LIBRARY OF CONGRESS

IN THE MATTER OF:)
)
UNITED STATES COPYRIGHT OFFICE)
SECTION 1201 PUBLIC HEARINGS)

Pages: 429 through 581

Place: Washington, D.C.

Date: April 8, 2021

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

LIBRARY OF CONGRESS

IN THE MATTER OF:)
)
UNITED STATES COPYRIGHT OFFICE)
SECTION 1201 PUBLIC HEARINGS)

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

Thursday,
April 8, 2021

The parties met remotely, pursuant to notice, at 10:33 a.m.

PARTICIPANTS:

Government Representatives:

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

Panelists:

STAN ADAMS, Center for Democracy and Technology
J. ALEX HALDERMAN, University of Michigan
KATE McCLELLAN, University of Southern California, Gould School of Law, Intellectual Property & Technology Law Clinic
CHRIS MOHR, Software and Information Industry Association
JEF PEARLMAN, University of Southern California, Gould School of Law, Intellectual Property & Technology Law Clinic

Panelists: (Cont'd)

MORGAN REED, ACT |The App Association
BLAKE REID, Samuelson-Glushko Technology Law & Policy Clinic at Colorado Law
WILSON SCARBEARY, Samuelson-Glushko Technology Law & Policy Clinic at Colorado Law
DAVID J. TAYLOR, AACS LA & DVD CCA
CHRISTIAN TRONCOSA, BSA | The Software Alliance
J. MATTHEW WILLIAMS, Joint Creators and Copyright Owners
AARON WILLIAMSON, Software Freedom Conservancy
KEON ZEMOUDEH, University of Southern California, Gould School of Law, Intellectual Property & Technology Law Clinic

P R O C E E D I N G S

(10:33 a.m.)

MS. SMITH: Great, I think we are all here. My name is Regan Smith. I'm General Counsel of the Copyright Office. We are on day four of our hearings for the § 1201 rulemaking, and this session is Proposed Exemption Class 13 regarding adjustments to the current regulatory exemption for security research.

So I think I most, but not all, people may have watched previous sessions, but just to go through a bit of how it will work, the Government participants will be asking questions, and if you wish to speak, we have found it works a little bit best if you can you use the Zoom "Raise Hand" feature. But, if that's not working for you for one reason or the other, you can raise your hand in the physical world and we'll see you, or indicate in the chat.

We do have a lot of issues to cover and so we'll try to provide a brief roadmap and make clear what the questions are. But, if you can please try to stick to a short answer to the question posed, I think that will help us clarify and refine the record that we have. We have read all of your comments. We appreciate those comments, and we're looking forward

to building on that through today's oral discussion.

And we have three sessions today, so if you are watching, it is the same link available. You can stay on it. The last session is what is called the audience participation session, so if anyone who wishes to speak on a particular class if they're not a panelist, you can sign up using the SurveyMonkey link which is being provided in the chat now. I think our sign-up cutoff for today is at 12:30, although we will have another audience participation session April 21, which is the last day of our hearings. So we're asking that comments for those sessions be limited to around three minutes on any of the topics at issue in the rulemaking.

For those who are panelists right now, keep in mind that this session is being live-streamed, and it will be recorded for posting on copyright.gov as well as transcribed by a court reporter, so please try to speak clearly and mute your audio when you are not speaking.

So now I think, from the Government side, we will introduce ourselves. If we could have Mr. Amer, Mr. Greenberg, and Ms. Kern.

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

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

MS. KERN: Melinda Kern, Ringer Fellow.

MS. SMITH: Thank you. And Mr. Zambrano Ramos.

MR. ZAMBRANO RAMOS: Hi, everyone. This is Luis Zambrano Ramos. I'm a policy analyst in NTIA's Office of Policy Analysis and Development.

MS. SMITH: Thank you. And now we will introduce those panelists who are in support of an expanded exemption. So, Mr. Adams.

MR. ADAMS: Stan Adams, Center for Democracy and Technology.

MS. SMITH: Thank you. Professor Halderman, could you please introduce yourself?

MR. HALDERMAN: I'm Alex Halderman. I'm Professor of Computer Security at the University of Michigan, and I'm a computer scientist.

MS. SMITH: Thank you. Professor Reid and Mr. Scarbeary.

MR. REID: Hey, good morning. Blake Reid, Director of the Samuelson-Glushko Technology Law & Policy Clinic at Colorado Law. We're counsel to Professor Halderman. And I'm here with my student attorney, Wilson Scarbeary. Wilson?

MR. SCARBEARY: Hi, I'm Wilson Scarbeary. I'm a 3L and a student attorney at the Samuelson-Glushko Technology Law & Policy Clinic here at Colorado Law. Thank you.

MS. SMITH: Thank you. Mr. Williamson.

MR. WILLIAMSON: Hi. Aaron Williamson. I'm here representing the Software Freedom Conservancy.

MS. SMITH: Thank you.

Now those who have filed comments in opposition to aspects of the proposed adjustment, if we could go Mr. Ayers, Mr. Mohr, Mr. Reed, Mr. Troncoso, then Mr. Williams, so that is alphabetical. Please go ahead.

MR. TAYLOR: Ms. Smith, this is David Taylor. Mr. Ayers will not be here today.

MS. SMITH: Oh, thank you.

MR. TAYLOR: So David Taylor for both DVD Copy Control Association and the Advanced Access Content System Licensing Administrator.

MS. SMITH: Thank you for reminding me, Mr. Taylor, and apologies for not catching that.

Mr. Mohr.

MR. MOHR: Chris Mohr, Vice President and General Counsel, SIA.

MR. REED: Morgan Reed, President of The App

Association and the Executive Director of the Connected Health Initiative.

MR. TRONCOSO: Christian Troncoso, Senior Director for Policy at BSA, the Software Alliance.

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

MS. SMITH: Okay. So thank you all for being here today. I guess the first question I have is this is the sort of third time we have looked at the need for a broader regulatory exemption for security research which has been in place since 2015 compared to the statutory exemption. And, you know, just keeping it to a minute or so because we will walk through some of the issues, I'm wondering, what are the main concerns with how the current exemption is operating or main concerns with broadening it in the ways requested through some of the submissions? And so, if you would like to speak to that, just indicate with the raised hand button.

MR. WILLIAMSON: So I don't see the raised hand button. I apologize. I'm usually quite savvy.

MS. SMITH: Oh. Okay, well, if you just wave, go ahead. But, if you would like to speak, Mr. Williamson, go ahead.

MR. WILLIAMSON: Okay. So the Software Freedom Conservancy is here primarily to comment on the lack of clarity around the scope of the existing temporary exemption as it applies to privacy research activities. You know, our comment was that it was not clear that privacy research that is not specifically about a security flaw or vulnerability is covered by the existing exemption. There have been some comments back and forth on whether those activities fall into security research. And so we seek clarity around that question primarily.

MS. SMITH: Thank you. And are you aware of projects that have not been taken up due to this alleged lack of clarity, and if so, could you describe any?

MR. WILLIAMSON: I cannot name a specific project that has not been undertaken because of this lack of clarity.

MS. SMITH: Thank you. Any others who wanted to speak to any overview issues? And, otherwise, I will turn the questioning to my colleague, Mr. Greenberg.

MR. REID: Ms. Smith, I had my hand up and I believe Mr. Adams did before me.

MS. SMITH: Okay. Well, I'm wondering if

maybe there is something going wrong on my end. But how about Professor Reid, then Mr. Adams?

MR. REID: Thanks very much. Appreciate that, and sorry for whatever the malfunction with the hand-raising tool. We'll try waving. I would just underscore I think that one of the main concerns that we hope to address today is the continuing inclusion of the other laws limitation, which, as the Department of Justice pointed out, really transforms the legal risk that security researchers who are trying to structure projects face.

And we hope we'll have an opportunity to discuss the Department of Justice's changed perspective on the other laws exemption and talk about whether we could better serve the needs of cybersecurity policy and better serve the needs of security researchers by removing the explicit tie between § 1201 and every other law, which includes not only laws like the Computer Fraud and Abuse Act but laws ranging from local ordinances, state statutes, all the way up to potentially foreign laws. And, again, that's something that significantly complicates the risk calculus for security researchers. Thanks.

MR. ADAMS: I'll just jump in to say that Professor Reid covered most of my points already, but

I wanted to say we see the inclusion of the conditional ties to the CFAA as the biggest adder of risk in the current exemption. Thank you.

MS. SMITH: Okay, thanks. And, in part, because I'm not seeing the raised hand button I asked everyone to use, I'm going to turn this to Mr. Greenberg, but I know that the other laws exemption is something where we're eager to get into that in particular because we also received a letter from our colleagues at the Department of Justice that we want to make sure we can aerate. Okay, so Mr. Greenberg.

MR. GREENBERG: Thanks, Ms. Smith. I'll just say I am seeing your raised hands, so rest assured that does work if you hit the button on my end at least. I also want to say that the DOJ letter and the other laws condition is one that we have a lot of questions on. But, before we get to that, we'd like to start with some other questions, and if we could sort of set aside the DOJ letter until we get to the other laws portion, it would probably be helpful for filling in the record on the other limitations that have been requested to be removed.

I also do want to caution this is a pretty large panel, so I just ask that everyone try to keep their responses specific but tight. So, just starting

with a high-level question, I wanted to raise that in the reply comments, proponents argued that opponents have provided no evidence beyond baseless speculation, nor is there any reason to expect that these concerns, the concerns related to infringing uses, if the exemption was expanded, are likely to materialize. At the same time, the opponents said something similar with regard to adverse effects and the fact that the chilling effects specifically that the proponents speak of they found to be also largely speculative and not based on clear evidence.

So I just wanted to ask, before we get into what is the additional evidence we have in the record for 2021 vis-a-vis 2018 and 2015, I want to ask the panelists, what is the appropriate degree of weight that you think the office should give to speculative concerns rather than concrete or proven or demonstrated harms? Mr. Reid, Mr. Blake Reid, or Professor Reid.

MR. REID: Thanks, and Morgan and I will try and disambiguate each other throughout the hearing. Thanks for your patience with that.

I think, you know, we've been doing hearings on security research for a long time. I think Professor Halderman and I were first here back in

2008, and I recall concerns about the security research on video games leading to a flood of piracy that never materialized. I think those concerns came up with the audio CD security research exemption back in 2005 and have been variously raised about everything from applications on smartphones to enterprise software to everything else.

And so what I would encourage the office to consider is that the speculation isn't just speculation, but it's repeated speculation that has never borne fruit, has never materialized, has never, to the best of my knowledge, resulted in any sort of litigation where anyone was able to raise even the presence of the exemption as an excuse for infringement.

And I think, on the flip side, you've seen over the years as the office has broadened this exemption, gradually and incrementally removed some of the limitations on this exemption, researchers like Professor Halderman have actually been able to do a lot more, and as cybersecurity of our nation's most vulnerable systems, such as election systems, has become more and more paramount, researchers have really been able to do more because of the increased certainty that simplifying this exemption provides.

So I'd encourage you as you're thinking about speculation, I don't think the speculation cuts evenly both ways. I think the lowered risk has improved our nation's cybersecurity, and the concerns about infringement and violation of other laws have never materialized despite more than a decade of claims that they would. Thanks.

MR. GREENBERG: Okay. Thank you, Professor Reid. I'm going to go just across the top of my window. So, Mr. Mohr?

(No response.)

MR. GREENBERG: Can everybody hear me okay? I'm having some bandwidth issues too. Yeah, okay. So I think we may have lost Mr. Mohr. So, Professor Halderman?

MR. MOHR: Can you hear me now?

MR. GREENBERG: I can. Yes, thank you.

MR. MOHR: Okay. Mr. Halderman, go ahead.

MR. HALDERMAN: All right. Thank you. So security researchers really do face legal uncertainty that is holding back our work on the basis of these problems with 1201. And let me give you just one example of that. Just two weeks ago, at my department's faculty meeting, I have a colleague who's an assistant professor, is a star security researcher,

who started talking about work that he's trying to do exploring a very important new class of vulnerabilities in computing systems, and as soon as he got through about two sentences of description, five different senior faculty members said, whoa, whoa, wait a minute, this sounds like it might touch on the DMCA, you've got to find a lawyer and not just university counsel, you need to find the kind of lawyer who understands the full breadth of the DMCA.

So what is my junior colleague having to do? It's not enough to just simply go through normal university process, make a quick phone call to the OGC. He's going to have to go and find an expert on this area of law, perhaps on other areas of law that touch on the broader contexts we're talking about with the other laws provision, and he's going to have to do that rather than spending his time actually advancing the science of computer security and trying to help keep everyone safe.

And this is what it looks like from the perspective of faculty, who are some of the most privileged and well-resourced security researchers. When it comes to the broader community of people who are just students getting started, people who are amateurs who are making real contributions to the

field in their free time or as part of a hobby, these people don't have the kinds of resources that we do and probably will never get to the level of confidence that a professional or an academic researcher would be able to have.

So all of this is unnecessary. There is no actual infringement that is resulting from the kind of research that I and my colleagues are talking about. But we're facing significant uncertainty, spending far too much of our lives talking to lawyers. No offense to the lawyers in the room, but it's time that we should be spending advancing security and keeping everyone safe.

MR. GREENBERG: Go ahead, Ms. Smith.

MS. SMITH: I guess, could you speak a second to the delta, right? Because there already is an exemption. So we can't change the DMCA, and we adopted an exemption trying to meet the needs of good-faith security researchers before. So part of this is trying to figure out what the Copyright Office can do here.

MR. HALDERMAN: Well, so a large part of the problem, as we've explained, comes from the various complicating factors in the existing exemption, including the other laws provision, which makes it

just so much harder to have a brief overview of someone's project and be able to determine whether it's safe to proceed. So, in my experience and the experience watching colleagues who have gone through this, the problem is not that there's no exemption. The problem is that the exemption has so many caveats.

MR. GREENBERG: Mr. Mohr?

MR. MOHR: All right. I think I unmuted myself, so hopefully I am not monologuing. So a couple of points. I mean, I think the fact that, look, a lot of these ecosystems, whether we're talking about the kinds that surround content or whether we're talking about cloud ecosystems, require tremendous investment and they are expensive and they are, as our friend just pointed out, being explored by people who are well-trained and highly ethical and those who hope to become well-trained and hopefully highly ethical, but they are also open to exploration by those who are not. And so that's something's that, I think, Congress recognized when it set up these exemptions in the first place, that this was likely to be the case.

And so, in terms of the way that the Copyright Office is supposed to give evidence or, you know, the lack of it, I mean, I would point out a few things. I mean, one is that if there are statements

in the record that I can't think of anything that's been actively thwarted or chilled, that to me would be fairly probative of a failure to meet the burden on the petition.

The other thing, you know, that's helpful to know, I think, are the kinds of activities, is the affirmative case on the other side, which we rarely here about, about the sorts of things that the text of the petition has actually enabled. And there is a difference between saying, well, we need specialized advice to get through this, you know, to understand what the ramifications of a particular course of study or inquiry are, and the statute actually chilling it.

The presence of a legal issue is not chilling, and we don't think that that should be viewed as chilling. What the statute requires is that it impeded its mere existence or the fact that you have to comply with it and figure out how to do that, whether or not you can do that. That's not chilling. What's chilling is theoretically at least, hey, I've got this clear fair use that I can't do because of the following factors. And that type, I mean, I think you've been through, like you said, we're in a bit of a Groundhog Day here, but this is an exercise that the office has been through before. And I'll have other

comments on the other law provisions and so forth. But, on that, that's the question I think. I wasn't sure.

MR. GREENBERG: Great. Mr. Taylor?

MR. TAYLOR: Thank you, Mr. Greenberg. I think that's a very difficult question to answer because it's asking us to prove a negative. And what we have seen so far is, is what we have in place legally seems to work. We spend a lot of time chasing after people who would put products in the market based on this research, that could put products in the market based on this research that they do, and, so far, we don't see a link to that. And that's probably because the exemption that the Copyright Office has repeatedly made has worked effectively. So it's kind of, again, hard to prove a negative.

And I would just quickly respond to this need to hire an outside lawyer specialist. I think that the recommendations of the register are very clear on the proposed opportunities or uses that the proponents want to make, and I don't see where there could be any uncertainty that someone with a advanced degree could not simply read for themselves what is allowed and what is not allowed. So thank you.

MR. GREENBERG: Mr. Scarbeary?

MR. SCARBEARY: Yes, to just briefly respond to a couple of things that Mr. Taylor and Mr. Mohr said. We've also identified the use limitations, the multiple references to "solely" and "primarily" that significantly cabin security research. These create problems as far as ancillary activities related to security research, such as scholarship and criticism, that we think is problematic. I'd also like to note that in Mr. Taylor's example, he claimed that security researchers might try and then use the products of their research to openly compete.

Now, if that was a clear case of infringement, contract holders would have alternative remedies to obviously go after those folks. But, in the recent case of Corellium v. Apple, the court found that Corellium's use in that case was a fair use. So, even in that instance, it seems highly speculative that security researchers are going to be going out and trying to turn the results of their research into competing products.

MR. GREENBERG: Great. I'm actually going to go to our colleague at NTIA. Luis, is there anything you wanted to add?

