sense -- I don't know if one phrase we're talking about is layered TPMs, but what you would need to circumvent in order to repair the infotainment module is separate than what you would need to circumvent to repair the brake system or the oils or the engine or other parts of the car?

MR. KEALEY: No, I think they are the same. That's why, for me, it's difficult to draw the distinction between the two.

MS. SMITH: Well, what are you circumventing?

MR. KEALEY: So, let's say the vehicle owner wants to replace their infotainment unit. That infotainment unit may be the same physical device on a Cadillac Escalade as it is on a GMC Yukon. What makes it unique to the Escalade versus the Yukon is the software that's loaded onto the device.

So, let's say the end-user decides that they can physically perform the repair, right? They can remove the old one. They can put the new device in. That end-user had no way to transfer the software that was in complete working order from their old device to their new device. So, there's no way for them to complete the repair. But they can physically do it. They could take the old one

out; they could put the new one in. But, once they put the new one in, it's not in working condition because it doesn't have the software on it. They need a way to be able to transfer the software from their old device to their new device.

Think about, to draw an analogy with the laptop, I mean, if you have a hard drive failure on your laptop, you can replace your hard drive and you can transfer the image of your old disk to your new disk. There's no way for anyone to do that with the modules on vehicles today. And that holds true whether it's an infotainment module or whether it's a braking control module.

MS. SMITH: So, is your business getting requests to transfer infotainment modules? Or is this something that you've looked into doing, but can't do because of section 1201?

MR. KEALEY: We certainly get requests to produce repaired infotainment modules.

MS. SMITH: All right.

MR. KEALEY: But we do not do them because there's no way to actually allow for the end-user to complete the repair. So, we could physically repair the device, but if we can't give the end-user a way to actually turn that into a

working product on their vehicles, it's not commercially viable.

MS. SMITH: What circumvention would be involved if you were to do that?

MR. KEALEY: The only circumvention would be to give the end-user a way to bypass the circumvention features and move the software from the failed unit to the new unit.

MS. SMITH: Okay. And it doesn't sound like -- I'm not sure if you under -- like is there specific technology you can reference. And if not, it's perfectly fine.

MR. KEALEY: I cannot reference the specific technology, no.

MS. SMITH: Okay. Mr. Lowe?

MS. SALTMAN: Mr. Kealey, I just had a quick question, a clarification on that. So, to reinstall a new entertainment module, would you need to circumvent the TPM, the same TPM that you would need to circumvent to repair the brake module, for example? I guess I'm trying to understand, is this a different type of TPM or a different TPM that's being circumvented or is it the same one? It's just to incorporate the entertainment module as opposed to like the brakes?

MR. KEALEY: I don't know if they are the same TPM or they're not.

MS. SALTMAN: Okay.

MR. KEALEY: But you have to bypass the circumvention feature on both.

MS. SALTMAN: Okay.

MS. SMITH: Mr. Lowe, do you know?

MR. LOWE: I don't know.

MS. SMITH: If you can turn on your microphone?

MR. LOWE: Sorry.

I don't know the exact, the answer to that question.

I was going to add that the telematic system is more than just the entertainment module. And the importance to the industry of the telematic system is growing because the vehicle manufacturers, the OBD port that we've used to obtain diagnostic information is going to either be limited to only the required emissions information or will go away entirely in the not-too-distant future because of cybersecurity concerns. So, the telematic system is going to become the only source of diagnostic repair data for the repair industry in the future. And so, we

don't even know at this point how far that will go, but we do know that the OBD system will be limited in the future.

MS. SMITH: What is this new system and when is it coming?

MR. LOWE: Telematics is already on vehicles now.

MS. SMITH: Right.

MR. LOWE: And it just transmits the diagnostic data, help data of your car, through some of the same units that the entertainment -- every vehicle is different the way they're configured, but it sends the data to the manufacturer.

And for the independent repair market, it is going to pose a lot of challenges and could require us to try to either go through -- to find ways to obtain that data from the vehicle or we would be forced to just go to the manufacturer's server to get that data, which is at their terms.

MS. SMITH: So, what I'm trying to understand is whether you agree or disagree with Mr. Kealey where he says the entertainment module is totally separate from the brake module and he would like to be able to offer repair for both of them. Are you currently or do you think there is

currently a prohibition or an inability to engage in repairing the brakes or any type of vehicular repair because there is a prohibition on circumventing the telematics ECUs?

MR. LOWE: Well, I guess, right now, because we're still able to obtain data from the vehicle, that issue probably is not there. But, right now, we're slowly seeing -- we've already seen BMW announce that they're going to take away the OBD system. So, yes, that could inhibit the ability to repair a brake module, if you can't get the data to know what's wrong with the brake module. So, currently, yes, we can do that, but that's only at the current moment.

MS. SMITH: Okay. So, you a couple of times referred to a change going to be coming in the future. Is this going to be done on an auto-manufacturer-by-auto-manufacturer basis? Is it a standard?

MR. LOWE: Yes.

MS. SMITH: What is this change and how do you get it --

MR. LOWE: It's just the manufacturers trying to address the cybersecurity issue in its vehicle, manufacturer-by-manufacturer attempting

to do that, yes. It will be different. There's no standard telling them that you have to do that. It's a question of how they choose to address it, and we're already seeing manufacturers announce that they're heading in a certain direction. So, it's not a fear that we've created; it's things that were actually being discussed.

MS. SMITH: So, you mention BMW. Is there anything else in the record where if we want to look into this --

MR. LOWE: I can give you the presentation where BMW talks about it, if that gives you some assistance.

MS. SMITH: No, I'm just looking to see what's already, I guess, in the record. So, BMW. Are there other auto manufacturers?

MR. LOWE: That's the only one I actually have at this moment in writing. The others are just ones we've seen. There has been others that we've seen kind of come and go in presentations, but I don't have those.

MR. AMER: I just want to make sure I understand. So, you're saying that, increasingly or in the near future, it's going to become necessary to access telematics data --

MR. LOWE: Yes.

MR. AMER: -- in order to repair a vehicle?

MR. LOWE: Correct.

MR. AMER: And you're being inhibited from doing that currently because of the limitation on the current exemption?

MR. LOWE: Well, currently, we can't get access to the telematic system. I mean, that data, we would not be able to do that currently, right.

MR. AMER: So, what about the entertainment system? Is the concern there that --

MR. LOWE: What about the what?

MR. AMER: The entertainment system. Is the concern essentially that you want to be able to, like Mr. Kealey I guess alluded to, that people want to be able to repair the entertainment system and that's just a limitation? Is there anything else that you were seeking to do with respect to the entertainment system that is --

MR. LOWE: The only thing, I mean, right now, those units, the telematic systems, every car company configures their system. Some of them, their entertainment systems are very separate. Some of them might be tied into the rest of the

vehicle.

I think, from an entertainment system, the actual entertainment device that's on the vehicle, those would have to be remanufactured and, then, reinstalled. And I think Mr. Kealey is talking about the fact that it would be difficult to do that, to make sure that that device does what it was doing exactly the same for the motorist without being able to circumvent that software. But I'm not technically the right one to ask. Mr. Kealey would have a lot more knowledge of that than I would.

MS. SMITH: Okay. Mr. Turnbull's had his placard up for a bit. And then, maybe Mr. Williams. If either of you could help explain your understanding of the technology, whether allowing circumvention of this telematics ECU goes right into the entertainment system or whether there are separate TPMs protecting it, such that it might be possible to repair the car-related things without getting into the piracy of music, such as you've submitted information on?

MR. TURNBULL: I'm not sure I can answer that question.

MS. SMITH: Okay. Well, either way.

MR. TURNBULL: What I'm concerned about is getting into the, for example, a Blu-Ray player that may be built into the entertainment system of an automobile, and that in the name of repair, somebody would modify that in a manner that would not otherwise be permitted, where it's not restored. In other words, if it's restoring it literally to the same functionality, meaning all the same outputs are protected, all the same inhibitions of various kinds are incorporated into that, it becomes something that, you know, maybe -- but I would also say that I think both of my clients would be very interested in entering licenses with people who want to do this, and we have a very open license process. We have nondiscriminatory and all of that. To my knowledge, no one has ever come to us to ask for a license, which would be a way of dealing with the entertainment part of this.

MS. SMITH: And what license would that be exactly?

MR. TURNBULL: There would be a license to use our technology for --- under the requirements and the rules and that sort of thing. It would allow access to the specifications. It would allow access to all of the requirements of the systems.

And if you wanted to repair a system, it would allow you to understand how the technology works.

MR. AMER: So, I don't want to get too far away from vehicles. I know we're talking about those specifically. But I just want to make sure I understand.

So, your view is that you wouldn't object to an exemption that included repair and that included DVD players. Is that --

MR. TURNBULL: No, what I'm saying, and maybe not as articulately as I might have, but it was that, to the extent that the exemption does cover those, that it would be absolutely critical that it be limited to restoring the system to exactly how it existed before in all --

MS. SMITH: I have a question. Is that possible? If you are looking through code, and the code is buggy, and you're trying to fix it ---

(Simultaneous speaking.)

MS. SMITH: -- is it possible to restore it to its original function and, then put --

MR. TURNBULL: Maybe not. Maybe not in a computer programmer's terms. But, in terms of, for example, does the output from that system, if there's a plug, if there's a connection to some port,

is that output protected or have you cut off the HDCP protection, so that it's now spewing out Cleartext data?

MS. SMITH: So, you're looking -- sorry -- for it to be restored to its state from a functional perspective --

MR. TURNBULL: Yes.

MS. SMITH: -- including the same locks on it --

MR. TURNBULL: Right.

MS. SMITH: -- as opposed to from a code perspective?

MR. TURNBULL: Right.

MS. SMITH: And does everyone agree that would be non-infringing under 117? Is that the proper way to look at that language?

MR. AMER: So, you know, we've been concerned, as you can imagine, with sort of trying to differentiate between embedded software and devices that sort of you know, where the software exists to sort of control the operation of the device, on the one hand, versus, on the other hand, things like video game consoles and DVD players, you know, types of devices that give access to more traditional creative expression.

So, what we have been told -- I mean, we've had comments from ESA where they've said, you know, at least in the context of video game consoles, the TPM that controls the access to the firmware is also a TPM that controls access to audiovisual works, you know, to video games, the content in video games.

And the concern is that their argument is that, well, if you allow a circumvention, even ostensibly for the purposes of repair of a video game console, you are allowing access to -- you're essentially not only allowing circumvention to allow access to the computer code, but also to audiovisual works in the form of video games.

Do you share that concern with respect to DVD players? I mean, I would have thought that the DVD players, you know, the CSS system, as I understood it, also acts as an access control for the movies and the content on DVDs. Are you saying that it's possible to circumvent access controls to the firmware controlling the operation of the system and not interfere with the CSS?

MR. TURNBULL: I think it would depend on the player, and would depend a little on what the problem was. I could imagine, for example, if

there was some problem with the power source and you needed to repair the power connection, you might need to take apart a DVD player and effectuate that repair. That wouldn't necessarily, and probably, from my understanding, wouldn't interfere with the AACS or CSS functionality of that product.

Now I don't know whether anybody would ever put a TPM around the power source. But there are --- and if there are, for example, you've got a player that has Blu-Ray functionality and it's also a music player. The access in at least some players that I'm aware of, those are completely separate functionalities on the player and you wouldn't have to touch AACS in order to repair the music functionality of the player.

What I was trying to get to before was just that, to the extent that -- we would be concerned if there was a broad-brush exemption to say, oh, yes, well, do whatever you want with the telematics infotainment system, because of the concerns that car manufacturers are only providing the car repair data through that system. It seems to us that you can slice that and say, to the extent that you're going to do something to deal with the problem that Mr. Lowe was talking about, you want

to be very clear that that is not also sort of slopping over and covering an AACS Blu-Ray functionality.

MR. AMER: Mr. Williams?

MR. WILLIAMS: Thank you.

I cannot answer the question about the technical distinction between circumvention to access to telematics versus accessing the entertainment system. My understanding is that, when we're in Los Angeles, the witness from Harman can speak to that better than I can.

I think it's important to look back at what you did in 2015, which is you looked at the record. You concluded it was sparse with respect to entertainment systems. On top of that, there were concerns about unauthorized access, unauthorized copying. Those two things together led to the exclusion of entertainment systems from the exemption.

I think the record is probably even sparser this time on the need to repair these systems. I didn't see any examples in the written comments about that need, and the concern about unauthorized access is still there.

The one thing that I did see a few times

referenced was not about repairing an entertainment system, but about modifying it, so that you could turn it into some kind of storage device. I was a little unclear on whether the goal there was to be able to copy the motion pictures or the music that you're watching or whether it was to, basically, turn it into a blank slate, so that you could upload new content to it. That I see as not a repair, but a modification, and I also see as something that's rather threatening to copyright interest, and really isn't necessary.

My also understanding is that -- and I'm not technically expert at this -- but there's not a lot of excess storage space to be used on these entertainment systems. So, I don't think that example standing alone is enough to grant an exemption.

We did submit a statement from Warner Music, their CTO, in this exemption. And he spoke directly to the fact that, from their point of view, the lock on the firmware on an entertainment system in a vehicle is part of the content protection system that they rely on and that they credit when they're thinking about this from a copyright owner's point of view. It's not just something that -- they have

no interest in locking someone into using any particular provider for repair. There's no competitive reason that my clients have to care about whether someone hacks that firmware.

The issue is that they do believe that, once that firmware is hacked and the entertainment system is accessed, especially when it's accessed through modification, that bad things can happen, that streaming services can be accessed in ways they're not supposed to be accessed; copies can be downloaded in ways they're not supposed to be copied, including from subscription services. So, our concerns go beyond just competitive issues and go directly to the copyright interest.

MR. AMER: Thank you.

Could I ask you about, could I follow up on that last point and Mr. Bell's statement specifically? I mean, reading his statement, I didn't get the impression that the companies you represent are directly involved in developing the access controls that exist on in-vehicle entertainment systems. I mean, I'm looking at paragraph 5 on page 2 of his statement.

He says, although WMG is not privy to the precise methods used to securely communicate

or store such key/token on every device, it is my opinion that obtaining root access to the firmware on devices used to access streaming music services may lead to compromise of the above-referenced protection schemes.

So, I guess what I'm asking -- I mean, these aren't your TPMs. So, should that affect our analysis? I mean, I understand that maybe the content that you own may incidentally benefit from TPMs that exist that protect access to the firmware on the entertainment system, but is it appropriate for us to sort of consider sort of downstream infringement of those types of works, given that you are not the party that -- I mean, am I correct, I guess, in reading his statement to suggest that you're not really involved in developing the TPMs or have any role in establishing those, the access controls that exist on the firmware on the entertainment system?

MR. WILLIAMS: I don't think that's entirely correct. So, I'm here on behalf of the Trade Association, which is made up of multiple members who, of course, are competitors within the same industry. And I'm not privy to all of their individual contracts with the device manufacturers

or with the streaming service providers, for example.

My understanding is that the members would look for some level of protection to be promised by the service providers and/or device manufacturers. Whether they actually get to consult on the individual TPMs that are used, I can't say for sure, but I'm sure that they would like to be involved in that process.

So, I don't think that they're just incidentally protected. I think the device manufacturers, in consultation with the subscription services and others, would work out an ecosystem that they feel meets whatever contractual obligations they may have to provide protection on the content. I don't believe the content would be licensed unless there was some representation of the ability to carry through on the nature of the license, which is usually limited to access in very specific ways, certain numbers of copies, certain numbers of time-limited downloads, whether you have premium access that involves no advertisements or a lower level of access that involves advertisements. And so, I think there would be some level of protection built

into the licensing structure. I don't think that the record companies or other copyright owners would have complete control over exactly how that's implemented.

And so, I think what Mr. Bell was trying to say is that he doesn't necessarily know how every little piece of the system might work, but that his expectation, going into a deal like that, is that there will be protections in place, and that one of those protections, in his view, is the underlying lock on the firmware.

MS. SMITH: So, I see a few placards up. And I wonder, does everyone want to speak about vehicles specifically? Because I think, then, we would like to move on to -- Mr. Turnbull, you do?

MR. TURNBULL: I want to answer the particular question you just posed ---

MS. SMITH: Okay.

MR. TURNBULL: -- and make it clear that both AACS LA and DVD CCA are consortia, in one case, an LLC, and in the other, a 501(c)(6), including studio members. And so, they are very much, AACS and CSS are very much the interest of and property of, if you will, the content owners as well as the -- and, in both instances, the content owners

have third-party beneficiary rights with respect to every implementation of the system, in the case that it's not implemented the way it's supposed to be.

MR. AMER: Yes, and that's helpful. And I understand that that's true with respect to your association and DVDs and DVD players.

And so, I guess what I'm asking is whether that situation and the situation that exists with video games is different from one in which content owners, music companies, are allowing content to be streamed to vehicles through services like Pandora or Spotify or Sirius Radio.

It doesn't seem to me that there is the same level of involvement -- and you can correct me if I'm wrong -- in developing the TPMs, or, in any case, whatever TPM Sirius and Pandora may have are sort of tied to that particular service and are separate from whatever access controls exist on the firmware on the entertainment system in the vehicle.

MR. WILLIAMS: I think that the Office has been wise to look at video game consoles as a unique ecosystem and has done a good job with recognizing that the access controls in place there are all designed to further a copyright interest,

both in the games and, also, in the other types of expressive works that you can get to through a console now, such as motion pictures and music.

And in that market, you can look at the actual consoles as part of the video game ecosystem. There are multiple types of expressive works accessed through a vehicle entertainment system as well. And I do think, as I was just saying, that the copyright owners who make their works available through those systems take into account the various layers of protection before they go into licensing agreements.

So, that I think is similar to the video game space. It's not exactly the same market, but it's that my clients' members look for protections to be in place before they enter licensing agreements. And I think that's also true of the video game space.

MS. SMITH: Mr. Shore?

MR. SHORE: So, I wanted to comment on the video games. I wanted to comment on the video games because it strikes me that the industry, the video game industry, in response to consumer complaints several years ago, where customers weren't going to be able to use their games, you

know, port them from one person's house to another, because the DVD has sort of gone away, and now, it's all stored in the cloud. They've made that available to consumers. You can play your game on my machine or on Jonathan's machine, because you're not really accessing it on the machine. You're accessing it in a cloud storage system.

So, I don't understand how you can kind of have it both ways. How can you say that the system is tied directly to the games, and then it's no, but it's not tied to the games because you can take it from machine to machine? I'm unclear on how you reconcile those two things.

MS. SMITH: Sure.

MR. WILLIAMS: My understanding is that an unjailbroken console would recognize whether or not the copy that's being played is authenticated and legitimate, regardless of whether it's accessed through a disk or through a remote server. And so, the TPMs on the console still further the copyright interest, regardless of the method of dissemination.

MR. SHORE: No, but it's not the TPM. It's the fact that I access it with my username and my password, right, that allows me to access the

game, regardless of the machine?

Again, I don't think you can sit there and say that the machine's -- well, anyway, I'm not ---

MS. SMITH: All right. Mr. Band, anything you would like to say about the telematics and entertainment ECUs? And then, I will ask a general question to you about expanding to other devices and what specifically is in the record.

What is ORI sort of looking to do? Is this --- there's not proposed regulatory language. I wonder, would it be consumer devices or firmware on a device, or how would we write this regulation, if we were to recommend exactly what you're asking for?

MR. BAND: Okay. So, first, I'll first respond to the telematics. And so, in that sense, in that context, I would just say that I have great confidence in the Copyright Office to come up with an exemption that gets to allowing -- or preventing users from being, and car owners from being locked into always going back to the manufacturer and the dealer, but --- while at the same time not allowing sort of like a torrent of hacking of these entertainment devices that will lead to

infringement.

