LIBRARY OF CONGRESS

UNITED STATES COPYRIGHT OFFICE

SIXTH TRIENNIAL 1201 RULEMAKING HEARINGS

Tuesday, May 26, 2015

Library of Congress

Mumford Room

Washington, D.C.

Reported by: Christine Allen,
Capital Reporting Company

APPEARANCES

JACQUELINE CHARLESWORTH,
U.S. Copyright Office

MICHELLE CHOE,
U.S. Copyright Office

REGAN SMITH,
U.S. Copyright Office

SY DAMLE,
U.S. Copyright Office

STEVE RUWE,
U.S. Copyright Office

JOHN RILEY,
U.S. Copyright Office

STACY CHENEY,
U.S. Department of Commerce

CONTENTS

PROCEEDINGS

MS. CHARLESWORTH: Good morning, everyone. I'm sorry for that brief delay. We were working on an exhibit issue, as I mentioned.

Welcome to the Sixth Triennial Section 1201 Rulemaking. I'm happy to see we have so many here with us today.

I'm Jacqueline Charlesworth, General Counsel of the U.S. Copyright Office, and I and my colleagues -- with my colleagues will be presiding over the hearing -- hearings here in Washington.

We had hearings last week which were very productive, and I'm looking forward to another week of hearings here that will be equally as productive.

I am joined here, as I mentioned, by several colleagues. I think I'll just go -- have them introduce themselves and say what their title is, starting with Michelle Choe.

MS. CHOE: Hi. I'm Michelle Choe. I'm a Ringer fellow at the U.S. Copyright Office.

MS. SMITH: Regan Smith, Assistant General Counsel.

MR. DAMLE: I'm Sy Damle. I'm Deputy General Counsel.

MR. RUWE: Steve Ruwe, Assistant General Counsel.

MR. RILEY: John Riley, Attorney-Advisor.

MR. CHENEY: And I'm Stacy Cheney. I'm a Senior Attorney at NTIA, Department of Commerce.

MS. CHARLESWORTH: Okay. So you have a large audience here. We're all very interested in what you have to say.

As I mentioned in Los Angeles, and I'll say it again today, the goal of the hearing process is really to clarify and amplify the record especially in areas where we have questions.

And so in making your comments and contributions today, it's helpful if you hone in on the areas of controversy, the sort of disputed areas rather than just sort of restating things that you've said in your written comments, which we've all read and -- carefully and digested.

So the format we're going to use is I'll go around -- we have quite a number of participants today -- ask for a brief opening statement that, again, sort of focuses on sort of what you think the key issues in the proposal are, maybe responding to the other side a bit.

And we do sometimes interrupt with questions. So be prepared.

And, you know, this -- we found that that worked well. And basically our goal is to kind of join the issues. We're particularly interested, especially in a very broad class like this, in how we might refine and kind of define what it is that's being proposed and, you know, looking at that in relation to the support in the record.

So just a few rules of the road. We have a court reporter who will, I think, speak up if she can't hear you. For her sake, let's try not to talk over one another.

The miking system, as I understand it, only allows four mikes to be on at a time. So as we came from L.A. -- we didn't have that issue in Los Angeles, but we have it here.

So the safest thing to do -- obviously, some of you are sharing mikes. Just turn them off when you're not speaking. And somewhat counterintuitively, red means on and white means off. This is a brain test, the mike system.

If you want to contribute to the

conversation, tip up your placard, and we will call on you as best we can. We try to get to everyone. Sometimes we're a little out of order because I don't see everyone. But we will -- we do try to get all the comments in.

And in terms of -- if you're referring to a particular piece of evidence in the record, if it was submitted with your written comments -- say, multimedia evidence -- it helps if you can be very specific of what you're referring to.

I think we have one -- just one exhibit today, right, that we've premarked. So that would be Exhibit 10. And when we get to that, if you can refer to it as Exhibit 10 just for the record because, when we go back through, sometimes it's hard to sort out what's what.

So without further ado, I'm going to ask you each to introduce yourself and just -- just go around quickly. Introduce yourself, explaining what your affiliation is or what interest you represent. And then we'll start again from left to right, and we'll have you make your brief opening statements.

So we'll start with you, Professor Green.

MR. GREEN: My name is Matthew Green. I'm a professor at Johns Hopkins, and I am one of the petitioners here today.

(Microphone interference.)

MS. CHARLESWORTH: What's that? It was not good.

How is your mike? Is your mike doing that, Mr. Reid?

MR. REID: It doesn't seem that way.

MS. CHARLESWORTH: Okay. So what I'm going to ask is that -- if you guys could share Mr. Reid's mike, and we'll take that one out of service.

MR. REID: Blake Reid, from the Samuelson-Glushko Technology Law and Policy Clinic at the University of Colorado.

MR. SAYLER: Andy Sayler, also from the Samuelson-Glushko Tech Law and Policy Clinic at University of Colorado.

MR. STANISLAV: Mark Stanislav From Rapid7.

MR. BELLOVIN: Steven Bellovin, a professor at Columbia University.

MS. MATWYSHYN: I'm Andrea Matwyshyn from Princeton University. I'm representing the security researchers, and I'm also here in my capacity as a law professor.

MR. BLAZE: I'm Matt Blaze. I am a professor in the computer science department at the University of Pennsylvania.

MS. MOY: Hi. I'm Laura Moy. I'm senior policy counsel at New America's Open Technology Institute.

MR. STALLMAN: Hi. Erik Stallman from the Center for Democracy and Technology, here in support of the petitioners.

MR. TRONCOSO: Hi. Christian Troncoso with BSA, the Software Alliance.

MR. LIGHTSEY: I'm Harry Lightsey with General Motors. And by way of introduction, to my immediate left is Anna Shaw. She's counsel for General Motors with Hogan and Lovells. She will not be providing any testimony or remarks in today's proceeding.

MS. CHARLESWORTH: Okay. Thank you. Thank you very much.

Professor Green, do you want to lead us off, then?

MR. GREEN: Okay. So my name is Matthew Green. I'm a professor of computer science at

Johns Hopkins, as I just said. My research is in the area of computer security and applied cryptography.

While I'm currently a professor, my career has spanned both academia and industry. Before I became a professor, I was a professional security researcher. I worked for companies such as MasterCard and the Walt Disney Company to find and close vulnerabilities in computer security systems before somebody else could exploit them for commercial gain.

Today, as a university professional, I do essentially the same thing, only now my clients are the general public. In both cases, the goal is the same. It's to find flaws in systems and to get them repaired before they can be exploited by somebody else.

One of the common themes in my career is risk and finding ways to mitigate risk. I'm not speaking here of only the risk caused by security vulnerabilities, although that risk is real and is increasing. I'm also speaking of the legal risk that security researchers such as myself and my colleagues here today face when they undertake good-faith security research into information security systems.

My first exposure to this risk came several years ago when I was a graduate student. More than a decade ago, my colleagues and I discovered serious vulnerabilities in a computer chip that was used to operate in one of the largest wireless payment systems at the time and also to implement the automotive security systems that kept people from stealing cars.

The project was the first public security research project that I had conducted at that time. And I have to admit that I was young and I was a bit naive. I didn't know exactly -- I don't know what exactly I was expecting to happen when we notified the manufacturer, but I do believe that -- I believed at the time that it was going to involve a discussion, it was going to involve some technical back-and-forth and perhaps an application of some of the repairs and mitigations that we had developed at the time.

That's not what happened. Instead what happened was that we encountered a great deal of resistance, pushback from the manufacturer and an active effort to ask us, as university researchers, to suppress our research and to not publish the fact that there were vulnerabilities in the system.

MS. CHARLESWORTH: Excuse me. Was that -- you mentioned it was on a chip.

I mean, when you say "manufacturer," is that the chip manufacturer?

MR. GREEN: The chip manufacturer.

MS. CHARLESWORTH: Okay.

MR. GREEN: Yes.

MS. CHARLESWORTH: Thank you.

MR. GREEN: Yes. So instead of repairing the system and discussing ways to repair the system, the manufacturer spent considerable resources in an effort to prevent us from publishing the work.

One of the several levers for that effort was to raise the specter of an expensive legal action based on the anti-circumvention provisions of Section 1201.

Since our work in that case did involve, as a small component, some degree of reverse engineering of software and the bypassing of an extraordinarily simple TPM. So in my opinion, the Section 1201 was never intended to prevent security researchers from publishing their results.

In the moment though, when you're a penniless grad student and somebody is presenting you with a possibility of a lawsuit you can't possibly afford, it's hard to argue about the merits of a case or the intent of a law. It's more tempting to simply comply and hide a serious vulnerability from public view.

MS. CHARLESWORTH: Can I -- I'm sorry. I promised I would interrupt you.

MR. GREEN: Sure.

MS. CHARLESWORTH: And I'm doing it.

MR. GREEN: Go ahead.

MS. CHARLESWORTH: But 1201(j) -- now that you have a better understanding of the law, can you explain why you think that might or might not have applied to that scenario you just described?

MR. GREEN: Well, so my understanding of the law is that -- and you -- stop me, Blake, if I'm saying anything wrong.

There are two issues. There is the bypassing of a technological prevention measure, a TPM -- a protection measure, sorry -- that allows you that -- that protects a copyrighted work. And separately, there is the issue of trafficking in tools that allow people to circumvent.

And so both of these issues could potentially be an issue depending on what it means to traffic.

In this case my understanding is that the issue was simply bypassing a TPM that may or may not have prevented -- protected a copyrighted work, such as a piece of software. That was what was raised to us at the time.