MR. ZAMBRANO RAMOS: Oh, thank you so much. I guess this question is to Professor Halderman.

Professor, could you talk about the role that transparency plays in the security research community? Things like writing research results, sharing investigational techniques, just how important is that to the development of the research community? Thank you.

MR. HALDERMAN: Sure, I'd be happy to. Transparency is often at the center of our work. We seek in general to improve security for the public at large, and there are two main ways that we do that. One, many researchers discover vulnerabilities in specific products or specific tools and protocols, and we work behind the scenes to get them fixed.

But then usually after the problems are fixed, but not always, usually after they're fixed, researchers go public with the results of their findings, and that's not only to disseminate knowledge to the broader research community about how similar problems could be found, but it's also to alert the public about the problems that have existed so people can make better choices in the future about what products or services they want to buy or rely on.

So we have most of the -- in the vast majority of projects I've worked on, they've resulted ultimately in some kind of publication that described

the findings and what we did. That's just core to the academic mission of a university.

MR. GREENBERG: Professor Halderman?

MR. HALDERMAN: Yes?

MR. GREENBERG: If I could interrupt -- if I can just interrupt you. And I apologize to the hands that are up, I know they are still -- but this will actually -- I want to jump ahead since you're sort of getting into the use limitation and purpose. I have a question I was already going to ask related to the register's past recommendations. In both 2018 and 2015, the register clarified that the access limitation does not prohibit teaching, academic dialogue, or scholarship involving the information derived from good-faith research.

The question I have is, what evidence is there of security researchers not actually sharing what they've learned via teaching or academic dialogue or scholarship because they're afraid that that will exceed the bounds of the exemption simply because it's not part of the C.F.R. even though it's part of the register's recommendation?

MR. HALDERMAN: You'll have to give me a minute to process your question, I think. Maybe someone else from our side wants to jump in while I

do.

MR. GREENBERG: Professor Reid, do you have thoughts on that?

MR. REID: I had thoughts on something else, but I saw Mr. Adams wanted to jump in.

MR. GREENBERG: Okay. Mr. Adams?

MR. ADAMS: Thank you. Yeah, I was just going to say, you know, a former colleague of mine, Joe Hall, also a computer security researcher, and I did a report that we submitted for the record last year indicating that many security researchers do fear coming forward with their research. They fear coming to the vendors out of sort of retaliation risk and they fear making it public for the same reason.

And so, you know, we, I believe, included this as an attachment or a footnote in our comments this year, but we also had it in the record last year that this is a documented fear here, that sort of publicizing results draws attention and often of the wrong kind, right? Not the great, thanks for helping solve this problem, but now we're going to seek legal action against you for making this public.

MR. GREENBERG: Go ahead, Ms. Smith.

MS. SMITH: Yeah, I hope, Mr. Greenberg, we can sort of keep teeing this up and probe in on it

because what we did in response to those comments last time was clarify in administrative guidance which was intended to be used that a researcher who at the time of circumvention intends to publish the results, a good-faith researcher used in teaching would not ordinarily exceed the bounds of the access limitations. So the office is not authorized to grant an exception to the service bar if we're getting over to that end. So that's, I think, why we're trying to figure out what particularly is not operative in light of that existing additional guidance we provided in 2018. So I guess maybe we could hear from Mr. Troncoso and then keep probing this issue.

MR. TRONCOSO: Thanks for letting me jump in. I fear that what I'm about to say is a little bit repetitive at this point, but just to make the point that for BSA and our member companies, they want to engage with the independent security research community and they often do, so they have a real vested interest in there being a very clear exemption to facilitate this type of activity.

As we look at the 2018 exemption, it seems sufficiently clear to us that there are not limits on post-circumvention activity that would in any way inhibit the type of scholarship that Professor Reid

and Professor Halderman are interested in pursuing. So, in the absence of some sort of demonstrated, you know, evident case that this language is unclear, it seems to us misguided to try to change it at this point. To the extent there is clearer language, we would be open to, you know, discussing that. But, you know, we think the exemption right now is fairly clear on that point.

I think the other, you know, difficulty in this space is that, you know, it sort straddles the line between prohibitions on acts of circumvention and the trafficking prohibitions, which this rulemaking, for better or worse, is not sort of equipped to address. So, to the extent, like, the concerns lay there, you know, I'm not sure that we're going to be able to resolve them through this rulemaking process.

MR. GREENBERG: Mr. Troncoso, are you referring to the concerns that if you have dialogue, I think it's what was Ms. Smith was saying a minute ago, but just for the record, if you have dialogue based on good-faith security research, that would then enable somebody else to --

MR. TRONCOSO: I'm not suggesting that's my interpretation of the DMCA.

MR. GREENBERG: Right.

MR. TRONCOSO: But it seems to me that, you know, we're sort of skirting around that issue in terms of whether some of this research activity may create issues there, right? To the extent that's where the uncertainty is, like, unfortunately, the Copyright Office probably isn't able to resolve that issue.

MR. GREENBERG: Right. Can you tell us what the value is that BSA sees in the solely limitation, what work that does?

MR. TRONCOSO: You know, if the limitation is not limited to activity that's undertaken solely for the purpose of security research, what is the exemption -- what does it then cover would be our sort of question. We don't see this as sort of an overly restrictive limitation. You know, the proponents want an exemption for security research. The exemption is specifically for security research. If the activity they seek an exemption for is broader than security research, I think we need to have a sort of more candid discussion about what those activities are.

MR. GREENBERG: So I didn't see, to the proponents, I didn't see in submissions any reference to some other kind of limiting principle, like primarily or something like that. But I did notice in

GitHub's reply comments, they talked -- they were looking for something that definitely was beyond solely, referencing the fact that there's ancillary benefits to good-faith security research and good-faith security research is often about many -- or computer research is often about many things and then quote, you know, that the exemption should not be limited to only one purpose but should provide enough flexibility that ancillary and beneficial activities consistent with but not limited to good-faith security research continue to fall within in it.

To the other proponents, I just want to know, you know, (a) do you have a different limiting principle besides "solely" that I just missed or forgot, and (b) to what extent, you know, do you share GitHub's feelings here that the exemption should cover more as long as it sort of shares similar principles or values to good-faith security research?

I actually can't tell at this point who wants to talk because hands have just been up for a while. Professor Reid? There we go.

MR. REID: Yeah, I'll be happy to take that one. And, Mr. Greenberg, I just observed that I didn't hear an answer to your question in Mr. Troncoso's response there. To the point that GitHub

raised, I think what you're hearing there is that this is not just a concern for academic researchers, but this is a concern out in industry that when folks are doing work like securing a supply chain that's integrated with other aspects of a business, these same sorts of concerns that we're talking about here are prevalent there as well.

But I think the important point to center on here, and I want to respond to Ms. Smith's question about the guidance. That guidance is extremely helpful if you have access to a lawyer who can go read a several-hundred-page administrative record and figure out how it applies in your case.

I would also make the observation that if you have a lawyer like that, you are probably doing research that is going to implicate the interests of some fairly large companies who may be fairly litigious. One example of a company like that is Apple. And if you look at the Corellium case that Apple just brought, what you see -- and this is the context of the trafficking ban, so I want to be careful to cabin the analogy -- they're talking about the use of the word "solely" in the context of the trafficking ban. But what you see is Apple picking apart the word "solely" in exactly the way that we're

talking about here. They're saying --

MR. GREENBERG: Yeah, but we have no -- we've given no guidance on "solely for the purposes of trafficking" because this rulemaking is not on the -- does not cover trafficking.

MR. REID: Of course. What I'm saying is the fact that even though Apple has basically gotten thrown off of the part of its case that is actually focused on copyright infringement, it's continuing to pursue extremely aggressive action based on stretched interpretations of the word "solely."

So I guess the message I'm trying to tell you, if you're talking to a sophisticated -- you know, if you don't have counsel, you're not going to get this guidance in the first place. If you're talking to counsel, they're going to say, gee, are you going to make a company like Apple mad? Because it seems like a company like Apple might not really care about what the guidance is because they are going to take you to court and they're going to bully you and they're going to try to shut down your work.

And that's why we think taking the language out of the exemption is really important. It provides clarity to folks who don't have lawyers, and it provides certainty to folks who do have access to

lawyers that these caveats are not going to get abused.

MS. SMITH: Sorry, you would just remove the word "solely" or you would use a different word? Can you answer Mr. Greenberg's question whether you have a different standard or not? And then I think --

MR. REID: Yeah, we think removing the word "solely" is the right way to go. And I think the way we framed the limitation was you have an exemption and I think some of the opponents have phrased it this way, you have an exemption for security research and if you can say that what we are doing is good-faith security research and meets all of the qualifications for that, then you qualify for the exemption.

And by doing that, we avoid basically creating a foothold for these sort of abusive arguments that say, well, you might be doing something else, we don't know about the publication of this paper, we don't know -- it seems like this is related to a business, you're getting paid for this. We cut off all of these arguments that may well not succeed by the time you actually get to a judgment on the merits in a litigation but are going to give the ability for a large company, like an Apple, to come in and basically bring an abusive litigation that's going

to shut somebody's research down before it gets out of the gates.

MR. GREENBERG: Okay. Mr. Reed and then Mr. -- I believe it's Williamson, not Williams, and then Mr. Williams, because I don't think any of you have spoken yet. Sorry about that.

MR. REED: Yeah, thank you. Christian covered several things, but both Professor Halderman and my fellow Reid have harped on the idea that boy, it's just so hard to have counsel. It's ironic because I run a trade association with more than 5,000 companies involved, and we literally have one of the leading experts on the DMCA as an on-staff attorney, and we regularly get questions from our members about the DMCA which we provide at no cost to our members and if you're a small business.

So, when Halderman says, oh, gosh, I just can't find an attorney, my junior associate -- well, I'm pretty sure that if he picks up the phone and makes a phone call to any of the trade associations that work in this space, there is a plethora of supportive help from attorneys.

And to Blake Reid's point about, well, you don't want to anger Apple, we've actually had our counsel engage directly and quietly with some of the

biggest players on some of the questions around this and engage directly. So I think this, gosh, we just need help because we can't find an attorney, is a little hard to swallow.

I found it interesting when Stan pointed out that Joe Hall, you know, Joe, also known well, he literally pre-COVID sat two floors below me in almost the same -- in the same office building. So the community of people who are experts on this issue is one in which it's not hard to find an expert able to provide some insights.

In addition, the Copyright Office has done a pretty good job of providing plain English understanding. So I want to kind of cabin that and say let's not pretend there aren't enough attorneys to find who have understanding of the DMCA.

But, additionally, I think the one problem, and I'm very sympathetic to the idea of security research, but the problem with the removal of the word "solely" is it basically removes any value for the words "good faith" because, if it's not solely for good faith, then it might also be for bad faith, and that's when we enter into this cascade of opportunity.

Halderman said that he was concerned about there was a sense -- oh, I'm sorry, Mr. Scarbeary said

that we were suggesting somehow that researchers are unlikely to turn their discovery into a competing product. He's probably right. Most academics are not. But the value of the research that they're doing, if you remove the good-faith exemption, is a hundred percent going to end up in products that are on the Dark Web and are available from people who do not have a good-faith intent. So I think that's the problem. If you remove "solely," you essentially create an entire ecosystem around bad faith.

MR. GREENBERG: Yeah.

MR. REED: And so I also stipulate to much of what Christian said. Thank you.

MR. GREENBERG: Okay. Thank you. Before I go to you, Mr. Williamson, I just want to point out that if you remove the word "solely," you know, part of what I hear proponents arguing for is they need more certainty so researchers know what they can and can't do. But if you remove the word "solely," you can also argue you end up with less certainty because there's not a clear limitation. I mean, we have to acknowledge there's a value to plain language, which the office has provided over the past two rulemakings with both the rule and then the administrative guidance to help interpret the rule. So I do think

that's a place we have to start from, the idea that if we're trying to provide certainty, removing words that have meaning doesn't necessarily give more certainty. Mr. Williamson?

MR. WILLIAMSON: Thank you. I'd like to first address the point that Mr. Reed made regarding there being plenty of attorneys. I've been the attorney for a software trade association, and I've been the attorney for a nonprofit that gave legal counsel to free and open-source software projects who couldn't afford it, et cetera, et cetera. There are two issues here. The one is that an attorney for a trade association that you're a member of is not your attorney, so you can't get privileged advice from that attorney, and so relying on, you know, their sense of what the law is with all of the caveats of I'm not your attorney is not of any comfort to somebody who is potentially risking litigation.

And, you know, as our colleagues have pointed out in their comments, nonprofit organizations like the Electronic Frontier Foundation that provide counsel to individual developers sometimes when they think the case is important enough, et cetera, are absolutely overwhelmed with requests for assistance. And so, you know, they can't really be relied on if

you have an urgent issue because they may well just not have the capacity for your case.

In my practice, I represent -- I advise clients on the DMCA in all its aspects. I advise clients on the CFAA. I defend criminal defendants in CFAA cases. You know, I advise clients on ECPA. And the most common counsel that I give to individuals who are doing something that might run afoul of the CFAA or the DMCA is, if you end up in litigation, you're done. They simply can't afford to even proceed to a verdict in district court against an Apple, et cetera. And so --

MR. GREENBERG: Real quick, I think we're spending a lot of time talking about how hard it is to hire attorneys, and I agree with that wholeheartedly, but we could talk about this with regard to almost any civil law, and we don't have a ton of time today, so I don't want to go too far down this rabbit hole. Any exemption that the office ends up recommending is still going to require an attorney to review it at some point where the researcher gets close to the line. So we can talk about this, but there's a whole lot more value in talking about removing specific limitations and why. So I just want to caution that if there's more you want to say on the "solely" and

the purpose and use exemption -- limitations, I would go to that.

And then I want to go to Mr. Williams and then, with apologies to Mr. Scarbeary and Mr. Morris, who still have their hands up, I want to move to the primary evidence that was submitted with regard to these limitations because I think that we're going to start running pretty behind here pretty quick because we still have lawfully acquired and other laws to get to.

MR. WILLIAMSON: So I would like to briefly address "solely." If you remove "solely," you're left with "for the purpose of good-faith security research," right? And so, you know, it's a lot easier to tell whether you're doing research in good faith than it is to tell whether you're doing research solely for -- or doing work solely for good-faith security research because, as Mr. Reid pointed out, Professor Reid pointed out, those who work in security research are often in a sort of dual-purpose role. A lot of them work in companies that are attempting to secure their own systems, and so they're not doing solely research, they're also doing remediation in their own networks. And every criticism I've heard of the word "solely" from the opposition would suggest

that they're looking at bad-faith potential uses. And so, when you remove "solely," I think "good faith" does all the work that they need "solely" to do.

MR. GREENBERG: I just want to ask this really quickly, but I do want to keep moving forward, do you think the word "primarily" would be any better, or would that be just as -- create in your mind just as much uncertainty and it would probably, I'm sure, be less palatable to the opponents, but would it be any more -- would it be any better of an exemption from the user standpoint?

MR. WILLIAMSON: I think that, you know, it is a small step but contains nearly all the uncertainty of "solely."

MR. GREENBERG: Okay, Mr. Williams, unless, Mr. Williamson, did you have anything else you wanted to add? I'm sorry, you did wait a long time. Okay, Mr. Williams.

MR. WILLIAMSON: Thank you.

MR. WILLIAMS: Thank you. I'm going to try to go back to kind of the beginning here just to address some of the questions. So, you know, I thought the first question was really an opportunity for the proponents, and I think this came from Ms. Smith, to provide some specific examples of chilled

projects, and I think we got none. We did get something useful from Professor Halderman, but it had no specifics. There was nothing about why the current exemption would not cover it. I don't know whether his colleagues are overly cautious or being appropriately cautious, but there was nothing that I can assess because there were no details there.

So, looking at the record, I think that says a lot. There's not evidence that research is being chilled beyond just abstract statements of the kind, Mr. Greenberg, that you referred to about, well, can I get a lawyer or not, which I agree with the point you made on that issue, so I won't dwell on it.

Like BSA, my clients think security research is important. We did not oppose renewal here. But, with no substantive examples of chilling effects from the current language, we don't understand why it needs to be changed.

On Apple v. Corellium, that's a project that moved ahead. It's a commercial project that moved ahead. And my understanding is that they'll go to trial and that will be tested, the limits of this exemption perhaps and also of the statutory exceptions. And we hear in this proceeding repeatedly that there's no test cases, there's no lawsuits,

there's not enough lawsuits for us to prove our case of chilling effects or that the statute needs to be changed. But then, if someone does file a lawsuit, and I'm not representing Apple here, but if someone does, they're accused of being a bully and of, you know, being excessive with their use of the law. And so there's no way to win in that scenario where, on the one hand, people beg for lawsuits and, on the other hand, they criticize them.

You know, on the issue of speculation, I think it was your question if I recall, Mr. Greenberg, what should be the standard here? I think speculation from the proponents is demonstrably not sufficient for them to meet their burden. The burden is initially on them. You can consider our concerns about the scope of exemptions to be speculation, and Professor Reid said, oh, there's no evidence of piracy, and he went back to things that happened, you know, 15 years ago, 12 years ago, in terms of proposals.