But, beyond that, I think it's really important, as you're fashioning the exemption and tinkering with the wording, to realize we have a little bit of a tail wagging the dog problem here, which is, okay, so there's no question that there's infringement out there and there's no question that there's infringement of Blu-Rays and Blu-Ray disks, and DVDs to probably a lesser extent now as that technology is going away, and I guess streaming.

I mean, yes, that all happens, but there's a lot of it, right? The amount that's ever going to be happening by virtue of what's going on in the car, and somehow hacking the entertainment system in the car, is going to be a drop in the bucket relative to what's going on out in the world.

Now weigh that against the fact that here we have this -- every American has, or not every American, I mean a lot of Americans, the vast majority of Americans have cars or access to cars. It's their largest investment other than their house, right? And they spend huge amounts of money in repairs, and so forth. And to what extent are we going to restrict competition in that market, in the repair market for automobiles and all kinds

of other devices, because there is some slight possibility of some slight amount of infringement relative to the vast amount of --

MS. SMITH: Just for a moment -- I hear what you're saying. And I think one thing we're trying to put our finger on is how are these Americans being prevented from repairing, diagnosing, or modifying anything having to do with this car they've owned, as opposed to their Sirius subscription or the DVDs? So, can't we just leave the line exactly where it is drawn and enable those beneficial uses without, I guess, risking the entertainment content? Like is it necessary to tinker with the language to achieve what you're talking about?

MR. BAND: Well, I would certainly say that --

MS. SMITH: And where is it in the record specifically?

MR. BAND: Well, the telematics I think is the problematic -- you know, entertainment is more discrete, but telematics is sort of this broad, undefined area, and especially as we are getting to more and more autonomous cars. I mean, I imagine all of that is, arguably, telematics and ---

MS. SMITH: But there's nothing in the record about autonomous cars in the next three years.

MR. BAND: Well, but, again, the term telematics sweeps in a lot, and a lot of these systems are bundled or will be bundled. And so then, I do recall seeing something in the record about these systems being bundled together and then, that can have an impact on what you're able to access, and that there's the problem of overbreadth.

So, do you want to have Mr. Lowe answer that or do you want to go to the next --

MS. SMITH: If we could maybe move onto devices, Mr. Lowe, unless it could be very quick. Is there something?

MR. LOWE: Yes. I just want to, I guess, add that the problem is that, going along and defining them separately is becoming an issue because the vehicles are becoming -- entertainment system is becoming intertwined with other systems. I mean, now a car owner goes on their app and they can play --- stream music through their system, but also get health data from the same system on their car.

And so, the defining line, because of

the way that manufacturers are designing their vehicles to become big entertainment centers and big computer information sources or being able to control things from offline, I guess the Internet of Things. It's creating -- it's making it harder to define that line anymore.

And we're not interested in music or hacking to get a Sirius XM or any of that. But, if that definition, then, prevents us from repairing a vehicle or car or getting data so that we can repair the vehicle or car, then we're interested.

And we're just seeing the car's systems becoming more intertwined with their entertainment systems. I'm afraid that while --- the way things were three years ago are not the way they are now or the way they will be in the next year or two. It's, technology is advancing so quickly on these cars that the definition is becoming more difficult.

So, we're interested in finding that definition to make sure they're protected, but at the same time we need to be able to repair that car as they're being configured now and in the future.

MS. SMITH: Okay. So, let's go back to Mr. Band to talk about, again, in a perfect world, what would this regulatory language say? Would it

be just software, period, or software embedded in a device?

MR. BAND: It would be like software that is necessary for the operation, you know, contained in and controlling the function of machines; that it would just be broadened, that it wouldn't be limited to the motorized land vehicles.

MS. SMITH: Would it have to be by the owner or authorized by the owner of the machine?

MR. BAND: Well, I mean, we have the same third-party -- yes, authorized by the owner, yes. I mean, obviously, we would have the same third-party repair issue.

MS. SMITH: Right, but there would be some authorization requirement? I mean, you're not asking to go repair an ATM machine without telling the bank, something like that, right?

MR. BAND: Oh, right, of course. Yes, right, right. No, it would basically be, right, again, that if you own a machine, you should be able to get it repaired wherever you want it repaired; that you shouldn't have to go to the authorized dealer because that's always going to cost a lot more.

MS. SMITH: I guess there's a couple of

questions because there's different levers we're playing with, because you also would like to make improvements. And would the owner have to make the improvements themselves or would a third party be able to do that?

MR. BAND: Now, again, that's just consistent with the previous discussion, that you should be able to get third-party assistance. I mean, that's --- in terms of what would be the desirable exemption.

MS. SMITH: Maybe you could talk a little more about what is specifically in the record? For example, the written comments suggested -- made a reference to compilations of data, but I don't know that there's any record supporting the need to circumvent something, protecting compilations of data or the specific types of devices. And so we need to draw something based on whether there's likely to be non-infringing uses, what types of machines --

MR. BAND: Right. So, the members of the ORI are companies or associations like the Association of Service and Computer Dealers. So, they repair servers, for example, or routers or switches. Or there are members who would be

repairing ---

MS. SMITH: So, your members are not individuals?

MR. BAND: So, our members typically would not be the individuals. These would be the people who would be in the service business. So, they would want to be the people who would be providing the circumvention service, but they're not in the circumvention business. They're in the repair business. But, to do that, they would need to engage in the circumvention.

But we also represent the interests of the owners themselves by allowing them to exercise ownership rights in their property.

MR. AMER: Could I ask about that modification aspect of your proposal? I mean, as you know, in 2015, we recommended, and the Librarian granted, an exemption that would extend to modification, that would allow circumvention for the purpose of lawful modification of a vehicle function. And we, as we talked about, excluded the entertainment system and the telematics, because we were comfortable, I think, that if you're sort of cabining the activity to modification of a vehicle function, something that is in controls,

the operation of the vehicle, we were comfortable that that was likely to be non-infringing as a general matter.

I think the concern is, if we expand that to all devices, can we sort of say categorically that any modification of software embedded in the device is categorically going to be non-infringing? And I understand sort of an answer to that is to say, well, we could define the exemption as non-infringing modifications. But does that get a little bit circular, I think?

I mean, our job is to sort of identify a class of non-infringing uses and to determine whether that activity is non-infringing. So, if we just sort of say, well, you can do whatever you want as long as it's non-infringing, are we sort of kind of exceeding the scope of this rulemaking?

MR. BAND: No, I don't think so, especially if you say, you define the modification for the purpose of engaging in a non-infringing activity. And especially if we're talking about refrigerators and toasters, and those kinds of devices, I mean, there is no possibility of infringing activity to begin with. So, I don't see a problem. I don't think that this would lead to

abuse.

And I think, again, this is just a recognition of reality, that we're sort of moving in this direction. The society is moving in this direction. Technology is moving in this direction. And again, it was never the intent of section 1201 to in any way sort of regulate the U.S. economy and restrict the ability, restrict the competition in repair and aftermarkets in the entire economy.

MS. SMITH: Well, let's take in the case of a software product where the software copyright owner has the exclusive rights, repair, derivative works. How would this proposed exemption tread on that or not tread on that? How could we protect that ability, which I think 1201 was also not supposed to change that contour?

MR. BAND: So, give me --- explain the example and what is it ---

MS. SMITH: You have listed toys, right? What if you change the software in a toy to do something else that is expressive, or speak in a different language, if it's a talking toy? Is that likely to be non-infringing? Does it matter if it's commercial or if it's just me changing it for a toy that's in my house?

MR. BAND: Well, I suppose, depending on the situation, that you could end up engaging -- it could be creating a derivative work, and that would be non-infringing and that would not be permitted.

MS. SMITH: Mr. Williams?

MR. WILLIAMS: Thank you.

This is a big topic, and I understand we're going to spend some time on it in Los Angeles.

MS. SMITH: Correct.

MR. WILLIAMS: But I just wanted to briefly respond to some of what Jonathan's had to say.

I appreciate that Jonathan is not interested in enabling unauthorized access to the types of products and content that my clients disseminate and that he acknowledges that 1201 at least is about not only infringement, but also unauthorized access.

But my point of view, and I think the point of view of the Office in the past, has been that the proponent has to draw a distinction, define a class of works that the Office can look at and say, okay, that is not going to harm copyright owners and that is a definable subset of copyrightable works or devices.

And the current proposal to just cover all devices for any type of repair, any type of modification, just goes very far beyond that. So, in our opposition, we said, well, at the very least, exclude devices that access expressive works of the type that my clients distribute.

MS. SMITH: I mean, we cannot write in a regulation, except for devices that include content that your clients distribute.

(Laughter.)

I mean, how would that work?

MR. WILLIAMS: We said expressive works, and then, I was saying, of the type that my clients are interested in. And the response was, well, there's lots of general purpose devices that you might also be able to access those types of work through. And I think that might be true, but there's nothing really in the record about a need to repair or modify those types of devices, even with respect to laptops. I think there's about three sentences in the EFF's submission that says that, in some circumstances, someone might need to circumvent to repair a laptop.

And I just don't think that record has been established. And if they want to expand this

beyond automobiles, which we did not oppose renewal of the automobile exemption, I think they have the burden of defining some category of devices that will not harm copyright owners. And I don't think there's enough evidence to come even close to doing that. If you go through the EFF's submissions, there's a small handful of very specific devices that they've identified that they want to facilitate repair or modification of, and it's really just modification. There's very, very little on repair.

And some of them, I don't think, just based on the very small amount of information they provided, would even be non-infringing. I don't think that circumventing to modify the software in a robotic dog, so that it does additional things that you want it to do, is --

MS. SMITH: Well, Mr. Band just said it might be infringing.

MR. WILLIAMS: Excuse me?

MS. SMITH: Mr. Band just said it may be infringing.

MR. WILLIAMS: Right. And in the 1201 study and the software study, you've said it's very difficult to draw a line between embedded software in devices that are not furthering traditional

copyright interests and those that are. And on that basis, you declined to exclude software in embedded devices from 1201 as a recommendation.

MS. SMITH: Well, we have, for example, granted a jailbreaking exemption for multipurpose devices and smart televisions, and certain other devices, but excluded it for video game consoles, for example. Why couldn't we do something similar here?

I keep looking to Mr. Band because his comment was joint with EFF. But they talked through Internet of Things, appliances, peripherals, computers, toys, vehicles, and environmental automation systems. I mean, it may be a little bit of a mouthful, but why not list that and say, excluding devices that are primarily media playback devices, or whatever, however we would term this expressive content device?

MR. WILLIAMS: Right. So, I think if you were inclined to do that -- and I don't think they've built a record to justify you doing that -- I would come at it in the opposite direction. Instead of trying to exclude media playback devices, I would look at the record. I would say, here's the exact types of devices that they've identified, that

they've provided evidence on. I would go through each of those examples and see whether, like the robotic dog, it might be infringing, or like another product, like a lightbulb, maybe it's not. And then, I would include a specific list of devices, the way you did with automobiles. I'm not saying you should do that again, but that's more of the approach that I would take.

I also think that, since the exemptions were granted in the spaces that you're referencing, we now have a new opinion from the Federal Circuit applying Ninth Circuit law in Oracle v. Google. And I would emphasize that I think you should take a careful look at that because it approaches software modification and software copying I think in a different way than the Office has looked at it. And I think it might shed some light on the fact that just because someone wants to copy and modify software doesn't mean that it's non-infringing just because the software might have some functional aspects.

MS. SMITH: Does that really bear on the case of a non-commercial use? I don't know that it would, you know --- just to start, there's obviously a lot in that opinion.

MR. WILLIAMS: I'm sorry, you said on a non-commercial use?

MS. SMITH: Right.

MR. WILLIAMS: Well, I think it would because I think the discussion of commerciality in the opinion is only a piece of it. And if you look at that, they're actually very express about the fact that commercial in the fair use landscape doesn't only mean that you're out there selling a product in the market. It also can mean that you avoid paying the customer in price for the conduct you're engaging in. And so, I think even that issue is a nuanced issue when you read the opinion, but there's also a lot in there that goes beyond just pure commercial conduct.

MR. AMER: So, Mr. Turnbull, I think you were next.

But, if it's okay, could I just ask Mr. Band quickly to respond to what Mr. Williams said? And specifically, do you think it's feasible to sort of define the exemption so as to exclude devices that provide access to works other than computer programs, or something like that? Is that sort of a feasible approach or would that exclude more than you think is necessary?

MR. BAND: It could possibly be worded in a way that, certainly, in terms of entertainment products or entertainment software. I mean, there probably is a way to word it so that it's much less likely to tread on the interests of that industry, or, again, that would facilitate infringement, which at the end of the day is what this is all really about.

But I just wanted to also respond to two other points. One is, in terms of Oracle v. Google, I wasn't expecting to talk about that today. And I think it's wrongly decided in 25 different ways. And so, we can talk about that at some other point.

But I do think that, in terms of the record and in terms of sort of like how do you approach this, do you kind of approach it by saying everything is permitted or everything is prohibited? You would have a long list or a narrow list.

I think, again, we're here because Congress sort of, perhaps unfortunately, decided to start with a very broad prohibition on circumvention. Instead of saying circumvention for the purpose of infringing activity, which is what they should have done, that's not what they

did. They instead came up with this really broad prohibition, and then with a few specific exceptions, and then with this rulemaking. So they took this huge, broad-brush approach. And now, we're sort of dealing with this, trying to clean up this mess, frankly, that no one ever intended, whether it's automobiles or whatever.

And so I think given that, then at least for this exemption when you're dealing with embedded software, I think it does make sense to start with a broad exemption with a few carveouts as opposed to a narrow exemption where you say, okay, well, here we have an example about a thermostat. So we'll allow thermostats, but not other household systems. I mean, I just think that that's completely unworkable.

And in terms of the evidence, there is a bit of a chicken-and-egg problem here, which is, okay, here we have a broad prohibition. And then you say, well give us examples of people who are breaking the law or who want to break the law.

MS. SMITH: I don't think that. I think --

MR. BAND: So, we know we have this huge auto repair industry, and this industry has been

willing to step forward and say, you know, we need an exemption to provide the service. But, you know, I've got to believe that if all this is going on in the automotive area, it's going on in the motorboat area, right? Because those engines are just as complicated.

MS. SMITH: I appreciate that perspective, and some of it I think is relevant to the policy issues and the policy study of what the statute should be. But here in this rulemaking, we have to look at whether or not there are adverse effects and non-infringing uses. And the Commerce Committee report says those should be distinct, measurable, and verifiable. So the Copyright Office cannot necessarily grant an exemption based on, I've got to believe. We've got to look at what evidence there is, and we will look to everyone to tell us the burden of production and how these TPMs work, and what is going on.

So I wonder, tying into that, if you can provide -- what devices, is there a need for repair or for modification? Do your, I guess, member companies -- or I don't know -- your members, do they have competitors who offer authorized repair services already? Are consumers finding it

difficult to get their appliances repaired?

MR. BAND: So, yes, it is an ongoing issue in the computer space. And this goes back to section 117 and MAI v. Peak. I mean, this is a long-term struggle between the independent repair folks in the computer area, in telecommunications equipment, and the original equipment manufacturers and their authorized repair people. And it's a constant issue.

So whether it's --- I mean, an issue that keeps on coming up now is that, if you repair a Cisco device with a perfectly compatible piece, but it's not a Cisco piece, that you get an error message, right? And then that sort of causes the users to freak out, and they say, wait a minute, why am I getting this error message?

Now is that an effective technological protection measure? I don't know. Probably not. But, if we ---

(Simultaneous speaking.)

MS. SMITH: --- then do you need an exemption to circumvent it?

MR. BAND: Well, probably not, but that's just an example of the kinds of -- there is this ongoing effort by manufacturers to prevent

independent repair. And our understanding is that there are other technological measures that people might have to repair, but people aren't willing to sort of raise their hand and say yes, I'm doing this to engage in this kind of activity.

MR. AMER: Can I ask, how would your proposal apply in situations where a TPM is controlling access to more than one type of work? So it's --- I mean, it seems like that is really at the heart of the concern here, I think. I mean, to the extent we're talking about software that is embedded in a device and does nothing other than to control a device function, that's one thing. But if the same access control is preventing access to something other than a computer program, you know, if it's protecting access to more than one type of work, how would your proposal apply in that situation?

Would you say that you should still be able to access the software, notwithstanding that it's controlling access to another type of work? Or would you be limited to computer programs that are controlling the device? I mean, is it --- and if it's the latter, is it feasible to limit it in such a way or does that sort of throw the baby out

with the bath water in terms of what you want to do?

MR. BAND: Well, again, it's hard to talk in response to a hypothetical like that. But I suppose I would say, you know, we would want it as broad as possible, but we would understand that you would be limited by (a) the statutory authority and (b) the competing interests. And certainly, at this point, we're looking at sort of like based on the wording of the existing exemption and saying, okay, contained in and control the functioning of. And that's what we're talking about, but going beyond, you know, the motorized land vehicle because that seems unduly narrow.

MS. SMITH: Actually, I have one question on that, just going back maybe to cars, I apologize, but -- so, MEMA and AFBF have requested, I think, language saying that control or assist in the function of, or maybe, Mr. Lowe, you said that facilitate the function of. Is there any specific examples of things that you would be able to do if we added that language and that you are not able to do now related to cars or other devices? I am wondering, is control the functioning of specific enough already?

MR. LOWE: We submitted this testimony, or was it MEMA?

MS. SMITH: It was AFBF and Auto Care Association with CTA. You said control or facilitate. It may have been inadvertent.

MR. LOWE: To control? So, to modify the code?

MS. SMITH: Yes. Why is the word facilitate -- what is that? What work would that be --

MR. LOWE: Well, I mean, an example, I think what we're talking about, it was an example of the Farm Bureau submission which talked about the gentleman who developed an emissions control device that would reduce emissions from agricultural equipment, and would have to modify the code to accept the new part on that car, but would not be able to do it under the current system.

MS. SMITH: Okay.

MR. LOWE: Okay?

MS. SMITH: Mr. Williams?

MR. WILLIAMS: Yes, I just wanted to quickly address something Jonathan mentioned that I think kind of highlights the difficulty with the line drawing that would be involved with trying to

carve out certain types of devices and then cover all the others, which is, he referred to trying to exclude entertainment works. And that's very important to us, of course, but we also are here representing book publishers and journal publishers, and they produce entertainment-related novels. They also produce very scholarly-oriented textbooks or things of that nature that wouldn't necessarily be treated as entertainment.

So if you just excluded devices that access entertainment products, they might not be carved out. And so, I think that kind of line drawing is very difficult to do. And again, I think it should be on the proponents to offer a workable definition. Otherwise, I think you should take a look at the actual devices in the record and see if they've met the burden.

MS. SMITH: Sure. Well, I mean, you use the phrase used to access expressive works. Obviously, like a refrigerator is not typically in that category, and repairing the software on a refrigerator, I don't know if there's, you know, improvements you can do to your refrigerator code.

I mean, if there was a sufficient record on that, would that --- as we consider the statutory

factors, I'm not sure how that would be risky, I guess, to the availability of copyrighted works generally or to, you know, things that your clients care about.

MR. WILLIAMS: Sure. Yes, I appreciate the example. I think there are now refrigerators with TVs built in. But setting that aside, I think, yes, if there was a sufficient record on refrigerators, and if you looked at that and you could tell what the proponents were looking to do, and you felt the need to grant an exemption, we wouldn't necessarily have an objection to that.

I do think when you're talking about modifying the software in the refrigerator, you get to something that's quite distinct just from repairing it and restoring it to the normal functionality that it had previous to the circumvention. But, yes.