MS. CHARLESWORTH: Okay. But there's an exemption for security testing.

Professor Reid, I think, has -- did you want to comment on that on behalf of --

MR. REID: Sure. And I hope we can get into this more today. There are actually several exemption sections in Section 1201, including Section 1201(j) for security tests, Section 1201(g) for encryption research, and Section 1201(f) for reverse engineering.

And I'm sure other folks on the panel can speak to these.

But as we detailed in our comments, there are shortcomings with each of these -- these exemptions. So for example, Section 1201(j), we -

- as we argued, fails to provide the sort of upfront certainty that folks need to know whether their security testing is going to be exempted or not because, for example, it's got a multifactor test that gets looked at after the fact that depends on things like whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer and whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement and so on and so forth.

And so I think the argument that we would make, if God forbid someone actually did follow through on a threat to sue Professor Green, is we might well argue that Section 1201(j) applies or that Section 1201(g) applies or that Section 1201(f) applies.

So I don't want to lay out a blueprint here for how those wouldn't apply because we might have to use them someday.

But as we've asked the office to do several times in the past and as the office and the librarian have done, we're asking for some additional clarity to make clear for folks up front before they start a project that, if they're proceeding in good faith, that they're doing the right thing, they're doing this only for security testing or security research and they're not doing it to facilitate any sort of copyright infringement, that they're free and clear.

And that's been the basis on which the register granted the exemptions in 2006 and 2010, and we think that -- or we hope the office will provide that direction again this time around.

MS. CHARLESWORTH: Right. No. Thank you.

And, Professor Green, when were these events -- the story you were telling about the chip? When did that --

MR. GREEN: This took place in 2004.

MS. CHARLESWORTH: 2004.

And I guess, just to put a little finer point -- and I understand what you're saying about the ex-post versus ex-ante analysis, Professor Reid.

But do you think that the activities that Dr. Green was describing would -- I mean, in your view, would they fall into the one of the exemptions?

MR. REID: I mean, I think it's hard to look at something that happened that long ago. I mean, I don't want to opine without getting into the deep specifics of it.

And, again, it's the sort of thing that, if we were in court, I would absolutely argue that they were -- that they were covered. I would argue that there was no copyrighted work. I would argue that there is no copyright infringement. I would argue --

MS. CHARLESWORTH: That's a very lawyerly response.

MR. REID: But I think if I were advising Professor Green beforehand -- and, again, I'm speaking hypothetically because I wasn't there for all of the details of this -- that he should be nervous about it because a lot of the provisions in this law are ambiguous and we don't ultimately know how they would be applied.

So that's the point we're trying to get at is the issue of certainty.

MR. GREEN: So I can actually add a little bit --

MS. CHARLESWORTH: Sure.

MR. GREEN: -- a less hypothetical to

that.

We were advised at the time by the Electronic Frontier Foundation. The attorneys there provided us with pro bono representation. And we were told that at the time they could provide no guarantee that any of the exception exemptions at the time in the law would have protected us if we were sued under that -- under Section 1201.

They didn't say that we were necessarily violating the section. They simply told us that the complexities of those exemptions were such that they could provide no guarantee to us as graduate students.

MS. CHARLESWORTH: Okay. And was that -- did you receive that information before you embarked on the testing project or after you got the letter?

MR. GREEN: We received that information -- we spoke about it before, during, and after we were -- we were --

MS. CHARLESWORTH: So you actually -- you sought legal advice before you went down this path?

MR. GREEN: Yes. My professor at the

time had been through an experience very similar to this and knew to do this beforehand.

MS. CHARLESWORTH: And --

MR. GREEN: We would not have.

MS. CHARLESWORTH: Okay. But you decided to proceed in any -- anyway?

MR. GREEN: Yes.

MS. CHARLESWORTH: Okay.

MR. GREEN: Our view is that it was necessary.

MS. CHARLESWORTH: Okay. Go ahead and finish your --

MR. GREEN: Sure.

MS. CHARLESWORTH: -- statement.

MR. GREEN: Okay.

MS. CHARLESWORTH: See.

MR. GREEN: My statement's almost over anyway.

So what I would like to say is that, in that case, we were very fortunate to have representation from the Electronic Frontier Foundation, which gave us the confidence to go forward.

And, of course, we were university researchers and grad students. We felt that the probability of a public lawsuit was relatively low. As a result of that, the system has been published -- I'm sorry -- the system has been repaired. We were able to publish our results.

But without that, the system may not have been repaired. It may still -- it might still be broken today.

So I'm not as naive anymore. While I still conduct research that involves commercial security systems, I now begin every project with a call to a lawyer to evaluate, among other things, whether there's a possible violation of Section 1201 and how to mitigate the risk to myself and to my own graduate students.

I'm still fortunate to receive pro bono representation from organizations such as the EFF, but many researchers are not so fortunate.

Moreover, good-faith research should not require the assistance of lawyers. At a minimum, the need for legal representation significantly increases the cost of each research project. At worst, it works to dissuade the necessary kind of research that we desperately need more of.

Thank you.

MS. CHARLESWORTH: Thank you, Professor.

Professor Reid?

MR. REID: Thank you and good morning.

I'm going try to keep my statement short so we can get to the many more questions. I know there are a lot of issues outstanding.

Just at the outset, I want to thank the office, and to the NTIA, for your continuing consideration of this issue. It's one that's persisted a long time, and it's a really serious one. So we thank you for the extended time in the hearing today.

It's actually been just over six years since I first came before the office back in 2009 with Professor Alex Halderman. And it's been about a decade since Professor Halderman first appeared before the office with Ed Felten during Sony rootkit saga in the 2006 rulemaking.

Back in 2009, we urged you and your former colleagues to grant a broad exemption for Section 1201 for good-faith security research. And Professor Halderman and I warned the office of increasing flaws in TPMs and of Section 1201 substantial chilling effects on security researchers that are attempting to study and fix those flaws in good faith.

Noting the shortcomings of the built-in statutory exemptions that we just discussed, we predicted that the Sony rootkit, SafeDisc, and SecuROM -- which were some of the problematic TPMs of that time -- would not be the last TPMs to cause collateral security harm. And we urged the office to allow security researchers to react accordingly to evolving threats.

The last six years, which are underscored by the substantial record in this proceeding -- and which you'll hear more about from Professor Green and his colleagues today -- illustrated that, if anything, we've absolutely underestimated the widespread proliferation of security vulnerabilities that could be both caused by and concealed by TPMs.

As we'll discuss today, these vulnerabilities now persist not just in music and video games but in the vast array of software that has become increasingly intermingled with a vast array of everyday consumer goods that comprise the Internet of things, which include cars and medical devices with elaborate but vulnerable networking features and in the software that underpins the Internet and the wide variety of applications that ride atop it.

Moreover, the chilling effects that we urged the office to recognize in 2009 have become ever more pernicious. As you heard from Professor Green, a room full of the nation's top security researchers stand before you today, and many more of them have affirmed their views on the record highlighting the threats that they, their colleagues, and their students face in simply trying to make America a safer place to live and to compute.

As the office acknowledged in 2010, while Section 1201's built-in exemption underscores Congress's recognition that security is a serious, overriding national priority, those exemptions still don't provide the certainty that researchers need to ensure that their good-faith efforts will not meet with unscrupulous attempts like Professor Green described to silence their work protected by the First Amendment and to protect consumers -- which I know Ms. Moy will speak to -- from serious and often life-threatening flaws in the wide universe of software that exists today.

In 2010, Register (ph) Peters rejected

Professor Halderman's prediction of worsening security vulnerabilities stemming from TPMs as -- and I quote -- "unverifiable, contradictory, or speculative" and recommended against creating a broad exemption.

And I think, unfortunately, the intervening five years is replete with evidence that Professor Halderman's prediction was prescient and correct.

You now have before you a lengthy record of security vulnerabilities that could have been avoided had security researchers acting in good faith not be chilled by the absence of a workable exemption in Section 1201.

I just want to close by saying the researchers who are before you today, including Professor Green, are the good guys. They care about abiding by the law, and they're here because they need you to clear breathing space for them to do the right thing.

Without your help, they'll be losing an arms race to bad guys who are, as we speak, circumventing TPMs and exploiting existing vulnerabilities and who don't care about the consequences of violating Section 1201.

Today, the office has the opportunity to make the right decision for the next three years by ensuring that security researchers sitting before you today and their colleagues and students who aren't here have the clarity and the certainty that they need to ensure our nation's cybersecurity and protect millions of Americans from serious harm.

The record and the law are clear, and so are the consequences for neglecting them. The office should grant -- should recommend and the librarian should grant a clear certain exemption for good-faith security research.

Thanks, and we look forward to your questions.

MS. SMITH: The exemption that was granted in 2012 was limited to video games, but did you find it a workable exemption for video games?

MR. REID: I think the issue with the exemption -- I think it was granted in 2010. My memory may be slipping on that too.

The issue was not with the piece of the exemption that was granted for video games but that the vulnerabilities around the DRM that was attached to video games was SecuROM and SafeDisc and several related pieces. That was just one piece of an evolving sort of threat.

So previously it had been the rootkit. Then it was SecuROM. But the evolving piece of it ended up being in things like we're going to talk about today, in cars and in medical devices and that sort of thing.

So I think it was that narrow piece that said, "Hey, security researchers, if you want to pursue an agenda around -- that involves circumvention, that involves looking at security flaws and technological protection measures, it's okay if it's for video games but it's not okay if it's for anything else."

So I think --

MS. SMITH: Yes. My question is, for video games specifically, the language included different provisions than what you have proposed on a broader level.