But, as Mr. Taylor, I think, said, proving a negative is very difficult, and us knowing where the piracy comes from is very hard. And so I think, when you're talking about speculation, yes, ideally, on the opposition side, you'd have specific evidence of harm. But I think it's common sense that if databases and

things of that nature are breached, there's a potential for harm, whereas there's no specifics on the proponents' side, and that's where the burden lies in this. And, as I said, we support the renewal of the existing exemption. We're fine with it being renewed. They already have a very broad exemption, and so we don't see the harm coming from it.

I will just mention very quickly two points. One, even the discussion draft that came out of the Judiciary Committee process recently incorporates all of the items, I believe, from the existing exemption that the proponents are criticizing. And I testified on the same panel that Professor Reid did. I know that members of Congress took that seriously, and the discussion draft seemed to endorse the office's approach to this exemption. And so I would just say that in that separate forum, there was also apparently not enough evidence to justify changing this proposal.

And, finally, I do just want to mention that there's some discussion of the Green v. DOJ case in the comments, and if we have time, I would love to get a chance to speak on that later on.

MR. GREENBERG: Yes. So that's actually where I'm going to go next. I do first want to clarify two things. One is that the Digital Copyright

Act discussion draft that came out of that process would have granted exemptions for trafficking also, so it does overlap a little bit here with the concerns of the proponents. I do also want to note Mr. Adams' point about the report that he had previously submitted regarding fear, you know, which is again more anecdotal evidence, but fear amongst some researchers about what they share.

Mr. Adams, for your clarification, I just checked all three of the submissions that CDT was on and I don't see it appended to any of that from this process at least.

So I do want to ask next, and I will start with -- well, why don't I actually ask the question first. So the primary alleged example of an adverse effect from proponents is different from what was present in the 2018 record, is the 2019 -- June 2019 ruling in Green v. DOJ, and I'm wondering both for proponents and opponents how much stock you think the office should put in that decision. I do want to note that on page 8 of the proponents' reply comments, they refer to the Green decision as a summary judgment motion. It was, in fact, a motion to dismiss, which is a different burden for the plaintiff.

So I'd like to hear from proponents and

opponents as to what the office should do in terms of interpreting the June 2019 decision in Green v. DOJ as evidence of a chilling effect from the circumvention prohibition. I'll start with Professor Reid and then Mr. Taylor.

MR. REID: Thanks, Mr. Greenberg. If I could before I move on to Green, just wanted to make one quick response on the "solely" and "primarily" language, which is I think that the one core concern that we hear that is cognizable under § 1201 as one that is within the ambit of the office's jurisdiction here is think about copyright infringement, and I'd note that there's a limitation in the existing exemption that restricts use of the information that's derived from the security research in a manner that facilitates copyright infringement.

Now we have concerns about the formulation of that particular limitation because it puts responsibility on basically for downstream third-party behavior, not of the researcher. We don't think that formulation is right. But, to the extent that the office wants to focus on extraneous concerns or bad faith, as Mr. Reed put forth, thinking about making sure that those concerns are actually narrowed to concerns of copyright infringement, I think, is

important. And I think it is really important, contrary to Mr. Williams' point, to focus on the fact that there's absolutely no evidence in the record of copyright infringement being a problem in the more than a decade that this exemption has basically been in the works.

To the point about Green, and I think this actually ties to the discussion earlier about why can't you just hire a lawyer, why can't you get the guidance that you need, you need to go jump through a bunch of threshold hoops to go about doing your research here, I think the sort of criticism, you know, of Professor Halderman and his colleagues and so forth, I think what Green v. DOJ underscores and it should serve as a strong reminder to everyone here is that what's being chilled here and what's at stake here is First Amendment protected speech, right?

So, in other words, we can look at a lot of the different activities that are being discussed during this triennial review, but there are very few that are so poignantly and directly directed at criticism of -- critical speech that's aimed at products that, frankly, have often a direct role in the administration of our elections, of our democracy that take on salience of a deeply political nature in

some cases.

And so we think the salience of Green v. DOJ is incredibly important for the office to remember that any overreach of this exemption, any way in which this exemption chills research, is stepping on the First Amendment toes of folks who are engaged in core First Amendment speech. And that's what the court is getting at there. I think the office should heed what the court had to say there as a warning to say, if you want to salvage § 1201, if you want to make sure that § 1201 as a whole doesn't come under constitutional scrutiny, it's incumbent on you to make sure that the exemption is drawn in such a way that it minimizes any ancillary effects on First Amendment protected speech.

And so we think that's a really important recognition of some of the same adverse effects, and, by the way, I'd point out that we brought many of these up in 2015 and 2018 and that the office chose to dismiss them in those triennial reviews. I would treat this as the court sending a message to the office that it is important to retract the exemption to make sure that the First Amendment isn't implicated. Thanks.

MS. SMITH: So thank you, Professor Reid, and I'm not here to comment on your statement because,

as we have all noted, it is an active litigation, but I do want, because of that, to sort of make sure we're clear on what has been said today, which is not that the Copyright Office has said why not just hire a lawyer, but we have pointed out that we have provided administrative guidance that professors are able to publish the results of their good-faith research or use them in the course of teaching. And that's just a quote from 2018. So I just want to be careful on that in terms of what the current exemption already permits, as the Agency has clarified.

Okay. Mr. Taylor?

MR. TAYLOR: Thank you. Before I turn to the question on Green, I just want to clarify a point that was maybe misunderstood. We certainly have no problem with responsible computer security researchers. I think Mr. Morgan clarified that it really is who can take advantage of that research and making sure that it's responsibly handled.

The second thing, on the "solely," I think "solely" really is there because this rulemaking has to follow the record and while I too read the reply comments and thought, well, perhaps some of these additional activities still could fall under good-faith computer research.

Now, turning to Green, I would just simply say that, you know, it's a motion to dismiss, and we have long recognized that the DMCA poses First Amendment issues. I mean, to say that you can raise a cognizable claim is very clear since Corley. And the facts have to be developed on the record and there has to be a final ruling. But even if the court does decide for whatever reason there is a First Amendment issue here, there are far more cases out there that suggest that the DMCA does not raise First Amendment concerns.

So, at that point, if the court were to decide, it would still be an outlier for the jurisprudence in this area. So I think it's a very far stretch for Mr. Reed to suggest that the Copyright Office should take the ruling on the motion to dismiss as a signal as to what is the correct way to interpret the exemptions and the exemption process in context of the First Amendment.

MR. GREENBERG: Okay, thank you. Mr. Williams?

MR. WILLIAMS: Yeah, thank you very much. On the Green case, as a couple of you have touched on, I mean, the procedural posture is quite different from how the case is characterized in the proponents'

comments. The comments, I think, say that Judge Sullivan said there was a compelling case of a First Amendment violation, for example. But none of that is in the case. It was a motion to dismiss. He repeatedly stressed that the government, on that posture, had the burden.

They are now on a preliminary injunction motion that's been pending for quite some time. The burden is going to shift. I find it quite interesting that when Judge Sullivan asked for the parties to come to some agreement on how to move forward with discovery, the plaintiffs didn't seem to want discovery. They wanted to jump right to this preliminary injunction motion without any discovery.

And I don't think they have enough evidence, but, of course, that will be up to Judge Sullivan. But he certainly did not hold in any shape or form that the DMCA generally or the specific security research exception in this proceeding violates the First Amendment. And so I believe under First Amendment scrutiny, under the Intermediate Scrutiny Standard, that this exemption, as well as the statute generally, should survive. But the comments vastly overstate the impact of that motion to dismiss decision.

MR. GREENBERG: Okay, thank you. Mr. Williams, I want to turn now to "lawfully acquired" before we move on to other laws. And, again, to the proponents, I'm wondering if you have any examples of researchers being discouraged from conducting good-faith security research because of contract terms that limit the ability for a security researcher to acquire the software device. As you are aware, in the 2018 recommendations of the Acting Register, there was clarifying language here and support from DOJ on our reading of the exemption so that it would not impose a problem for good-faith security researchers.

So I'm wondering if, in the three years since, you have come across examples of researchers who are being discouraged or prevented from engaging in good-faith security research because of the lawfully acquired limitation. Professor Reid, I see your hand.

MR. REID: Thanks, Mr. Greenberg. And I'll defer to Professor Halderman if he's got any particular examples. I just wanted to, in the interest of hopefully shortcutting too long of a discussion on "lawfully acquired," point out that basically our concerns with "lawfully acquired" are a subset of the concerns with other laws. In other

words, the set of legal issues, the set of risks, the set of uncertainty, the complexity of dealing with it, is just -- we kind of see "lawfully acquired" as an example of the kinds of problems that occur with other law but obviously a narrower subset, a narrower set of laws that are potentially implicated, a slightly simpler question. So just wanted to sort of say our concerns are basically the same as what we've been discussing for the last hour or so, albeit in a little bit of miniature, if that makes any sense.

MR. GREENBERG: Well, can I then just ask as a follow-up, what do you make of the fact that DOJ -- and, again, we're going to talk more about other laws in a minute, so no need to spend time on that yet -- but what do you make of the fact that DOJ does think that the "lawfully acquired" limitation still serves an important purpose and coupled with the register's administrative language is not creating significant adverse effects, whereas they do support removing the other laws limitation? What do you make of that distinction?

MR. REID: Well, I think we obviously diverge from DOJ on the salience of the "lawfully acquired" limitation. I think we come to a different place. Obviously, we're in big agreement that the

broader swath of laws that are implicated by the other laws limitation impose a more significant chilling effect. And so I think we are directionally in the same place as the Department of Justice, albeit we come to a different place on the "lawfully acquired" exemption. My colleague, Mr. Scarbeary, may have something to add there.

MR. GREENBERG: Yeah, Mr. Scarbeary, do you want to add anything? And after Mr. Scarbeary, does anyone from the opponents have anything they want to add to why, I know from the reading of the comments, you think that sort of the concern with "lawfully acquired" is sort of an overly narrow and implausible reading? Is there anything you want to add to what's already in the record there? Mr. Scarbeary?

MR. SCARBEARY: Yes, on the "lawfully acquired" limitation, our concern here is simply that that clause allows software developers to essentially weaponize the DMCA in a way to totally preclude security research simply by including a contractual clause that devices cannot be resold to security researchers. And we pointed out in our comments one area where this is particularly common, is in the context of election machine security research, where these companies frequently try and dissuade security

researchers from analyzing their systems by including these kind of contractual restraints.

MR. GREENBERG: I did take note of that, so thank you for bringing that up, but I did see that in the comments. Mr. Troncoso?

MR. TRONCOSO: You know, again, I think that what we just heard runs counter to the clear guidance that the Copyright Office tried to give in issuing the 2018 exemption where they made clear that the "lawfully acquired" limitation applies only to the acquisition and whether or not it itself is in violation of law. To the extent there are contractual issues, I don't think that those are implicated at the point of acquisition.

So, again, I understand that there is a legal overlay to a lot of the activity that is in play with security research, but that legal overlay is not going to go away merely by removing the limitations in this exemption. That legal overlay is the natural byproduct of there being a statutory prohibition that can cover this activity and other statutes, the CFAA and others that I'm sure we'll discuss in a moment.

MR. AMER: Can I ask a --

MR. GREENBERG: Well, and I'm sure you have something to say on the election --

MR. AMER: Can I -- sorry, Mr. Greenberg.

MR. GREENBERG: Yes?

MR. AMER: Could I just ask a follow-up question? This is a more general question to proponents and Professor Halderman is here, you can maybe incorporate this into your answer if you'd like. But, I mean, it strikes me that, you know, sometimes we get criticized in the office for having exemptions that are too detailed, right, you know, and this goes to your concern about needing lawyers to help with understanding them.

And so your approach is to just remove all of this language. But, I mean, I think we've heard, you know, a countervailing concern from the opponents that by doing that, that could at least suggest that we're, in fact, broadening the exemptions, right, and that there is a change. And we can say all we want in our recommendation that it's not intended to do that. But, from what we've heard today, that doesn't seem to carry very much weight in some people's eyes.

So, you know, I wonder how much -- you know, so I think we would be reluctant to just sort of take out a lot of language, and so, you know, our approach was to provide clarification in the recommendation. If we were to take the approach of sort of adding

language to the regulatory text, saying things like, you know, this includes good-faith, you know, publication of research results, teaching, et cetera, and it doesn't encompass situations where there are restrictive contractual terms, et cetera, it seems to me that that's sort of -- I don't know that that helps you very much from the proponents' standpoint because it's making the exemption more complicated and potentially open to different interpretations. I wonder if any of you could speak to that.

MR. HALDERMAN: Well, let me just say that clarification is --

MR. GREENBERG: Real quick. I'm sorry, Professor Halderman, real quick just for the court reporter, Professor Halderman, I can see you have something that you want to say.

MR. HALDERMAN: Yes, thank you. Clarification is, of course, appreciated, although, as we pointed out, the overriding complexity of the existing exemption and the kinds of complicated legal queries that it raises, especially in things like the other laws provision, wouldn't be helped so much by the kind of clarification that you mentioned, Mr. Amer.

I wanted to just also mention on the

question of "lawfully acquired" just one example that has come up in my area of election security research in the last few years has been about the Defcon Voting Machine Village, which is a public event every year at the security community's largest annual conference in which the public is invited to come for a weekend and engage in hands-on research on the security of election equipment.

The organizers of that event bring voting machines and other equipment that they've acquired on eBay, some that's been donated to them, some that participants have brought with them, and although they believe it to be lawfully acquired, they have no way of verifying whether equipment that's been, for instance, purchased on eBay was, in fact, resold after some breach of a contract. It's quite common that the sales contracts on voting machines will prohibit reverse engineering them, will prohibit further resale, and this has caused real uncertainty and risk and serious risk for the organizers of that event, so that's just one example.

And looking ahead, this same kind of, say, contractual limitation on resale of voting machines is something that I worry will prevent further research that I would like to do trying to understand and

improve the security of voting machines that are being marketed today, which are virtually impossible so far to acquire secondhand because those contracts prohibit their resale. But, if one were to be sent to me tomorrow from an anonymous source, I would love to be able to study it, but I'm not sure what my lawyers would say in terms of whether I was able to do that with the current scope of the exemption.

MS. SMITH: Can I ask you a follow-up question about the Voting Village? Because that is something the office has looked at. We cited it favorably as an example of making use of the exemption in the proposed rule in 2018, so that was referring back to two exemptions ago, right? So my question is whether are you seeing any instances that the Voting Village was unable to make use of good-faith security research because of § 1201 since 2015? Because just in terms of what's in the record to the office so far, it seems we're not aware of anything that needed to be held back.

MR. HALDERMAN: I am not myself an organizer of the Village, although I'm a close colleague of the people who are the organizers, so I can't speak to what they might not have done that they otherwise would have. But I can tell you that they agonize over

whether they would be able to hold the Village under the current exemption. And --

MS. SMITH: But I guess, when the Agency says this is an example of using the exemption, I'm wondering why they're agonizing. Do you have any insights?

MR. HALDERMAN: Well, it's the Agency saying that this is a good example but then saying that equipment has to have been lawfully acquired. When they don't know the ultimate origins of the equipment, it leaves them -- it creates an apparent contradiction.

MR. GREENBERG: Okay. Thank you. Mr. Zambrano Ramos, do you have any question you wanted to ask? I see your hand up. And then, Mr. Williams, so I did see your hand up. And then Mr. Troncoso and I think I see Professor Reid. My screen keeps moving around, so I'm having a hard time keeping track of people. But does sound right to everyone? Yes? Okay. Mr. Zambrano Ramos?

MR. ZAMBRANO RAMOS: Thank you so much, Mr. Greenberg. This question would be for Professor Reid, and it's kind of an issue that's been interwoven in these discussions, and that's the idea of the administrative guidance language versus the exemption

language. I'm just curious, in your experience with the security research community, there is a lot of different kinds of security researchers, how easy is it for the community to kind of use that language that's in the administrative guidance for their specific uses? And can you specifically talk about use cases where you may have security researchers in a university or one institution versus more independent security researchers? Thank you.

MR. REID: Thanks, Mr. Ramos. And I may defer to Professor Halderman and Mr. Adams to speak further on this question. But just to tie back to themes from earlier in the week, this dynamic of can we seek clarity in the exemption language itself versus in the Agency record or the recommendation from the register that comes out or the final rule from the librarian has been a theme, and I think it's important to underscore that there are different communities served by each of these exemptions, some of them quite small and quite tightknit and then some of them quite large and quite diffuse and quite diverse.

And I think this exemption presents an example of a quite large and quite diverse and quite diffuse community for whom having the sort of guidance that for other exemptions might be filtered into the

community quite readily is going to be more difficult here because there are different groups of folks who do research in the context of academic institutions. As Professor Halderman mentioned earlier, there are numerous independent security researchers, there are researchers that work in house at companies of various sizes and various levels of sophistication. So I think it's important to underscore that this exemption is aimed at and important to a broader set of actors than perhaps some of the other exemptions.

And, Mr. Amer, to your point, I know the office is navigating some difficult tensions here in terms of trying to figure out how can we clarify this. In the recommendations we ultimately put out, how can we deal with the specificity of the exemption? And we appreciate your efforts to get this calibrated, but I think this is one where you're contending with a complicated user community for this exemption. And so simplicity really reigns supreme here. Simplicity is really important for the long tail of researchers who take this exemption.