MR. AMER: But what about my question to Mr. Band? I mean, rather than having to sort of delineate different types of devices, could you just say -- and we could be clear about this in the text of the exemption -- this applies only to circumvention of access controls to computer programs controlling the functioning of a device.

And if the same TPM that controls the operation of your refrigerator also somehow controls the refrigerator's ability to get Sirius Radio, or whatever, then you're out of luck, you know, because it's also, we haven't granted an exemption allowing you to circumvent access controls to anything other than a computer program. And you're sort of at your peril to determine whether this access control is limited to the firmware or it controls something else. What about that approach?

MR. WILLIAMS: Sure. I mean, that's certainly preferable to what has been requested. I think there are some problems with it. So, as we've discussed earlier, you've gone through previous records related to video game consoles. Accessing that computer program on the console to modify the console ultimately results in unauthorized access to video games. Now video games are computer programs. They're also audiovisual works. So maybe proper drafting would exclude video games because they're also audiovisual works.

But I am sure that there are also all types of expressive computer programs that unauthorized access could be enabled to through

circumvention to access some other computer program. So, I think we're always willing to take a look at drafting and respond to letters and try to be helpful, but I don't see that as necessarily a perfect solution.

MS. SMITH: Yes, Mr. Turnbull?

MR. TURNBULL: Well, now two points. One may have passed the discussion by some time ago. But I was --- originally put my card up to respond to Mr. Band's formulation that talked about circumvention for any non-infringing activity, and simply wanted to make the point that in relation to DVD and Blu-Ray exemptions that have been formulated precisely that way have been rejected uniformly by the Copyright Office and the Librarian. And I wouldn't want this to be some kind of back door to that kind of broad-based exemption.

The second point, however, came up just now. And that is that I think you need to be careful because Blu-Ray players, DVD players have what would normally be called computer programs and firmware. And so --- and those control the CSS and the AACS functionality of the product. And so, I would be concerned about an exemption that talked about something that, a computer program that performed

-- that controls the functioning of the product and including firmware for that, because that would include the AACS application on the Blu-Ray player.

MS. SMITH: Is that right? So, if you were to circumvent AACS, it would go on like a player-by-player basis as opposed to work-by-work? You know, it's not movie-by-movie. It's the specific Blu-Ray player would get, I guess, its keys revoked. Or how does the technology work?

MR. TURNBULL: I'm sorry. I mean, a Blu-Ray player, taking our latest incarnation, AACS 2.0, which we'll have some discussion about tomorrow, but there are requirements that the firmware be upgradeable. So that, if the player turns out to be hacked for some reason, that the firmware implementing the AACS functionality must be upgradeable, so that that can be corrected. And that, so --- and what you're actually doing is downloading a new computer program.

MS. SMITH: Thank you.

Mr. Shore?

MR. SHORE: Yes, you know, we laugh about the TV and the refrigerator example. But if you don't adopt a broad definition, ultimately, you could end up with a system where the refrigerator,

the microwave, all of these sort of broke technologies that we don't really think are problematic, you end up embedding some sort of technology that could be used to access creative works, and then it's thrown out the window, right? Then you can't have that particular refrigerator because there's either a controller in there or it has a TV or it has some system by which you can, you know, hack Pandora.

And I think that's a pretty perverse incentive to start really rolling back and limiting what devices people can then repair or use third-party maintenance to repair.

MS. SMITH: And do you have a sense for whether these devices, right now, they're on --- there's a need to repair them or there's a need for third-party repair?

MR. SHORE: Well there's a pretty --- I mean, we actually have a study we did a few years ago on the size of the resell and repair market that we would be happy to share. It wasn't directed at this particular issue, but it would give you some sense of scope and scale of what's out there.

MS. SMITH: Did you send us that?

MR. SHORE: What's that?

MS. SMITH: Was it submitted?

MR. SHORE: No, no, no, because it wasn't done for this purpose. It was something unrelated. But it might be of interest to you.

But it's a pretty sizable market and it extends beyond just computers. It is, it's refrigerators. It's the technology in your home. But it's also a lot of -- we're not talking about just laptops -- we're talking about multimillion dollar robotic arms that need to be repaired and machines of that magnitude.

We have members that do repairs for government agencies that have very complicated technology systems that are off-warranty or that need a part that isn't made anymore in order to make the technology work.

But we can --- I'm happy to share with you --

MS. SMITH: Well, I guess in that example section 1201 is not posing a barrier ---

MR. SHORE: Sure. Right.

MS. SMITH: --- it's going on, right?

MR. SHORE: Right.

MS. SMITH: I mean, what are the types of repairs that I guess there's a need or a desire

to do that cannot currently be fulfilled because of section 1201?

MR. SHORE: Well, it's the things that our members' servers, routers, computers, I mean all of the things that the other side claims could be used to then access protected works.

Again, we have --- you can drive up and down any street in northern Virginia and you see these shops, some of whom are members and some of whom aren't. And they have particular challenges often accessing the firmware because of the limitations that are placed on by the manufacturers. In fact, you go to their websites, and they tell you that you're violating the terms of service if you access the underlying firmware.

MS. SMITH: But terms of service is separate from section 1201.

MR. SHORE: I understand.

MS. SMITH: Do you turn people away because of section 1201?

MR. SHORE: Right. It's always difficult to get members to, as Jonathan pointed out, to stand up and say exactly what they're doing, because nobody -- particularly because most of these guys are pretty small businesses. And it is, it's ---

granted, it's a challenge to ferret out who is engaging in that type of behavior.

There is the possibility that we could get some people to talk to you, you know, in a private situation. But I just, I think that we see time and time again the heavy hand of the large manufacturer in other settings that -- and there's a case going on at the ITC right now where some of the large manufacturers are coming after some of the smaller technology repair companies for a variety of issues.

MS. SMITH: Not for section 1201?

MR. SHORE: No, not for 1201. But again, because it's very difficult to ask these businesses to raise their hand and admit to engaging in this type of behavior, it's a challenge; I concede that.

MS. SMITH: Okay. So, I have a slightly different question, which is maybe to start with Mr. Band. But, when I read on the ORI comment on modification, it is tilted towards like the personal user tinkering with the device for their own education or for non-commercial use. And I don't really see, personally, the record having been built out to make a case for commerciality of lawful modifications. Do you agree or how would you think

that would change if it was outside of a device? You own it; you bought it; you're tinkering with it and you're using it yourself without distributing it.

MR. BAND: Well, going back to your section 1201 study, which was very good by the way, drawing the line between commercial/non-commercial gets very, very blurry and it's very hard. I guess it was the computer-embedded software study which was also very good. But there was an acknowledgment that saying it's commercial/non-commercial gets very blurry in this environment where this device, which actually someone back there lent to me --

MS. SMITH: Well, here's the --

MR. BAND: You know, it can be used for commercial and non-commercial purposes. And so, that's why I'm not sure. I mean, even though a lot of the modification, a lot of times a person would want to modify it for a personal use, but it could be modifying it for a business use as well.

MS. SMITH: But I guess where I'm going is I'm trying to look at what potential uses have been submitted in the record as being adversely affected. For example, there's a current exemption for non-commercial remixed videos which was based

on a record saying people want to engage in remixed videos; this is for non-commercial purposes. Because of that, the Office looked at it, said it's likely to be fair use, in fact, under the fourth factor.

And so, can we at least say there's -- at least I don't think there's a record saying there is commercial modification of devices which are not vehicles. Do you agree with that? And if there's something else in the record, let me know. Why couldn't we say, if the Office were inclined to draw, allow a lawful modification to other devices, that it would need to be for non-commercial use?

MR. BAND: That would be certainly a positive step if it were, you know --

MS. SMITH: I don't know that we could say for commercial use because I don't know that there's anything there.

MR. BAND: Right. Well, I guess the only refinement on that is that, as opposed to the remix situation, it's where you're modifying the work. Here we're not modifying the work. We're leaving the work intact. We're circumventing, I mean, typically, it's --

MS. SMITH: No, no. You have the whole

submission; you would like to circumvent to modify software. That would be modifying the work.

MR. BAND: Right, but a lot of times what we're really trying to do is modify the device. But I guess to modify the device, you might need to modify the software. I mean, it just depends.

But the goal, whereas in the remix situation the objective, the end purpose is to change, to reuse a little bit or to change the work, because that's the purpose, in our context, because we don't care, nobody cares about the embedded software, it's what you're able to do with it. And it's the device that you're controlling. And so, I think that could be an argument as to why the restriction to non-commercial, it's different from the remix situation. But it certainly is a positive step forward.

MS. SMITH: Did you want to ask a question?

MR. GOLDBERG: So, as we have been having this discussion, it has kind of struck me that, at least in the non-vehicle context, some of what we're talking about actually starts to sound kind of similar to the jailbreaking exemption and to some of the proposals around that.

So, I don't know if you've had an opportunity to review the record in that context. Do you think some of what you're asking for might be covered by one of the jailbreaking proposals?

MR. BAND: Well, I mean, some of the language might be, but in terms of the activity, I mean, because jailbreaking, it's a different kind of activity. I mean, it's sort of trying to have these different apps that could be used on a system.

MS. SMITH: If not repair and if not jailbreaking or interoperability, what types of modifications specifically are you looking to do, I guess? Could you give examples?

MR. BAND: Off the top, I'm not a technologist, so I don't know what exactly the kinds of modifications. I mean, certainly, our members, as a general matter, are probably less interested in modification and more in repair.

But, certainly, like the example that Andrew gave about the robotic arms, when you are repairing these robotic arms, I mean, it might come from the manufacturer or originally be programmed by the manufacturer to kind of go this way, but maybe you want to now have it go this way. And that requires circumventing the technological

protection measure, and it could be -- or it's actually controlled by a laptop. And so, you have to circumvent the software, the protection of the software. And I guess that would be you have to modify the software to make it go this way as opposed to this way. But again, you don't care about the software. I mean, you want to make sure that it's going up or down. And I'm not sure any of the other exemptions would allow you to do that.

MR. GOLDBERG: Yes, so certainly the emphasis is not the same; that's true. But, increasingly, a lot of these devices are, obviously, controlled by software. And one of the reasons people may jailbreak is to be able to run a different app or to be able to change a setting in a particular way.

And I wonder if, at least in some situations, that might cover being able to move the robotic arm in a different way, or something like that, which, ultimately, is probably controlled by software.

MR. BAND: Certainly, it's possible that some of the activities would be, might be able to use that exemption. And then, it could be, certainly, as you mentioned, the interoperability

exemption, exception is certainly helpful when you fall within the four corners of that exception. But there's a lot of situations I think that would fall into neither of those provisions.

MS. SMITH: Mr. Williams?

MR. WILLIAMS: I just wanted to quickly say that, at least in the EFF comments, they kind of toss in a couple of sentences about jailbreaking video game consoles in this proposed class. And I think that just emphasizes kind of the overbreadth of what we're dealing with here. It covers so many things, including things that the Office has built extensive records on in the past and determined are not worthy of exemptions and would lead to piracy, and would lead to harm to copyright owners.

Even if you only are talking about repair, there's prior records on video game console repair, and that was not a justified exemption. And there's a similar record this time on that issue with evidence from ESA as to the availability of repair, and really nothing on the other side.

So, I think you're putting your finger on kind of an overbreadth issue with this exemption. It includes a vast array of things that really need to be looked at one-by-one to determine whether

there's harm involved.

MS. SALTMAN: Mr. Band, I have a question for you. Sort of getting back to the questions that Ms. Smith was asking, do you think that the 1201(f), the provision in section 1201 that exempts reverse engineering, would cover some of the activities that you've described you feel fall through the cracks here?

MR. BAND: Well, it certainly would apply to some situations, but I don't think it would apply to, let's say, all the aftermarket or repair situations, because I think one of the things is that my recollection is that it applies to interoperability between two pieces of software. And so, would it extend if it was between software and hardware? And that's an example of where it might not go far enough to allow --

MS. SALTMAN: Is there anything in the record that sort of delineates these different types of activities? Because I think that's maybe some of the difficulty that we're having in this discussion, is there's not a lot of record evidence to point to about these types of activities that you argue should be included in the exemption. It's hard to know how to draw a line when there's not

a full record to explain what exactly the line encompasses.

MR. BAND: No, I acknowledge that we tried to find more evidence. As we discussed it, it was difficult to get people to be as forthcoming as one would like.

But, again, what is in the record, this specific record, I mean, you do have your two studies, the 1201 study and the embedded software study, that do go into a lot of these issues. And so, there is evidence out there.

MS. SMITH: Okay. I think if no one has any more questions, we're a little bit over and we need to start again promptly at 11:30. So, we'll take a 20-minute break and, then, come back to discuss Class 10.

Thank you.

(Whereupon, the above-entitled matter went off the record at 11:12 a.m. and resumed at 11:31 a.m.)

MS. SMITH: Hello again, everybody, thank you for coming. This is our second panel of the day for the section 1201 rulemaking proceedings. I think most all of you were either in the audience or participated. Basically, what we will do after

introductions is try to narrow down the record and hone in on areas of dispute or understand a little bit better what is in the written comments.

This class is Class 10, Security Research. Make sure to speak into your microphone, and after you've spoken, if you can turn it off so it doesn't create a problem with the networking. And also I guess cellphones were creating a weird feedback sound last time, so if you can keep your cellphone away from the microphone, that seemed to have been helping things.

So my name's Regan Smith, I'm Deputy General Counsel of the Copyright Office. And maybe we can go around and introduce ourselves, starting with Jason and ending with Alex.

MR. SLOAN: Jason Sloan, Attorney-Advisor in the General Counsel's Office of the Copyright Office.

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

MR. AMER: Kevin Amer, Senior Counsel in the Office of Policy and International Affairs, the Copyright Office.

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

MR. GOLDBERG: And I'm Rafi Goldberg. I'm a Policy Analyst at the National Telecommunications and Information Administration.

MR. TRONCOSO: Hi, I'm Christian Troncoso with BSA, the Software Alliance Policy Director.

MR. ZUCK: I'm Jonathan Zuck from the Innovators Network Foundation, but here speaking on behalf of ACT, The App Association, of which I was President for 20 years.

MR. MOHR: Chris Mohr, Software and Information Industry Association.

MR. TAYLOR: David Taylor today here on behalf of DVD CCA, and AACS LA.

MR. WILLIAMS: Matt Williams from Mitchell, Silberberg & Knupp. I'm here for AAP, ESA, MPAA, and RIAA.

MR. ENGLUND: Steve Englund from Jenner & Block, here on behalf of what we've referred to as the Election System Providers, Dominion, ES&S, and Hart.

MS. WALSH: Kit Walsh from Electronic Frontier Foundation. I'm here on behalf of Professor Matthew Green.

MR. FREEMAN: Jay Freeman, SaurikIT, the developer of Cydia, for jailbroken iPhones.

DR. HALL: Hi, everyone, my name is Joseph Lorenzo Hall, the Chief Technologist at the Center for Democracy and Technology.

MR. GEIGER: I'm Harley Geiger, Director of Public Policy at Rapid7.

DR. HALDERMAN: I'm Alex Halderman, I'm a security researcher and professor of computer science and engineering at the University of Michigan.

MR. REID: Blake Reid from the Samuelson-Glushko Technology Law & Policy Clinic at the University of Colorado. We're here representing Professor Halderman and Professor Ed Felten. Thanks.

MR. HILDEBRAND: Brett Hildebrand, student attorney.

MR. KIMATA: And Alex Kimata, student attorney at Samuelson-Glushko Clinic.

MS. SMITH: Okay, terrific. So I think that this is our largest panel of the rulemaking, so it's also our last panel of the day. If we need to go over a little bit, we can, but we'll try to make sure everyone gets a chance to say what they

need to say about the topics.

In terms of structure, I think we would like to generally follow, there's been, so there's an existing exemption for security research in the statute. There's also a temporary exemption, which the Register has concluded it's appropriate to recommend renewal for. So we're really talking about modifying that temporary exemption.

Now, Professors Felten and Halderman have identified five specific areas, and I think that plus Election Systems' specific questions, are the six topic areas we'd look to focus on, although of course if anything else comes up, we can look at it under those lenses too.

But those would be sort of the buckets upon which I think we'd plan to progress in our questioning. So the first bucket I'd like to turn to is the device limitation. So right now there's a list of enumerated devices, all of which must be lawfully acquired in order to engage in security research. And I would like to understand, if this regulatory exemption were to be recommended for modification, how it should do so.

And I think the first question is whether it could at least be limited to computer programs,

or whether there's something in the record beyond computer programs. So just tip your placard up if you'd like to speak. Mr. Reid, Professor Reid.

MR. REID: Sure, so I think we're comfortable with that piece of the existing exemption, that it's recommended, or that it exempts the study of computer programs.

We did make an allusion to ancillary copyrighted works that might be included in computer programs, so that those might be user interface elements, or might be pictorial, graphical, sculptural works or music, or something that might be part of a piece of computer software that by virtue of accessing that computer software by breaking a TPM, you might, in an incidental way, get access to that.

That's obviously not the target of the circumvention. The target of the circumvention is in every case the code, but we wanted to clarify that piece of it. Other than that, that sort of ancillary add-on, I think we're comfortable with computer software.

MS. SMITH: Okay, I guess I wonder if one, someone could speak to whether section 1201 is, what types of research section 1201 is currently

inhibiting, given, you know, factoring in the regulatory exemption. Is it not possible to get permission to engage in security research outside of the current exemption? Ms. Walsh.

MS. WALSH: So Professor Green does research and seeks to do research on devices that are not clearly devices intended for use by individual consumers. So these are things like hardware security modules that are used to secure credit card transactions. They're things like industrial-grade firewalls that are used at a business scale and not typically at an individual scale. Things like non-implanted medical devices.

So if you look at an implanted, basically a defibrillator that's implanted, there are a couple of components of it. So you have the implanted device, you have the home monitoring system, which are referred to in the current exemption. But another critical component of that system is the programming wand that's used to interface with that. And security vulnerabilities could be located there that would threaten that system.

So that's, those are some examples, as well as toll collection systems for public transit, for vehicles, where there's a security research

need. There are potential vulnerabilities, and when Professor Green approaches them, he has to take a black boxing approach. So he's not able to circumvent in order to look at the code. He has to reverse engineer in a black box manner that doesn't give you confidence that in fact there are vulnerabilities.

It's just by looking at this small portion of the attack surface, we can say there is or is not a vulnerability here, but there's an extensive additional attack surface that a wrongdoer would be able to take advantage of that good faith security researchers aren't able to vet.

MS. SMITH: So in the case of the toll collection system, could he get permission to look at it outside of this black box, to look at the actual code? Or why is section 1201, or is not, the obstacle to the research you would like to do?

MS. WALSH: Right, so for these devices, independent security researchers like Professor Green are not able to get authorization from the rights holder in order to do that research.

MS. SMITH: What about the, is the rights holder the same person as the owner of the toll collection system?

MS. WALSH: I'm using rights holder, I was using rights holder to refer to the copyright owner as well as the TPM manufacturer, basically anyone with standing to bring a suit under section 1201.

Being the owner of the toll collection system doesn't necessarily mean that you're able to do this work. So the exemption is necessary, regardless of -- if you're asking would he be seeking to do this research on the toll collection system where the owner is not authorizing him do it --

MS. SMITH: That's part of it.

MS. WALSH: The answer is no.

MS. SMITH: Okay. Professor Halderman.

DR. HALDERMAN: Yes, so there are a number of different kinds of systems beyond what the existing exemption permits that are of interest to me and to other security researchers. Things like traffic control systems, the systems that in a municipality change the state of the traffic signals. Can you access traffic lights and other traffic control devices in order to cause them to behave incorrectly.

Beyond that, things like the networking

equipment used by businesses and institutions or internet service providers. The industrial control equipment used by factories or used in other industrial facilities. The avionics on airplanes or the control software on drones that are used commercially.