So, for example, for video games, it said that the information derived from security testing must be used primarily to promote the security of the owner, operator of the computer, or the information should be used or maintained in a manner that does not facilitate copyright infringement.

Those are two limitations that I don't see in your current proposal. And I'm wondering -

MR. REID: Sure.

MS. SMITH: -- whether or not they restricted research to be performed on video games for what was granted in 2010.

MR. REID: I mean, again, it's hard to tell you because the flaws and -- and I'm sorry I'm going to respond with the same answer that I gave to the last question.

It was hard to test the exemption because the subsequent vulnerabilities that evolved were not necessarily in video games. And I think what you'll hear from a lot of folks today is they took a look at the exemption and said, "We just got this narrow exemption for video games. We're not going to do research in this area."

So I can't tell you how those limitations played out in practice for people because there was so much chill that came from just being able to focus on video games and nothing else that I can't tell you how those limitations worked out.

And I think if you asked --

MS. SMITH: Okay.

MR. REID: -- us to talk about how they would work out if you added them to a broad exemption today, I think we would have some of the same concerns that I -- that I mentioned earlier, which is that they don't have any certainty. They've got words like "primarily."

What exactly does that mean? So we saw in the cell phone unlocking context --

MS. SMITH: Well, in your proposal, it says "for the purpose." I mean, you can only take it so far, "primarily for the purpose" or "for the purpose."

How much more certainty does that provide you? In the statute, you list the exemptions that -- solely for the purpose. So we might want to read a little bit into rational intent.

MR. REID: I mean, I guess all I can respond is that the more certainty we can get out of the exemption, the more mileage researchers are going to get out of it. And the language like "primarily" that evokes a post-hoc judgment is going to be problematic because it's going to be hard for counsel to people like Professor Green to say up front, "Well, is what you're doing primarily for this purpose or not so much?"

The easier it is to answer that question, the better.

MS. CHARLESWORTH: But there's always going to be post-hoc judgment, right?

MR. REID: Sure.

MS. CHARLESWORTH: I mean, in other words, if you end up in court on something like this, you're always going to have a court looking at whether you fall in the exemption.

And I take the point that some of the language here, you know, is -- you know, it's a multifactor test and kind of a balancing test. Maybe there are different ways you could structure a standard that might be more or less predictable.

But I think that -- you know, I mean, I would ask the same question. I mean, what is good faith? You know, a court is going to be looking backward at the events if you're litigating this, and they're -- you know, we have to draft language

MR. REID: Sure.

MS. CHARLESWORTH: -- if we're going to grant an exemption.

So and this goes for, I think, everyone here. You know, we're -- we want to understand, again, sort of where you're -- I mean, to Regan's point, you know, we want to understand where you're coming from and what kinds of limitations or -- you know, might be appropriate in language that sort of balance the need for maybe less of a post-hoc analysis or -- and, you know, with kind of some definition of what it is we would be allowing.

MR. REID: Sure.

MS. CHARLESWORTH: Okay. So that's -- that's why it's helpful to explore -- the language and think about, like, looking at -- I mean, we have some -- Congress did act in this area. And so --

MR. REID: Sure.

MS. CHARLESWORTH: -- that's really good guidance, though, at least about what Congress was thinking at the time. So that -- we're kind of -- that's one sort of very important benchmark for us, as we discuss these issues.

MR. REID: So, I mean, -- I think I'd underscore to the extent a limitation like the ones that were going to previously winds up in the exemption and we have some concerns about that -- to the extent you can make clear in your guidance in the order about what those limitations mean and what sort of circumstances they cover and which ones they don't -- for example, the limitation about copyright infringement or being used to facilitate copyright infringement.

I think we've heard some concerns from the opponent in the record here that simply publishing information about a particular TPM or about particular copyrighted software, that might be facilitating copyright infringement under a really broad theory of what that means.

And so I think if you can provide guidance that -- the facts that we're concerned about here -- and we've outlined these -- and we tried to do this in pretty strong detail in our comments, which are investigating security flaws, doing the research into it in a classroom environment for the most part and then being able to publicly disclose in a responsible way the results of that research, that that's what's covered under the exemption.

I think if you can provide guidance that enables that, then that's -- that's the most important piece we're looking for out of these limitations.

MS. CHARLESWORTH: Okay. I guess I had one more question.

MR. REID: Sure.

MS. CHARLESWORTH: When you say "a classroom environment" -- so tell me more about that and whether, you know, an exemption should be tied to sort of the academic community in some way.

MR. REID: Sure. And I'll probably kick this back over to Professor Green or others on the panel, if you don't mind.

But I'll just say at the outset: I think it's important from the context that we're coming from that students are able to work on this. This is a really important piece of Professor Green's work.

But I don't think we would support a limitation that would restrict it to classroom use. I think the contributions of folks from the private sector and even from the amateur community of security researchers of folks that are out there building skills at doing this kind of stuff are really important.

And I think Professor Green could probably speak to that a little better than me. But I think we would be uncomfortable with a limitation that restricted it to the classroom.

MS. CHARLESWORTH: Yeah. I mean, not just the classroom. But should sort of any project of this nature be overseen by a university scholar such as yourself, Dr. Green, or where you could have students working with you?

I mean, that's obviously another big factor. Who could -- who could use the exemption and should that be limited?

MR. GREEN: I would be -- I would be very concerned about an exemption that focused only on university research. And the reason is that the most dynamic and the most important research being done right now is being done by people in the private sector and people we refer to as commercial security researchers.

So, for example, the vehicle security research -- which I'm sure you discussed in the previous hearings -- is being worked on by -- funded by DARPA but being worked on by individuals such as Charlie Miller, who's not affiliated with a university. Very similar situation with a great deal of other security research.

It would be a huge loss to restrict the exemption to that.

MS. CHARLESWORTH: Although a lot of that is authorized by the manufacturers, isn't it?

MR. GREEN: Some is authorized, but the vast majority of security research is done by private individuals who have access to open-source software or to devices. There have been cases very recently with security researchers being told, "You found a vulnerability. We have to -- you may have to back off because of a possible DMCA violation."

Just a couple of weeks ago, that happened. So there's a great deal of research being done without authorization.

MS. CHARLESWORTH: Okay. I think we'll -- oh. We'll move to Mr. Sayler.

MR. SAYLER: Thank you and good morning.

I'd like to start by thanking the members of the Copyright Office and the NTIA for inviting me and my colleagues to testify before you here today.

Like it says on the placard, my name is Andy Sayler. I'm a doctoral candidate studying computer science and security and privacy at the University of Colorado in Boulder.

I'm joining you today as a member of the Samuelson-Glushko Technology Law and Policy Clinic at Colorado Law and on behalf of our client, Professor Green.

As you're aware, we filed several long-form comments on behalf of Professor Green in support of the proposed class 25 exemption allowing the circumvention of TPMs for the purpose of performing good-faith security research.

I'd like to reiterate our request that the Copyright Office grant the proposed class 25 exemptions for the reasons I'll -- and I'm sure others -- will discuss here today.

In particular, this exemption is being considered at a critical time in the history of cybersecurity and research and development. Computers are ubiquitous components of our daily lives from the cell phones in our pockets to the vehicles we drive to life-saving medical devices and much more.

Unfortunately, it's rare to have a week go by without a new story about some new security flaw or data breach in our computing systems.

Indeed, just last week, Professor Green, Professor Heninger -- who hopefully will join us at some point -- and a number of their colleagues released a report disclosing the logjam vulnerability in the core protocol we use to keep the Web secure.

Such research demonstrates the critical importance of independent good-faith security research in the community.

Last week's vulnerability is not unique. It joins a list of significant vulnerabilities discovered by independent researchers in a range of software and devices over the previous few years, including the Heartbleed SSL flaw, the Shellshock Bash bug, and numerous vulnerabilities in vehicles and medical devices.

MS. CHARLESWORTH: Can I -- I'm sorry. Just on the one you mentioned from a week or so ago, the logjam issue, I mean, was that done without circumvention?

MR. SAYLER: I think Professor Green, being the expert on the panel, would be the one to comment on that.

MR. GREEN: It involved primarily looking at public specifications, but there was some degree of looking at other devices. I'm not sure if it involved circumvention in that case.

MS. CHARLESWORTH: So we don't know. Okay.

MR. GREEN: Yeah. Thank you.

Continue, Mr. Sayler.

MR. SAYLER: Independent security research, much as Professor Green noted, is actually funded by the U.S. government via the National Science Foundation, DARPA, and other agencies. It is a critical component of the effort to better secure the software and computing devices on which we rely.

Unfortunately, Section 1201 is being used to discourage the very independent security research that has shown itself to be critically important to our cybersecurity. Congress never intended Section 1201 to be used to suppress good-faith security research and even included the specific exemptions we've mentioned for encryption research and security testing in the original statute.

These exemptions, however, are somewhat ambiguous and impose a number of undue burdens on researchers, making it difficult for them to know whether or not their work runs afoul of the law.

Furthermore, certain parties with an interest in suppressing public knowledge regarding the flaws and insecurities in their products have taken advantage of the ambiguities in Section 1201 to threaten security researchers performing good-faith research or disclosing the flaws they discover.

As Professor Green mentioned, just two weeks ago, a researcher for the security firm IOActive was threatened under Section 1201 for disclosing serious flaws in the CyberLock line the secure door locks. CyberLock secure door locks.

These ambiguities and the threats they allow have the net effect of discouraging researchers from studying the security of many of the computing devices on which we rely.