And to the point Mr. Adams raised earlier, there's a lot of fear, and fear counts as an adverse effect under the statute, and sometimes that fear comes from folks who are just not well steeped in

administrative law or how to read a recommendation or even how to read the C.F.R. and are relying on guidance, are relying on community norms, are relying on folk wisdom that sort of makes it around.

And so I think it's really important in this exemption, to the extent that you can draw it in a very narrow way that says, hey, security researchers, are you doing good-faith security research by a standard that I think everybody understands applies here. If so, don't worry about all these little caveats. In fact, we'd like to really dispel that fear, right? And you should tell your colleagues that do this work that this exemption is safe to use. And I think where Professor Halderman left us here is having guidance buried somewhere in the recommendation doesn't penetrate all the way out into the communities that are affected here.

MR. GREENBERG: Okay. If there's any more to add to that, it was Mr. Troncoso and Mr. Scarbeary next. However, I do want to note that we are already at 11:50 and we still haven't gotten to sort of probably the more significant portion to discuss in terms of what is new in the record since that DOJ letter came in with the reply comments, and we do still need to get to the privacy portion of this

panel. So, if there's no real objection here, I'd like to move on to other laws.

MR. TRONCOSO: Can I just jump in for literally less than a minute? I think I do want to respond to something that Professor Reid just said. I think part of the concern that we have about this exemption is that we do think it is sufficiently clear, but there seems to be an effort to intentionally misinterpret the 2018 exemption, making arguments that, you know, "primarily" might be read as "solely," for instance.

And I think, you know, proffering those types of arguments can lead to concerns in the security research community that the 2018 exemption is much narrower than it, in fact, is. And so I think we need to take a really realistic look at the 2018 exemption and not sort of allow for really wild interpretations of how it might be read to dictate sort of what --

MR. GREENBERG: Yeah, Mr. Troncoso, I can stop you there. I mean, the record is really clear on the fact that the proponents and the opponents just disagree with the meaning of the 2018 recommendation. So that's pretty well-developed in the record. I'd appreciate everyone bearing with us on moving on to

other laws.

So let's just start with the proponents. Before we get to the DOJ letter, we're looking for any examples of litigation or legal threats made against security researchers that allege a 1201 violation in conjunction with a meritless violation of another law, such as but not limited to the CFAA, where the conduct at issue would otherwise be permitted under the existing temporary exemption. So I didn't see anything in the comments submitted. That doesn't mean I didn't miss it. There was a lot of reviewing going on. But I do wonder if there's anything you want to verbally add to supplement the record.

MR. REID: Mr. Greenberg, if I could respond?

MR. GREENBERG: Yeah, Mr. Reid, go ahead -- or Professor Reid, go ahead.

MR. REID: And defer to my colleagues on concrete examples as well. But I take a little bit of issue with the framing of the question as being around lawsuits. Again, there's not a lot of --

MR. GREENBERG: I said or legal threats, which does not necessarily mean, you know, that a lawsuit is being filed but that it was, you know, threatened. But we don't need to hash that out.

MR. REID: Well, I mean, I think it's important to respond to even if your framing is legal threats here. And I think this has been a thread throughout the day today. It's important to consider that the users of this exemption are often in the case, as Professor Halderman often is, not simply of avoiding litigation but of demonstrating that their conduct is affirmatively in compliance with the law, right? And I think a lot of our concerns here are rooted in a need for certainty that the users of the exemption are indeed complying with the law and not merely that they're avoiding getting sued.

So I would urge the office to be thinking about adverse effects in that respect. The presence of litigation as a general matter of the type that we referenced earlier with Apple v. Corellium around the trafficking exemption, that creates an incredible chilling effect for anybody that's doing research that is in that space. And so folks who are working with, whether it's university counsel or counsel to nonprofit organizations, like Mr. Williamson, have got to go further. They've got to be able to say we know that this is going to be safe and that we're not going to get dragged into court by somebody like Apple, who's going to put our organization out of business or

is going to --

MR. GREENBERG: Sure, but just to interrupt, I apologize for interrupting you, but first off, we've been over Apple v. Corellium, and I do want to just warn folks we have a limited amount of time. So the record, we have a court reporter, we don't need to go over things we've already gone over. I'm looking for anything additional to that and really examples, concrete examples or affirmative proof here of folks who are being chilled because of the other laws limitation.

MR. REID: I'd point you to the example that Professor Halderman raised earlier, and I think the other laws limitation is precisely part of that example and that's a conversation that happens all the time. And I think you've got a plenty sufficient record coupled with the Department of Justice letter to advance the removal of the others law exemption.

MR. GREENBERG: Was there any further proponents' side, does anyone else want to add anything before we move to the DOJ letter?

(No response.)

MR. GREENBERG: I'm not hearing anyone. So I'm going to assume everyone is familiar with the DOJ letter, but, just in summary, what they said was that

they now support removing the other laws limitation for a number of reasons, which we can get to a little later. But just I wanted to start with what both proponents and opponents make of this switch or this reversal on DOJ's position. Let's start with Mr. Mohr. Mr. Mohr, you're muted.

MR. MOHR: Apologies. The biggest problem I have with the DOJ submission is it ignores basic rules of statutory construction and it doesn't reference them, account for them, or explain why those rules don't apply. Specifically, there is a presumption about extraterritorial -- against extraterritorial construction. And so, when the United States statute and regulation says --

MR. GREENBERG: Just to be clear on this point, you're referring to where DOJ talks about the fact that the other laws might sweep in foreign laws where there's researchers working --

MR. MOHR: That's correct.

MR. GREENBERG: -- them across different -- in different countries here and somewhere else and where those laws might be inconsistent with U.S. law or even against U.S. policy is that right? -- or obscure.

MR. MOHR: Or obscure or just -- I mean,

that is not how, as a general rule -- I mean, there are, of course, exceptions, there are exceptions in the antitrust area, I believe. But, as a general rule, you do not read them, and the copyright laws certainly have not been interpreted to have extraterritorial reach. So those kinds of things, I mean, that kind of thing suggests a bit of an overbroad -- a well-intentioned but overbroad concern and the type of concern that could easily be addressed, you know, through clarification rather than amendment.

MR. GREENBERG: Mr. Adams?

MR. ADAMS: Thank you, Mr. Greenberg. So my take on the DOJ's -- you know, I'd like to think it was a clarification of what they meant to say in 2018. But, you know, I think the way I read it is the DOJ is saying we don't need this tie to DMCA 1201. You know, we're confident in our abilities to sort of take on the CFAA cases as we see fit and that it is not necessary to tie compliance with that to a copyright law because, you know, we can handle it. We don't need that extra support either from DMCA 1201 and we don't think, as proponents, that DMCA 1201 needs that extra support or confusion from CFAA.

MR. GREENBERG: Can I ask you a follow-up to

Mr. Mohr's point about extraterritoriality? Because, I mean, I did notice that as one of the sweeping concerns of DOJ, was that, you know, it was basically that and the point you just made that it may not be really necessary. So is there any point you'd like to make contrary to what Mr. Mohr said regarding the fact that courts are not likely to see, you know, foreign laws as applicable in this area?

MR. ADAMS: You know, even if they don't, there are still plenty of laws here domestically that could complicate this issue, right? And so we appreciate the DOJ recognizing that, you know, research may occur across national borders and that that is yet another area of complication. But even domestically, we see this as a problem.

MR. GREENBERG: Sure. Mr. Williams?

MR. WILLIAMS: Yes, thank you very much. I mean, we, of course, respect DOJ's opinion, but I agree that if the main problem there is foreign laws, I mean, I've never thought of foreign laws as being part of that limitation on the exemption. So, if you need to clarify that, you know, I don't think my clients would have a problem with that, and we would support otherwise retaining the limitation.

I will say one important thing to note about

DOJ's involvement here is that we often hear that there's this ominous threat of criminal prosecution against good-faith actors. And I think DOJ's participation in this proceeding over time has demonstrated that that's just not realistic. DOJ is not out there looking to prosecute people who have done nothing wrong, who have accidently violated this exemption. That's just not reality. And DOJ's participation, even though I may not entirely agree with their ultimate recommendation, shows me that they're taking their responsibility seriously. They're not looking to file unnecessary cases, and the speculation and fear that's out there is stoked not by DOJ filing cases but by something else entirely.

MR. AMER: Can I ask a follow-up --

MR. GREENBERG: I'm sorry, go ahead, Mr. Amer.

MR. AMER: Sorry. So, I mean, you know, I take your point on that score, but I think a question still is, what work is the other laws provision really doing from a copyright owner's perspective? I mean, if the other laws still apply and, you know, people are on the hook to know what their obligations are regardless, is there a need to tie that compliance to liability under § 1201?

MR. WILLIAMS: Sure, thank you for that question. I think, if I recall correctly, DOJ discussed this a bit, and their recommendation in the filing was, you know, remove it from the regulatory language but insert it into the recommendation to make it clear to people that this exemption doesn't allow them to violate any other law. And so my view on that was why change the exemption language that we've had for some time that clearly states in the body of the C.F.R. that you can't violate other laws and move it into what has been criticized today as an overly lengthy recommendation. It's in the regulatory language that other laws need to be complied with.

I would also say that Congress included that language in the statute in a number of places, and DOJ acknowledged that. I think I have a different opinion than what they reached in that they said, well, over time, you know, maybe Congress shouldn't have done that. I think Congress was wise to do that. So that's a difference of opinion, but that's where we come out on that point.

MR. GREENBERG: Sorry, go ahead, Mr. Amer.

MR. AMER: No, I'm sorry. I mean, I think, you know, the response to that seems to be, well, the current regulation does more than put people on notice

that other laws still apply. It ties coverage of the exemption to compliance with other laws, and so it raises the stakes in terms of to one liability for violations of other laws. So, you know, do you have a -- do you see that as a legitimate concern and could we, you know, take DOJ's suggestion of just incorporating instead language in the exemption that says this doesn't obviously, you know, free you from the obligation to comply with other laws?

MR. WILLIAMS: A legitimate concern, yes. Justification for changing the regulation, no. I mean, I do assume and believe in the good faith of the folks who are putting forth these concerns. But, as I said, Congress saw fit to incorporate this into the statute itself, and that indicates a preference that when you're dealing with exceptions to the statutory regime, you don't beg for other laws to be violated, and I don't think that it's wise policymaking to separate the two.

MR. GREENBERG: I want to get back in a minute to the issue of how it appears in the permanent exemption in 1201(j). But, first, I do want to clarify and put a finer point on what Mr. Amer just said, which is that DOJ is not recommending, you know, a carte blanche or a get-out-of-jail-free card with

other laws. It's not saying that the 1201 exemption is a safe harbor from other laws but saying that 1201 is not conditioned on compliance with other laws, but liability under those laws may still be a concern.

And I don't think they were actually saying, unless I misread, to move the current other laws language into the recommendation language. They actually provided separate language they thought struck a slightly different balance. So I do want to hear from other folks, other hands up, starting with Mr. Scarbeary and then Mr. Mohr, what they think about that approach to the balance. And then I want to get to this issue of statutory construction and 1201(j). And then we really do need to turn to the privacy portion of this panel. So, Mr. Scarbeary?

MR. SCARBEARY: Yes, just to briefly address something there. As far for the rules of statutory construction here, 1201 is somewhat of an oddity in that it includes this reference to all other laws. Obviously, § 106 doesn't include similar language, so it's somewhat odd that this language is included there, and we think DOJ's modification fixes some of the conditional problems we've identified, but we still maintain that there's no way the exemption could really be read to also be an exemption to the CFAA.

Also, to briefly address something, I can't remember who said it, I believe it was Mr. Williams, that we should confine this here to the language in the permanent exemptions in the statute. The purpose of this rulemaking is because Congress recognized that those exemptions would probably and most likely be insufficient going forward, and so simply sort of anchoring the language to how it exists in the statute makes no sense in that context. But I'd be happy to let Professor Reid and Mr. Adams expand on that point.

MR. GREENBERG: Well, I recognize your point that this is supplemental to what's in the permanent exemptions. I do want to get back to that question in a second. But, first, I want to sort of wrap this up on DOJ's proposal. Mr. Mohr? Mr. Mohr, you're muted.

MR. MOHR: Yeah, this is not my day for muting. My point will be extremely brief, which is, you know, the more we start talking, our friends have been discussing the problems with all these other laws, and, to me, that seems to pose quite a hurdle in causation. In other words, if all of these other laws are problematic in stopping this kind of research and they are somehow in the way, then the statute is not in the way. I believe the Copyright Office raised these concerns in 2018 at a minimum.

And so, you know, to the extent that that's a factor here, I mean, that is not -- I don't think it's wise to broaden the exemption based on that. That's it.

MR. GREENBERG: Okay. So I actually had that question lined up because it is in our 2018 report that this a consideration for causation. So I see Mr. Adams' and Professor Reid's hands up, so if I can start with Mr. Adams and then Professor Reid, just your thoughts on this issue that if causation -- if these other laws play into causation that 1201 is not, in fact, the cause of the adverse effect, it's that this act of circumvention would violate some other law. Do you have a response to that, Mr. Adams?

MR. ADAMS: Yes, and so my response is pretty simple, is that because they are tied conditionally to 1201, all these other laws become part of 1201 and are part of the problem here, right, and so severing that conditional link doesn't make them not a problem for researchers, right?

Here's my other way I think about this conditional link, is that, you know, tying all other laws to a temporary exemption is like sedating a wolf in the wild for scientific research except the sedative stops working if you disturb any other

animal, right? Disturbing other animals, including bears like the CFAA, always comes with its own risks, but it shouldn't cause the wolf to wake up and eat you, right?

MR. GREENBERG: I'm definitely not sure I follow the analogy, but I think I understand, I think the point you're trying to make, is that, you know, you should be able to tinker with one without being -- without worrying about that other one being what bites you effectively?

MR. ADAMS: Exactly. You know, the legal landscape around security research is complex and tangled, but severing this conditional tie here helps to simplify the sort of legal analysis that researchers have to go through.

If I could, I wanted to quickly respond to Mr. Amer's question about what work this conditional relationship does is that it provides a world of other legal triggers for litigants who might like to use the DMCA, but there's actually no copyright infringement going on, right? And so it's, oh, you can find any other violation of law and then proceed under DMCA rather than whatever that other law might be.

MR. GREENBERG: Why would someone do that?

MR. REID: Well, Mr. Greenberg, if I could

put a finer point on it, I think that the --

MR. GREENBERG: Yeah, Professor Reid, go ahead.

MR. REID: I think the trigger here is § 1203, which says any person injured by a violation of § 1201 or 1202 can bring a civil action, right? So this takes the violation of any law and, indeed, now that the Department of Justice has sort of suggested that extraterritorial laws might apply, that's a new concern to grapple with. But also, thinking about the array of mundane and local laws that we might never think of, I think Professor Halderman brought up in one of the previous hearings the example of the electoral code.

If I'm considering legal risk for violating the electoral code, I'm not worried about a company like Apple coming and suing me for violating the electoral code, but I might worry about a company being able to use a violation of something like the electoral code to drag me into federal court to seek statutory damages --

MR. GREENBERG: Does that raise a concern that the penalty can be disproportionate to what it would be under the other law? Is that what you're saying?

MR. REID: Correct. I mean, we could be talking about minor civil violations with small or no fines. There could be code enforcement. And I think also I would tie it to the level of risk, right, where you'd say that the likelihood of a local code inspector ever even knowing about something like that is low. But, if you've got a very motivated opponent who is looking for things and you say, you want to shut down this security research, go find any law that they have violated at the local, state, federal, or international level during the course of their research, that's a much --

MS. SMITH: Can I --

MR. REID: -- tougher risk calculus to deal with. I'm sorry, Ms. Smith.

MS. SMITH: Can I just probe the 1203 point for a second since this is, like, marrying the statutory language and regulatory exemption. Are you aware of any threatened or actual litigation brought by -- I don't know how you would describe this universe, but let's say a universe like the electoral code purveyors who kind of get into 1201 land because of this limitation that has been brought. Is this a real concern?

MR. REID: It's a real concern for people

who are doing -- and perhaps somebody like Mr. Williamson can speak to this. This is a real concern for people who are providing legal advice because the range of questions that they've got to answer is not simply, are you doing good-faith security research within the metes and bounds of § 1201, but is everything that you are doing consistent with every other law at every other level of abstraction, and that's the issue we're --

MS. SMITH: Sure, but I think my question is in the 23 years of the DMCA, have we seen § 1201 being brought on, you know, added to a state law claim or a foreign law claim or something else where otherwise you wouldn't normally think it would be implicated because of this provision?

MR. REID: I mean, again, to the point that's raised earlier, we've seen relatively little 1201 litigation, and, again, we're operating here around the need to affirmatively demonstrate. And I see my colleague, Mr. Reed, raising his hands here. I would say --

MS. SMITH: He's gesticulating.

MR. REID: -- no one wants more lawsuits here, by the way, to the point earlier. But we're dealing with people who need to affirmatively

demonstrate that their behavior is sufficiently not risky, for example, to get the go-ahead from their university or their company to move ahead. And when somebody like Mr. Williams --

MS. SMITH: Okay.