These are just a few examples of classes of equipment well beyond consumer devices. In fact, I would say that most security research, or a large fraction of security research, really isn't about devices that individual consumers are using. But it's about devices that are critical to business, to industry, to making the communications networks and the systems that we all rely on operate correctly and securely.

MS. SMITH: And do you agree with Ms. Walsh that you're not seeking to do anything where you wouldn't have permission from the sort of systems owner, if not the rights holder or TPM holder for example, whoever is in charge of the traffic control system? And how do you go about getting that permission in advance, or would you?

DR. HALDERMAN: So in general, security researchers don't try to do research on systems where they don't have some permission to come in

and access that system, except in cases of things that are just generally available and observable to the public.

Like you would go out, one category of research there is just looking at the devices, at the websites that are accessible on the internet and asking questions about them broadly but in a noninvasive way.

But in general, if I were, or another researcher is going to perform testing on a device or a piece of equipment, we're going to be doing so with the permission of the device owner.

MS. SMITH: Mr. Geiger. Thank you.

MR. GEIGER: So I just wanted to make the point that for some of these categories, some of these other categories, we're not just necessarily talking about scenarios where a researcher goes to infrastructure held in another building or owned by another person.

That in many cases, for example avionics, you can actually buy this equipment online. Like it's used equipment is actually available for a price on eBay. You can just buy the equipment and have it there.

Now, I don't know, you know, it's

available to an individual person, but may not necessarily fit within the bounds of the device description that is in the current rule. So I just wanted to make clear that you can be the owner of the hardware in research scenarios, and still be outside of these device limitations.

And there are some very compelling, we think some very serious cyber security issues in several of the categories that Professor Halderman just mentioned, not without limit being avionics and drones.

Now, we're not advocating for a complete removal of the device limit. I think that there are, it makes sense to have some limits, given potential negative scenarios, negative externalities. But some of them we do think should be included and reflected. You know, the --

MS. SMITH: How would you structure a device limitation based on the record of abuses that people seek to do and given what you said?

MR. GEIGER: I think that, A, I think it's difficult. B, I think that the issue is going to, it comes down to the devices designed for individual consumer use or primarily for individual consumer use. It creates a gray area for things

like small Office, home Office, but also for, as I said, hardware that an individual consumer can purchase.

So I guess I'll have to get back to you on specific language, I just wanted the record to reflect those points.

MR. AMER: Could I just clarify one thing you said? So did you suggest that the exemption as it's currently written would in some cases not allow you to do the kind of research you're talking about on a device that you've lawfully purchased, as distinguished from the software? Because you know, the exception talks about lawfully acquired device or machine.

So that to me doesn't speak to the concern about, you know, whether the software is lawfully owned or whether it's licensed, or something else.

MR. GEIGER: No, I'm not talking about the lawfully acquired device; I was talking about the limitation on the type of device.

MS. SMITH: In a consumer use.

MR. GEIGER: Right.

MR. AMER: I understand, so I mean I understand that you're saying that you want to

expand to systems that, you know, may not be a device that you can, you know, to the extent you're talking about infrastructure or something that's not a device that you can own.

But I just, I thought I heard you say that there was a concern that you couldn't, that you would be, you know, limited in the research that you could do on a device that you've lawfully acquired, and I just wanted to clarify that.

MR. GEIGER: I thought I did clarify it. So if you lawfully acquire the device but the device is not one that is generally for consumer use.

MR. AMER: No, I understand, right.

MR. GEIGER: Yeah, that's, okay.

MS. SMITH: Mr. Hall.

DR. HALL: So certainly the statutory exemption is inadequate. I think the Register's report on 1201 made a good case for that. There are a set of things here that we're particularly concerned with. When it comes to, specifically to gaining authorization, you had asked how difficult is it to gain authorization.

This is only tangentially in the record due to a footnote from the paper that we had, that CDT had provided that we put into the record. There

was a study recently by Professor Stefan Savage where they actually empirically tested the ability to get affirmative authorization from companies to do things like circumvention of TPMs.

And it was abysmally poor in terms of the response. Academic researchers got a better response than non-academic researchers. But even academic researchers, I think it was in the ten or twenty percent level of even trying as hard as you can, trying to get authorization for these kinds of things.

MS. SMITH: Well then, do you agree with Ms. Walsh and I guess Professor Halderman that if you couldn't get permission from the hardware owner or the person who owns the thing, that you could not, an exemption would be improper for the Office to --

DR. HALL: So there are certainly forms of security research that we value that don't, that because of how they're designed, cannot by design get an authorization. But those are not necessarily in the circumvention of TPM space.

I can probably think of one involving remote access to like locks, like doors and things like that. But you don't want me to make something

up.

MS. SMITH: No.

DR. HALL: So I won't.

(Laughter.)

MS. SMITH: Ms. Walsh.

MS. WALSH: I want to make sure that the potential confusion that arose from Mr. Geiger's comment is resolved. I think what Mr. Geiger was saying is there are devices that are not intended for use by individual consumers, which you nonetheless are able to purchase.

You can get old voting machines at a county clerk's auction. You can get hardware security modules and industrial grade firewall equipment to do security research. So the mere fact that you're able to acquire them doesn't seem to clearly fall within the language of the existing exemption.

MS. SMITH: Professor Reid.

MR. REID: Just to pick up on a couple of points. I imagine we'll get in the subsequent questions, into the question of your ability to lawfully acquire a device, there's obviously been some concerns raised by opponents in the record about the extent to which restrictions on the

transfer of, whether it's an ownership or a license and software, and the extent to which those might be intertwined with contractual provisions that purport to prohibit resale and all of those sort of things.

So we have highlighted in the record some ambiguity about the lawfully acquired provision and have asked to get rid of that, so I hope --

MS. SMITH: So that's another one of our buckets and we are excited to talk about that a little bit later.

MR. REID: Perfect. A couple of other quick clarifications. One, I want to make sure, as we're talking about getting permission from the owner of the device or the system, that in many cases is not going to be the copyright holder. And that may be implicit from the discussion here, but I want to make sure that's --

MS. SMITH: I think that's what we're trying to build out. Because if you don't have the permission from the person who owns the physical device or you know, someone owns the physical device or the actual device, or the copyright owner, it becomes less obvious, to me at least, that 1201 is the thing preventing you from engaging in the

security research, for one. And two, it might affect on infringing use analysis.

MR. REID: So just to give an example on that front, we might talk about doing a security research experiment on the HVAC system in a building. Now, in a case like that, we're obviously going to do coordination with the owner or the operator of the building. So the folks who do facilities management make sure that the inhabitants of the building are safe and all of that sort of thing.

However, the HVAC system might be designed by a third-party vendor and encumbered with some sort of technological protection measure with whom we're not going to go seek permission. And we are seeking to cover that scenario in the ambit of this exemption. So I just want to make sure that piece is clear.

MS. SMITH: Do you think the owner of the HVAC software would not give permission, or?

MR. REID: I'll defer to Alex and Joe to speak for that.

MS. SMITH: Any of the software people know whether it's likely to, that permission is not given for security research on these sort of, you

know, industrial-grade things? Professor Halderman, I guess.

DR. HALDERMAN: The problem is most often not that companies wouldn't give permission if they were to fully analyze the question. It's that companies are not reachable to contact for security-related purposes.

So in many studies that I've done where we've found vulnerabilities in large classes of devices and gone to try to reach out to the manufacturers afterwards, just to let them know about the vulnerability, that we have a real problem in their system that's affecting people and they need to fix, they haven't been responsive or reachable to those requests.

So if you're not a, directly a customer of a vendor, you aren't the individual who bought a support contract from them, the device is out of service and no longer being supported, it can be extremely difficult to get a company to act on such a request.

MS. SMITH: Thank you. Mr. Troncoso.

MR. TRONCOSO: So I can't speak specifically to whether HVAC or building owners or operators do or do not give permission, but I think

I just wanted to comment generally on the request to remove the device limitation, just to point out that I think the removal of that limitation is going to make for just an exceptionally broad category of exemption.

And I don't think that, you know, we need to look closely at whether proponents of that request are meeting their burden with respect to that entire new class. And so it's worth pointing that at least for like industrial control systems, oftentimes there are regulatory requirements that the owner or operator of an ICS in a highly regulated industry needs to perform its own security testing on those systems.

So that suggests to me that there are opportunities for this type of independent research, at least in some of the contexts that are going to get dragged into this exemption if we go down the path of sort of opening it up to all forms of systems.

And so again, just, you know, not to belabor the point, I think there certainly will be categories of devices for which authorization to perform security research is a viable path, if we remove the device limitation entirely.

MS. SMITH: One question, and this, maybe Mr. Englund can also speak to this too, is, I've noticed that everyone has been talking about devices that are not consumer devices but still using the word device, if that makes sense.

And whether if an exemption were broadened based on this description of uses people, things people want to research, should be devices which are not necessarily consumer devices, whether this solves some of the concern that the Office might be granting an exemption for beyond a narrow and focused subset of work. So if it is software on devices. So starting with Mr. Englund.

MR. ENGLUND: Sure, so to take your last question first, I think the proposal that's been made here is beyond the scope of a permissible class in this proceeding. It is essentially all software, once you remove the device limitation.

MS. SMITH: I guess I just said what if it's software on devices?

MR. ENGLUND: So I think that is narrower, but there are a lot of devices in the world. And that kind of goes to your previous question and Mr. Troncoso's response, which I wanted to follow up with, because that's very much the

position of the election systems providers.

Once you've removed the device limitation, there are two kinds of election software that are relevant, one of which is addressed by your suggestion of referring to a device and one not.

So there is software in the election context that is intended for use on specific kinds of devices, like voting machines or tabulators. There is also software that is intended to run on general purpose computers. And so if you retain some kind of special purpose device limitation, you would at least take the general purpose computer software off the table.

But following up on Mr. Troncoso's point, in the election context, there are abundant opportunities for independent testing and consent when it's to be had. So as described in our written comments, the Election Systems Commission has voluntary voting system guidelines.

Many products in the marketplace, voting products in the marketplace, are independently tested by federally certified labs to conform to those. Many states and localities have their own certification requirements. As part of the procurement process, there can potentially

be additional testing.

And the election systems providers and states and localities cooperate to authorize testing in these contexts.

But, and there's been other testing beyond the certification and procurement processes. There was, in 2007 in California, a so-called top-to-bottom review. And one of the proponents talks about that in his comments.

But the evidence in the record shows that the states and localities are not particularly interested in working with independent testing organizations and independent researchers to do testing beyond that.

I heard from the National Association of Secretaries of State, and from the Secretary of State of North Dakota, that they like the certification and testing processes that exist and are not interested in having people testing without consent.

MS. SMITH: Okay, Mr. Williams.

MR. WILLIAMS: Thank you. Most of the devices that are of interest to my clients are already covered by the consumer devices provision. So I think from our point of view, what you're

describing, just expanding it to a somewhat broader category of devices is of less concern than some of the other things that have been mentioned about network access or database access.

And I appreciate Blake saying that, you know, that they're not looking to get into things other than software, but that sometimes incidentally or as an ancillary matter, they may also access other types of works, and I think he even included music. That's really our concern, is that if you go beyond devices and open up things like online databases of content, that could really lead to some significant harms.

And although I know the individuals in the room today are acting in good faith and doing their best to avoid any mistakes, not everyone is always going to being able to avoid mistakes. And so I just think it's pretty dangerous to open up kind of testing of internet-based databases of content.

MS. SMITH: Okay, so Professor Halderman, if you could do that question, and I don't know if it was you or Professor Green who wanted to research or is researching internet-wide scanning, or I think the cyber physical systems.

Are those things still devices?

DR. HALDERMAN: So I, yes, I am researching internet-wide scanning. And just for a little bit of context, internet-wide scanning is now one of the most important methodologies for studying the health of security across the internet as an ecosystem, of considering the entire global population of computers in an epidemiological way and tracking how vulnerabilities are patched or being exploited.

And so internet-wide scanning involves connecting to every device on the internet with a public IP address, and attempting to make usually just a normal connection as someone from the public trying to access that machine would, and observing what comes back.

That is an absolutely essential methodology for the security community, but one where we necessarily cannot in advance seek the permission of every device holder, because every device holder is everyone running a computer that is serving public connections.

MS. SMITH: So in that instance, you're trying to make connections with other internet users or devices. How is section 1201 -- it sounds like

you're able to conduct that research currently.

DR. HALDERMAN: So what we worry about with 1201 is the ambiguity of whether this is going to be permitted or not. And I think the very --

MS. SMITH: Well, what circumvention are you engaging in in this internet-wide scanning research?

DR. HALDERMAN: Well, we're making a handshake to every remote computer, and we don't know in advance of making that handshake whether the system we're connecting to is employing some kind of not very well functioning access control mechanism that's intended to prevent those handshakes from succeeding.

So we, I think the worry is that for certain systems, merely making a handshake to them might be construed as violating an access control mechanism. Perhaps the mechanism is one in which just the address of the remote system not being published to the world, or links to that system being made available to others, is intended to keep people from accessing it.

And internet-wide scanning would be incidentally bypassing that.

MR. AMER: Could I just ask, so are there

other types of research that you would like to do? I mean, it sounds like you're saying that, you know, authorization would be impractical in that circumstance, doing that type of research.

Are there other types of research where an authorization requirement or a requirement that you make a good faith effort to seek permission of the device owner or the operator of the system would be inadequate for the research you'd like to do?

MR. REID: If I can chime in on this one, I'm very concerned about the idea that we're going to insert a permission structure, for a few reasons here, that we're talking about this idea of a permission structure.

The first is we're not talking about situations where you can necessarily track someone down. But even if you can, we are trying to analyze legal risk ex ante. We're trying to understand, when we're advising a researcher, whether this is going to be copacetic, or whether somebody is going to come after them.

The mere act of asking for permission might well be answered positively, but it might well be answered negatively. And it might well be answered so negatively that there's a threat of a

lawsuit. A letter gets sent to the dean of a school. A letter gets sent to the organizer of a conference.

It might even be a situation where there's not an access control present. It might be a situation where there's no copyrighted work present, but someone is invoking the DMCA as the nature of the, as the underlying threat.

MR. AMER: Right.

MR. REID: And so what we're trying to get at here are the adverse effects that we're required to demonstrate on the statute is that we are making non-infringing uses of copyrighted works, right?

MR. AMER: Yes, and that's helpful. And I mean, just to be clear, I'm not talking about permission of the owner of the copyright on the software. I'm talking about the owner of the, you know, the toll collection system, or the, you know, the building that you're trying to research the HVAC system on.

I mean, and I think we're trying to sort of, you know, if we're going to sort of expand the existing exemption, which is conditioned on the device being lawfully acquired, and I know we're going to talk about that condition later on, is it

a burden on your research in general to, you know -- and it sounds like it was consistent with your general practice, apart from maybe the, you know, the internet-wide scanning, you know, to try to seek authorization from the owner of whatever device you're -- or system, you're researching.

DR. HALDERMAN: So if security researchers are doing research that has the possibility of causing harm to the operator of the device, they're going to make sure that that device is one that they have, that they own or have the permission of the device owner to test with, and they're going to take steps to mitigate that harm.

But in other cases where security research doesn't carry a possibility of harming the public or the owner of the device or the device itself, these are cases where we may just want to be measuring something about the world and the population.

Doing a measurement that involves the cellphones in this room or the wi-fi devices in a neighborhood, that might be a case where we aren't going to necessarily need to go and get the permission of device holders --

MS. SMITH: Sorry, if you wanted to

security research the cellphones of all the people in this room, you would not need our permission? What would you be doing, and what would you be circumventing?

DR. HALDERMAN: If the --

MS. SMITH: Why would that be non --

DR. HALDERMAN: So if there was a question about whether the cellphone, the cellphones operating in a particular space were running a network protocol that was vulnerable or had received software updates, if we wanted to anonymously measure the population in order to track the frequency of software updates or the uptake of new versions of software.

That's an example of a scenario where it's basically just observing the world rather than infiltrating.

MS. SMITH: In that example, do you have any concerns about other laws, such as the CFAA? It just strikes me as like, would you be literally circumventing everybody's individual cellphone here without their permission? I wonder if this is like a hypothetical that went off, or if this an actual research project.

MR. REID: I think the response to that

is no. Obviously researchers are considering a wide variety of other constraints on what they can do, and I assume we'll talk about this in more detail when we get to the other laws section.

But I think the important consideration for us here is we have now diverged a very long way from talking about anything to do with copyright or the intent of the DMCA. We're talking about a regulatory structure about how security researchers do their work in general, absent copyright concerns.

And I think there's a worthwhile discussion to be had, and is happening. For example, computer scientists are having discussions about what the ethics of research look like and how that intersects with institutional review boards and how that intersects with the common rule.

We're also having other conversations in the context of the Computer Fraud and Abuse Act about how that works. That is not necessarily a discussion that ought to be happening in this room today.

MS. SMITH: I'm not disagreeing with that, but I think we started off saying let's ease

up on the limitation of consumer devices because there is a numerated category of things that security researchers want to research. And perhaps it's hard to specifically list them out, or not.

But then we got into let's, even without the permission, which I guess Professor Green would have sought, research into individual, you know, devices people own without telling them to. And I wonder, I don't know what they're, under the copyright law. We'd have to see whether that change is analogous or not, because that's not the way the Office has previously looked at his recommendation.

MR. REID: Well, I mean, I think it might be worthwhile to divert back to the original inquiry, which is whether the device limitation makes sense.

And I think what you've heard is for that particular part of the existing exemption, there's a wide variety of software embodied on devices that are either ambiguously, maybe, maybe not within the ambit of consumer devices, or are industrial commercial devices that are completely outside of the intended ambit of the existing category.

So if we want to stick on that point, I think there's pretty clear evidence in the record

of a desire to do research on those categories of devices in ways that permission from the copyright holder is not forthcoming. Again, to this question about permission from the device-holder I think is a different question.

MS. SMITH: Okay, let's, I think we'd like to do the last round on the device limitation. We'll go to controlled environment next, just to give a roadmap. So just going down the line, Mr. Hall.

DR. HALL: Thank you. I just wanted to say a couple things about what the election system providers, election service providers, election system providers said. There are two people on this panel who are part of large, mostly academic efforts to study voting systems. The election systems providers were dragged kicking and screaming to that.

Part of that is because the testing that goes in there, the regulatory testing that happens is not security testing. That's not, it's often shake and bake testing, you know, like is this thing going to withstand being on a semi truck for ten years or something like that.

The kind of testing that we do as

security researchers is more adversarial. In some cases, it's been called open-ended vulnerability testing or penetration testing. I mean basically, ask yourself, you know, what can we do with the public knowledge that's out there with this system.

So it's a little bit different here. You know, unlike Rapid7, I think we are asking you to remove the device limitation to the extent you can to apply to software and software-controlled systems. I think, I'm not sure we submitted this in our filing, but I think we would be okay with some extreme limit to that.

So for example, there are types of critical infrastructure, like nuclear power plants and things like that, water systems, energy systems, that we might want to actually say, no, look, this is a place where it should be a no-go zone for this kind of action, activity, so to speak.

Part of that is on those operators of those systems themselves as well, isolating those systems so that when people touch them or get close to them or are able to access them, they aren't as exposed as many of the systems that we work with today, that you know, surround us, including the cameras in front of us right now.

And that's really the meat of what we're talking about with the device limitation. Having an enumerated list means every three years we have to come back and add more things to it, rather than having a presumption that anything with software, anything that's a software-controlled system should be something that security researchers should use --

MS. SMITH: Well, we typically tend to recommend exemptions or to adopt exemptions which are based on the record. And in 2015, the record was based on sort of consumer-facing devices, so that is why the language is as it is right now. And we're debating whether to change it.