Even those who do choose to study such software and devices must do so at significant personal risk of liability and are forced to incur unreasonable legal expenses to mitigate that risk.

It is thus imperative that the Copyright Office grant the petition for this exemption, relieving researchers of the undue burden placed on them by Section 1201.

For the noninfringing actor practicing

good-faith security research, such an exemption is critical to ensuring the security of our nation, the security of its citizens, and the security of the digital world at large.

Thank you for your time, and I look forward to your questions.

MS. CHARLESWORTH: Okay. Mr. Stanislav?

MR. STANISLAV: Put my props up front for you.

So good morning. My name is Mark Stanislav. I am a security consultant and researcher.

Last year, I assessed the security of an Internet-connected children's toy, which is right here, that allows parents to send audio messages -

MS. CHARLESWORTH: I'm going to -- let the record reflect that you're holding up something.

What is that?

MR. STANISLAV: A plastic -- it's a pig. His name is Snort. Literally, the name of the toy. And it's a mailbox because that -- the audio communication that you can send to your child to this device is effectively a mailbox for the child to get a letter but via audio.

MS. CHARLESWORTH: So that would go -- forgive me for not being familiar with that.

MR. STANISLAV: It's a brave, new world. I understand.

MS. CHARLESWORTH: So that would go -- like, the child would be near that and would hear -- would hear you transmitting an audio communication?

MR. STANISLAV: It will actually "oink" at you to let the child know there is a new message. And then there is a "play" button and then the arrow can actually have the child reply back to the parent or whomever might be sending that message.

MS. CHARLESWORTH: So it's like a baby voicemail system?

MR. STANISLAV: Yes. That is a great way to put it.

MS. CHARLESWORTH: Okay. Thank you. You may continue.

MR. STANISLAV: You're welcome.

And so, as I mentioned, the child can reply back using this toy.

I was able to determine that the security features of this device were flawed, allowing an unauthorized person to be able to communicate with the child's device.

Worse, however, was that the same person that would have access to send these messages to a child and receive replies back, another flaw in this device platform actually allowed for the name of the child, their date of birth, and a picture of the child to all be gathered as well.

Upon completion of my research, I contacted the vendor to explain these issues. Despite my offer to go into details with their engineers, the vendor would not engage with me.

Ultimately, my employer at the time received a call from the legal staff of this vendor stating that I must have hacked their company, as that's the only way I could possess this knowledge or have found these vulnerabilities.

After a few tense conversations with our respective legal teams, it was determined that the vendor's perception of my actions was not accurate, and productive dialogue finally occurred. The issues were quietly resolved without notifying customers.

Still, the situation did make me fear

for my livelihood as the DMCA could have been used against me at any point for the circumvention of the authorization controls even though they were very flawed.

MS. SMITH: Can I ask --

MR. STANISLAV: Yes.

MS. SMITH: Did you discuss the specific exemptions of the DMCA for personal information or 1201(j) in that instance?

MR. STANISLAV: So the legal staff of my employer at the time took over these conversations. I wasn't privy to the direct conversation.

MS. SMITH: But you understood that your employer felt that at least there was a risk that you would not be able to rely on 1201(j) or --

MR. STANISLAV: Absolutely. My firm that I worked for at the time had numerous security researchers over the last probably 20 years. So they were very privy to the concerns around DMCA and what would have been done for the DMCA.

Thank you.

With the goal of protecting children, you know, honestly, that was worth the unfortunate risk of a lawsuit.

The possibility that a pedophile could anonymously communicate over the Internet to a child while possessing details of that child is certainly a concern and a terrifying reality of the modern age we live in.

In another example of research, I found that my own home's web camera that I had been using for quite a while actually had vulnerabilities that could allow a criminal to control full access over the device, including looking at the streaming audio and video of the device that was transmitting from my home.

MS. CHARLESWORTH: Okay. And I'll just say again, for the record, that you held up a -- that's a camera? A web camera?

MR. STANISLAV: Yes.

MS. CHARLESWORTH: Okay. What we may do after -- well, we may take a break. Since this is a long panel, we may photograph those and --

MR. STANISLAV: Sure.

MS. SMITH: -- with your permission, enter them as exhibits for the hearing a little later on. Okay.

MR. STANISLAV: Not a problem. Thank

you.

These issues, obviously, directly risked my privacy and possibly the safety of the other camera owners.

I contacted the vendor to alert them to these issues and offered my assistance to see these issues resolved. The final e-mail I received from their CTO, after going from a range of friendly to threatening, ended up wanting to meet with me to understand how I found these issues as I may have come across confidential information, in their eyes, during this process.

Despite my prompt replies, the vendor stopped replying to me and eventually these issues were again quietly resolved without notifying customers.

Looking to today, the entrepreneurs who made this connected children's toy actually have gone on to win numerous awards, including monetary prizes from organizations such as Cisco. One has to believe that their ability to win such prizes and continue their business would have not been possible had a criminal abused these vulnerabilities and actively put children in harm's way.

The vendor of my web camera actually had a change in leadership, and the new leadership there apologized for their predecessor's indifference and lack of communication from the prior experience.

These are clear examples of how security research not only prevented harm and violations of privacy but also ensured that businesses could continue their business by fixing critical flaws before it impacted their customers adversely The exemption of security research under the DMCA would remove a large obstacle for doing what we do best, helping people that are unaware they are in harm's way or helping businesses putting customers in harm's way unintentionally.

Americans are becoming inundated with devices. They are watching us, tracking us, and ultimately possibly endangering us. We live in a time where literally someone's mobile phone can control the oven in your home and set it to a temperature.

We have smart TVs that actually have microphones listening to what we are saying all the time in order to act on certain commands it overhears.

Please help widen the collective efforts of security research by -- for the researchers who do stay away from the DMCA for fear of legal action. Our collective safety and privacy depend on it.

Thank you very much for your time, and I would be happy to answer any questions you have.

MS. CHARLESWORTH: Thank you.

MR. CHENEY: May I ask a question?

MR. STANISLAV: Sure.

MR. CHENEY: Mr. Stanislav, have those vulnerabilities been fixed in these products or in subsequent releases of these production?

MR. STANISLAV: Yes, sir.

MR. CHENEY: Okay.

MS. CHARLESWORTH: Professor Bellovin?

MR. BELLOVIN: Thank you for giving me this opportunity to talk.

I'm Steven Bellovin, a professor of computer science at Columbia University. Before I joined the faculty there, I spent more than 20 years at AT&T Labs research and, before that, Bell Labs to the corporate whatevers.

Before I go on to what I was going to say, I wanted to make a comment about academic research versus independent security researchers.

Academic security research, at this point, is generally concerned with new classes of vulnerability, not -- you know, if somebody found a well-known flaw such as a buffer overflow -- I won't bother explaining that -- in a product like this, it would not be publishable in a computer science venue. It's just not a new, interesting contribution to knowledge.

Whereas, this is what is -- most of the flaws that we see affecting the devices that we all rely on are instances of well-known vulnerabilities. These are very serious. They're very important, practical import but are not the subject of academic research. This is conducted by the independent security researchers, and they're the ones who are actively protecting us from flawed devices.

So it's not the sort of thing that a professor would be likely to do or students possibly, except as an exercise. And frankly, I would discourage my students from looking for well-known vulnerabilities because it's not going to get them any academic credit, at least not if they're Ph.D. students.

It's not the kind of research that academics do at this point. Twenty years ago it was, but it's not -- we're not here 20 years ago.

I actually want to go back in my ancient history where I was in high school a very long time ago and learned a program when that was a very unusual thing. And I wanted to understand how the operating system worked.

So I wrote a program called "the disassembler" to go convert the binary code of the operating system back into marginally comprehensible source code and studied it. That's what got me to where I am today, studying that way.

You know, that was a program that won an honorable mention in a programming contest -- a student programming contest. Arguably, in many circumstances, it would be illegal today if I wanted to go look at, say, something protected by technical measures such as a smart phone.

Four years later, I caught my first hackers while I was still an undergraduate.

I teach my students how to analyze and attack programs. More than 20 years ago, I coauthored the first book on firewalls and Internet security. We had a chapter called "The Hackers Workbench" to explain here's how you do attack. You have to know this because this is the way you secure your system.

I teach my students how to evaluate things, and I teach that one of the ways to do it is to actually try an attack. That's one of the homework assignments that I give. You have to know how to do this in order to secure a system. It's not the only way, but it's one of the ways.

I mentioned this book more than 20 years ago. I would add, by the way, that two years later, in 1996, I found a copy of this book online -- it had been scanned and OCR'd online, on the very new-to-the-world Web. The publisher had never heard of such a thing at the time. It took them a month to figure out how to cope.

And this was a book that sold over a hundred thousand copies. So I'm not unmindful of the importance of copyright. I personally profited by it a great deal. But I'm also looking for the proper balance.

In that chapter called "The Hackers Workbench," I have a page excerpt from a book from

1853 -- no copyright issue involved. The book was called "A Rudimentary Treatise on the Construction of Locks," discussing whether or not it was proper to discuss lock-picking and vulnerabilities. I won't read the whole page, but...

"If others differ from the lock maker about the quality, it's open to them to say so, and a discussion truthfully conducted must lead to public advantage. Discussion stimulates curiosity. Nothing but a partial unlimited view of the question could lead to the opinion that harm can result. If there be harm, we much more than counterbalanced by good."

Thank you.

MS. CHARLESWORTH: Thank you, Professor.

Professor Matwyshyn? Did I say that correctly?

MS. MATWYSHYN: You did.

MS. CHARLESWORTH: Oh, wow.