MR. REID: -- is giving them advice, he might well say, hey, look, if I've got to justify that you are complying with every single other law, I cannot bless you doing this given that you're likely to run into --

MR. GREENBERG: But, again, the question is, are researchers being told that by university counsel? Are they being told not, well I can't say you can do this, but I actually am telling you as, you know, the legal counsel for your employer that if you do this, you will not be covered by the university or protected by the university?

MR. REID: I might defer to my colleague, Professor Halderman, or Mr. Williamson on that one.

MR. GREENBERG: Professor Halderman, do you want to have a response or, if not, Mr. Williamson?

MR. HALDERMAN: This is Professor Halderman. There's only so much that I can say about the content of conversations with university counsel.

MR. GREENBERG: Sure.

MR. HALDERMAN: But I will say that this has been a dimension of conversations that I've had, just speaking personally.

MR. GREENSBERG: Okay. I probably can't -- I hear you just saying you can't really say more than that. Mr. Williamson?

MR. WILLIAMSON: I'll speak to a comparable limitation, which is, in the reverse engineering exemption, the "lawfully obtained" language, which I think in a similar way sweeps in other laws because you have to ask the question of, you know, what law might you have broken in obtaining this thing. And so I have certainly advised developers who were reverse-engineering software in a way that would otherwise have been exempt under the exemption, but there was a concern as to whether they might have violated terms of service or simply breached contract and, you know, what other laws might count and how minor a violation might then give rise to CFAA liability is a real concern and has been a point of advice.

MR. GREENBERG: Okay. Before we move on to the last thing I wanted to ask about with regard to the statute itself, but I do want to just ask again what Ms. Smith mentioned and particularly to you, Professor Reid, since I know you're really well-versed

in this and have been working in this area for many years, as have many of you, I know. But the fact that after 23 years, we've seen so few cases regarding a security research exemption generally, what does that tell you about how well the exemption is working? It would seem -- I mean, we hear in this context often that if something isn't resulting in litigation, it must be because parties have figured out a way to make it work.

MR. REID: So I think the way to read that is twofold, and I'll go back to my remarks at the beginning just very briefly to say, one, the office has significantly broadened the scope of the exemption since 2005 and, in tandem, the degree of security research and the degree of cybersecurity as a national both threat and policy priority has increased pretty commensurately. So I think what we're doing each time we come to this exemption is bringing to you the increased seriousness, and I think we're in a very different place than we were 15 years ago in terms of the type of research that's being done.

And so I think, you know, one thing to read that is the office's continued broadening of the exemption has been helpful. I think the other way I would read this, and I would broaden this to § 1201

generally, is, as you're considering the balance of the equities here, consider that § 1201 is basically never used by the opponents of the exemption in litigation against, as far as I can tell, just about anyone for just about anything so that the equities on the other side are fairly marginal here, particularly because copyright infringement is always available as a remedy, as are the other laws that we're talking about here if they're indeed violated, though, because of the way that 1203 operates, they may not be available to the same people, and so that may raise a different set of questions.

MR. GREENBERG: Do the opponents have anything they want to say in regard to that since that did sort of sweep in their equities? If not -- yeah, Mr. Mohr?

MR. MOHR: Just that some of this discussion has been a bit confusing to me in terms of basic concepts of Article III standing and how -- one, standing, two, you know, concepts of fair notice that are routinely imported into the construction of statutes. Again, you know, there are aspects of this discussion, I think, where Mr. Troncoso's earlier comments about the wide range of hypotheticals that come subject to this proceeding are particularly apt.

That's all.

MR. GREENBERG: Okay. All right. I --

MR. AMER: Can I just follow up quickly before we move on?

MR. GREENBERG: Yeah.

MR. AMER: I'm not trying to belabor this, but, I mean, can you or any of the other opponents give an example of what sort of work this provision is doing that is relevant to copyright? I mean, if we're being told by the agency that enforces these statutes criminally that this link is not necessary to protect criminal enforcement of the CFAA or any other relevant law outside the copyright context, what's the best argument for retaining it? Yeah, Mr. Williams?

MR. WILLIAMS: Thank you. I mean, I think it's hard to come up with every potential hypothetical, but there are related statutes that are of great import to content creators and distributors. One would be cable and satellite piracy, for example. And the DMCA was passed after the statute that covers cable and satellite piracy, and there's a lot of cases if you go looking out there. There may be more cases actually under the DMCA related to this than any other issue about cable and satellite piracy. And so that's one example of another law that does have a

content-based focus that is complementary to the DMCA and that I don't see a harm in requiring compliance with both in order to get the benefit of this exemption. There's probably more examples out there, but I don't think it's fair to say that all of the other laws that could be violated have no relationship to content protection, including the CFAA as well.

MR. GREENBERG: Thank you, Mr. Williams. I am going to move us on to one last question on this and then the privacy issue, and this is because we already touched on this and I said we were going to come back to it. But, to the proponents, I wanted to ask, because several of the opponents noted the similar language in 1201(j) regarding other laws, and the office in 2018 said that it believes it's generally appropriate for the exemptions to track the relevant statutory language where possible.

Obviously, at the same time, as was noted, this proceeding is supplemental to the permanent exemptions and is designed to fill gaps where a need may have arisen that Congress didn't foresee. So the question the office has is, why shouldn't that principle continue to apply, that principle of tracking the relevant permanent exemption language where appropriate? And do you find a problem with the

register recommending temporary exemptions that use broader language on this limitation than the permanent exemption? Mr. Reid?

MR. REID: This is Blake Reid. Mr. Greenberg, could I ask you to clarify what you mean by "broader" in the last question?

MR. GREENBERG: Yeah, broader in terms of it maybe would remove some of the limitations that would be in the permanent exemption.

MR. REID: Absolutely. So I'd first note, you know, I think it was 12 or 13 years ago when we first -- when I was first asked about 1201(j), and we've established many times over the years the infirmities and shortcomings of § 1201(j), and I would note that those are baked into the office's renewal of the existing exemption. The scope of the current exemption importantly goes beyond 1201(j) in a whole range of respects.

And so I would suggest that as a general matter, that's a settled question that hasn't been properly noticed in the current context that we're in, whether it's appropriate as a general matter. I think it's well-settled, and I think proponents and opponents alike have stipulated to that.

As to the specifics of the exemption, I

think Mr. Scarbeary pointed out earlier exactly the point here, which is Congress didn't know in 1998 what sort of world we would be living in. I think, if you said to the drafters of the DMCA that we would be dealing with, you know, foreign actors conducting cyber attacks on electronic voting machines and that copyright law was somehow going to be in the mix, I think they would have been quite horrified and I think they might have drafted the DMCA in a different way.

The one wise thing that the drafters of the DMCA did, or one of the wise things that the drafters did, was they put in this triennial review process and quite explicitly in the legislative history at several points that the purpose of this is to exercise some humility here and understand that the world that we were living in in 1998 may not be the world that we live in for the duration of this exemption.

And so I think the sort of calls to import pieces of the permanent exemption, whether that's 1201(j) or 1201(i) or (g) or (f), are appropriate only insofar as the current world that we live in bears any resemblance to the world that we lived in in 1998. And I think I could pretty unequivocally say, and I'm sure Professor Halderman can speak to it in greater depth, that with respect to security and with respect

to the kinds of security threats that we deal with and the important role of in dependent security research, that the world we live in today looks almost nothing like 1998, and so continuing to call back to the statutory exemptions, I think they are effectively, you know, relative to the temporary exemption, we've so far moved past them in the last dozen years of this rulemaking that I'd urge us not to go back to them. I don't think they have much relevance here.

MR. GREENBERG: Okay. Thank you.

Professor Halderman, can I just ask you to briefly, and I really mean briefly, respond to what Professor Reid just said about how much the world has changed? Then I want to go to Mr. Taylor and Mr. Williams, if your hand is still meaning to be up -- it's not. So Mr. Taylor and then I want to move on. So, Professor Halderman, is there anything you want to quickly add to what Professor Reid just said?

MR. HALDERMAN: Well, just Professor Reid is exactly right. The world looks completely different today in terms of cybersecurity threats and in terms of the shape of the defensive community of how much we are relying on a broad community of academics and individuals and companies to keep all parts of our infrastructure and society safe. So --

MR. GREENBERG: I just want -- really quickly, I'm sorry, I didn't want to ask this, but I do now. Causation, though, remains an issue, right? So you're saying that circumvention is needed to do the research that you and others want to be doing. It is needed in the 21st century. It can't be done through other means that don't involve circumvention?

MR. HALDERMAN: Often that's the case, yes.

MR. GREENBERG: Okay. Mr. Taylor?

MR. TAYLOR: Yes, real quick. I would just point out that when you ask about whether or not the statutory language should be imported into the exemption, I would just go back to the purpose of this rulemaking. The prohibition is a broad prohibition. The permanent exemptions are fairly narrow, and the exemptions that you're supposed to create in this rulemaking are supposed to be on evidentiary record. So, if there is no compelling reason to remove the statutory language, then that's because the proponents haven't proffered enough evidence.

MR. GREENBERG: Okay. Thank you. So I want to move on now to privacy. I do want to make sure everyone saw in Software Freedom Conservancy -- did I get that right? I believe I did. In their reply comments, that they originally had made a proposal for

a temporary exemption. The substance of the exemption didn't really change. But, in their reply comments, they did take the position which had been suggested by some of the opponents that it really belongs in a different request for a different temporary exemption. So just want to make sure everyone's aware of that. And then I just want to ask a few questions regarding the substance of the exemption itself.

So several of the commenters said they opposed the privacy exemption for security research because the current exemption already covers privacy research. DOJ and Rapid-7 both basically said, if I understood correctly, the current good-faith security research exemption covers the type of privacy research that Software Freedom Conservancy was asking for an exemption for. And Consumer Reports said that they were in support of the office simply clarifying that the current exemption already covers this, so maybe they didn't think the language was clear enough in the register's recommendations but that the regulatory language itself should and did.

So to what extent does the current security research exemption cover these uses? And to be clear, Software Freedom Conservancy asked for support to cover not just privacy research but permitting the

disabling of functionalities that enable a product to obtain access to personal information. So if we could start with, Mr. Williamson, I'm curious of your thoughts on to what extent the current exemption covers that, and then some hands.

MR. WILLIAMSON: Sure. So, you know, what we pointed out in our initial proposal is that the security research exemption, you know, requires this nexus to a security flaw or vulnerability, and we gave examples of a couple of specific, you know, sort of privacy research publications where, you know, the researchers were effectively researching whether personal information was being disclosed in a way that was not necessarily insecure but was otherwise violative of privacy. For example, it was contrary to the product producers' disclosed privacy practices. And so our contention there was it was not clear that these issues could be called security flaws or vulnerabilities.

Now I also want to exercise some humility here. Software Freedom Conservancy represents the interests of users of products and software. We do not necessarily represent the security research community directly, and I recognize that there is expertise on this panel that we don't necessarily

have, and so I certainly, you know, would like to give proper deference to the opinions of those who are in the weeds doing this work.

MR. GREENBERG: So I do want to hear from others, but I do want to ask you one quick follow-up question, which is the request asking for the exemption to cover disabling of functionalities, et cetera. That has some historic comparison in the phone unlocking situation. But the justification for allowing circumvention for this purpose was not clearly spelled out in the petition or the subsequent comments that were filed. So can you just clarify the rationale for why that would be justified under the triennial rulemaking process and under this exemption?

MR. WILLIAMSON: So, you know, I think that we distinguished in our initial comment that, you know, we recognize that that consideration was really more relevant to the permanent statutory exemption at § 1201(i) and that this process probably wasn't the appropriate place to discuss sort of individual remediations of privacy issues. And so, you know, that was sort of our position, was that we were focusing on the exemption for researchers and we made a sort of general recommendation to the office to consider some expansions to 1201(i) as a sort of

recommendation to Congress, but we recognize that that's not something we can really address here.

MR. GREENBERG: I'm actually kind of wondering if we can resolve this pretty easily. I just wonder if -- it sounds to me, and I did see that in your comments, but like you would support removing that portion of the requested temporary exemption and just we could clarify the language so that it would cover the type of privacy research that DOJ and Rapid-7 and others are saying already is covered by the current good-faith security research exemption. Would that be an accurate framing of your position on this?

MR. WILLIAMSON: Yeah, if the office was willing to clarify that these activities that we've outlined are covered by the existing exemption, then I think that that would cover our concerns.

MR. GREENBERG: Okay. Thank you.

Mr. Troncoso, do you have thoughts on that? I know actually BSA was cited specifically in the comments as being supportive potentially of this as a separate exemption.

MR. TRONCOSO: So I think that it is certainly deserving of consideration, and I think we would need to look at a fulsome record to really put a finger on sort of the scope of what that sort of

exemption would cover. I do want to flag some concerns with the Software Freedom Conversancy's reply filing and the sort of language that they highlighted as a potential path for creating a new exemption. If you look at the language that they've suggested, it would allow for circumvention to remove functionality in any software program that collects or disseminates personally identifiable information regardless of whether that is functionality that the user of that program is made well aware of.

So this is not necessarily like a flaw in the program or a vulnerability in the program. So, you know, I take the Software Freedom Conservancy's point that there are certainly instances where there are flaws in programs that are making people's personally identifiable information available in ways that neither they nor any reasonable user would expect, and we want people researching that sort of thing. But the language that they've proffered here would be a far broader exemption than that.

MR. GREENBERG: Yeah, I do want to follow up on that, Mr. Williamson. To what extent is the problem here caused by anti-circumvention prohibitions? And to what extent is it about market decisions and is there a market solution, right? You

walk with your feet. You know, as a consumer, you just don't use the cell phone company that's selling all of your data and all of your geotracking location information. You go to a cell phone company that's offering you more privacy.

MR. WILLIAMSON: Sure. Well, I'd first like to point out that, you know, I think the language being referred to is in our initial comments and not in our reply. Our reply was basically on the security research exemption. You know, we addressed this general point that, you know, privacy concerns in the U.S. are sort of generally addressed by this. You know, you've got notice and choice to, you know, choose the products that you think will preserve your privacy.

I think what history has borne out is that consumers are not well-equipped to make these judgments sort of a priori. It tends to be after security researchers, privacy researchers, have gotten in there and demonstrated issues. So I think of, for example, the Samsung television that responds to voice commands, and, you know, a lot of people bought it and then were surprised to find out what responding to voice commands means is that there's this constant stream of voice communication being recorded, you

know, all the time and being sent back to Samsung's computers somewhere, right?

And so even where the feature itself is sort of well-disclosed and you could say, you know, they had notice of it, it's not clear to most consumers what that actually means in terms of privacy concerns. And so I think that it's not sufficient to protect consumers.

MR. GREENBERG: Okay, Mr. Reed? And then Professor Reid. Mr. Reed, you're muted.

MR. REED: I think I'd love to see what Mr. Williamson's text is. But he does point to something that we're all working on and considering, which is the differentiation between what's disclosed in a notice-and-consent regime where, in fact, people are consenting to something they're not aware of. So, like Christian, this is something that our industry is obviously very attentive to. And it's worth recalling that the FTC has oversight over this under Unfair and Deceptive Trade Practice, but to Mr. Williamson's point that I'm sure he would make is, but if we don't know that that's happening, then we can't go to the FTC.

So I want to make sure whatever exemption that they're requesting is limited to the ability of

security researchers to help find that and to work with industry to discover those problems as opposed to the original proposal, which also included the ability to make tools that would essentially disable functionality. That creates its own separate problems.

So we're probably in a place where we may be able to agree. I'm caveating that. But I think Mr. Williamson raises points that I think all of us on the software industry side are very well aware of and are participating in this kind of industry shift away from a consent regime that doesn't reflect what people are accurately consenting to. So I'd love to see the final language on that so that we may be able to support.

MR. GREENBERG: Can I just ask, do any of the opponents disagree that the current good-faith security research exemption covers good-faith security research for the purpose of detecting privacy flaws and things like that?

MR. REED: No, we do not disagree.

MR. GREENBERG: Okay. Mr. Troncoso, I saw you nodding your head. BSA does not disagree with that either?

MR. TRONCOSO: I don't disagree.

MR. GREENBERG: I think, on this, we may have a point of agreement that we could clarify or solidify through a post-hearing letter, so we may follow up on this. I need to talk with my colleagues. This is my first time doing this, so, hopefully, I'm not speaking out of turn. But it is nice to hear the proponents and the opponents sharing some agreement on this point. Unless there's anything -- yes, Professor Reid, I see your hand is still up. If it's brief, I'll note we're almost 10 minutes over. But, if it's brief -- just anything you wanted to add?

MR. REID: I'll note that Mr. Scarbeary and I are late for my class, so I'll be very quick and say that I think we're largely in agreement as well with the position that Rapid 7 has struck out that the security exemption largely covers the kinds of privacy researching activities that have been discussed. We would urge if the office were to take a different result to recall that the scope of the term "security" has been recommended for renewal in the existing exemption. So that should take great care not to suggest any narrowing of that term that hasn't been properly noticed or comments solicited on it, which would potentially give some rise to some APA problems. Thanks.