DR. HALL: And we tried to supplement the record. In our initial filing, we issued another paper that was used for case studies that talked about voting systems, internet of things devices, automotive systems, and other kinds of non-land based vehicles.

And one, anyway, but we tried to supplement that to say, look, here's examples of things that security researchers are finding flaws in that we want to not exclude from their attention, but actually include these things in their attention

and give them fewer excuses to avoid those kinds of systems.

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

MR. FREEMAN: Another hat that I wear is I'm actually an elected local government official. And so in this comment that came up just a little bit earlier about the statement from the Executive Board of the National Association of Secretaries of State, it is very often the case that there will be an issue that will come before the larger body that is not agreed to by all of the individual smaller groups.

And I do think it is a little bit weird that, if for example, in our district, we were interested in having some kind of independent security audit for a particular reason, that would be something we would only have the opportunity to do during the general testing process. Which as was just mentioned, is largely more for just verifying functionality in many ways.

And then back on my iPhone jail-breaking hat, I will point out that, I mean the iPhone goes through a tremendous amount of security testing by very smart people at Apple. And yet, time after

time, independent security researchers have come and shown vulnerabilities that have made the world a much more secure place by getting those things fixed.

And so having the opportunity to have independent security research being able to be done on these systems at the will of independent local governments that are interested in having this thing, this checked I think is very important.

MS. SMITH: And when you say these things, can you?

MR. FREEMAN: The voting machines, sorry.

MS. SMITH: Voting machines, and so --

MR. FREEMAN: That was the example specifically brought up by the election systems.

MS. SMITH: So Mr. Englund, I think you've said that the state and local governments, they may not have the ability to give permission for security research because your, the companies you represent restrict it via license agreements? Do you want to speak on that?

MR. ENGLUND: Sure, so the point I was making a minute ago was not that point, however.

MS. SMITH: Right, I'm asking you about

specific...

MR. ENGLUND: Just to be clear that the election systems providers do cooperate with their customers to satisfy their customers that their devices are secure.

With respect to license agreements, elections system software is licensed pursuant to license agreements that look a lot like commercial software licenses. They contain all the kinds of restrictions on use that you'd expect to see in commercial database software and the software provided by Mr. Troncoso's clients.

So but among other things, they would prohibit distributing the software that's licensed to, say, the municipality to somebody else. And that's kind of the point we were making in our comments concerning infringement, that if municipality X is authorized to use a particular piece of software to conduct elections in its jurisdiction does not authorize it to distribute copies of the software to anyone else.

It was infringement for them to provide a copy of that to the security researcher. Their customer, they're simply coming to talk to the vendor about whether that's something they'd like

to do. But --

MS. SMITH: Well if the vendor, I mean, doesn't the vendor perhaps have an incentive -- is the vendor appropriately incentivized to research, find and disclose all of the problems?

MR. ENGLUND: Absolutely. It's a competitive market. My three clients, all jointly represented today, are commercial competitors with each other. And one very important feature that they sell is security.

In addition, there are these certification requirements, both federal and state and local, which contrary to something that Mr. Hall said or at least implied, do include some security requirements. So security is something that is of great concern to the systems providers and their customers. And --

MS. SMITH: Have they ever, you said that not even state and local governments would qualify as owners. Have, are there examples where your, the companies you're representing would have turned down requests for security research?

MR. ENGLUND: Independent of their customers?

MR. AMER: Well, by -- I think maybe what

you're getting, so you know, has there ever been a situation where a government has requested a term in the license or, you know, requested permission from the vendor from your clients to allow third-party researchers to conduct security research on the software?

MR. ENGLUND: I don't know the specific answer to that question. One of the things I don't know whether or any state or local, to the extent to which state and local governments ever asked. I do know that there are circumstances where state and local governments have expressed a desire to conduct security testing, and that has happened.

MR. AMER: I'm just thinking, you know, if Mr. Freeman mentioned, you know, his jurisdiction. If, you know, his jurisdiction decided that it wanted to allow, in addition to the research that it does itself, wanted to bring in Mr. Halderman or, you know, an academic institution to conduct third-party research on the voting software, do you think that's something that your organizations would be amenable to?

MR. ENGLUND: I think they should certainly talk to the vendor of their equipment. They have some market power. So that sort of thing

has happened.

MS. SMITH: Okay, I think maybe we can hear from Professor Halderman who, on the other side, has had experience.

DR. HALDERMAN: Yes, there absolutely have been cases where local governments have wanted to conduct independent security testing on voting systems and have either been denied permission or have refrained from seeking permission because they were convinced it would be denied if sought.

And that has been a constant inhibition to independent security testing of voting systems since the introduction of computer voting.

This is getting all the more urgent to perform independent testing of voting systems. The Senate Intelligence Committee, which has been investigating interference in and hacking of election infrastructure, recommended just last month that states and local governments pursue security testing from the Department of Homeland Security for their election infrastructure.

And furthermore, because the Department of Homeland Security doesn't have the resources to test every local and state system in a timely way, the Senate Intelligence Committee recommended that

-- recommended the use of private security testing firms as well to perform that same kind of test.

So it's essential to allow non-government security testing of election systems -- be it at the local level or the state level -- in order to make sure that they're going to be secure, even for this year's elections.

MS. SMITH: So I hear a couple of things out of what you're saying. I hear first it sounds like you disagree with Mr. Englund that the independent research is exhaustive on voting systems, okay.

But secondly, if the Senate Intelligence -- if this is happening, how is section 1201 -- or is it proving an obstacle to this independent research if there are a lot of resources and other governmental resources mobilizing to making this research happen?

DR. HALDERMAN: Well, so 1201 is going to be a significant concern. If a state or local government came to me today and asked me to participate in such a test, I would have to have a serious conversation with my attorneys about whether I would be at risk of doing that research due to 1201.

MS. SMITH: Would you go to the copyright owner? If you sought permission, it would alleviate that problem.

DR. HALDERMAN: Well, so if we sought permission, if I sought permission to do such testing, I'm not sure it would be granted. In fact, my strong suspicion is that if a local government wanted to bring me in to do a security test of the voting machines from the makers represented here today, that those companies would object.

MS. SMITH: Mr. Mohr. Microphone.

MR. MOHR: Oh, sorry about that. We don't necessarily have a dog in the voting fight. What we are concerned about is the specificity of the record with respect to particular kinds of tailoring of any issued exemption.

And this is, you know, this is kind of a good example of that, because as I listen to this, it strikes me that a lot of this ought to be covered by 1201(e), which allows, does not prohibit any lawfully authorized information, I'm going to insert ellipses here.

The section does not prohibit any lawfully authorized information security or intelligence activity of an employee of the United

States, a state, or a political subdivision of a state, or a person acting pursuant to a contract with the United States, a state or a political subdivision of the state.

And for purposes of the section, information security means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network.

So to the extent that there's a need for a further exemption beyond what's in the statute already, I am puzzled as to what it is that our friends would like to do that is not allowed by 1201(e).

MS. SMITH: Professor Reid, if you want to respond to that directly, that would be helpful.

MR. REID: Yes, I'd be happy to chime in. Thinking back to ten years ago when we sat and first talked about 1201(j) and heard a similar argument about the extent to which 1201(j) might apply --

MS. SMITH: But I mean, specifically when we're talking about voting systems and --

MR. REID: 1201.

MS. SMITH: Everyone's been discussing state and local governments, Senate Intelligence,

Department of Homeland, there seems to be a large government -- I'm not sure, it might be a different question.

MR. REID: Sure, so the first thing I'll say is if litigation were ever instituted over this and Professor Halderman, for example, was working with a local government, one of the first -- to do independent security testing, and the DMCA was brought up by one of the election vendors as a claim -- very likely one of the first things we would assert as a defense is 1201(e).

Now, I don't think I have to tell you that 1201(e), at least to the best of my knowledge, had never been tested in court. And there are a number of ambiguous provisions. And I know that this, as far as I'm aware, has not been briefed on the record. But I'd note that it is referring, it refers to investigative protective information security or intelligence activity.

Now, whether the scope of security testing of election system falls within the ambit of those terms, I'm not sure. And because we haven't had an opportunity to brief this on the record, I'm uncomfortable sitting here today saying, yes, absolutely 1201(e) is going to cover

that.

But to the extent that the Office opines that 1201(e) is likely to cover the types of activities that we're talking about today, as we've asked in the past with 1201(j), positive interpretations of the scope of the built-in exemptions are helpful. The lack of clarity about them is the reason that we have come and asked for a specific exemption that covers the activity.

But if it's the Office's perspective that 1201(e) covers everything that we've asked for in our briefs that pertains to election security, that would be very helpful to have a declaration in the final rule to that effect.

MS. SMITH: I think it would have to be in concert with someone connected to a state, because that's what 1201(e) does. But it's much shorter than 1201(j), so in some ways I think it's a little less ambiguous. Ms. Walsh, do you have thoughts on that?

MS. WALSH: Yeah, I think we've discussed the use case where a voting machine is acquired by independent researchers because we all, as residents of the United States, have an interest in the integrity of our elections. And so an

independent researcher who acquires the voting machine, does research, doesn't necessarily have a government sponsor --

MS. SMITH: But that's permitted under the current exemption, right? I mean, if you're going to test a live election system, shouldn't you somehow coordinate with a local facility or state facility? I mean, right now a decommissioned voting machine or something, not networked, not connected, an independent researcher can get that and can conduct that research.

MS. WALSH: Subject to the other limitations in the existing exemption.

MS. SMITH: Yes.

MS. WALSH: Yes. I also wanted to add, when we've had a few references to seeking permission from the copyright owner, one of the issues with that and one of the reasons why it's dangerous to even approach a copyright owner in the first place is because often what security researchers are doing is they're criticizing the functional aspects of the works.

They're discovering vulnerabilities and putting pubic pressure on the companies to get them fixed. And when the election vendors, for

instance, say that they compete on security, that's competing on the perception of security of their purchasers.

And that's part of why there's a financial interest from these companies not to allow their brand to be tarnished by truthful reporting about vulnerabilities in their software.

MS. SMITH: Mr. Zuck, I think you've been waiting for a while.

MR. ZUCK: Thank you. Jonathan Zuck for the record. I'm not an attorney, so I won't delve into the rule itself as much as the, try to backstop this a little bit with a philosophical point that I think is going to end up being a framework from which I'd want to approach this conversation going forward. Which is that if there's a TPM in place, the default ought to be to leave it in place.

And so this idea of permissionless access on a broader and broader scale I think needs to be viewed with some scrutiny. And the idea that in the majority of the cases the answer is no I think is okay. Right?

It's the idea that the de facto, the default should be that anybody that wants to perform

a search should be able to do it, and we should get all of the doubt out of the way for doing it, feels like the wrong place to start the conversation. So maybe only 20 percent get back, maybe 20 percent of researchers having access to your system is plenty. You know, for example, for a particular security test.

And so I just want to say that I think from a philosophical standpoint we ought to start from the standpoint, as the law does, of calling it an exemption. But that everything isn't by default okay, and that we should just get everybody, every barrier out of the way and every ambiguity out of the way for anybody doing whatever they want to do.

And instead make it about permission, make it about exemptions, and start from that place. So maybe voting machines are something that need further discussion, but creating this broad expansion of the exemption feels like the wrong move just in an effort to clear the clutter for anybody that wants to get at these systems for any reason.

MS. SMITH: Okay, thank you. So Mr. Williams, if you wanted to be responsive to what has been raised before.

Also, I'm going to move onto the next topic, which is the controlled environment limitation. If you have any thoughts on whether that is an important limitation in the current temporary regulation towards the statutory factors and what were project here under 1201(a)(1).

MR. WILLIAMS: Sure, thank you. I did want to respond to something Blake said earlier, just so that it didn't go left unaddressed. And I know we're trying to go bucket by bucket, but his comment was kind of expansive in covering the purpose of why we're here in general, so I'm going to speak to that first, and then I'll answer your question.

When we were discussing whether someone who wanted to circumvent everyone's cell phones in the room in order to do some research should need everyone's permission, and if so, whether that might also violate the CFAA, the point was made that somehow because a lot of security research is non-infringing, that all of this is just outside of the scope of what Congress intended to address in the DMCA, and that it's completely outside of section 1201.

And therefore, the Office should not be

engaged in the careful process that it is engaged in to date to try to draw some limitations and make sure that you're defining a class of works that doesn't lead to abuse.

And I just think the discussion we've been having about 1201(e), about 1201(j), it just shows that that's not true. That Congress was very aware of these issues, that Congress addressed them in various provisions in the statute. And then it also gave you the authority to move beyond those provisions, if a very good record was built.

And part of what Congress did in 1201(j) was also refer to other laws, including the CFAA. And so I think the approach you've been taking -- trying to come up with common sense limitations, referring to the other law's limitation -- all of that is well within your purview. And all of this was anticipated to some degree by Congress.

The controlled environment limitation to me is just another one of those common sense limitations. I don't see it as unduly burdensome to suggest that when you're engaging in this kind of activity, you take some special care to prevent harm occurring. And so I think that should be retained.

MS. SMITH: Thank you. Mr. Geiger, can you talk about the controlled environment limitation and what research that's impeding, including whether perhaps the Office could provide interpretive guidance as opposed to, say, removing it entirely to assuage sort of protecting the research that is, I guess, not dangerous from other types of research.

Which I think every researcher who has filed a comment has said there are strict ethical norms and rules. It might depend upon what is being researched, but no one is really endorsing I guess non-safe research, if you wanted to talk a little bit about that.

MR. GEIGER: So I'm sensing from you that that is, that you want me to focus on just the controlled environment portion. I had actually put my card up to address some of the things that were momentarily said. But they may fall better under the other laws bucket. I'm happy to wait for that bucket in order to address the legislative history on that if you'd prefer.

MS. SMITH: You know, if we can stick with controlled environment now, I think that might help keep it --

MR. GEIGER: Understand.

MS. SMITH: --- orderly. And I'll certainly let you say, get back to you when we get to the other laws, yup. Mr. Reid, Professor Reid.

MR. REID: I wanted to just quickly circle back to 1201(e) and point out as a technical matter one reason 1201(e) won't work in many situations, because it doesn't apply to territories of the United States including Puerto Rico. So there's always going to be a number of elections where voting machines are going to be deployed and where it's directly not applicable.

I wanted to respond to Mr. Williams' point about the notion of addressing non-copyright concerns in this proceeding. And there was sort of a watershed moment in the last hearing where all the other agencies dissented and said, whoa, hold on a second. We've got all these other policy concerns that relate to cyber-security, that relate to environmental protection, that relate to all of this other stuff.

And the Office, for better or for worse, accommodated that interest by delaying the rollout of the last security exemption by a year and setting an expectation that other agencies would have time

to respond. To the best of my knowledge, there's almost nothing on the record that suggests anything happened as a result of that.

In other words, that agencies came in and said, uh oh, we have got real problems with this exemption. And we need to create new policies, new regimes to accommodate the fact that security researchers are going to be coming in and doing new types of work.

And the Office said in its policy study that it was going to, that was the shot that everyone had to bring up these non-copyright concerns, and that the Office did not expect that it would be addressing health, safety, and environmental concerns here.

So I want to underscore that historical point not because we don't think that safety is important. Obviously it is, and Alex will speak to that. But we don't think this is the appropriate venue in which to be considering that. We don't think that copyright policy and the body that is responsible with setting the contours of copyright policy ought to also be setting the contours of responsible security research.

There are a lot of complicated questions

about how this shakes out, and I think the responses on the record about the nature of the controlled environment limitation go exactly to this. I counted at least three different interpretations of exactly what that means from the opponents.

So that very ambiguity is the problem, and also I don't think we want the Copyright Office going in and being more specific about what we mean by that. We want you to defer to other agencies, who by the way haven't raised any concerns about it on the record this time around, and to researchers who are engaged in good faith security research to set those contours themselves.

And I think the proponents of this exemption are among the most credible and trustworthy and serious security researchers that do this kind of work. And the insinuation that they need a check from the Copyright Office to tell them how to do their work I think is inappropriate.

MR. AMER: So I -- oh.

MS. SMITH: I don't think I'm making any insinuation. I think we're trying to follow from the law and from the existing statutory exemptions as well as what the legislative history is telling us to do. I mean I just, we're not questioning the,

I guess, practices of any participant here. I think that should be clear. Yes.

MR. AMER: I just wanted, and I, you, Mr. Halderman, Professor Halderman, you may want to address this, or Professor Reid, you can as well. But I mean to sort of clarify this purported ambiguity about controlled environment. I mean, I think that grew out of what a lot of commenters have described as sort of universal agreement in the last rule-making that this sort of testing shouldn't extend to live environments, live testing.

And then I know, Professor Halderman, in your reply comments you said, well, there should be a distinction between live testing and testing in real life environments carefully designed to avoid harm. To me, that latter phrase sounds a lot like controlled environment, as sort of a lay person.

And so I wonder, you know, is there a distinction there? Is there, you know, are there types of environments that are uncontrolled but that nevertheless sort of have the sort of safeguards that you seem to be talking about?

DR. HALDERMAN: Well, so let me just start by emphasizing that the security community

and security research absolutely recognizes an obligation and a community norm of testing security in a way that is safe, that is not harmful to the general public or to the operators of systems.

And I think that ethical core of our behavior of researchers is a large part of what separates security research from activities that are harmful and malicious.

But the problem with the controlled environment limitation is maybe you feel like you have some sense of what a controlled environment looks like. I don't know how to interpret that, and I'm the one having to make that call in the work that I undertake.

So a controlled environment, to me, maybe that sounds like that means I have to take the device into the laboratory, isolate it from the rest of the world, and make sure that nothing is going to come in or out of that isolated controlled environment unless it's accounted for. Something like that.

It's that notion of it being a controlled environment that is the part that causes me the most problem, not the notion that security researchers are going to try to design their experiments and

their research not to cause harm. Of course we're going to do that.

But if you invite me to, say you invite me to test the security of your home network. Is that a controlled environment or not, right? And because it's operating in the real world, we're going to presumably take steps to make sure that I'm not going to destroy the networking equipment in the process of testing it or otherwise leak sensitive data of value.

We can do all of these things to make sure that there aren't harms, but I'm still not sure that that's a controlled environment if it's something that's taking place within a person's actual home network.

MR. AMER: Well is it, and that's helpful. I mean, would you say that that phrase or maybe the, what you see as the ambiguity in that phrase, is imposing a requirement that goes beyond what other laws would require?

I guess another way of asking that is, you know, is it ever lawful to do this kind of research in something that's not reasonably described as a controlled environment, according to other laws?

DR. HALDERMAN: Well, Blake, you're the --

MR. REID: Yeah, so --- okay if I turn mine on at this point? I think it's important to remember the context in which we are making this evaluation. The evaluation is not when we're sitting down in the example of, say, testing a piece of home networking equipment, whether the person whose home we are in is going to be upset about it. We're going to have a fruitful discussion with them beforehand.

If we're testing the HVAC system in a building, it's not that the building owner is going to be upset about it.

The context that we're in is, in the software that we are looking at, we are going to find a potentially embarrassing bug that suggests in fact this piece of widely deployed software has got a serious security vulnerability that everyone else who has deployed this piece of software has now got to fix.

There is a significant incentive for the folks who are the copyright holders in that software, the vendor of that software to say, we would really like that not to be released. And what

are the ways that we're going to shut down the release of that vulnerability or shut down publicity of that vulnerability, shut down conference papers about that vulnerability.

Well, we're going to go look at this exemption, and we're going to look at every piece of this exemption and see if we can figure out some way that this research arguably, or maybe even not arguably but in enough that we can assert it in a demand letter, violates the exemption.