MS. MATWYSHYN: Thank you to the esteemed panel for permitting me to be with you here today to speak about the topics that are at issue in our requested exemption.

So I'm here in my capacity representing security researchers, but I'm also here as a legal academic who has studied these issues for over a decade and the question of the litigation threats that arise from Section 1201.

And I should say my background is as a corporate attorney. I've helped companies start businesses, create intellectual property, protect intellectual property, and engage with both consumers and attackers of their intellectual property.

The questions that we're considering today at root deal with a type of frivolous litigation. They are an attempt to mitigate disclosure and conversation around existing flaws that may impact consumers, the safety of our economy, the safety of our critical infrastructure.

And as such the request that we're making of this esteemed panel is to help curb the frivolous litigation that arises as a consequence of Section 1201.

MS. CHARLESWORTH: So I have a question. I mean, this is a question that really is for probably the entire panel, pretty much.

But on the issue of disclosure, I mean, obviously, what you're suggesting is -- you know, and we heard this earlier -- manufacturers tend to shut down the conversation. They want to shut down the conversation.

But isn't there a countervailing interest in at least giving a manufacturer of a deficient product some time to correct it before there's public dissemination of the hack?

Which, you know, I understand for sophisticated really bad-hat people that are out there working, that's the argument.

But for, say, hacking into something more mundane -- say, a video console or something like that -- a video game console -- I mean, there are probably a lot of people who don't know how to do that who might be educated after reading a disclosure.

And so I'd be really interested, since you sort of have the law and the technical piece of this, in hearing your thoughts on how to balance those two interests.

MS. MATWYSHYN: So in my experience, there are two types of companies. Some companies are very receptive to receiving this type of information; in fact, they welcome it. There are sophisticated entities, such as Facebook and

Google and Tesla who have bug bounty programs where they compensate, in fact, researchers asking them to help with securing their products.

And so there's this affirmative solicitation. They have processes in place with a clear reporting mechanism on their websites, for example, and internal identifying personnel to engage with these conversations.

The second type of company, unfortunately, has not yet grown into that sophisticated model of vulnerability handling. And so it's this second category of company that does not possess the external hallmarks of sophistication that I mentioned with respect to the first category.

These are the companies that react viscerally through overzealous legal means and, unfortunately, threaten security researchers. And so, if I may, the PowerPoint that I shared has a copy of one of the DMCA threats that was received on April 29th of this year. And this --

MS. CHARLESWORTH: Okay. So this now -- Ms. Smith, this -- okay. Yes. This is Exhibit 10 -- Hearing Exhibit 10, for the record, that we're looking at now on the screen, which is a letter from a law firm to Mike.

(Whereupon, Hearing Exhibit No. 10 was marked for identification.)

MS. MATWYSHYN: Yes. So this is a letter from an attorney at Jones Day to Mike Davis, who is a security researcher at IOActive, a security consultancy, in connection with Mike's repeated attempt, as documented in a "Wired" article to contact CyberLock, a manufacturer of locks used in various financial services and infrastructure applications, as I understood their product from their website.

Mike Davis attempted to communicate with them on multiple occasions and discuss with their technical team the vulnerabilities that he discovered, in particular, my understanding is the ability to clone the lock, which is a serious flaw in their product line.

The attorney here was, in Mike's recounting -- and on the subsequent slide you have a letter -- an e-mail from their general counsel to be explaining the general counsel's experience with interacting with Jones Day on this matter.

The attorney from Jones Day used the DMCA as the sole legal basis for the threat against the security vulnerability disclosure.

MS. SMITH: Looking at this letter, the third paragraph says, "When I reached out to discuss this matter with you, you declined to share any information about your activities concerning the products."

And I'm wondering -- my reading of it as part of the hearing was that, you know, I wasn't sure exactly what had gone on, but there seems to be CyberLock taking the position that Davis had insufficiently disclosed the vulnerabilities.

Did you -- and also I'll note, in your proposal, you have outlined an annex that would require, I think, Mr. Davis to disclose the type of things that Jones Day is saying he failed to do.

MS. MATWYSHYN: So my understanding is that those disclosable items were shared or were ready to be shared with the technical team. And so you have in additional slides not only a slide from the general counsel but also a subsequent follow-up e-mail that Mike Davis sent to me explaining a little more in detail the exchange as well as identifying some prior instances where he's been threatened with the DMCA.

MS. SMITH: That actually makes me wonder whether, if your proposed exemption were just granted in full, whether that would change the outcome of this case.

Because, you know, we can grant an exemption, but if a company is going to engage in frivolous litigation -- and I don't know that this is frivolous -- but if it's going to, we can't change, you know, them from taking that posture.

MS. MATWYSHYN: So I believe that it would remedy the situation significantly.

On the next slide, which I can advance -- which I forgot, sorry -- here, actually, I'll advance two to the note from IOActive's general counsel. And so in the general counsel's perspective on this incident and on similar instances, the general counsel is seeking a strong basis to be able to defend his company.

And he expresses concern that merely getting litigation to the point of discovery can cost -- he quotes the figure of somewhere in excess of $250,000.

And so when we're talking about a small security consultancy or an independent researcher, this transaction cost of purely hiring an attorney and engaging with the legal system is cost-prohibitive.

And so that's why having an exemption that provides a nice roadmap would give a one-line statement of reassurance that a security researcher or general counsel could send to a potential plaintiff informing them that the conduct of the researcher has been within the strictures of the law and that no basis exists for litigation.

And so that would give comfort to the security research community in a dramatic way.

MS. SMITH: And so is it Part B of the proposal mainly that you're thinking would have deterred this incidence from happening if the proposed exemption were in place?

MS. MATWYSHYN: Yes. I believe that, if this exemption were in place, it would have been far less likely that the attorney at Jones Day would have felt at liberty to mention the Digital Millennium Copyright Act as a basis for potential litigation.

MS. SMITH: And that's because --

MS. MATWYSHYN: So provided that CyberLock has in place a reporting channel and that the researcher used the reporting channel and the reasonable vulnerability management practices exist and the researcher disclosed the list of disclosables that we've delineated in our proposal, this would provide a clear roadmap for both sides' relationship to each other in the context of a vulnerability disclosure.

MS. SMITH: Okay. So they could -- they could fight over whether the disclosure had, in fact, taken place. But there would be a little bit less areas that are murky, you're saying?

MS. MATWYSHYN: There would be a significant improvement in the murkiness, and it would be ultimately a more easily discernible question of fact rather than an interpretive matter for the law.

MR. DAMLE: Sorry. I have a question about this.

So one of the elements here of -- of this is that the -- that the manufacturer or the company have an internal corporate vulnerability management handling process.

How would an independent security researcher be able to verify that?

MS. MATWYSHYN: So from the perspective of the researcher, the most important piece of this is the location of a prominently placed reporting channel. These additional requirements are not researcher-centric; they're for assisting a subsequent analysis of a situation, if it were to go awry.

But the bottom line is we want researchers to use provided channels of reporting. And so if a provided channel of reporting exists, this directs the researcher to use that channel. And that's the most important element from a researcher's ability to assess whether a company is hostile or receptive to vulnerability reporting.

MR. DAMLE: Right. So that -- so it seems to me that you're talking about the front door.

MS. MATWYSHYN: I am talking about the front door.

MR. DAMLE: But then you've separately said in your proposal -- I'm just trying to understand sort of what the element -- all the elements of your proposal.

The one that gave me pause was on No. 3, page 2 of your reply comments, which talks about the creation of an internal corporate vulnerability management handling process.

And what the opponents have said is, "Look, for an independent security researcher, how would they even know whether a company has those internal processes in place?"

MS. MATWYSHYN: Mm-hmm.

MR. DAMLE: So setting aside the front door -- which obviously they could find out about -- how would they know about the internal processes?

MS. MATWYSHYN: So from the perspective of the researcher, the important element is the front door.

MR. DAMLE: Okay.

MS. MATWYSHYN: From the perspective of analysis subsequently for a judge or another finder of fact, the question would be not only whether the front door existed but let's say that the front door existed, the front door was used but the rest of these processes were not in place and the vulnerability disclosure goes awry because the report was lost on the desk of someone in the sales department who did not pass it on.

MR. DAMLE: Yes. But -- okay. But then it doesn't do -- that element doesn't do -- it's not very helpful, going to Professor Reid's point, in giving sort of ex-ante comfort if you don't know, well, what are the internal processes going to shake out as.

MS. MATWYSHYN: So the first -- yeah. So the first point gives immediate, in-the-moment comfort. The other points give comfort knowing that, if the vulnerability disclosure process goes off the rails --

MR. DAMLE: Right.

MS. MATWYSHYN: -- not because of the failure to report but because the internal processes weren't in place and the subsequent threat is levied against the researcher, that the researcher has a second-tier ability to defend if the later rounds of the vulnerability disclosure are not successful and result in a threat under the DMCA.

MR. DAMLE: I see. Okay. All right. Thank you.

MR. BELLOVIN: May I add something here?

MR. DAMLE: Yes.

MR. BELLOVIN: It's often remarkably

hard to find out how to report a vulnerability that you have found. More than once -- and I've been doing security research for almost 30 years. More than once -- and I know people all over the industry.

More than once, I've been able to help people who've come to me saying, "Steve, I found a problem in such-and-such. Can you help me report it? There's no way to get in contact with this company."

I know people at most of the major companies, the security people. I can generally find a way -- an artificial channel.

But think of yourself -- put yourself in the position of someone who has found a flaw and doesn't say "not me." What do you do with it? Do you have any choice but to go public if it's a threat to life and safety if there's no mechanism provided?