MR. GREENBERG: Okay. Thank you. So, with that, I'm going to dismiss us all for lunch. I know a handful of us are getting back on this in about 30 minutes probably. So thank you all for being a part of this session. I hope it was as much fun for you as it was for me. And it was definitely very informative to have you all helping us fill out this record. So thank you.

(Whereupon, at 12:39 p.m., the hearing in the above entitled matter recessed, to reconvene at 1:30 p.m. this same day, Thursday, April 8, 2021.)

//

//

//

//

//

//

//

//

//

//

//

//

//

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

(1:30 p.m.)

MS. SMITH: Hello, everyone. Welcome back. Could those who are participating in this next panel please turn on their video.

MR. REED: Hello again.

MS. SMITH: Hello. Great. Well, I think we're all here, and I will just very quickly summarize what we're doing. So I'm Regan Smith, General Counsel at the Copyright Office. We are here for our hearing on Class 9 for the § 1201 rulemaking, so this concerns the proposed adjustment to the exemption for literary works in connection with medical device data.

So someone from the Government will be posing questions. You can use the "Raise Hand" button on Zoom or waive your hand if that's not working for you. Try to speak slowly for the court reporter and mute your audio when you're not speaking. And I think, with that, we can just introduce ourselves. So, Mr. Amer, Ms. Kern, and Mr. Greenberg?

MR. AMER: Hello. Kevin Amer, Deputy General Counsel.

MS. KERN: Melinda Kern, Ringer Fellow.

MR. GREENBERG: Brad Greenberg, Assistant General Counsel.

MS. SMITH: Mr. Zambrano Ramos?

MR. ZAMBRANO RAMOS: Hi. Good afternoon, everyone. Luis Zambrano Ramos, Policy Analyst at NTIA's Office of Policy Analysis and Development.

MS. SMITH: Thank you. And, Mr. Pearlman, could you please introduce yourself and have your students introduce themselves as well?

MR. PEARLMAN: Jef Pearlman from USC on behalf of the Coalition of Medical Device Patients and Researchers, along with my two students, who will introduce themselves. Keon, let's have you go first.

MR. ZEMOUDEH: Hi. Keon Zemoudeh, Clinical Intern at the USC Intellectual Property & Technology Clinic, on behalf of the Coalition as well.

MS. MCCLELLAN: And Kate McClellan, Clinical Intern with the USC Intellectual Property & Technology Law Clinic, also representing the Coalition.

MS. SMITH: Great. And, Mr. Reed, could you introduce yourself for the record?

MR. REED: Yes. My name is Morgan Reed. I am the President of The App Association, but, for today, I am here in my role as the Executive Director of The Connected Health Initiative. I am also a member of Health & Human Services' Federal Advisory Committee for Education and Outreach and am an

intervener with the FDA's work on quality metrics.

MS. SMITH: Great. Well, we're looking forward to this afternoon's discussion.

Mr. Amer, would you like to kick it off?

MR. AMER: Sure, thank you. So I think we wanted to start off with just sort of a general question for the proponents. You know, we see that you are seeking to remove certain language from the current exemption. If you could just kind of briefly summarize what the need is for the expansion, including any particular examples you can provide of, you know, an interest in or a need to circumvent additional categories of devices beyond what's currently covered.

MS. MCCLELLAN: Yeah. So we're currently seeking an expansion to include non-implanted medical devices. The current exemption includes just implanted or partially implanted medical devices. So some examples of those would be CPAP machines, hearing aids that contain data-logging mechanisms and, you know, maybe wearable cardioverter defibrillators. But, essentially, we're seeking the expansion because patients should be able to access the data from medical devices regardless of whether or not they're implanted or non-implanted. And there's been growth

in this area with non-implanted medical devices. It's continuing. It will be, you know, an area where there's going to be continued growth in new medical devices that aren't implanted. And so we're seeking to expand the exemption to, you know, allow that in the next three years.

MR. AMER: Thank you. Mr. Reed, I'd like to turn to you. I just want to make sure I am clear on the basis for your objection. So I know you're not here specifically on behalf of The App Association, but your comments do talk about an impact on app developers. You say it would, the expansion would impact the ability of app developers to successfully compete in the mobile health marketplace. Could you expand on sort of the specific basis for your concern or your concerns?

MR. REED: Right. I think the easiest thing is that we agree with Ms. McClellan that patient access to data is something that's really important. In fact, in our filings with the Office of National Coordinator under the anti-blocking rules, our work with Food and Drug Administration on, jeeze, dating back to the September 2013 mobile medical applications guidance and the cybersecurity guidance as well, a through line on this has been ensuring patient access

to data.

The problem with the petitioners' request is it essentially ignores the work that's being done by quite literally every other regulatory body in this space to make patient information more available in a safe and secure manner because, on its face, the petitioners' request is more about a right to hack than it is for a patient to access information.

So we think that right now the existence of the Food and Drug Administration's recommendation, the Center for Excellence, and the 2015 guidance that now Center for Excellence head Bakul Patel put forth is still vital and valid, and that is that the methodology by which patients should have access to their records is something that is viable under other laws, and a copyright change is something that raises significant security risks that we think is not warranted, and so long as we have these other avenues, we think that's the better process to pursue.

MR. AMER: Okay. Thank you. Let me just mention one sort of logistical item, and that is, if you would like to speak, we found it helpful if folks could use the "Raise Hand" function that hopefully you can see on your screens. It's also fine to just sort of wave your hand. We have a small enough group here

that I think we should be able to see everybody pretty easily. So, Mr. Reed, if I can just follow up, so just to sort of make sure I understand the specific basis, so is this objection one that is tied specifically to a change that is being proposed here? I mean there --

MR. REED: Correct.

MR. AMER: I mean, so how is that concern or to what extent is your concern applicable in the context of this new expansion but maybe less relevant under the current exemption?

MR. REED: Right. I think the real problem is that the -- we're facing an obvious push and pull. The Food and Drug Administration, the FDA's device center is essentially saying to us we must increase our use of TPMs, we must increase our use of encryption and, as the Petitioner notes, that this change is happening at the FDA, their request is fairly straightforward and that is, well, if the FDA is going to require all of these TPMs to be put into place, we should have an exemption that allows us to circumvent said TPMs in order to have access to the patient data.

And since the FDA already offers methodologies for patients to request data and to

petition the FDA if the devices aren't providing it appropriately, it puts us in a real conundrum: how do you meet the requirements of your 510K and the upcoming suggested whole effort that we're doing around a pre-certification program if there exist in copyright law in a 1201 exemption that we have to allow for our devices to be hacked or that we have no legal recourse if our device is hacked?

So it puts a lot of question as to how we could move forward. Specifically, if you look at the Petitioners' request, as noted, they want to move beyond the embedded devices. But it also goes so far as to say it's not just merely to pull the data out passively. It's to engage with that data to then do other activities with it and the device itself. So it really is a more intrusive hack then merely monitoring the stream of data that comes off.

So, with regards to the request, I think we all agree patient access to data is the outcome that should be, that's worth seeking. But having the access only done through violating a TPM or to break a TPM is essentially putting patients at risk, and we see that as the biggest part of the problem with the request as it stands.

MR. AMER: Okay. So you mentioned a couple

of items there. So you mentioned the piece about removing the passive monitoring language, and we're going to get to that. But the first thing you said seemed to have to do with circumvention more generally, and I know that there was no opposition filed to renewal of the current medical device exemption. So I'm just trying to understand, you know, if circumstances have changed such that there are different, you know, FDA obligations that we should be aware of?

MR. REED: Oh, yeah. So that's a good question, Mr. Amer. The part to think about is so our industry -- and I know this gets into an area that isn't normally covered, Software as a Medical Device, sometimes called SaMD or SaMD. We're really moving to a world where the FDA is very engaged on questions around not a device that's just implanted but that software itself can be considered a medical device.

And as part of that, the FDA is moving forward on something called a pre-certification program because, frankly, again, when you develop a medical device, whether it's software or something physical, you build it, you complete the product, then you go through what's called a 510K process, whereby they review the product as it stands.

Now, within that context, you are allowed to provide certain security updates or modifications for cybersecurity risks, but they're very limited and very narrow because, if any of the changes you make after you receive your 510K approval make substantive changes or changes the labeling of your medical product, you have to repeat your 510K process altogether. So the FDA is now moving forward and saying wait a minute, this slows the process by which medical devices can get into the hands of consumers, into hands of patients.

So they've undertaken a move forward on a pilot project called a pre-certification program, which essentially says, as a company, I can go to the FDA and I can show them my development methodology, my -- the way that I do privacy and security internally, the way I do privacy by design and security by design, and I essentially can shorten the period of time that it takes to get my device from the entry door at the FDA into the hands of patients. And the FDA has said at multiple sessions that both privacy and security, security in particular, cybersecurity in particular is of paramount importance for being approved as part of a pre-certification process.

If the 1201 process now says, yeah, but

really, you know, there's going to be people hacking your device and they want to be able to modify it and make changes to it --

MR. AMER: Yeah. Could I just interrupt you for --

MR. REED: -- the FDA is going to -- so the major change that's going on right now is an industrywide change to figure out how do we get products in the hands of consumers faster yet still meet the FDA's cybersecurity requirements.

MR. AMER: Right. But the question was, wasn't that also true previously under -- or now under the current exemption?

MR. REED: No, no, there has been a change in the philosophy at the FDA. The FDA has starting -- you can see it start with their 2013 guidance around mobile medical applications and the addition of what's called a risk triangle, through to more recent guidance that's come out under Gottlieb and now moving forward under the new administration, is this idea of how do we get products through the pipeline quicker, so it is a change philosophically in what the FDA is asking us to do.

Now, notably, sorry to go on, but notably, the thing to note is that the Office of National

Coordinator over at HHS is doing the very thing that Ms. McClellan asked for, which is to demand from EHR vendors and everyone else that patients have access to their health records. So FDA is saying make it secure. HHS is saying make sure there's patient access. Right now, the industry can meet those goals, well, hopefully, will meet those goals and will do it successfully. The injection of this idea of, oh, yes, and there's also this 1201 exemption for hacking and essentially right to hack or right to change the device really puts a lot of that in question.

MR. AMER: Okay. And I'm going to just ask one more follow-up and then I'm going to ask the proponents to step in. But it's not really an injection of anything new from our standpoint, is it? I mean, I guess I'm kind of --

MR. REED: Yeah, I'm sorry. If their exemption were granted, yes, it wouldn't change.

MR. AMER: But can you explain then why you did not oppose the renewal of the existing exemption?

MR. REED: The current exemption is passive for data or wholly implanted devices. And so, again, passive data collecting isn't the same as actually changing the underlying software or directly engaging with the underlying software of the device. I think

as an industry we can find ways to ensure that the underpinning code base is secure, and I want to be very careful. I think that we have a -- we can be in a good position where the passive gathering of data -- and remember it's patient records, their data. I think that's something that can be done in a way that facilitates patient access but doesn't put the underlying secure code at risk. This expansion is a change in that.

MS. SMITH: Can I ask, is it two aspects of the expansion that we're talking about, or is it the same aspect?

MR. REED: Two.

MS. SMITH: Because there's passive collection of data, okay.

MR. REED: You're on it.

MS. SMITH: So there's passive collection of data that seems okay. And the difference is whether the medical device is implanted or not implanted, is that not a distinction really worth worrying about to you?

MR. REED: Yeah, I think that's a distinction.

MS. SMITH: Okay.

MR. REED: I think we agree with the

petitioner in the sense that the continued growth of medical devices that are, in fact, wholly contained in software is something that is going to continue to expand. The question is, how do we properly secure patient safety in that environment? And so the passive collection of data is something that can -- there are ways to do it. But hacking the device is something that puts patient safety at risk and really puts us at odds with what our regulators are asking us to do in these other environments.

MS. SMITH: Okay. So implanted versus not implanted is not the question. Okay. Thank you.

MR. REED: I think it ends up being a distinction without a difference because, you know, where it sits on your skin, how we engage with it, I think it's one of those where, again, a lot of this is in constant motion. We're hopefully developing amazing wearables that are more able to do things than you can do with an implanted today. But that's where the industry is hoping to go. So I think that the passive gathering of data is something that, whether it's implanted or not, is not the primary area of concern that we have.

MR. AMER: Okay. Mr. Zambrano Ramos, I think you have a question?

MR. ZAMBRANO RAMOS: Yes. Thank you, Mr. Amer. This question is for Mr. Reed. I was hoping you could elaborate a little bit more on this notion that the 1201 process kind of would inhibit you from following other directives from other federal agencies, that you have to build a strong network. I'm not sure that the 1201 process requires you to not do that or do the opposite. So I'm just curious if you could elaborate a little bit more what you're saying about that.

MR. REED: Right. No, that's a great question. So the problem is, again, back to the direction that the FDA and other regulatory bodies have headed with us, which is we want you to show us how you are securing your device, how are you limiting access to your device, right? So they want us to demonstrate, as petitioner noted, all of the ways in which we are building stronger and more capable TPMs.

So within that framework, if there exists the idea that there is no legal recourse under 1201 or under any legal recourse -- because, remember, there was a little confusion in the petitioners' request. The FDA doesn't regulate patients, it regulates medical devices. And so Petitioners said, well, the existing FDA laws still apply, and so, if a patient

does something, nothing happens to a patient. The FDA doesn't regulate patient activity, it regulates us, medical devices.

So the problem that we run into is, in order to allow what's being requested by petitioners, we will find ourselves in a position where we need to demonstrate to the FDA all of the TPMs that we're putting into place. And if there is a legitimate 1201 exempted use that's undergoing at the same time, especially one that could end up leading to harm, the FDA is going to say, well, what are you doing to prevent this use?

And it's very reminiscent of what happened recently to Medtronic and the Minimed 503. There was not actually a hack, nobody died, and there was no harm to patients, but what was discovered is that Medtronic had not secured their network stack carefully enough and they had to do a recall on an insulin pump. So even though petitioners are requesting the ability to do a little more intrusive hacking and listening, we have our regulators saying, if you don't light it down -- lock it down tighter, we're going to make you pull your product off the market until you then make that modification. So that's some of the concern.

MR. AMER: Okay. But you can make the TPMs as strong as you want, right? I mean, this doesn't place in any respect --

MR. REED: Well, that's -- yeah, that's the -- and then we have the escalated --

MR. AMER: -- a genuine exemption -- a genuine exemption --

MR. REED: Right. That's --

MR. AMER: -- doesn't place any obligation on you to alter your practices with respect to implementing code of law.

MR. REED: So now we're in the arms race game, right? Now we get into the arms race game. And what makes this a little different than the traditional consumer products as far as arms race is remember we are very limited on the changes that we can make that don't trigger an additional 510K process. So, unlike the arms race that could happen on say Netflix, where somebody hacks it, they modify the code, it gets hacked, they modify it, we have to be very careful that modifications that we make to a medical software doesn't trigger an additional 510K review. So what you described, Kevin, is right, we can build better TPMs and we will. But understand, if there are legitimate legal attacks that are coming,

we're going to be facing additional escalation.

MS. SMITH: Well, I guess I have a question. Are you suggesting that if this adjustment is made that the TPMs that are employed will be so, you know, deprecated that you'll be able to no longer use them? In which case I wonder, is that something we could address by the contours of the proposed adjustment? Because we do have exemptions in other instances, right --

MR. REED: Right.

MS. SMITH: -- for Blu-ray discs or DVDs, and those are still in the market because they are --

MR. REED: Right. They're in the --

MS. SMITH: -- we do not prohibit going after people who violate, you know, who go outside the bounds of something that is likely to be non-infringing.

MR. REED: So I think part of the problem with this is I would make a venue argument. The proposed construct of the ONC rules guarantees sharing of patient information with reasonable safeguards, including ones that protect security. So we're bound by those Office of National Coordinator rules to do this. So that's part of the problem that we have from the get-go. Your question is, well, could we find

contours? I'd argue the goal of the petitioner is already being met in other venues, and this opens the door to abuses or potential abuses that I don't think are necessary to achieve the goal.

MS. SMITH: Well, I guess there's two issues, right? Under the statute, if there's not an adverse effect, and it's already achievable, that's another issue we can look at, we should probe those questions. But, if you are saying on this question that this exemption will cause some harm to the industry, I think we want to understand a little bit more where that concern is coming from and I want to, like, have a little history.

MR. REED: Oh. Yeah, I think -- I'm sorry.

MS. SMITH: But let me just say one thing because we heard from the FDA in 2015 and they didn't really indicate a reliance interest on the DMCA. They did express some statements about the original medical device data limitation, and how the Register addressed it at that time was to give a 12-month grace period to allow agencies to adjust and, you know, to the extent there was any reliance interest, you know, take it back into their own areas of expertise and not part of the copyright law, right, because we're trying to center our rulemaking on the adverse effects on likely

non-infringing use questions.

MR. REED: Right.

MS. SMITH: So I don't know if you can say anything to help us figure out if conditions have changed --

MR. REED: Yeah, I think --

MS. SMITH: -- or what to make of it. Thank you.

MR. REED: I think that the reality is the petitioner has gone further than the 2015 requests. Remember this is much more akin to a right-to-hack exemption than it is merely a patient data access question, and I think that's the thing that is concerning. As you point out, the previous exemption -- and we didn't object to the previous exemption in this case as well because I think it's something that, as you say, can respectfully center itself in where it should be standing on copyright law.