And we're going to look at that controlled environment limitation and say, we've just been having a ten-minute colloquy about what it means.

That's uncertain enough that we are concerned about that. And that means that we can't go to folks that are trying to get some ex ante clarity about the ability to do this and disabuse the notion that there's going to be some serious legal risk when this is ultimately published.

So it is critical that the Office bear in mind that that is the context. It's not the homeowner, it's not the building owner. It's not the operator of the system. It's the copyright holder for whom the release of the vulnerability

might be fairly economically devastating that we're concerned about.

MR. AMER: I mean, I think one -- oh.

MS. CHAUVET: Well, I was going to say because there are examples. Like for example like Apple has a page on its website specifically for security researchers to go and tell Apple if they find bugs in the software. So it's not like every company across the board doesn't want that type of information.

And so I guess if there's ambiguity about the term "controlled environment," which you guys seem to think that there is, is there another alternative way to or another phrase to use so that, obviously you guys are very ethical, you know. I'm not -- no one is saying that you're not. But maybe not everyone to rely on this exemption would be as ethical.

So I think it's just trying to put some type of safeguard to protect the public. So I don't know if you have a suggested alternative phrase that could be implemented.

DR. HALDERMAN: Well, I think the safeguards come from other existing statutes, things like the Computer Fraud and Abuse Act, which

doesn't talk about a controlled environment. It talks about authorization from the operator of a computing system.

MR. REID: I think the point is that the policy dimensions of how you might want to control an environment such as we're talking about here are so broad and so deep and so complicated and so under dispute that to embed all of those considerations in the exemption --- that's what we're getting at.

It's not that we couldn't have a robust policy discussion about what a controlled environment is and an appropriate way to conduct research. It's that embedding it in this exemption to copyright law is not the appropriate place to do it.

And so it's also not to suggest that in situations where, take Apple for example, they might well work closely with security researchers. And that's great, and they, you know, there might be situations where you're working hand in glove and asking permission.

But again, that, we're talking about the entire industry. We're talking about every single purveyor of software. We're talking about every single device that's out in the world. And we need

something that covers all of those possible situations. And that's why we're asking to get rid of this limitation.

MR. GOLDBERG: So sort of building off of that point, obviously there are companies that not only are willing to work with security researchers, but even have the bug bounty programs in some cases. And in fact I, you know, I have a few examples.

I know Microsoft and Adobe, among others, have bug bounty programs, and they're not necessarily limited to your local devices. They actually in some cases invite you to test their cloud-based services.

Have you had trouble actually taking advantage of something like a bug bounty program because you think it might still be a DMCA violation?

DR. HALDERMAN: I think the major problem is the companies that don't have bug bounty programs, which is almost all companies. We're talking about bug bounty programs being things that are provided by a very, a relatively small fraction of companies that are mostly the companies that are already the most responsible actors and security-conscious ones.

If I were to be doing research about corporate routers and firewalls involved in routing internet traffic that are manufactured by, say, certain Chinese companies that are already suspected of embedding back doors in their products, I probably would not receive permission from those companies to go and do those tests. But the tests still would be essential for the security and safety of the public.

MR. REID: And if I could just chime in and discourage the Office and NTIA from considering incorporating a bug bounty caveat to this limitation, because then we're going to have to sit here for another half an hour and talk about what a bug bounty program is and what features it has to have and what's an appropriate level of response and all of that sort of stuff.

And again, that's a complicated policy debate, and this is not the place for it.

MR. GOLDBERG: Right, so if I could just follow up, I was actually, you know, thinking more of trying to get the opposite situation to a lot of what we're talking about, which is, you know, whether you can get that permission or not. I'm just you know, using that as an example. You know,

sometimes you actually, you know, have enthusiastic support from the software developers.

But you know, a seemingly, you know, as it's currently worded, a 1201 might, you know, still not allow you to take advantage of those programs. Is that your experience?

MR. REID: So the hypothetical that you're teeing up is a situation where 1201 would prevent a bug bounty program --- a researcher from participating in a bug bounty program. I'm not familiar with any particular examples where that's shaken out.

You might be able to think about a situation where there are multiple copyright holders involved and the company running the bug bounty program is one of them. But you then have to go get permission from the other one, something along those lines.

DR. HALDERMAN: I think 1201 would be one of the factors that I would be looking for in reviewing the language of the bug bounty permission statement, where the bug bounty is going to say that the company promises not to take legal action against a good faith security researcher under certain laws. And I'd want to make sure that

whatever wording there was there included 1201, definitely.

MS. SMITH: If we could go to Mr. Troncoso, I think he's been waiting for a while.

MR. TRONCOSO: Sure, thank you. I just wanted to follow up in on one of the points Blake made. He made reference to the fact that just because some companies have bug bounties doesn't obviate the need for an exemption. And I mean, I would totally concede that point.

But I think on the other side is that, you know, just because the researchers in this room abide by the certain norms that would, you know, guide them in the construction of their research projects to mitigate harms to third parties doesn't mean that every sort of purported security researcher out there is doing the same thing.

So I think that counsel that we need to make sure that there are at least reasonable safeguards built into this exemption. And from our perspective, the controlled environment is precisely that. You know, one of the purported sort of interpretations of the controlled environment limitation is that it would require all research to be performed in a lab setting.

I mean, I don't think that that's a very reasonable interpretation of the limitation, and I'd simply point out that several of the examples that the proponents have proffered of the types of security research they've engaged in under the auspices of a 2015 exemption were not performed in sort of lab settings.

So I mean, we could have a discussion about sort of what the contours of a controlled environment are. And I think it would be reasonable for perhaps the Copyright Office to sort of, you know, to explain that in the context of the recommendation that they make, that you make. But I think, you know, our view is that sort of it is not a lab setting.

And I'd also just make one other point, that several of our companies have big security research sort of wings of their companies. So in many ways, Microsoft, for instance, is both a beneficiary of this exemption, as are several of our other companies.

And they have not flagged concerns with me in the course of this sort of project that they view these as unreasonable constraints on their ability to perform security research.

MS. SMITH: Thank you. Mr. Mohr, I think you were also waiting.

MR. MOHR: Sorry, thanks, just a couple of points on this. I mean, the first is that, you know, there's a difference. A demand letter is not the statute, in the sense that the fact that somebody makes a threat does not mean that the statute's actually causing it. I think we've probably all seen good examples of creative writing in that context.

The second thing I would say that in this instance, we agree with the premise of what Mr. Halderman said, if not the precise language, which is the idea that if there, the obligation on the researcher is essentially if they're going to go nosing around, not to cause harm and to take steps to prevent that harm.

In the regulation now, that's encompassed by the phrase "controlled environment." If that needs to be fleshed out in certain ways, that's fine. The idea of internet-wide scanning, as it's been described in this context, is not something that we're uncomfortable with. I'm not quite sure, again, that that's something that the statute prevents in

any way.

But to the extent that you're looking for areas of consensus, I mean, we don't believe that this limitation should be dropped. But if it's refined further to get at the same condition in a different formulation, that's something I think we would be okay with.

MR. AMER: I think Ms. Walsh was next. And I guess maybe in your answer and others, if you want to address that too. I mean, is this something that sort of more clarification would be adequate to address, short of dropping the language altogether?

MS. WALSH: So in answering that question, I'm going to take up Mr. Zuck's invitation to think about what is the default about whether this research is going to be permitted or not. And it's not an abstract philosophical question; it's a question that's answered by the First Amendment.

This is protected First Amendment activity, so you need to have a darn good reason to restrict it, and your restrictions have to be narrowly tailored. Congress took the approach of passing this really over-broad law, and it's your problem to try to mitigate some of the over-broad

impacts on speech that that law has. That's what this rule-making is here to do.

So in that context, none of what we've talked about in the controlled environment context has anything to do with the purpose of section 1201 of combating infringement. It's all you might hurt somebody, you might commit a tort against somebody. It doesn't speak to the ultimate question of: are there adverse effects on non-infringing uses?

MR. AMER: Well, that's the point, isn't it? And I'm sorry to interrupt. I mean, to the extent that this is unlawful, you know, that it's sort of an academic question, you know, because other laws prohibit you from doing this type of research in an uncontrolled environment, or however you want to describe it in a way that exposes people to harm, can we really say that 1201 is the cause of any adverse effect that you're experiencing?

MS. WALSH: So 1201 increases the adverse effect because it's duplicative, redundant, unnecessary penalization of conduct that may be prohibited by other laws. So that's half of the answer, which is where, and I'll expand on that, which is where there actually is some other law that is broken.

The other scenario is you don't do it in a controlled environment, you don't actually wind up causing any unlawful harm, you don't actually commit a tort against anybody. There's no harm, but under the language of the exemption, you're potentially liable to the copyright owner for circumventing 1201 because you didn't do it in a controlled environment.

So that's one scenario. There is no harm, other laws don't really apply. In the scenario where you do wind up, you know, say you do automobile research and you run somebody over. Okay, there are tort laws, there are personal injury laws that are generally thought to adequately disincentivize that kind of conduct.

People are not counting on section 1201 of the DMCA to dissuade people from running them over in the streets. And it's illogical if I get harmed by someone who has physically injured me, sure, I have a cause of action against them.

But why does a copyright owner now have a cause of action against that person? How is that -- how does that remain proportionate to the harm, particularly when section 1201 has statutory damages and has potential criminal penalties?

It doesn't, and it interferes with the ability of other regulatory agencies to say, this is a harm where maybe you should be fined $500, but it's not that big a deal. Okay, you're fined $500, but then the copyright owner can see you get statutory damages, and if you did it willfully and commercially, you can go to jail.

MS. SMITH: We're not affecting what any other regulatory agency can or cannot do.

MS. WALSH: You are connecting liability under section 1201 to what other agencies try to do in their regulations. So put yourself in the shoes of -- I am an environmental regulator, and I think that this activity is bad. It's not that bad, I'm going to fine you $500 if you violate it. I think that's the right level of deterrence.

And now the Copyright Office has come in and said, "Ah, but if anyone violates that provision, actually also you have potential criminal penalties and a private cause of action so that the rights holder can come in and penalize you further."

MS. SMITH: Well, we haven't removed that from the existing permanent exemption, just to be clear, right. I mean, we haven't come in and

affirmatively decided to regulate and put in language. We've said we're not, we didn't see a record to remove it, I think, from 1201(j) is what has happened in terms of the Copyright Office's role.

Another question for you is Consumer Union filed a comment which in general supported many of the eliminating or amending, I guess, the regulation. But they said the controlled environment limitation is very important for consumer safety. I wonder if you had a thought of why they felt that way, since they perhaps shared Professor Green's views on other points.

MS. WALSH: So I think something that's very clear is that there is a norm in the security research community that you do your research safely. And that's a professional norm; it's not necessarily something that anyone thinks the government can or should impose as a matter of law.

Just like in the journalism context, there have been professional norms about when you disclose victims' names, when you don't. And you might say it's irresponsible as a journalist to violate that norm, but you wouldn't say the government can prohibit you from doing it.

MS. SMITH: I don't know if that really answers the question of if the Copyright Office were to remove the controlled environment limitation, is it signaling that that norm is not important?

MS. WALSH: No, the Copyright Office, the professional norms being things that are matters of professional ethics and not government mandates is an important traditional feature of the way that the speech-related professions operate. It's not clear to me what the authority of the Copyright Office is to impose a limitation like that that has nothing to do with whether the activity is infringing or not.

MS. SMITH: Mr. Englund.

MR. ENGLUND: I'd like to just very briefly respond to Ms. Walsh, who said in essence that the controlled environment limitation doesn't have anything to do with copyright. And I think that's just wrong. 1201 is about TPMs that are used to control access to copyrighted works.

And the ask here by the security researchers is to circumvent those, and thereby obtain access to copyrighted work. This becomes somewhat bound up in the consent issues and that lawful device, all the copy issues we were talking

about a few minutes ago. But the proponents want all of those limitations to go away.

One thing the controlled environment requirement does for standing alone is prevent someone from hacking into live systems and thereby obtaining access to copyrighted works. So if you do away with the device limitation, as the proponents have asked, and you do away with any kind of consent that we shouldn't, as the Office proposed in the previous panel.

And you also do away with the controlled environment limitation, hack TPMs to obtain unauthorized access to copyrighted works, and that's something that Copyright cares about.

MR. AMER: Who's next? Mr. Freeman.

MR. FREEMAN: I just wanted to respond to the question of if the Copyright Office were to remove this clause, whether that would signal that they believe that that's an appropriate thing to be doing. And I would say that no, because you've been stating that you believe that many of these activities would already be covered by other laws.

What I would say that it's doing is it's showing that Copyright Office is not interested in rewriting in different wording a summary of another

law that will then cause a new form of like legal cases to have to be argued about how that new wording is. Instead, it's more just signaling that they're more interested in utilizing the existing legal base and the existing laws than creating more confusion.

MR. AMER: But you're also asking us to drop the other laws requirement. So I mean I could see the argument that the controlled environment is duplicative of other laws to the extent that they also require provision for public safety, etc.

But then you're also, you're asking us then to take a next step of removing the requirement of compliance with other laws, which is in the permanent exemptions in the statute.

So I mean, I think our thinking has been that there's a, you know, a basis for inferring that Congress wanted to include compliance with other laws as a condition of 1201 exemption.

So you know, how do you reconcile sort of wanting us, I mean if you're saying, if what you're saying is that the controlled environment is duplicative of other laws and it's unnecessary, how do you then take the next step of asking us to drop the, I guess we're bleeding into the other laws section. So maybe you could address that.

MR. FREEMAN: Well, I will say that they are different arguments, in a way. I mean, there's different points there to be made about different sections of this. And I mean, I really liked Ms. Walsh's argument about the ones that reference other laws end up causing a situation whereby you can increase the penalty accidentally of another law.

Or the argument I believe was made by Mr. Reid, which was that by -- or actually no maybe it was actually Mr. Halderman -- which is that it will change who is able to make that claim, such as being able to make it the randomly, now it's a copyright owner that's able to come out in order to make an argument, whereas before it was somebody you made a tort against.

MS. SMITH: Well, maybe we can zigzag between copyright owners and security researchers. So Mr. Williams and then Mr. Hall.

MR. WILLIAMS: Thank you. I just wanted to briefly touch on the First Amendment issues that Ms. Walsh raised. There have been several opinions, especially at the beginning of the application of section 1201 that addressed the First Amendment issues, Corley and Reimerdes and Elcom and others.

And they do carefully walk through all of these arguments, they identify it as content-neutral, they apply intermediate scrutiny, they observe the existing statutory exemptions that you've been referencing as one of the protections built into the statute.

They even discuss cases like journalism cases, like *New York Times v. United States*. And they've all come out and said this statute is perfectly constitutional under the First Amendment.

So I just wanted to say that at least based on those cases, I don't think there's anything inappropriate about you trying to draw similar limitations into these regulatory exemptions as to what Congress did in the statute.

DR. HALDERMAN: Thank you. So in our joint filing, we actually did -- as you asked, Mr. Amer -- provide some narrower language that we think could help. So I think what we actually said was specify the controlled environment requires only that, quote, "harmed individuals or the public can be mitigated." So that gives us a little bit more.

I am going to point out that we've learned more since we made this filing, so we did

submit a research report as part of the record. Everyone got a copy of that; I don't know what exhibit it is. But in that research report, we actually did a qualitative investigation speaking to hackers and security researchers about what kinds of considerations shape their work.

And half of them mentioned the DMCA in some part of the conversation. But the important thing is that when it came to questions about live systems, you know, how far is too far is an example of a question we asked these researchers and hackers.

It was, as you said, there was some unanimity in talking about things like cyber physical systems that can actually have an effect, with a software change, on the physical world and can move kinetic things and hurt people.

But it's more than just to people, right. It's harm to property, machines, things like that. And also invasions of privacy. So you can imagine like wiretapping kinds of things, where there are very serious laws that prevent you or should prevent you from doing those kinds of things.

And so I think while we do definitely think the easier way is to eliminate the controlled

environment specification entirely, there are probably ways to write language that could get at, you know, harm to people, harm to machines, invasions of privacy that may not be all the one things.

But as you can see, it's already becoming a pretty complicated set of things to specify in the exemption text. But I'm sure that we could work on it.

MS. SMITH: Okay, thank you. So I think we'll go to Mr. Mohr then Mr. Geiger.

MR. MOHR: Yeah, I just wanted to respond to a couple of things. First is the idea that professional norms are not part of or shouldn't be codified in the law. I mean, I'd suggest that happens all the time.

I'd suggest it also happens in the First Amendment context, especially when you think of when you're trying to prove libel and you're defending and you have to, as a reporter, prove that you were following established journalistic practice, that you were not reckless. That's part of the First Amendment law.

There's no categorical right to do whatever you want, even it's for a noble purpose,

if it causes -- if it violates some other statute. Other examples, a notable example where trade usage is incorporated broadly into a variety of situations is Article 2 of the U.C.C., where course of dealing, usage of trade, etc.

What we believe the controlled environment did was to simply incorporate what the kind of thing that -- things that the responsible folks at this table tend to do when they do security research. And that's why we, you know, we supported the inclusion of that language, we didn't object to the reissuance of this particular exemption, and welcome dialogue on how to construct that particular point better.

But the premise of what's, of that particular attack is not one that I think we accept.

The second thing that, when crafting this exemption, and this goes to the overlapping remedy problem, I mean, that's an interesting policy question. I'm not sure that once you get, it's one thing to discuss it in terms of a First Amendment analysis.

In terms of this statute is not narrowly tailored because there are all these other laws to deal with that, I'm not sure that's the way the

analysis is supposed to work. I think it more has to do with this statute cuts off the following types of speech, and there are other ways to do it.

And so if you get sidetracked, my concern is that if you go down that road too far, you're going to get sidetracked into things that aren't necessarily relevant to what the statute charges you to do.

MR. GEIGER: So the conversation has bled frequently into the question of other laws, and in particular --

MS. SMITH: Yes, I think we're there, and you should make your point.

MR. GEIGER: Yeah, I mean, it's hard to know, but it keeps coming up. But I also think --

MS. SMITH: We're definitely on the other laws about --

MR. GEIGER: --- underpinning a lot of the discussion, from our perspective, this is probably the most critical change that you could make to this exception. There is a tremendous amount of uncertainty that is foisted upon researchers because of that requirement that all other laws be adhered to.

And it's not just the CFAA. The CFAA of

course gets a great deal of attention, and it's certainly relevant. But we're talking about every state law -- and not just computer crime laws, we're talking about environmental laws, you know, driving safety, etc., etc., it's everything.

And in, I'll give you a specific example of a state law that directly implicates common research. Maryland, so just across the border. In Maryland it is a crime to even attempt to identify an access code. Separately, it's a crime to distribute or circulate that access code to an unauthorized person. I just say that identifying the access code is without authorization.

And this is a common feature of, for example, IoT research, where finding a hard-coded password or a very weak password then leads to vulnerabilities that cause serious flaws in IoT. And this was a feature of the Mirai botnet. We actually see this in home security and lots of other types of devices.

And does it suppress the research? In Maryland, it does, right? In Maryland, it would. But you know, if you go across the border, then I suppose you can escape it. So is there a way to work around it? Sure, but should that be the analysis?

And to the question that Kevin asked and that, sorry, Mr. Amer, and Ms. Walsh had responded to, the issue is the uncertainty, but also that DMCA compounds those penalties, right. So and the private right of action compounds it further, right.

So if you were prosecuted for a violation of one of these laws and you'd be facing a fine under that, then potentially a fine under DMCA. But the statute and the exemption currently don't say that there's needs to be a conviction, it just says that there has to be a violation.

And so it's an open question, and one that worries us, whether or not then you are conferring a private right of action to copyright holders, even in instances where prosecutors are not actually pursuing a charge.