That alone would be a tremendous benefit.

MS. MATWYSHYN: If I may, as a case study of a typical disclosure, Professor Heninger was going to provide this panel with some statistics from a particular vulnerability disclosure that she engaged with. So Professor Heninger attempted to contact 61 companies with respect to an existing vulnerability. Thirteen had some kind of contact information available. For the others, she was forced to guess at what the best point of contact might be.

There was a human-generated response from 28 of these companies out of 61. A different 13 of the companies said that they had already fixed the problem at some point in time. And six subsequently released security advisories because of the report from Professor Heninger's team. And three of those were after the intervention of ICS-CERT contacting the particular vendor in question to nudge the disclosure and correction process.

And so that's out of the 61 companies that she could identify were impacted. So that's one case study.

MS. CHARLESWORTH: Right. Although, in that case she, I think -- I guess the suggestion is she did a good-faith attempt that she probably documented -- and clearly did because she has all the results --

MS. MATWYSHYN: Yes.

MS. CHARLESWORTH: -- to notify all

those affected companies.

MS. MATWYSHYN: Yes.

MS. CHARLESWORTH: And in some cases may have been unsuccessful but in some cases was successful.

So, I mean, that's another way to look at that. It's a more objective standard rather than having her know, again, to my colleague's point, what the internal processes of these companies may or may not be in terms of judging how to -- how she should behave.

MS. MATWYSHYN: So, again, if I may, the judgment point for the researcher is whether there is a front door for reporting. If there is a front door for reporting the vulnerability, the researcher should use it.

MS. CHARLESWORTH: Well, that's one way to judge it. But another way is just that you do your -- you make a good-faith effort to track down the company and do -- and document that. And if you -- you know, in many cases, you probably will find them -- in many cases, they may have a front door. In some cases, they won't but perhaps you could figure out how to contact them and keep a record of that.

And in some cases, you might be unsuccessful and you could keep a record of your efforts to attempt that.

I'm just saying that's another way to sort of approach this problem.

MS. MATWYSHYN: Mm-hmm.

MS. CHARLESWORTH: I think in some sense you end up with this -- at the -- largely at the same place, but you're not using a standard that requires you to know something about the internal workings of the company.

MS. MATWYSHYN: So I agree. This is certainly one paradigm of contact, and it's the one that most researchers currently use.

The challenge happens in the researchers' documentation not being believed by the company who, nevertheless, threatens DMCA litigation. And so the transaction cost of the litigation threat is happening even in instances when there is an internal, thorough documentation of the researchers' reasonable attempts to contact.

And so --

MS. CHARLESWORTH: Right. But you're not -- you're not going to avoid -- I mean, this gets to -- I mean, some companies are just going to do that, right, because they have money and resources to threaten people even if they -- if they can come up with some basis to, you know, in their heads at least, to do that. So you're not going to avoid that entirely.

But we're trying to -- we're struggling with if we were to go down this road and grant an exemption --

MS. MATWYSHYN: Mm-hmm.

MS. CHARLESWORTH: -- how do we deal with the disclosure issue? And so one of the issues we're having with the ISO standard or whatever -- you know, that kind of model is it's hard for people to know what the internal policies of companies are.

MS. MATWYSHYN: So, again, the front door is publicly visible on any website. There either is or is no reporting mechanism on a company's web side.

MS. CHARLESWORTH: Right. But -- okay. I guess we've gone back and forth.

I think some of the standard, as I understand it, is how they handle things internally.

MS. MATWYSHYN: Those are secondary standards. The first cut, from the researcher's perspective, is whether there is a visible, public point of reporting. If that exists, the researcher should use it.

If the disclosure goes off the rails at some later point, then those secondary internal processes will be assessed, probably with the assistance of counsel.

But having that first prong allows for an independent researcher without the benefit of a legal team to have assurance that this is the appropriate reporting channel, this is where they should report, and if that front door is not findable, not visible, not usable, it gives the researcher assurance that the good-faith effort will have an empirical basis for --

MS. CHARLESWORTH: Right. But if they don't have a -- I mean, I don't want to belabor this too much. I want to -- but, I mean, if they don't have a front door, I mean, why shouldn't they try other means to contact the company if they can?

In other words -- I mean, this happens all the time in copyright when you're trying to find who owns something and you do research basically and try to make a good-faith effort to figure out who owns something.

So in other words, if there's no front door -- I mean, basically, what you're saying is "We here should -- we should have a standard that says everyone has to have a front door or people can disseminate their research" is, I think, sort of where this ends up.

And on the other hand, you could have a standard that says, "If they have a front door, use it. But if they don't, do -- you know, use good-faith efforts to try and contact them."

You know, there's a more nuanced standard, I think, that could also be considered here. I guess that's -- that's what we're driving at.

MS. MATWYSHYN: So the -- the basis for this approach that we proposed is arising, as you mentioned, out of the ISO approach that was a negotiated standard across eight years among many different constituencies.

And so that is why we have suggested this --

MS. CHARLESWORTH: Yeah. I mean, one of

my concerns about that standard is that it's like -- those are big-tech -- for the most part, big, sophisticated tech companies, I think, who negotiated and partake of that standard.

But, I mean, this law would apply across the board. And I think you're going to have, I'm guessing, a lot of manufacturers and companies out there who may not participate in that, may not have internal resources to be engaged with that kind of process.

And so we have to think of them as well.

MS. MATWYSHYN: Mm-hmm. So the notion of designating a copyright contact as the appropriate point of contact also for security vulnerability disclosure as one of those points or have some sort of overlapping approach but designating the correct channel from the perspective of the company the same way that they designate the correct channel for copyright reporting?

MS. CHARLESWORTH: Well, that's -- for DMCA, that's a statutory requirement and that's -- that Congress thought about for a long time and enacted.

MS. MATWYSHYN: Mm-hmm.

MS. CHARLESWORTH: So -- but, you know, we're in a slightly different posture here.

MS. MATWYSHYN: But if I may follow up on that. I think Congress was contemplating the ability of this kind of information flow when Congress discussed and included Section 1201(i). And so, for example, if we look at the language of Representative Markey, when he was proposing this, he mentioned that the goal was to provide an opportunity for consumers to object to personal data-gathering, to have privacy and data-flow integrity considered.

And so these issues of the back-and-forth of information flows was presciently considered by Congress. And so the approach of a designated point of contact, Congress considered them the DMCA as well. And so these two policy considerations that permeate the DMCA are, I believe, consonant and so lend themselves to expansion and clarification in the ways that we've proposed.

MS. CHARLESWORTH: Okay. Do you want to wrap up and then we'll go on to Professor Blaze?

MS. MATWYSHYN: Sure. I can reserve the remainder of my time for questions.

But the issues of DMCA litigation threats have been a concern in the security research community for well over a decade, and there are examples of threats such as the one on the screen that date back over a decade.

And so this has been a consistent, long-running, frivolous litigation concern arising out of Section 1201.

And with that, we look forward to continuing to address any concerns or questions that you have.

MS. CHARLESWORTH: Thank you.

Professor Blaze?

MR. BLAZE: Okay. So first of all, thank you very much for considering our proposed exemption. And thanks for the opportunity to speak with you today.

I'm a professor in the computer science department at the University of Pennsylvania where I study how we build secure systems. A focus of my work is the applications of cryptography, but I'm more broadly concerned with the secure implementation of computing systems.

Like my colleague Professor Bellovin, prior to entering academia, I worked for about a dozen years at Bell Laboratories, also as a security researcher, doing much the kind of work that I do today but without students or the troubles of getting funding.

The -- much of my work, both before the enactment of DMCA and since, has been concerned with or has stumbled upon vulnerabilities in fielded systems. And some of these fielded systems are traditional Internet-connected systems. Others are not.

For example, in 1994, I discovered some fundamental flaws in a U.S. government-proposed encryption standard called the Clipper chip. In 2008, I examined a number of electronic voting systems and found -- in 2007-2008, I found flaws in a number of fielded electronic voting systems.

And in 2004 and in 2005, I discovered some fundamental weaknesses in various wiretappings systems used by the -- by the government for conducting electronic surveillance.

I'd like to talk about two examples where the DMCA has specifically either played a role or not played a role in the -- in the work that I've done, though it's loomed over virtually every bit of nontrivial work that I've done since the legislation has passed.

The first thing I'd like to talk about is analogous to the IOActive and CyberLock case in Exhibit 10 that was discussed earlier in this hearing.

In 2003, I decided to look at the applications of cryptographic techniques to other types of security. And I looked at mechanical locks and in particular the kind of mechanical locks that we use in offices with a master key that can open all of the doors. These are purely mechanical devices.

And I discovered a flaw remarkably similar to the flaws discovered by IOActive that allowed somebody to take an ordinary house key and convert that into the master key that would open all of the locks in the system. And I, you know, discussed how you could use cryptographic techniques to analyze locks and it would lead you to this result fairly straightforwardly.

And it was, from my perspective, a fairly, you know, interesting example of -- illustrative and educational example of using cryptography. But it also had a real-world impact that it demonstrated that master keyed locks need to have their security reevaluated.

Now, this was a purely mechanical system and didn't contain, as a result, any TPMs that would bring the DMCA into consideration. And so when I published my work, I did so without fear of having to defend myself against frivolous DMCA claims because such claims really wouldn't be possible.

Nonetheless, the lock industry was unhappy about my criticism of its products even though they claimed that they had known about this vulnerability for several decades and had chosen not it fix it because essentially it would be too expensive and make locks a little less convenient to use and more expensive to manufacture.