But the door-opener here to much more intrusive hacking onto medical devices is the area that raises the concern. So I think, if you look back at the 2015 letter and what they said and how do they do it, I think the two changes in industry between 2015 and now is this incredible pressure to provide a

quality basis and a pre-approval on privacy and security before your product -- before you've even gone through a 510K. So between 2015 and now, you have our primary regulator asking for this.

So I think back to your primary question, if we center this on the copyright angle, it's broader than -- it's far broader than 2015. I don't think petitioners' request makes the case that it's vital. And since other agencies are doing the very things that they're asking to do, I think the uncertainty created by their request, the potential harm created by their request and the breadth of the potential request, I just don't think there's enough there there to merit where their request is going. And, again, we stand by the fact that we're not opposed to their original 2015 request moving forward as it stands.

MR. AMER: Okay. I see, Mr. Zemoudeh, I'm going to go to you if you'd like to respond to what's been said. And then I do think we want to after that drill down a bit on this idea of passive versus active monitoring, and so we'll have some questions on that. Mr. Zemoudeh?

MR. ZEMOUDEH: Sure, yeah, and I can address some of that right now. Just to respond to a few things that opposer has said, first of all, this is a

modest expansion, we are not going to be attempting to change requirements for device manufacturers. As the Copyright Office has stated, we wouldn't be -- the exemption wouldn't be limiting the ways in which manufacturers can implement TPMs on their devices. And moreover, this is just -- this exemption is just for access to data. Opposer suggests that non-passive monitoring would lead to access to software code, but that is not the case in many cases of non-passive monitoring.

For example, in our comment, we describe SD cards on CPAP machines, and to get the data off an SD card in no way touches on the software code of the device. The SD card only stores data. That is its main function. And there is some circumvention of TPMs that is required to get that data, but there is no software code that is implicated. And we can go into other ways of non-passive monitoring that we foresee happening in the future, but, before we get there, I'd also like to mention some other points that opposer made.

MR. AMER: Sure.

MR. ZEMOUDEH: Yeah. So, as far as other penalties under other regulations, those would still be available. And even if the FDA does not regulate

patients, as opposer suggests, there are other laws and regulations that would, such as the CFAA or HIPAA. So those penalties are still in place and those might even be more tailored and more nuanced regulations that would be able to address the violations in a better way, and they might even be less severe, those penalties under those other regulations, and we wouldn't want to overpenalize patients under the DMCA when other regulations do a better job of it.

Further, opposer mentioned that there are other procedures under the FDA under which patients can get data. However, that is not the case. Under the FDA website that opposer pointed to in their opposition, you could complain to the FDA about malfunctions in your device, but that in no way implicated getting data from the device itself through those complaint procedures.

MR. AMER: Okay. Let me just stop you there. That's helpful.

MR. REED: I need to -- yeah, sorry.

MR. AMER: Well, wait, I do want to just make sure we're sort of proceeding to each topic in turn. So it seems to me that this -- and, Mr. Reed, I think you indicated that the main change that, you know, at least you've been talking about so far is the

removal of the passive monitoring language. So I think we'd like to ask --

MR. REED: Yeah.

MR. AMER: Well, let me just finish. I think we'd like to ask first the proponents some questions about what that means, and I believe my colleague, Melinda Kern, has some questions about that.

MS. KERN: Thank you, Mr. Amer. So I do have a couple questions for the proponents. So I just wanted you guys to explain a little bit how passive monitoring is having an adverse effect on any users. And specifically, like, in the initial and reply comments, the only reference was to CPAP machines and I believe to the SD cards that were within them. So I was wondering if you could also give us a couple more examples of both implanted and non-implanted medical devices that are impacted by the passive monitoring limitation.

MR. ZEMOUDEH: Yeah. So, to the first part of your question as far as other types of non-passive monitoring that might occur and how it might work in the future, although we don't have specific examples of those in our comment, some ways that might work include reading the memory off your phone from data

that your phone collects from a device. In that case, there may or may not be circumvention necessary, but it might be required -- you might be required to decode the data off the memory on your phone.

Another way that non-passive monitoring might work is to actively connect to a medical device or a receiver on that device to request the data from a program on that device, so that might include, given if the device were connected to the internet, that might include a web request on the device, and that may require authentication, and that might implicate the TPM as well.

Another way that non-passive monitoring might work would be to actively intercept the data while the data is in route to a server from the device. So although that does sound like passive monitoring in that there is a wireless communication that you intercept, the difference there is that you might actually have to communicate with the device in order to get the data. So, although you're intercepting wireless data, you will have to still communicate with the device in order to gather all the data. So those are three ways that we might see non-passive monitoring happen in the future.

MS. KERN: (Technical interference.)

MR. AMER: I think --

MR. PEARLMAN: Did anyone else have difficulty hearing that? I had a little trouble. Okay.

MR. AMER: Yeah, we had a little -- there may be an issue.

MS. KERN: Can you hear me now?

MR. AMER: No, it's still a little garbled.

MR. GREENBERG: Melinda, it might help if you turn off your video.

MS. KERN: Okay. Can everyone hear me now? I just asked, -- no, no.

MS. SMITH: No, I think that didn't work. I don't know if you have headphones to try. If not, we can -- maybe it will go away.

MR. AMER: Yeah, so this is the world we're in now where little technical issues come up with Zoom, so we appreciate everybody understanding. Just to follow up, so there are certain -- those are examples of activities that you think are currently or at least arguably not permitted under the current language, is that right?

MR. ZEMOUDEH: Yes, that's correct.

MR. AMER: Okay. I'm going to give Mr. Reed a chance to respond to that, does that -- and what I

would like you to answer specifically is, does the sort of activity that the proponents described implicate any greater copyright concerns than passive monitoring?

MR. REED: Yeah, I think two things. Well, there's three things to cover, but I want to get to yours. This is probably my fault, but I should have referred directly to the copy here. I'd remind everyone that the petitioners' request also includes number two, to permit third parties to perform the circumvention with permission on behalf of the patients. So remember this is not merely that the patient has access to the passive data, whether it's implanted or otherwise, but it's the ability of third parties to create tool sets that would allow for that change.

And that I think -- I realized as we're talking about this maybe that's part of why we're talking past each other. It's that allowance of third parties I've been referring it to as kind of the right to hack, that ability to develop third-party tool sets that raises the greatest amount of question. And, again, I don't think the Copyright Office is in the habit of granting exceptions on might, but I do want to go back a little bit to something that's very

worrisome and nationally we need to correct.

The earlier mention of HIPAA. HIPAA doesn't regulate patients, it's actually a portability, it's the insurance portability, not a privacy act. It has something called the privacy rule that was passed in 2000. But the only people that the Office of Civil Rights, which oversees HIPAA, can engage with are what are called covered entities or BAs, Business Associates, of covered entities. So the idea that the Office of Civil Rights could bring some action against a patient is ludicrous.

And that's actually what's very interesting about this whole question. HIPAA is exactly what empowers the ability for patients to go to a provider and request that information. It's an underpinning of the entire patient access to data. So the onus of HIPPA is on the provider of the covered entity, not on the patient.

And earlier there was a comment about the FDA -- you know, the FDA isn't the right vehicle. But I'd note that the 2016 guidance for everyone playing at home, I pulled it up on the screen, dated -- the manufacturer sharing patient specific information for medical devices with patients upon request is a 2016 guidance that was provided to us, and it actually

includes that manufacturers are strongly encouraged to provide patient-specific information, including data a healthcare provider inputs in the device to record the status or ongoing treatment of an individual patient --

MR. AMER: Okay, let me just --

MR. REED: -- et cetera, et cetera.

MR. AMER: Let me just --

MR. REED: So I'll jump ahead. But that's --

MR. AMER: Okay. Let me just jump in, and we do have a few different -- I mean, just to sort of preview things and we want to be conscious of time, you've raised concern -- you've raised possible alternatives to circumvention, which you just were mentioning there, so we'll get to that. You also mentioned third-party assistance, which I also want to get to. But just to sort of wrap up this question on passive monitoring, and I'm going to first ask the proponents, so there seems to be a suggestion, although it's not entirely clear to me, that active monitoring could in some cases involve altering the software of the device. And I know, you know, the copyrighted work that we're talking about here is these compilations of medical device, which is separate from the software used to operate the device.

But I think I'm interested in knowing to what extent these additional monitoring activities you're talking about may necessitate alteration or involve alteration of the device firmware?

MR. ZEMOUDEH: Yeah, to address that, it is unlikely that any of these non-passive monitoring techniques would alter the software or firmware of the device. Specifically, to go back to some of the examples that we gave, if you were to read data off the memory of your phone, that wouldn't require any hacking of the software, as opposer describes. That would just be data on the memory of your phone that you read. And in other cases, you would just be requesting the data actively or intercepting the data. So there wouldn't be any -- for the most part, there wouldn't be any touching of software.

MS. SMITH: Can I ask a question? Is there a need for an exemption that would permit touching the firmware or software, or is that something we could just exclude?

MR. ZEMOUDEH: No, there is --

MR. PEARLMAN: I can --

MR. ZEMOUDEH: There is not a -- oh, go ahead, sure.

MR. PEARLMAN: I think part of this is that,

you know, due to the chilling effect we don't know exactly what would be needed. But we do know that if someone were to, you know, to access the firmware for purposes other than accessing their medical data, that that would still be outside our proposed exemption. And, you know, you have the Copyright Office in previous exemptions, if you look at the 2018 exemptions, in several places has specifically said and not to access it for the purposes of gaining access to other copyrighted works, which could include media but could also include software.

But I'm not sure we would -- I don't think we would want to carve it out of the exemption because there might be some circumstances in which there is overlap, that in order to get to the data, something else is inadvertently accessed even though it's not used for any purpose.

MS. SMITH: Right. Well, I appreciate your spirit of invoking how we approached similar requests because that is sort of what I am thinking because it seems like if there's an opportunity for consensus to carve out some of the activities that Mr. Reed is worried about that you're not aware of a need for that might be a good way to adjust this exemption.

And one thing I wonder if you could

consider, and if you don't have an answer now, that's okay. But, in 2015, there was an exemption for auto repair that excluded access to the telematic system because there was not a record showing that was necessary. There was some concern about incidental access that was raised later. But we sort of did that incrementally upon a showing of need, and I'm wondering if that is an appropriate course to take here if we're not sure that we need to access or adjust the firmware or software.

MR. PEARLMAN: I think we might need to look a little more. I think part of the challenge here is there's not as clear a division between the telematic system and the other systems. There's not as clear a division in medical devices because we're talking about such a broad array of types of devices as there is with cars between the telematic systems and other systems. So I think it's harder to clearly carve that out without inadvertently impacting sort of normal forms of access.

I think this is a little bit closer to -- and to be clear, I'm only talking about the case you're talking about where you need to access the software in order to get access to the data. I think it's a little closer to say the carrier unlocking

exemptions, which did allow access to software sort of inadvertently along the way, but still we're not permitted to modify the software or do other things that were not otherwise exempt. So I'm not sure it works as clearly in this instance as it does, but I don't think we are against it conceptually if that makes sense.

MS. SMITH: Yeah. Mr. Reed did you want to weigh in on any of the typical design features if there are? And I realize that I did put you on the spot, Mr. Pearlman, so thank you for engaging, and keeping the line open would be good.

MR. REED: No, it's okay. I think, though, that I think it's interesting to note that I kind of feel like Jef made my point, which is there is this close overlap between the software as a medical device, what it does, and I think when you couple that with Mr. Zemoudeh's point where he said it's "unlikely that it would have an impact." The difference between a DVD player is, if you get it wrong, it doesn't kill grandma. And we are talking about devices that do deliver insulin, that do deliver shocks to the heart, that do deliver information about your blood pressure, that can affect the medication that your doctor prescribes.

So I don't think the petitioners made a case when they acknowledged that the scope is broad because of the way the devices work and the best they can merit is it's unlikely when one considers the Medtronic impact on insulin pumps that merely had a potentially readable signal and that pulled 4,000 pumps off the market. I just don't think the petitioners' case is strong enough in light of the fact that other agencies are doing the work to meet their stated need of access to patient data.

MR. AMER: Well, so, I mean, as the exemption is framed now, it refers to literary works consisting of compilations of data, but we do have lots of other exemptions that allow circumvention to access computer programs for various purposes and, you know, in many cases, you know, jailbreaking, security research, et cetera. And, you know, we have a pretty -- there are lots of examples where the Office has said, you know, that that sort of activity may well be fair use. So I'm not sure if the --, you know, to the extent that TPMs may be protecting both medical data and computer software, you know, I wonder if that would --, you know, one answer might be to consider expanding the exemption and then including language like we've talked about, you know, so long as the

circumvention is not undertaken for an infringing purpose with respect to the software.

MR. REED: I guess I don't know if that was directed at me, but I think the problem with it is, is I don't see the petitioners made the case that an exemption is needed as, again, as I said, the stated goal of the exemption is to make sure that patients have access to their data. Quite literally, most of the other arms of government in this instance are doing everything in their power to make sure that patients have access to data. And since this process, exemptions are to be granted narrowly and carefully, I'm not really sure that the barrier has been overcome, as I said, especially in light of the fact that there are these enormous forces coming to bear to get the outcome petitioners requested. I just don't think it meets the test yet, and maybe if it does, if we see in three years with it including, you know, with SaMD hitting more places, we can revisit it. But, right now, it's just not ready for primetime.

MR. AMER: Okay. Thank you. Ms. McClellan?

MS. MCCLELLAN: Yes. I'd like to just address Mr. Reed's point that he keeps, you know, repeating that patients do have access to their data or that other people, other organizations are working

to provide access to that data. But, in fact, this data isn't included in a health record that you request from your doctor. It's, you know, the raw data from a CPAP machine, that's a lot of information and I don't think that's written down anywhere in a health file that the patient can access from their doctor.

Furthermore, we're requesting real-time access for patients, so patients being able to access this data without having to go through talking to someone and filing a form and waiting to hear back and we're requesting for people to be able to access this stuff in real time.

MR. REED: So I would be happy to facilitate a conversation with the Office of National Coordinator with Micky Tripathi because the scope of the ONC rule actually does impact the ability of patients to request data. In fact, in our filings, we've actually been pushing hard to encourage the Office of National Coordinator to include two AAPIs for ability to access information where it's passed to a covered entity. Now we do have to occupy the space that is covered under OCR.

But I do think you should note that it is required that the data be provided in a reasonable and

timely way and that it even has cost restrictions. Your ability to request your data is limited; in other words, you can't be given an onerous cost when you request that data. So I think there are opportunities for us to work together to achieve the same goal, which is patient access to the data, and if that's the goal, that's great. If the goal is to encourage the development of third-party hacking tools, that's where I think we part ways.

And so I think, right now, back to Kevin's question, I don't think the bar has been met to include the language that says to permit third parties to perform circumvention. But I am happy to work with petitioners to extend the goal of data either through ONC or FDA on this.

MR. AMER: Okay. So let's take those in turn. So let's just put third-party assistance to the side for one second. But I do want to make sure I understand this dispute about whether there are adequate alternatives to circumvention. So let me start with the proponents. So I'd like you to respond to, you know, the potential alternative avenues that Mr. Reed mentioned. I know specifically in the App Association's submissions they talked about the CURES Act or the FDA's website. Could you address whether

those can provide the same type of data that you're seeking with this exemption?

MS. MCCLELLAN: Yes, I believe we discussed it in our reply comment, but we don't believe that this does provide the same access to that data, that it doesn't provide the same access to, like, the raw data from say a CPAP machine that you're going to get from reading the SD card and also, that going through that method you're still not getting real-time access, which is what we're seeking for patients who are looking to circumvent TPMs and access that data.

Also, I would just note that Mr. Reed said a couple times that, you know, he would like to work with us on gaining access to that data for patients. And, you know, we're happy to pursue other avenues as well, but the reality is that this shouldn't be a DMCA violation. And I think also just going to note that saying that, you know, his organization is working to provide better ways for patients to access that data just shows the fact that they can't access that data.

MR. AMER: Mr. Reed, would you like to respond?

MR. REED: Just to clarify, yeah, I think --

MR. AMER: Just one second. I'm especially interested in whether you have a response to the

specific point about, you know, whether through these alternative methods people can get access to the raw data and to do so in real time.

MR. REED: Right. So there are some really interesting questions about raw data access and what does it go through and what kind of APIs are available and what APIs government agencies are essentially requiring. The problem -- the thing that we're pushing for actually is kind of a step further, which is how do we make sure that the data is accessible in real time and also manageable by a third-party authorized application. So our solution to this problem, which is something that is supported by the FDA and others, is to ensure either through the use of the -- you know, we talk about fire standard and HLC-7 and all that stuff. But, ultimately, the real goal should be that your medical device has a standardized API and standardized data formats that the patient can then choose their own application to run on. But, in order to do that, there has to be an assurance of security and privacy and security most importantly.

So what the problem that it's created is, again, taking them on a good-faith effort, if the end goal is to make sure that the patients can say access their CPAP data on an app on their phone and then can

engage with their doctor, their only way the physician is going to want that data to be provided to them is if they have some sense of the providence of the data and the way that it reaches there. And that's part of the reason that you've seen these other agencies really adopt this idea of standardized messages, standardized APIs, and a way for that material to reach the physician in a format that's usable.