MS. SMITH: Could you provide, like is there a specific example you can give where you say, well, you know, I'm running a risk of a gray area of a Maryland law or a specific other law, and I'm willing to roll the dice on that, but 1201 is, you know, coupled with that, okay, I'm going to step back? Is there anything specific?

Because I think one question we have is -- goes to adverse effects. If it's already

prohibited by separate other laws, it's not clear that 1201 is really restricting this activity.

MR. GEIGER: The private right of action question with 1201 distinct from criminal laws is, does make 1201 a unique problem distinct from those criminal laws. Now, what happens --

MS. SMITH: But I'm saying in your --

MR. GEIGER: What happens in these conversations is that it is the compounded uncertainty. I haven't been privy to a conversation where someone says, Well, it's this plus 1201, and it's just, it's too much.

What does happen though is saying, well, I don't think that I'm going to be facing a criminal charge for this, but I might be facing a private right of action, and that is scary.

Because a company may have more incentive than a prosecutor to go after an innocuous problem that is security research-based that might then harm their reputation. Prosecutors in some cases have shown greater discretion in our experience than some companies.

And on the question of legislative history, which Mr. Amer brought up, the conference report has that door lock analogy, which I know the

BSA brought up as well in their comments. I would argue in 1998, Congress did not contemplate just the plethora of laws that security research now implicates, right?

Security research has become completely decentralized. There's a machine in everything now. And so the number of laws is well beyond CFAA. That door lock analogy, which is, really unless I missed something, was the bulk of the discussion on this other law's question.

That door lock analogy goes to the question of consent and lawful acquisition, which I think the Copyright Office has tried to accommodate in the temporary rule. So I think that the legislative history had not thought about things like password disclosure.

MS. SMITH: Well, but I think you're asking us, or we are being asked to remove consent and the acquisition limitations as well, to remove basically all limitations, aside from it being security research.

So just to confirm, you're not, you are or are not aware of a situation where despite another law precluding it, there's been a determination not to go forward with a research project just because

of 1201. I don't know if that makes sense.

MR. GEIGER: I can't say that I am, actually. I will say that it has caused creative work-arounds, and it does restrict the venue where the research may be performed. But that is, it has come up, particularly the private right of action.

But in many cases what we see is that somebody then tries to, as I said, tries to shift where it occurs to avoid a law, or -- sorry?

MS. WALSH: Yes, they're going to do the project they're going to do.

MR. GEIGER: Or they did it elsewhere, or they did it elsewhere. I will also just note that these laws, when it comes to the uncertainty, it's always changing, right? So the uncertainty that exists for researchers is constantly in flux.

State laws are changing very quickly. Georgia, this is happening right now. And even, they're passing a new computer crime law that removes mens rea, it removes any sort of changing of data as a requirement.

And the legislators themselves, we've been listening in on the hearings and speaking to the legislators, they themselves are not entirely sure how security research fits within exceptions

that they've created. There's been a lot of speculation about that. And so even if the legislators don't know, it is -- I think it is very, very difficult to say that security research ought to know.

MS. CHAUVET: But isn't that uncertainty still going to exist, even if you have the applicable law limitation dropped from the 1201 exemption? I mean they, you're still going to have to abide by these other laws, right? So if there's uncertainty about those other laws, that uncertainty is going to continue, whether or not it's referenced in the 1201 exemption or not.

MR. GEIGER: The uncertainty is going to continue, but the -- at the very least, the private right of action and the compounding effect of DMCA would not be present. For DMCA, I mean, let's not overlook the potential effect that a private right of action would have on the researcher.

I mean, it's not just you know, $2500 in statutory damages. It's also the potential for impounding equipment, attorney's fees, discovery costs, and so forth. And for a researcher, particularly one that is not backed by legal representation, that's completely devastating.

MS. SMITH: Thank you. So to sort of keep the discussion going back and forth, I know that Professor Halderman's had his placard raised for a while. So if you could answer the same question I asked Mr. Geiger, and then we'll go to Mr. Englund.

DR. HALDERMAN: Well, I wanted to point out a scenario that I would worry about even more, and something that's actually come up in my work, is cases in which we are being very careful to comply with the legal requirements on security research, but an aspect of the legal code that has no real bearing on security comes up.

There was a case fairly recently where I was doing research with some devices that we had bought, and the grad student who plugged them in used an improperly rated extension cord. And this was found to be in violation of the electrical code.

Is that then, after that is there and documented, that in the process of doing the research, we had inadvertently violated the law about the electrical code, going to expose all of that research and the fruits of it to liability under the DMCA?

MS. SMITH: So have you been stopped in

doing any research where you think it is in violation of another law, but it's really the 1201 -- the private right of action or compounding effect, as Mr. Geiger said -- that is making the difference, as opposed to knowing of the other law, including this electrical socket?

DR. HALDERMAN: The, it certainly causes me to have to go and talk to the attorneys and have much more careful conversations about whether we are safe -- my students and I are safe --- in proceeding with the research.

I am a researcher in a relatively protected position, being one, someone operating out of a public university with the resources of that university and its legal department behind me.

But I think someone who is not in that position, someone who is a researcher operating privately, or an amateur investigator who is nevertheless contributing to the safety of the public, might be in a much worse position.

MS. SMITH: Mr. Englund.

MR. ENGLUND: Yeah, I'd just very briefly like to agree with the thrust of the questions coming from the Copyright Office for the last few minutes and disagree with some of the

responses coming with -- from the proponents.

There's been talk from the proponents about the Office extending the effect of other laws or creating a private right of action, and that's exactly backwards. Congress created prohibition on circumvention, and with it a private right of action. The Office is being asked to grant an exemption from that.

And there's a statutory standard for when the Office can grant such an exemption. That's when the prohibition in section 1201 is adversely affecting a non-infringing use. If, and the sort of lead on the non-infringing use is unlawful, it isn't section 1201 that's adversely affecting it. So it should not affect anybody's behavior to keep this provision in or take it out.

But highly consistent with the statutory standard that governs the action that the Office has to take to leave it in. Because there can't be an adverse effect from the prohibition in limiting activity that is already unlawful.

MS. SMITH: Another question related to that, and then I'll let Professor Reid respond to both questions, that, you just spoke about whether or not 1201 is acting as the adverse effect of the

causation requirement. But do you think in the instance where the activity that would be engaged in is barred by another law, does that affect the fair use analysis?

Such as like Harper and Row if you're doing something in bad faith.

MR. ENGLUND: Potentially. There is certainly judicial authority that indicates that the intent in good faith of that person engaging in an act is relevant to fair use. Obviously the four factors are nonexclusive. The courts have occasionally considered other factors.

So I think if somebody were engaged in unlawful activity, that could factor into the fair use analysis. I just don't think you need to go there because there can't be an adverse effect.

MS. SMITH: Professor Reid.

MR. REID: If I can respond and tie back to a point that was made a while ago, and I promise I'll get to this question of other laws in fair use. I want to get back to the notion that was raised about the First Amendment having been resolved in Reimerdes and other cases.

I think we're in a very different factual situation here, and it's one that really bears on

both the controlled environment and the other laws limitation and the other laws limitation, which is that security research isn't just about the circumvention. It isn't just about identifying the vulnerability, but it's about reporting that vulnerability out.

And in some cases, about an activity that is core to our democracy, right, determining whether a nation-state is hacking an election. Right, determining whether there are security vulnerabilities in the machines that are used to administer an election.

And in a case where permission might not be forthcoming and circumvention is not just one of the convenient ways by which you might obtain this very important information, it might be the only way to obtain this information. So in effect, 1201 serves as a gateway to effectuating First Amendment speech.

And to Ms. Walsh's point, the Copyright Office has got to identify, at a bare minimum to survive constitutional scrutiny, a really, really good reason for imposing these limitations. So the question is not in this case, and I think we've demonstrated some good reasons why you should get

rid of this, but you also need to independently identify a good reason to keep these limitations in.

Now, I appreciate on the controlled environment limitation Mr. Troncoso and others have suggested, we might adopt a very narrow construction of what controlled environment is and all of that sort of thing. But I would ask you to think about what exactly is the policy reason that the Office is including that limitation.

And what it sounds like is that policy limitation is every legal regime that somebody might use against a researcher if anything from something malicious to something that's an accident happens.

Likewise with this other laws regime, you are literally importing into the DMCA every other law, literally every other law. So that's everything from the Computer Fraud and Abuse Act, and if you've seen the *Sandvig* case in the last week, a law where there's an incredible amount of uncertainty.

There's circuit splits on virtually the definition of every single term in the Statute, all the way on down to the electrical code, which the building inspector is -- could theoretically show

up and enforce, but is never going to do.

So I think when you view all of these questions in light of the First Amendment, you have to say why are we importing every other legal regime into what's supposed to be a fairly narrow question, which is are there impacts on copyright infringement that are going to result from the circumvention of technological protection measures?

And there's nothing on the record to suggest that that's the case. And so I think, again, that's the reason that we're asking to remove both the controlled environment limitation and the other laws limitation.

MS. SMITH: Thank you. Did you want to speak to whether if activity was in contravention of other law, whether that would affect the analysis and whether the use is likely to be non-infringing or not?

MR. REID: I think in general the answer to that question is no. So the fair use analysis, again, we're looking at a transformative use, and in particular, one that is aimed at not impacting a legitimate market for the underlying copyrighted software. There's no interest in infringement being demonstrated.

And the question of whether that activity might, say, violate the electrical code, I don't think that's a winner that the, suddenly fair use doesn't apply because you've violated some local ordinance. So I think in general the answer to that question is no.

MS. SMITH: Well, what if it was, you know, this is obviously a sort of out-there hypothetical, but to do security research, we drop the limitation on, you know, primarily for security research and it's also to like, you know, steal money or something. Is that still likely not infringing?

MR. REID: I'm sorry, I'm not sure I understand the hypothetical. So the idea is someone who's going to commit some kind of larceny or something, and then is also on their way to that doing security research?

MS. SMITH: No, I guess they're engaging in circumvention and they're cloaking it saying they're doing security research.

MR. REID: So this is an argument that's come up, to the best of my knowledge, in every single hearing back to 2003, since the first security research exemption was adopted, was the idea that this is somehow cloaking some kind of piracy or some

kind of illicit activity.

To that I can only say the folks who are represented on this panel here are never engaged in that kind of activity. But moreover, there's never been any assertion in the record of any actual incident of anyone within the ambit of the exemption or anyone adjacent to the exemption actually invoking the exemption to get out of something. To your point, theft, to the point that Mr. Williams and others have raised, copyright infringement.

In fact, there's very little evidence in the record that section 1201 is ever used at all to deter just about anything. So the idea of maintaining the existence of all of these limitations in the law when there are such profound First Amendment interests at stake on the basis of what are, frankly, completely hypothetical concerns that in more than a decade and a half have never been substantiated we really don't think is warranted.

MS. SMITH: Thank you. Mr. Hall.

DR. HALL: Thank you. So I'm going to stick to the CFAA specifically since it's called out specifically. The CFAA prohibits exceeding authorized access on protected computers.

Protected computers is a very broad definition. It's basically anything connected to a network capable of affecting interstate commerce.

One thing that's been changing quite a bit is software is also increasingly cloudy. Increasingly software is provided from something that's off the device. And so there are things like cloud-enabled door locks where, yes, you have a key, but you also have a way to use an app that will authorize via cloud service the door to unlock for some period of time.

The other laws limitation here allows companies to add liability under two statutes to their threat arsenal, essentially contract enforcement. You know, companies can effectively use pretty aggressive terms of service and user license agreements as access controls to the access controls.

They can use both the breadth of CFAA's coverage to preclude research that would otherwise fit within the exemption.

The research report that we submitted as part of the record shows that disclosing vulnerabilities is one of the riskiest things that a security researcher can do. That's often the

moment that things get legal and heated very, very quickly. Nearly every legal threat on record is triggered by an attempt to disclose these kind of research findings.

But that means that it's incentivizing researchers to keep their work quiet. And when they feel safer keeping information to themselves, no one benefits.

And so if we can remove the porting of a vast quantity of other laws, including the CFAA, which is just this miasma, into the calculus security researchers have to make with circumvention of TPMs, that would dramatically improve the state for security researchers seeking to engage in those kinds of activities.

MS. SMITH: Thank you. Mr. Geiger, you can have the last word on this limitation, and then we'll start to talk about the last two.

MR. GEIGER: So this other laws clause it seems causes a great deal of uncertainty in both directions, right. So for researchers, but then also for concerned stakeholders, rights holders who, whether unintentionally or intentionally to introduce fear, uncertainty, and doubt, seem to regularly confuse this question of liability.

If you look through the record, this happens pretty frequently. The election providers talked about accessing election software on the computers of local election officials, right, creating a new threat that state, federal, state, and local government officials must defend against.

The National Association of Secretaries of State, they talk about unfettered election hacking activities if this were removed. SIAA, too, mentions being permitted by the DMCA to hack flying aircraft or building climate control systems.

There's a sense that -- one gets the sense that if other laws were removed, some stakeholders have the impression that then there would be no law, that it is a get-out-of-jail-free ticket for researchers.

And one of the concerns that we have is that the reliance and the attention on DMCA section 1201 is sort of preventing an evolution of regulation and making security researchers more aware of these other laws. And instead folks are just relying on section 1201 as their gatekeeper.

Absolutely the other laws apply, and security researchers should be made aware of that.

But the incentive to try to deal with security researchers in regulation, make them come to a compromise, which is happening in some places, but in many, many places it is not, and to put forth educational material. And on both sides, the incentive is taken away when 1201 is so easy to rely on.

To Mr. Englund's point about how other laws, that behavior won't change, I wanted to make very clear, behavior did change. Right, I mean, and I described it. And maybe Ms. Walsh had the right answer, that the research that I described did not -- was not able to go forth in the venue that it was originally selected. It did have to move because of what the law is.

So behavior does change. Now, you know, are there ways to get it done? If you have enough resources, possibly. But it does take some creativity. So it is absolutely chilled.

MS. SMITH: All right, thank you. I think given our time, we're going to move on to the last two limitations and discuss them in tandem. So the access limitation, the current regulation says that circumvention, the work should be solely for the purpose of good faith security research.

And the so-called use limitation is that the information derived from the activity is used primarily to promote the security or safety of the class of devices.

And I think both of these sort of go on a really broad topics words, this should be for good faith security research. And so I guess I'll just heave a broad question why these limitations are or are not important to keep.

I think BSA has said maybe some of this can be sort of misunderstood, I guess, that primarily to promote security doesn't mean only to promote security. There's been some concerns this might prohibit publication of academic papers.

And I'm wondering do any opponents agree with this, or do they think no, actually, the Copyright Office can clarify that post-circumvention in publication for in academic or other uses is permitted and not this -- and not prohibited by the current regulation. So Mr. Hall.

DR. HALL: I just wanted to get my tent up quickly to make a very small point, which is that -- and I think Andrea Matwyshyn's filing at some point made this point, which is that often the fruits of security researchers or other expressive works

like, you know, academic papers.

There's a really good example of one that is, you can check it out, it's called, Have I been pwned, P-W-N-E-D. And it's a way for you to figure out if you've ever been included in any data breach that we know about. And that requires you know, having fruits of the security research that are things like, you know, access codes and things like that that we can check against.

And so I just wanted to put a pin in the ground and say, you know, on some level, these are other forms of expressive works. And we've heard a little bit about that in terms of the First Amendment concerns.

But you know, specifically when we get to the solely useful for, that means you can't do the kind of work that I'm -- I like to do which involves taking the fruit of research and making practical tools that people can use to protect themselves.

Another example is the 500 million password list. Yes, there's actually a list on the internet of 500 million passwords. People like me can use that when we design systems to make sure that if you put in any password that we've ever known

has been breached before, we just say no, please try again. It may be pretty frustrating, but it's not as frustrating as you think.

So the solely --

MS. SMITH: But in that case, the circumvention is still for security research, right? So I'm wondering what?

DR. HALL: But the use you're making is not necessarily solely for those purposes, correct?

MR. TRONCOSO: And specifically to those examples, I don't think it's fair to characterize either as even implicating the DMCA, because the Have I been pwned example is an example where a researcher monitors sort of the dark web to see when people are selling or making available lists of people's credentials and gets them that way.

They're not sort of behind an access control, and then creates a database where you can essentially ping the database to see if --

DR. HALL: Not true. So I --

MR. TRONCOSO: We can go down a rabbit hole, but either way.

DR. HALL: Well, I was going to get to that, which is that, you know, often, when you're

doing this kind of research, you run into things like lists of credentials, like malware.

MR. TRONCOSO: I'm not questioning that a lot of your research does implicate the DMCA. The two examples, though, that were just provided --

DR. HALL: So a lot of the passwords that were produced from that 500 million list are specifically mined from devices that have technology protector measures on there.

MR. TRONCOSO: For, okay, I'll --

DR. HALL: I mean, anyway, so --

MR. TRONCOSO: I just also wanted to jump in quickly because it's I think a critically important distinction that there's an access limitation and a use limitation. The access limitation has a solely in front of it, the use limitation is not bound that strictly. It is used primarily to promote the security of software.

I think in virtually every example that is in any of the papers that have been submitted as part of this proceeding, all of the research we're talking about is done for purposes of security research. Otherwise what is the, you know, what are we here to talk about?

The question is whether you can take

knowledge that you've derived from that research and use it in an educational setting. That's where the use limitation comes in, and as long as it, you know, you're primarily using that information to promote security of the class and it's not used in a manner that facilitates copyright infringement, again, I don't think that these types of uses are implicated.

And I think that there's, in fact, in the 2015 recommendation, the Copyright Office made reference to the fact that sort of some of the activity that was involved on that record would involve follow-on sort of educational uses.

So again, I just don't want to get us into a situation where we're reading these things so narrowly and in such an unreasonable manner, and then hanging our hats on that to say, look, we need to change the 2015 exemption because it's possible someone is going to misread that statute. Ergo, we should just not have any limitations at all in whatever 2018 exemption is recommended by the Office. That's sort of my principal concern.

MR. AMER: I mean, to pick up on that -- I mean, that's helpful. You know, to the proponents, I would ask, you know, is the concern

basically that this somehow could be read to -- I mean, I think you alluded to this in your comments, that this somehow governs the conduct of third parties and what they do with the research that you publish?

I mean, to me that seems a little farfetched just given that what this is talking about, you know, this is providing an exemption for the party that is doing the circumvention and it's laying out conditions that are required to be eligible for the exemption. I don't know that it is reasonably read to --

DR. HALL: Isn't the case that if I publish research, and that research is then used subsequently to infringe copyright and it's not something that I necessarily thought of or could predict, that then that affects my exemption under, my liability under this exemption? I think so.

MR. AMER: You're saying that you're --

DR. HALL: So say I publish a paper or something and within it it has some morsel someone uses to mint whole copies of the software I studied or something.

MR. AMER: I mean, I think it would turn on, you know, whether you as the circumventing

party, as the researcher, were primarily, you know, whether your intention was primarily to promote the security or safety of the class of devices.

DR. HALL: I would hope so.

MR. GEIGER: The question is where the word primarily appears in the rule, right? I mean, it says and is not used. It seems broken off from primarily as the modifier. And I mean our filing recommended putting primarily in there again to make clear that those third party scenarios, which are very real for security research, because a lot of vulnerabilities are publicized, and they can, you know, if they're not patched they can be used for good or for ill.

But to make clear that the -- it's not on the researcher if an unintended and unforeseen third party then goes and uses it in a manner that it infringes on copyright infringement. I'm sorry ---

MR. AMER: So this language, as you know, tracks the statute. This is the phrase that appears in 1201(j). You know, I suppose we could, if it were in active voice, I mean, would it say that the researcher does not, you know, that the researcher acts primarily to do that?