So I was able to, you know, publish my work. It had its educational value. And we were able to warn the industrial lock community about this flaw without the kinds of concerns that I would have had had these -- the only difference been that these locks were implemented electronically rather than mechanically.

So the -- you know, essentially the very same technology that IOActive examined in the CyberLock and had to -- to respond to, you know, what I assume is a frivolous DMCA claim, I was able to do without -- without those fears only because I happened to be looking at this in the purely mechanical realm.

A second example of work that I've done that's been chilled by the DMCA: In 2011, I and some graduate students of mine embarked on a study of a communications system called P25 that's used as a digital two-way radio system used by first responders, by the federal government, and by others who are concerned with secure, reliable, two-way radio systems.

And I examined the standards for the P25 system as well as the broad behavior of a variety of radio products that use them for these two-way radio systems used by first responder and by federal surveillance officers.

And we discovered a number of fundamental weaknesses in the published protocols, and we discovered a number of usability failures in the way that these are used. But we also discovered a number of ways in which the protocols could lead to implementation failures.

In order to study those implementation failures, we would have had to extract the firmware from some of the radio products, which we had access to -- we bought on the secondary market. We went and bought some on eBay and so on. But we were sufficiently concerned that in order to extract the firmware from these devices, reverse engineer it, and study it, and in particular develop and trade in tools that would allow us to extract the firmware from these products, that there would be no way of doing so without running afoul of the DMCA.

And so we left that line of research essentially untouched.

Now, it's possible that, if we were -- if we had the resources and the time to engage, you know, a large legal effort to denote parameters with which we could work, we'd be able to navigate that. But under the DMCA, as written, we were -- we just decided that this was too risky to proceed with.

MS. SMITH: So I'm a little bit wondering why 1201(j) did not apply in that instance. I don't know if you sought legal advice or if you could share what that was.

MR. BLAZE: So we did -- so, you know, without getting into too many specifics of, you know, the attorney-client conversations we had, you know, essentially, we -- the conclusion was that we were on extremely treacherous territory primarily because we would have had take some devices, reverse engineer the software, attempt to see if the implementation failures that the standard -- that we anticipated might be present in the standard were there, and effectively build a -- build our own test bed along the way to doing that.

We did approach a few of the manufacturers of the -- of the equipment and attempted to engage with them and were ignored or rebuffed at every phase. So we realized that this would be a very hostile relationship if we -- if we proceeded.

Now --

MS. SMITH: So it sounds -- and you don't have to answer if it's a little too legal. But it sounds like maybe some of the concern might have been the anti-trafficking provision in addition.

Do you know if that's --

MR. BLAZE: That's right. The anti-trafficking provision would have been particularly problematic because we would have required tools for extracting this.

There was a colleague -- another researcher in Australia who had also been examining the same system who had developed tools who expressed some interest in working with us. And we basically, couldn't pursue that relationship because of the trafficking considerations. And we'd want to be able to, you know, publish the work that we've done along these lines.

MS. SMITH: On a different topic, I'm wondering if there is sort of a norm in your community -- the academic community of sort of trying -- if you can find the person, disclosing in good faith before publication.

MR. BLAZE: Right. So, again, certainly, there are simple cases and there are hard cases. In the simplest case, we find, you know, a particular flaw in a particular product that has a well-defined manufacturer and we're able to go to a point of contact or if we can't go to a point of contact, use informal, asking around who should we call.

And sometimes we're able to do that. And obviously, as someone, who is an academic in the security community who wants to work in the public interest I don't want to do harm in -- as a result of my work. And disclosing to the -- to the vendor flaws in their products is certainly an important part of avoiding harm.

However, in other cases, even identifying the stakeholders is often not so clear. So one example would be flaws that are found in libraries that are used to build a variety of other products.

And we won't always know what all, most, or even some of the dominant stakeholders are there.

MS. SMITH: So let's take the example, though, when you do know --

MR. BLAZE: Mm-hmm.

MS. SMITH: When you do know --

MR. BLAZE: Mm-hmm.

MS. SMITH: -- does it make sense or is it a norm of responsible security research --

MR. BLAZE: Right.

MS. SMITH: -- to disclose in advance of publication as opposed to concurrently?

MR. BLAZE: Right. So I think it's really a question that has to be answered on a case-by-case basis. I think there is certainly a large class of cases where we have a specific vulnerability that we know is limited to a specific product and we can - we can say, "Okay. If this manufacturer repairs it, then we can mitigate this harm."

There are other cases in which it's less clear where the vulnerability is present, and it may be more prudent to warn the public immediately that, you know, the product is fundamentally unsafe.

So I'm reluctant to make a categorical statement of what the norm is because there's a range of circumstances at work here.

MS. SMITH: Maybe Professor Green?

MR. GREEN: So one thing I would like to add to that is, in some cases like the vulnerability last week, you have a case of mass disclosure where you simply can't notify all of the stakeholders at once. And that actually works against you because now you have the issue where, if you notify people, they can leak the information, which causes it to become public before you'd like it to, which actually puts people at risk.

So you have to be very selective in choosing to whom you disclose. And that actually is very, very difficult. You can't notify people. You're going to be in a position where the only solution you have is to avoid notifying everybody who's affected.

MS. SMITH: Meaning the companies?

MR. GREEN: Right. So if you have a situation where, let's say, 200 companies are affected, certainly you could notify some companies. You can go to Google. You could probably go to Apple and you could trust that the information would not leak out.

But beyond a certain point -- and I've had this happen -- if you notify everybody, the probability that the information becomes public unexpectedly, before significant remediations can be made, rapidly approaches one. It's something that is almost inevitable if you do a mass disclosure.

So you have to find a balance between notifying as many people and protecting as many individuals on the Internet as possible without creating a situation where you have an unintended leak.

And I'd like to add that Heartbleed, which we're probably all familiar with, was an unintended leak. Too many people were notified of a mass vulnerability, and it came out two weeks before it was supposed to. And as a result, many systems, including Google and Yahoo were not patched.

MS. CHARLESWORTH: So in that situation, I mean, is what you're suggesting that you should only notify selected manufacturers? Or what is your solution to that scenario? I mean, because I thought what we were really talking about was notifying the manufacturer versus just disseminating the information publicly.

So what -- what is -- if you could elaborate a little bit on --

MR. GREEN: Sure.

MS. CHARLESWORTH: -- what you're saying and how you would approach the Heartbleed problem correctly, in your view.

MR. GREEN: So I think the simplest answer to that question is there is no single answer that you could write down on paper that would cover every situation.

With Heartbleed, the situation was you had a massive vulnerability that affected thousands of separate websites. You could notify Google, and you would have a high probability that the information would be -- would stay secret and that they would fix. And that would protect maybe 50 percent of the individual end users on the Internet. You could go to Yahoo, and that would protect 25 percent.

And you can see that there are diminishing returns as you go to additional websites. As you go to a small website that has maybe 200 end users, now you are protecting 200 people by notifying them. But at the same time, the probability that that small website operator leaks the information is fairly high.

And then with a public leak, you could have criminals now exploiting that vulnerability before everybody has a chance to fix it. So there has to be a balance. It has to be customized to every single potential security vulnerability.

MR. REID: And I could chime in too. I think the theme that you're hearing consistently here is that this is a very complicated issue that's long been the province and the judgment of security researchers who do this as a profession and as an advocation. And it's only because of the DMCA, as Professor Blaze alluded, that suddenly this has moved into the realm of copyright law.

And I think it's getting pretty far afield of the intent of Congress, in enacting this law, to mediate these type of judgments and the complexities of these judgments, which take a lot of negotiation, as Professor Matwyshyn underscored.

There are a lot of negotiations to go into developing this ISO standard. So there's a lot of complexities here, and we would strongly caution the office in being too prescriptive about how this disclosure happens, I think, for two reasons.

One, if there's no -- if there wasn't a lock involved and the DMCA wasn't involved, we'd just be talking about fair use. And in that case, it would absolutely be up to the researchers' judgment how to do it and there would be no question about what they did with the disclosure or after the fact, the initial -- whatever copying was necessary to do the research is all we're talking about. And after that, I think the research is -- the researcher is free and clear.

And I think it's also important to underscore that, when we're talking about the disclosure of the research, we're talking about First Amendment-protected speech. So you've got some serious limitations on the level of prior restraint that you can apply, and I think there are some serious concerns that I have when we start talking about a really ridged structure that governs when someone is allowed to say something and when they're not, particularly when the policy judgments underlying it are complicated.

But even if they weren't, I think there are some serious First Amendment issues that you have to consider before you go too far down this road.

MS. CHARLESWORTH: Have you briefed the First Amendment issues to us, I mean, other than mentioning them?

MR. REID: No. They're not in our brief, and we'd be happy to provide some supplemental briefing on that if that would be helpful.

MS. CHARLESWORTH: We'll let you know.

But I mean, here's the thing. I mean, kind of where we're coming around is that, when Congress said, "Well, we'll just consider whether you disclosed it as a factor," I mean, this loose standard, maybe Congress had -- was thinking correctly about that when they put that in there.

Because what you're -- what I'm hearing from Dr. Green and others is that -- and what you're saying right here -- is sometimes you should disclose, sometimes not; you have to figure out how to do it. I mean, that's maybe why -- you know, perhaps that is the reason behind the standard that we have today in the law for (j).

And why -- I mean, you're kind of making a pretty good argument for that.