Now, that said, we want engaged patients. So finding that middle ground, I just kind of go back to the primary. The Copyright Office is really -- this is a space that isn't really the Copyright space's primary occupation. And so I think involving a 1201 language in this is disruptive to the end goal stated by the petitioner, and that is to get the communities aligned so that there's access to the data.

But, to your primary point, I disagree. Our meetings with the Health & Human Services, with FDA and others have made it very clear that it is a strong goal and something that they are attempting to achieve, and there are multiple opportunities to petition FDA and ONC to accomplish a more accurate and a more timely release of data.

So the rule, by the way, that governs this

went into effect literally three days ago. That's part of why my voice is worn out. The Office of National Coordinator's enforcement literally kicked off three days ago. So I don't think we're at the place where we need the Copyright Office to step in. We need to see how the 21st century CURES Act and the ONC anti-blocking rule play out a little longer than three days.

MR. AMER: Okay. Let me just -- thank you. Let me just make sure I understand. And you're right, this is not the space that we usually occupy, so this may be a very basic question. But, I mean, so say I'm a patient and, you know, I have a CPAP machine and for whatever reason I want to access the data that it's producing. What would be the procedure that you're suggesting I should follow in order to get that information short of circumventing the device?

MR. REED: Great question. So I think part of it is we are on a fast-moving treadmill. If your CPAP machine doesn't include its own connection to an application and doesn't provide that information to an EHR or doesn't provide the data to the EHR or to the physician with all of the metrics that the patient is requesting, I think that's something that's worth contacting the manufacturer about and saying where is

this data, why are we not being able to see it. Remember the patient can request information from any health developer or health info network.

So, in large part, what we're seeing is a reversal, that the industry is moving to devices that are providing data to the patients, are doing more to tie it to a mobile application that's available on your phone, to use the either Epic or Cerner or someone else's methodology to import that information into EHR. So, if you have that CPAP, the first thing I'd suggest you do is get a new CPAP that includes a connection to an app. If it doesn't have that, there are places to petition in the appropriate oversight areas of Food and Drug or the Office of National Coordinator. So products are on the market that do what they want, but I also respect that some people may not have those, so I think, you know, there is the ability to do that.

MR. AMER: Let me just jump in, and we're running short on time and I do want to get to third-party assistance, but I just want to make sure I understand this point. So you talk about going to the manufacturer. That's one option. And then what's the process that -- how would the -- if I go to the FDA, how do I get from that point to obtaining data from

this device that I have here in my house and the FDA, you know, doesn't have any connection to? That's what I'm not understanding.

MR. REED: Yeah, I understand. I mean, we're so far outside of copyright, so it's a little bit awkward. I'm trying to keep bringing it back to the copyright space. But, roughly speaking, under the guidance that's been in effect since 2016, you'd go to the FDA and say, hey, manufacturer X is not following the 2016 guidance on manufacturers sharing patient-specific information for medical devices. You can go and petition them. You'd also -- That is assuming your initial -- Kevin, that your initial question is, I went to the manufacturer and they told me no, they won't give me the data. If you're told that, then now we're into the legal recourse, and that is you can go to the FDA and say they're not abiding by the 2016 guidance.

If that doesn't work, you can also or concomitantly go to the Office of National Coordinator and say they are in violation of the anti-blocking rule or suggest that the data they're providing isn't appropriate and that the ONC's Inspector General Office needs to take action against that manufacturer. Those are all avenues that exist, and they are still

ones that exist in the framework of making sure that you don't kill grandma because you hacked her insulin pump and it overloads her insulin levels.

So I think that's -- And that's back to your third-party point, which is a lot of the areas in which you can get access to your data do involve taking an action to one of the existing regulators, and that's because they are concerned about life and welfare of the patient. So that's the juxtaposition on the -- on where we sit.

MR. AMER: Okay. Thank you very much. I want to go to Mr. Zambrano Ramos, and then I do want to just turn quickly to third-party assistance. I know we're getting close to time. Hopefully, everyone can run over just a few minutes. So Mr. Zambrano Ramos?

MR. ZAMBRANO RAMOS: Thank you so much, Mr. Amer.

Mr. Reed, first, going back to the point about this not being really the primary space where the Copyright Office plays, it's not also the space where NTIA plays. And I'm just curious that given that this is a process about copyright, should health and safety issues really figure in? On the one hand, it seemed the earlier discussion was about not

granting the exemption because it's dangerous from a health perspective. But, on the other hand, this is also, you know, a copyright proceeding. So I'm just curious if you could kind of square those few things together so that we can better understand?

MR. REED: So I think morally yes. I think the idea that the Copyright Office should be blind to the implications for health and safety is a little bit of an abrogation of kind of moral duty, which is to be a thinking person and say, yes, I understand this is outside the scope of it, but what are the implications, what doors am I opening, and as we started this, petitioner has one example of one CPAP machine. So I would say there's a little bit of a weighing of the equities here to say there is a little bit of a duty to be a thoughtful person about this. And since we're not being flooded with examples of company after company after company restricting access to patient data, I think it's pretty easy to take a stand that says, you know what, let's err on the side of safety in this instance.

So, yeah, I do think there's a little bit of a responsibility given that the proponents have brought one CPAP example from one company.

MR. AMER: Mr. Zemoudeh, if you could

respond very, very quickly, and then we're going to move to the next topic.

MR. ZEMOUDEH: Yeah, I just wanted to make the one point that as the Copyright Office has noted, the question here is whether adverse effects are occurring and whether the patients are making non-infringing uses of the underlying data. And if Congress wants to directly or indirectly regulate medical device safety, they can, but there has been no indication that Congress wants the Copyright Office to do this. And the amount of time that we have spent trying to parse out FDA regulations and the CURES Act here underlies the fact that really this is a congressional area and not something the Copyright Office needs to deal with.

MR. REED: I'd agree and that's why we shouldn't grant the petitioner, it's really not necessary.

MR. AMER: Okay. Thanks. So I'm going to turn it -- hopefully Ms. Kern's audio is back on track. So I think she had some questions on third-party assistance. Just bear with us one second.

(Pause.)

MR. AMER: Okay. I think it's still not working unfortunately. That's okay. So, on the third

parties, to the petitioners, you've asked to add language that would allow circumvention to be undertaken on or on behalf -- by or on behalf of a patient.

So, you know, as you may know, you know, we've had a lot of requests in previous years regarding third-party assistance, and the approach that we took, you know, we've always been conscious about not suggesting that not sort of potentially running afoul of the anti-trafficking provisions. So, in the repair exemption the last time, we were essentially silent on whether third parties might be able to be within the class of beneficiaries for an exemption. I'm wondering if you're familiar with that and if there's a reason, if you have views about whether we should take that same approach here.

MS. MCCLELLAN: Yes --

MR. AMER: Ms. McClellan?

MS. MCCLELLAN: Yes. We are cognizant of the fact that, you know, understandably, the Copyright Office has intent to write any exemption that might -- in a way that might imply something is okay that wouldn't be okay under the anti-trafficking provisions, and as such, we're more than happy -- we're okay with the idea of restructuring the

exemption language that we proposed to reflect similar language used by the Copyright Office in the repair exemption or in the exemption for, you know, changing devices for accessibility purposes for blind people or other disabled persons trying to use a copyrighted work that they otherwise couldn't. So both of those ways I think the Copyright Office used more passive language and kind of left it open for maybe a future court to provide more elaboration on what exactly would constitute a violation of the anti-trafficking provisions, and that's something that we would be okay with in this instance as well.

MR. AMER: Okay. Thank you. That's helpful. I want to give Mr. Reed a chance to address that and then just to let you know where we're going, I would like to also -- I'm going to have a question after that about the proposal that would take out the language regarding compliance with other applicable laws. So, Mr. Reed, I know that you are opposed and you've talked about the concern about third parties potentially being within the class of beneficiaries here. Is there anything else you would like to say on that? And I'm particularly interested in, you know, is the concern based on the sort of safety issues that you raised, or is there a particular sort of

copyright-related concern that you also want to bring to our attention?

MR. REED: No, I mean, I think the easiest way to note is that third parties are not subject to the obligations that we are, that health tech companies are obligated before the FDA, ONC. You know, we talked about HIPAA, covered entities. So, yeah, the real problem is third parties are not subject to the rigor and standard that we expect.

As far as beyond that, what you're talking about going further, I come back to the need to make sure that we are not erring on the side of putting things at greater risk. So, when it comes to the copyright language, you said how do we fit this into a copyright box. I guess I would say that I don't think that we're there yet on the third-party access because, as you noted, the likely outcome based on the petitioners' language is really the ability to engage with the underlying software that is built and, if it's SaMD or otherwise, has been approved through the FDA. So, bluntly put, yeah, I just don't think third parties will be regulated, and if they're not regulated, that puts health risks in play.

MR. AMER: Okay. Thank you. The last topic -- and I appreciate everyone's patience. The

last topic I wanted to ask about was the proposal to remove language about compliance with other laws. We talked about the same issue this morning in the context of the security research exemption. I'd like to ask the proponents, you know, as we noted before, you know, this language does track the language in the statutory permanent exemption in 1201(j) regarding security testing. In general, you know, the Office has tried where possible to retain the statutory language.

I'm wondering if you could elaborate on the particular basis for wanting to remove this language and in particular, whether, you know, there are any examples you want to introduce into the record about, you know, people being deterred or reluctant to engage in this kind of activity because of the other laws language.

MR. ZEMOUDEH: Yeah. So just to elaborate again on why we want to remove this language, we just think it's unnecessary and redundant to condition the exemption on compliance with other laws and regulations. As we've addressed, there are penalties under other laws and regulations that are deterrent enough. We do have one example regarding researchers. We mention in the comment researchers who did not want

to undertake research, you know, because of risk of not complying with security-related laws.

And, moreover, we did listen in on the hearings this morning, and we do think that the DOJ's recommendation on adding language about notifying people on having to comply with other laws, we do think that would be a good addition to the language in place of something like having to comply with other laws or lawfully accessing the data.

So I believe DOJ's recommendation was to add language requiring -- stating that qualification for an exemption is not a safe harbor or defense to liability under other applicable laws. And we think that would do a great job of notifying the public while not adding further penalties under the DMCA.

MR. AMER: Thank you. Mr. Reed?

MR. REED: Yeah. We did go over this this morning at great length. The one difference which compounds why we should not move forward with this exemption is, unlike the discussion this morning, if that device harms a patient, we're liable. So, if an anti-circumvention technology is used to break into a DVD so that you can stream it or watch it, the company manufacturing the DVD player isn't liable. If the medical device is hacked and it ends up harming a

patient in the methodology that its circumvention was undertaken, we're going to get sued, and people will die. So that's the difference in this context. And, again, Petitioner keeps saying that other regulations apply. Those regulations wouldn't apply in this instance because, in the example of third parties, they're not a regulated medical device manufacturer. They aren't --

Again, HIPAA only applies to covered entities or business associates of covered entities, and that requires the filing of an electronics insurance claim. So, in these instances, there's a lot of hand waving about laws that apply. But outside of the Federal Trade Commission's ability under unfair and deceptive, the laws apply to manufacturers of medical devices, including software as a medical device, and those engaged in the practice and provision of medicine.

So, yeah, it's a lot different than the conversation we had earlier this morning because the outcome of a mistake is so much more dramatic. But, other than that, you noted it. We covered all the four corners of the copyright portion earlier this morning.

MR. AMER: I'm not sure I understand the

liability concern. I mean, if a patient alters their device in such a way that, you know, it affects the way the device operates or is dangerous or something like that, is there a realistic likelihood that --

MR. REED: Yes.

MR. AMER: -- that the manufacturer would be liable?

MR. REED: A hundred percent. Happens regularly. Again, I mentioned the Medtronic Minimed 503. They literally pulled that off the market on the possibility that the security hole was broad enough that it could, in fact, do that. No patient was harmed, nobody died. Medtronic had to pull 4,000 insulin pumps off the market, recall them, re-alter the software and put in new devices to everybody. And that didn't actually even harm anyone, and yet the FDA was concerned enough about it to request strongly that Medtronic pull those products off the market.

So there are dozens of examples like that. It doesn't take a death to create the possibility of liability. It can create the -- that you did not do enough to prevent harm to the patient. So, absolutely, and if someone dies, they absolutely will sue and their claim in court would be, yes, Bob Jones altered the software on that product, but you,

manufacturer of the product, should have done more to prevent the ability to hack that product in a way that wouldn't have put the patient's safety at risk. That's a very standard conversation in the medical device marketplace, which it isn't just caveat emptor. It's what are you doing to proactively protect the patient. And so, yes, definitely liability would play a role.

MR. AMER: Okay. And so, I mean, I guess what we heard this morning, though, is that, you know, given that these laws continue to apply regardless of what the Copyright Office does, is there a need to tie eligibility for the 1201 exemption to compliance with laws that, as you say, are not really within our expertise?

MR. REED: Well, I think we kind of just said it. The idea of at least the exemption as it previously exists does say you need to comply with these other laws. The idea of removing that makes the negative outcomes more likely. At least this provides some band-aid to a third party that might wait to do it to say, well, we can't just claim a 1201 exemption because we still will have to make sure that we're meeting the 2013 guidance around medical -- mobile medical applications, for example. You know, we'll

still have to look at the risk framework, we still need to make sure we're meeting FIPS. So a third party that would look at this and say can I take advantage of it would have to say yeah, but we still need to comply with these other things, so we have a duty to do a better job. So, yeah, I think it would be a mistake to take them out.

MR. AMER: Thank you. We've run a little bit over, but I think I don't have any more questions. Do any of my Copyright Office colleagues or Mr. Zambrano Ramos have any questions? Yes, Mr. Zambrano Ramos?

MR. ZAMBRANO RAMOS: Thank you so much, Mr. Amer. This question is for Mr. Reed.

Would you just expand briefly on this point? I'm just curious how does -- I guess, how does § 1201 foreclose the kind of losses that you're talking about -- because some of these exemption methods -- sorry, some of these tools to circumvent already exist. Whether or not they are lawful, I'm not speaking to that. So I'm just curious, what's the mechanism by which granting an exemption would lead to an increase in these lawsuits? Thank you.

MR. REED: You're essentially saying, you know, the barn door is open, so what does it really

matter? I think the difference really goes to that question about the petitioners' request to open the door to third-party tools being made available and we get into the trafficking area. I think to grant this exemption does open the barn door and does change what's inside. The fact that you would essentially have a product that now I can go and make a product that hacks into it and I can stand by the copyright's language to say this third-party tool allows me to do these things does create a market for tool sets that I can now publicly, not just on the Dark Web, but I can put out publicly and say buy my product to hack your insulin pump or your diabetes tool.

So I think that it does -- the real reason is this is a trafficking question. And, yes, there are some very interesting open-source products that exist that do provide ways to passively monitor the information that come off these devices, and I think that that's something that has to be constantly looked at by the FDA and others. But I think opening the door and saying yes, come on in, the water's fine, third parties build tools, that absolutely changes the environment in a way that has the potential to negatively impact patients. So, yeah, I don't think granting it accomplishes -- it's not foreclosed.

MR. ZAMBRANO RAMOS: Thanks. And just to be clear, I wasn't suggesting sort of the barn scenario. I was just asking about the connections between that and 1201. Thank you so much.

MR. AMER: Ms. McClellan?

MS. MCCLELLAN: Yeah. I just wanted to address, you know, the concept of, I guess, widespread commercial use of third-party tools. That's not really what we're advocating for here. Primarily, what we're trying to allow is for third-party assistance of patients just in this narrow exemption to be able to access their medical data, not, you know, like, widespread commercial release of a circumvented tool. I think we can all agree that would very clearly violate the anti-trafficking provisions in § 1201.

MR. AMER: Okay. Thank you all very much. I think that will conclude this session, and we will now move to our audience participation session. Thank you.

MS. SMITH: Thank you all. So I think if you are concluding this panel you can turn off your video. And I think, actually, we have one speaker, which is Mr. Richart, who was unable to participate in a panel on Monday. So if we can find him and either

promote him or perhaps someone from the Copyright Office can contact him and we can receive his contribution.

(Pause.)

MR. AMER: I think we're just waiting for the gentleman who asked to participate in the session, so -- so stay tuned.

(Pause.)

MR. AMER: Okay. So the person who had asked to participate doesn't seem to be on, so I think we're going to adjourn for today. And just as a reminder, we will have another audience participation session on April 21, so we will give him an opportunity to contribute then. Thank you all very much for participating, and we will see you on April 19.

(Whereupon, at 2:51 p.m., the hearing in the above entitled matter adjourned.)

//

//

//

//

//

//

//

CERTIFICATE

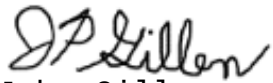
CASE TITLE: Section 1201 Rulemaking Hearing

DATE: April 8, 2021

LOCATION: Washington, D.C.

I hereby certify that the proceedings and evidence are contained fully and accurately on the digital recording and notes reported by me at the meeting in the above case before the Library of Congress.

Date: April 8, 2021



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

B

M

Q

R

S

T

U

Y

Z