MR. GEIGER: So our suggestion is simply to include the word, and others may disagree, but our suggestion was simply to include the word primarily again in that last part of the phrase. So that it is primarily not used for copyright infringement.

And in our experience, and most cases of security research, the fruits of the research are used primarily for computer security. And you know, so you will often make a vulnerability publicly available through several different systems, CVSS, and which can then be used for penetration testing to improve security.

But they can also be used by individuals who are fishing around for old vulnerabilities that haven't yet been patched. And our concern is making sure that the research is not suppressed because of that particular scenario. I think it's a relatively easy fix.

And to the, just to an earlier point that was made about pwned to owned, I interpreted what Joe was saying as emphasizing for the record that security research is not just a non-infringing activity. That it is also, that it implicates copyright because research itself spawns a host of

other creative works.

I mean there is the research, there's academic articles, journalism, that, you know, that comes from the research. There's further research that is conducted. And software patches that, and then new operating systems that avoid the old vulnerabilities. And often when we're talking about section 1201 being used in these contexts, it's to suppress the research, which then in turn suppresses those creative works.

Now, in fact, in most cases, I would argue that 1201 is asserted to stop the publication. It's not even the research, it's just that they don't the word to get out, which is itself spawning other creative works. So it is not just a security research as in something that doesn't implicate copyright on the researcher's side either.

MR. AMER: I'm not sure who was next. Mr. Freeman.

MR. FREEMAN: I'm actually going to go further on that because I, so I'm -- this is actually the part that I am least comfortable with in the current wording, and the thing that I actually was most wanting to be here in order to address.

I actually am not sufficiently

comfortable with just adding primarily. And the reason why is that it is just so difficult to determine what somebody's going to do with information.

You might think that people are going to use it for all sorts of things, and it turns out that the primary thing that people end up doing with it ends up being something that's infringing. And the reason why this ends up actually really ends up mattering in the wording is, Mr. Troncoso mentioned that the way word solely is.

But the word solely is actually in the text twice. So the word solely says it's solely for the purpose of good faith security research, and then good faith security research is defined. It includes the word solely there, but the word solely was already now applying to that entire definition.

And then if you read like that definition, essentially just in its like plain wording of it, it states that purposes of this exemption good faith security researcher -- research means accessing, yada yada yada, where that activity is carried out in a controlled environment designed to avoid any harm, yada yada yada, where the information derived from the activity, yada yada

yada, is not used or maintained in a matter that facilitates copyright infringement.

And so you end up with this scenario whereby somebody has performed an infringing activity, but that is exempt because it was for security research. It was actively designed, when the person was doing it, they really did truly have the purpose of good faith testing investigation, their goals was to do security work.

And then they go and they publish the research work on it. And it turns out that the way that they -- the thing that they actually ended up tampering with also happens to be the primary mechanism that, for example, an iPhone uses in order to do the encryption of the application.

And it wasn't even clear when you were doing it that was what was going -- that would mean you were enabling that. But now you have facilitated that infringement.

MS. SMITH: Wouldn't the circumvention be solely for good faith security research in your example? I mean, I'm sort of sympathetic.

MR. FREEMAN: But the information was -- the problem was is that by having published that information, you are now in violation of that the

information derived from the activity, right, is not --

MS. SMITH: Right, so we're past the solely limitation though.

MR. FREEMAN: Used or maintained.

MS. SMITH: Right, you would --

MR. FREEMAN: The solely actually applies to that entire clause, because back in the definition it says that computer programs where the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates solely for the purpose of good faith security research.

And then good faith security research is defined. So the solely actually applies to everything related to good faith security research, not just the second usage of solely, which applies in (7)(2).

And so what we're looking at here is trying to strike both. And I remember specifically in the petitions it was stated that our goal was to strike both the usages of solely, not just one of them.

MR. AMER: Well, but I mean, you know, even if this use clause could be read somehow to

apply to the conduct of third parties, which I think is questionable, you know, you have primarily there. So I mean, you know, that gives you some additional flexibility.

I mean, if there might be some circumstance where someone down the line, some third party uses your research to facilitate copyright infringement, you know, isn't that sort of that possibility? Aren't you protected in that circumstance by the fact that it's a primarily and not solely once again?

MR. FREEMAN: So first of all, I will argue that I actually believe that this clause absolutely was put here in order to work on the third party infringement that occurs down the line. That is why it is about the information and the way that that information is maintained after the activity.

It is on the information that was derived from the activity, the way in which it was maintained. And that that maintenance of that information could end up facilitating copyright infringement.

Then, the usage of the word primarily as it currently stands in the documentation is limited to the primarily to promote the security

and safety. It is not applicable to the use or maintain. That was an addition, which is what Mr. Geiger was hoping to add, is to put the word primarily on and is not primarily used or maintained in a manner that facilitates copyright infringement.

But I don't think that actually goes, that that actually is sufficient in a way. Because that still leaves open the possibility that the third party infringement that ends up occurring after the point of fact of the publication of the information that now has been poorly maintained from the activity ends up getting used in a manner that happens to be primarily for infringement.

And that was in no way something that anyone would have determined at the time when they were doing the research primarily for the promoting the security and safety of the class of devices.

MS. SMITH: Mr. Williams, did you agree with that reading or did you otherwise want to speak as to how these limitations are relevant to, from a copyright owner's perspective?

MR. WILLIAMS: Sure. So the clients I represent, preserving free speech rights is kind of one of the foundational reasons they exist. So

we're not here to try to step on anyone's free speech rights, and we're not here to try to oppose publication of scholarly works.

On the other hand, preserving copyright protections, and the cases have said preventing unauthorized access to copyrighted works is a countervailing free speech interest. And if you look at the cases I referred to previously, Reimerdes and Corley and Elcom, they'll all discuss that.

And so I don't think the right place to draw the line is whether -- is to say if any third party is involved at all, then that's not on the researcher, for lack of a better word.

Because if you look at these cases, and particularly at the dissemination early on of DeCSS, it was very clear, even though some of them said, well, we're just researchers, we're just doing this as a point of study, they were setting up websites to intentionally attract other people to download a product and then strip circumvention.

So some of that did involve downstream usage, but was also found by the court to be unlawful, and also unlawful in a way that was perfectly within the bounds of the First Amendment.

So I think you have to be careful there.

I'm not opposed to trying to come up with a way to draft this that preserves people's academic rights and right to engage in study and publication, but that also does not enable that kind of widespread dissemination of code that will immediately get people access to copies of works in the clear when they haven't paid for those copies.

The courts in these cases have a lot of metaphors, but you know, one was a metaphor of an epidemic that can't be cut off at the source, because once it's released, it spreads virally, for lack of a better word. And that's what can happen in these cases if misuse is occurring.

So I just think you have to be careful there. Personally, I don't think adding primarily where they're suggesting it would be a good idea, although I think I understand what they're getting at.

But to say that it's not primarily used or maintained in a manner that facilitates infringement, to me that would imply that if 90% of the time they're not engaged in infringement, but then ten percent of the time they did themselves even directly engage in infringement, maybe they'd

still be covered, which I don't think would be your intent.

So if you do try do something with the language that, you know, protects good faith activity, I don't think that would be the best drafting.

MS. SMITH: Thank you. I think we're getting tight on time, so maybe we'll just start going back and forth on this topic. So I think Professor Halderman, you were up next. Mr. Kimata, okay.

MR. KIMATA: I just wanted to quickly say that even I didn't turn to the discussion at 1:30, and we've been talking about it for 15 minutes. So the ambiguity around this discussion is an already adverse effect that really does chill research in this area.

MS. SMITH: Okay, how about Mr. Zuck.

MR. ZUCK: Thanks. One thing that's probably you don't have time to go into is that there are adverse effects to copyright holders and public safety for countervening technical protection measures, right. I mean if I'm hacking a drone or something like that, I can cause damage to public safety.

So there is a counterbalancing concern here. And so what this ends up being is balance of risks. And completely understandably, security researchers would like to eliminate all of their risk, all of their responsibility, and all of their accountability in this situation. And I would want that too.

And so what the net result of that, though, is shifting it all to copyright holders. Well, we published it, so if you didn't patch it in time, if you didn't get all your customers to download patches in time and somebody used it to hack your drone, that's not my fault. I'm just exercising my First Amendment right to publish my research results in a way that easily facilitated use by a third party.

So I think that there has to be a balance of risks here. I think the current exemption strikes that balance of risks here, and I think it's inappropriate to request that all my risks and ambiguities should be removed at the expense of the copyright owner that now needs to assume those risks to public safety. Thanks.

MS. SMITH: Ms. Walsh.

MS. WALSH: So first I want to be clear

about some of the purposes that are potentially not encompassed under solely for good faith security research but are nonetheless often engaged in by academic researchers. And one of those is teaching, another is publication.

So often Professor Green works as part of a team with students, and part of the mission is to educate those students. With the solely limitation, because solely is such an extreme word, it creates the possibility that a rights holder would argue if you had some additional purpose that's on equal footing or even not on equal footing because it's not the same as primarily, it's not in order to, that having those additional purposes which are also valid and non-infringing puts you at risk of falling outside the exemption.

That's why we prefer the language in the NTIA's 2015 recommendation in order to conduct good faith security research.

So not to entirely litigate the First Amendment questions here, I'll just note there's a circuit split on how section 1201 interacts with the traditional contours of copyright law, whether there's a requirement of nexus to infringement.

The cases that my colleague is referring

to predate Eldred and Golan for the most part, I'd refer you to our briefs in Green v. DOJ for the details of the First Amendment argument on that count.

DR. HALDERMAN: Can I just say that as an educator, I'm also concerned about 1201's effects on my educational speech.

MS. SMITH: Mr. Mohr.

MR. MOHR: I think, well first of all with respect this specific -- I'm sorry, I keep forgetting to do that. With respect to the use limitation, we have many members who are publishers of journals and so forth.

This provision, the limitations in this provision have to my knowledge never interfered with any of their activities on a whole myriad of subjects. Many of those have, in fairness, have nothing to do with copyright whatsoever or circumvention, but some of them do.

The second thing I would say is, you know, if you're going to look at this, and I'm not sure you need to, but in my mind the right way to look at this is as an intent requirement. In other words, that's really what you're trying to do here is if the elements here are, what does good faith

look like.

Well, good faith looks pretty bad when 99% of everything that a particular device is used for is an infringement or rather a circumvention of access controls for the purpose of infringement. It -- there's a suggestion there that maybe the reason the circumvention was performed was perhaps not a legal one.

I think it's appropriate for the exemption to take note of what happens afterwards. That's it.

MS. SMITH: Thank you. Mr. Freeman.

MR. FREEMAN: So one of the fun things with this law goes back to the earlier comments that are about good actors in the community versus bad actors in the community. And so the idea that oftentimes when we do security research and we're targeting a product by a company like Apple, we end up feeling somewhat emboldened.

But when we're targeting products that are by other companies, I'm just going to point out Sony, we oftentimes are just very afraid.

And so you end up with scenarios, like you can bring up a concrete example here of work that was done with the -- on Apple products, where

people were reverse engineering for purposes of determining the security implications of Apple iMessage, the messaging protocol that people can use in order to talk to each other.

But the mechanism by which that system is protected is Apple Fair Play, which is the exact same obfuscation technique which is used in order to obfuscate the anti- -- sorry, obfuscate the encryption algorithm that is used in order to encrypt applications on the iPhone.

And so the work that was published on iMessage ended up being utilized by people who were trying to understand and reverse engineer that encryption algorithm on those applications. Now in this case with something like Apple, I would not necessarily feel that concerned going in and reverse engineering something like iMessage.

But if when people contact me about doing any form of security work or any type of research work related to anything involving Sony Online or anything involving any of the, you know, any of the products that are released for any video game console really, when people contact me about things related to General Motors vehicles, when people contact me about -- I tell them, no, don't do there.

Like if you've got work you can do, go work on something that is by somebody like Apple or Google that's probably not going to burn you on that.

But we've seen people get burned on 1201 from some of these other companies. We see those people, those other companies show up at these panels in order to argue why these exemptions should be more toward limited in order to make certain so they continue to have those powers of control.

I do see this kind of chilling effect occurring in the security research community related to these sections, and that's why I am very concerned about making certain that we remove some of these restrictions on this exemption.

MS. SMITH: And has that happened, for example, with automobiles after 2015?

MR. FREEMAN: Well, so I was bringing that up, it'd be good if, we have an explicit exemption on automobiles now. But I'm --

MS. SMITH: Right, we're discussing whether to change it.

MR. FREEMAN: I'm sorry, I was -- I should not have brought up the example. I'm sorry, I will take that back, of General Motors. I'm just

used to General Motors being the enemy, even showing up for the jailbreak panels and saying that I think you're classifying a general, all-purpose mobile computing device, that sounds like a car.

And so, but yes, for all these other devices that we do not currently have exemptions for.

MS. SMITH: Thank you. Mr. Geiger.

MR. GEIGER: I wanted to quickly respond to the concern that was raised about that used or maintained in a manner that facilitates copyright infringement, and the concern that if it was 90% used for security and then ten percent used for copyright infringement, that then the researcher would still be covered.

And in that scenario, I think that's an incorrect read of the exemption. Because it still has to be -- the circumvention still has to be done solely for the purpose of good faith testing, investigation, and/or correction. So your circumvention of it must still be used for that.

What we are concerned about, again, is third parties who then take that information and can use it. I mean, as it is now, because of where the placement of primarily is and because we don't

attach it to that last part of the sentence, it is an absolute bar, it seems, on any type of copyright infringement.

MS. SMITH: So if your element were taken and primarily was also attached to the second part of the, you know, the final part of the clause, that's what I think you're suggesting. Is that right?

MR. GEIGER: So I take the point of some of my colleagues that it may not go far enough in every scenario, but in our opinion it does mitigate it. And you know, the very common concern that we have is submitting vulnerabilities to, for example, the CD database, and then it becomes public.

And then these vulnerabilities are often not patched by companies that are even aware of them, and then can be used for purposes that are good or purposes that could implicate copyright. But those are all done by third parties, not the researcher. The researchers are generally almost exclusively acting for, solely for the purposes of good faith testing and security.

MS. SMITH: Okay, thank you. So we really appreciate everyone's time and participation. I think this is sort of last call

because we're well over. So if you have your placard up, we'll get to you. But Mr. Troncoso.

MR. TRONCOSO: Yeah, on the use limitation in particular, I just want to point out that there's an amazing amount of agreement from everyone who submitted comments that sort of coordinated vulnerability disclosure processes are very important to mitigating potential third-party risks. And ultimately we're all here to improve security, and we all sort of agree on this point.

We also agree that coordinated vulnerability disclosure is not something -- it's sort -- it's more of a norm than a science. And so pursuing some sort of different rule that is going to be stricter I don't think is necessarily in the interest of anyone in this room.

So again, I would just sort of leave you to consider you know, I'm open to sort of some wordsmithing where you think that there really legitimate sort of potential ambiguity in the 2015 exemption, but I would discourage you from sort of changing elements of the 2015 exemption unless, you know, a reasonable reading would give rise to those ambiguities. Because I think in several instances, you know, I'm not sure that that's really the case.

MS. SMITH: Thank you. Mr. Williams, then Professor Halderman.

MR. WILLIAMS: Yes, sorry, I don't want to belabor this, but just to respond to what I think it was Mr. Geiger said. So first he said, well, it wouldn't be a problem to put primarily where he's suggesting because you would still have the fallback that it's solely for good faith research. But they want to delete that, so that would presume that you do not grant that part of the requested expansion.

And then the second piece of it is, you know, even if they were not ten percent of the time directly engaged in infringement, if they were ten percent of the time actively encouraging other people to engage in infringement in some of the ways at issue in the cases that I referenced, that would still, I think, cause a problem.

So again, I think what he's put forward is a good faith attempt to try to revise the language in a way that gets to where he wants to be, and I don't think he's trying to encourage infringement, but I just don't think the drafting suggesting works quite well. And I'd be happy in post-hearing letters to weigh in on any thoughts on how to draft it better.

MR. GEIGER: Just to be clear, we have not -- Rapid7 has not asked for the solely for a good faith testing language to be removed. That's just our position, and I understand that others have, and you know, and I'll let their arguments carry forward. I'm not speaking in opposition to it, but we have not asked for it to be removed.

MR. WILLIAMS: Okay, my apologies.

MS. SMITH: Professor Halderman.

DR. HALDERMAN: To wrap up, I would like to just return to the subject of elections one more time, pointing out again that we are in a critical election year, that 2020 is around the corner. And that security research, especially research by individuals working without authorization of voting machine manufacturers has been absolutely essential to uncovering vulnerabilities affecting many kinds of American election equipment and getting those vulnerabilities fixed.

So the existing exemption and its inclusion of voting machines has been very supportive of that, I'm grateful for that. And I hope that an even more expanded exemption allowing further testing of voting machines, even in environments that are not necessarily the

controlled environments that look like a laboratory, but could be other environments that still protect the safety of the general public is something that you will consider.

MS. SMITH: Thank you. Do you have any suggestions as to I guess what would that look like. I assume it wouldn't be conducting research while voting was going on, right?

DR. HALDERMAN: Right. Well, I think the critical thing is that the research is following the norms of protecting people from harm, and not that the research is conducted in any particular kind of laboratory setting.

MS. SMITH: Thank you. Looks like Mr. Hildebrand.

MR. HILDEBRAND: Yeah, if you are considering any changes to the access and use language, we just would like to request the opportunity, that it hasn't been addressed in the initial comments, the opportunity to have post-hearing comments on that as well.

MS. SMITH: On which specifically?

MR. HILDEBRAND: On the access and use limitations.

MR. REID: Just to clarify, some of the

previous discussion seemed to contemplate that there might be some changes around how that exemption is formulated, and just to underscore the notice of proposed rule-making purported to renew the existing exemption.

So I think it's critical, just as an administrative procedure and notice to all of the parties in the room here, that everybody gets a chance if the Office is doing that's not been teed up by the record, that we get an opportunity to comment on it.

MS. SMITH: Yes, I would say typically the Office, if they have issued post-hearing letters, they have done so to every participant on the panel list. Mr. Englund.

MR. ENGLUND: Thank you, just to very briefly respond to Professor Halderman. The election systems providers did not oppose renewal of the existing exemption. The Register's already said she's going to recommend that. So clearly there is some independent security research with respect to voting machines that is permitted.

We do oppose and think it is unnecessary and inappropriate to make changes to that. And at one point Mr. Halderman referred to it as the

controlled environment. I think it is possible, as discussed earlier, that there is just semantic disagreement here about what means.

Certainly the Def Con voting village that's referred to in the comments did not take place in a laboratory in the sense that it had stainless steel countertops or something. It seems like a controlled environment to me. It was not a live election.

And so whatever you do here, it ought to be very clear that hacking voting machines during real elections is not permissible. And despite the fact that simply deleting that requirement might permit that.

And as Dr. Halderman said, obviously this is an election year. But, and had an election year last year and the year before. But all the intelligence information, security information that's available to my clients and me is that no actual voting was compromised in the 2016 election. And I think it's a mistake for the Office to think that what will save the next election is having people hacking voting machines.

There are many layers of security that are created by local election officials backed up

by security that is built into the systems that are used in voting, including TPMs that are relevant to this proceeding, and also federal assistance through the Department of Homeland Security and Election Assistance Commission.

It is not the Copyright Office's job to ensure the security of the next election by granting the exemption that's been requested here.

MS. SMITH: All right, thank you, everyone. A lot to talk about. Appreciate it. Thank you.

(Whereupon, the above-entitled matter went off the record at 2:02 p.m.)