MR. REID: Well, I think there's two responses to that. One, Congress can't contravene the First Amendment even in enacting the DMCA. So to the extent that you're advocating for a reading of Section 1201(j) that would contravene the First

Amendment --

MS. CHARLESWORTH: I'm not -- I'm not advocating for that.

What Congress said, just to be clear, is that, in looking at whether there's a violation, they're going to consider whether there was a disclosure to the manufacturer. I don't think that contravenes the First Amendment.

And what I'm saying is -- what I'm hearing now is that maybe that's not such a bad way to think about this.

MR. REID: I think -- the other thing that I would put out there is that the factors that are mentioned by Congress in Section (j), to the extent that they're compatible with the First Amendment, can be read as being probative of the intent of the researcher and whether what they were up to was, in fact, security testing or whether it was something else.

So you might look to those things as evidence of the act that the security researcher would engage in. But I think reading them as limitations on speech that can be made after the circumvention is performed is constitutionally troubling

MS. CHARLESWORTH: Well, that -- that's -- I mean, first of all, that's a brand-new argument that wasn't, as you just acknowledged, briefed before. And I don't read what's in -- currently in 1201(j) as constitutionally troubling in the way that you're suggesting.

But there's a lot of commentary, and this request for an exemption has to do with disclosure. We've had one suggestion that we basically adopt ISO standards. Some of have suggested that we look at -- to the -- Google as a 90-day disclosure standard. You're saying there should be no standard, I think, if I'm hearing you correctly. Although there's one -- you know, Congress clearly had something in mind to some degree at least about whether you fall under the exemption.

So that's -- you know, that's what we're exploring.

But, I mean, I -- I don't know that -- I mean, Congress clearly had some concern about this area, and many of the commentators have concerns about it as well. And there's a lot of practices around this area.

So anyway, thank you for your comments.

MR. BLAZE: If I might just respond to the --

MS. CHARLESWORTH: Dr. Blaze, yes.

MR. BLAZE: -- disclosure issue. I'm sorry. My attorney wants to do that.

All right. So one -- as academics and as members of the public research community and as scientists, right, I mean, the aim of our work is to disclose it. Right? I mean, the scientific method demands disclosure.

I think there's no question that somebody building -- building tools for the purpose of infringing copyright is not the aim of research.

My aim as a researcher is to discover new things and tell everyone and to one, the public. And included in that is, of course, disclosure to the vendor.

So I think the question of disclosure, as discussed in the DMCA, is whether or not the work is kept secret or disclosed to the -- to the vendor, not a question of whether it's disclosed to the vendor in advance or what the period of time is.

And I think nobody here is advocating

conducting -- conducting research and keeping it secret. In fact, quite the contrary. We're trying to protect our ability to do research that we will -- that we will publish and we will disclose and that we can all benefit from.

So, sorry...

MS. CHARLESWORTH: Okay. Did you -- was that the conclusion of your opening -- so-called opening remarks?

MR. BLAZE: I will --

MS. CHARLESWORTH: I realize we're past the opening, but that's okay. This is the way this goes.

MR. BLAZE: I will shut up now, yes.

MS. CHARLESWORTH: No, no, no. That's fine.

Dr. Bellovin?

MR. BELLOVIN: Yeah. Twice in my career, I have withheld from publication significant security flaws; once in a 1991 paper of mine, once the very last change that we made to the firewalls before sending it off the printer was to delete a paragraph describing an attack that we didn't know how to fix.

In both cases, the security community

knew about both. The first vulnerability I shared with CERT, the Computer Emergency Response Team funded by the Department of Defense; meetings in Washington and so on.

Both cases, because the security community publicly was not made aware of this, the bad guys exploited the flaws before fixes were in place. It was never seen as urgent enough.

And the 1990 paper of mine with the flaw, I published in 1995 with some -- almost unchanged except for a couple of paragraphs of commentary saying, you know, "Here's how I discovered it. Here's the history." And we decided to publish after -- first of all, it was being used in the wild by bad guys. And second, my original memo, shared only very closely with very responsible parties, ended up on a convicted hacker's site.

So there's no doubt about how the hacker had learned of it. The security community as a whole, though, didn't take it seriously enough because it didn't seem to be a real threat because it wasn't public.

In the other case, the vendors were aware of the problem, didn't see a fix. But once it came out in the wild, the security community as a whole -- many more people than I could personally engage -- found solutions, and it's not the threat to the Internet that it seemed to be in 1994 because a lot more people were looking at it than found the fix.

So in both of those cases, I would say that trying this very private disclosure and not saying anything publicly actually hurt security. We saw the exploits before the community bothered to react or, in one case, was able to.

MS. CHARLESWORTH: Professor Matwyshyn?

MS. MATWYSHYN: Just four brief points, if I may.

So first, to clarify, the security researchers believe that our request stems from primarily 1201(i) and, therefore, the concerns that were noted in the context of 1201(j) are a slightly different set of issues for us.

Secondly, on the point of the First Amendment, in our filings, we did reference a First Amendment argument. And there's a footnote to an article extensively discussing the First Amendment implications of security vulnerability disclosure.

Should the panel wish to review, I'd be happy to provide a full copy of that document that was referenced in our filings.

Next, on the point of Google's period of 90-day disclosure, I would like to point out that Google is a member of the Internet Association, which has filed comments in support of our exemptions. So Google is on board with our approach to this problem.

And finally, on the point of frivolous litigation, the benefits of an exemption such as ours which provides clarity and comfort to researchers allows for them to feel more comfortable contacting vendors on an earlier basis rather than needing to weigh the risk of litigation to themselves and putting them in a position to decide how to -- what degree of legal risk to separate, which nudge them toward a later contacting of the vendor, to try to give the vendor less time to sue before the public disclosure.

And I think Professor Blaze can speak to his experiences of needing to run that calculus for self-preservation concerns on the point of vendor disclosure and litigation.

So providing the comfort of the exemption that we're requesting will encourage researchers to contact companies earlier.

MS. CHARLESWORTH: Okay. I think, unless -- I think we're going to skip over you for now, Professor Blaze. I don't know if you have anything to add.

I felt like -- I felt like you spoke to that issue earlier, but there will be more opportunity.

And we'll move over to the very patient other side of the room.

Ms. Moy, could you let us know what's on your mind?

MS. MOY: Great. Thank you. Thanks so much. And thank you very much for your attention to this issue. Thank you very much for inviting me -- or allowing me, I should say, to testify on behalf of the proposed exemption.

So I -- in addition to working on copyright issues, I work a lot on consumer privacy issues. Most recently, I've been doing a lot of work on -- in response to legislative proposals on breach notification and data security standards.

So I appear before you today to talk a

little bit about consumer privacy concerns in the context of the proposed exemption, some of which I did -- I did comment about in this -- in the -- in this docket.

And I think it -- I think it's -- although I have -- I have encouraged the Copyright Office to focus most heavily on the strict copyright issues and to -- and to, you know, sort of not weigh the policy issues as heavily as some opponents in particular have suggested that we do.

If the context of this rulemaking, I do think that consumer privacy is relevant here for at least two reasons. One is that the statutory exemption for privacy indicates that Congress was concerned with privacy and how 1201 might affect consumer privacy issues.

And the other is that some opposition commenters, in the context of this proceeding, have cited consumer privacy concerns as a reason actually to deny the granting of an exemption for security research.

So I want to make three -- at least three reasons -- point out at least three reasons that we think it's absolutely critical to encourage the discovery of security vulnerabilities by removing roadblocks such as the anti-circumvention provisions as faced by security researchers who might find vulnerabilities in the consumer privacy context.

So first and most obviously, as many others have pointed out, vulnerabilities have to be discovered so that they can be fixed. And vulnerabilities are often what are exposing consumer information.

So in this proceeding, expert after expert have emphasized that malicious attackers are not waiting for the good guys to expose vulnerabilities through research so that they can pounce on them for ill ends. Malicious attackers are conducting their own security research, racing to find the exploitable vulnerabilities themselves first. And they're succeeding.

So this time last year, "CNN Money" reported that, in the preceding 12 months, hackers had exposed the personal information of roughly 110 million Americans. And that's half of American adults.

These are just the breaches that we know about. Many entities that suffer breaches never know.

So we have to assist the researchers in finding vulnerabilities as soon as possible, most ideally before they're discovered and exploited by malicious attackers.

To protect consumers, we have to dismantle the roadblocks, such as anti-circumvention provisions.

Second, vulnerabilities should disclosed so that consumers who are considering which products and services to purchase or patronize can incorporate security considerations into their decision-making.

Customers have a right to as much information we can provide them as possible about the security features of products that are available in the marketplace. Not only does robust security research, including disclosure of the results, help consumers make informed choices, but it also bolsters vendors' economic incentive to invest in security. And that's because vendors suffer costs associated with reputational harm following a vulnerability or breach made public. And that's as it should be.

The cost -- the threat of costly bad press over security failures encourages vendors to do better. We think that that's really important.

So, you know, others have spoken about the CyberLock vulnerability. Certainly, if you're a consumer in the marketplace considering different options for a secure lock, as a consumer, you ought to know that there is a -- that there is a known vulnerability with the product before you purchase it.

Third, vulnerability -- and I think that this one is one that's often overlooked in this context. Vulnerability should be disclosed so that regulators who are enforcing security requirements, unfair trade practices know whether the vendors are adequately protecting personal information as well as whether -- excuse me -- whether vendors are adhering to the promises they've made to consumers regarding security.

So vendors don't just have a responsibility to consumers to make their products secure and to protect personal information. They also have security responsibilities under the law.

For example, the Federal Trade Commission has determined that failing to implement reasonable security standards -- reasonable security practices with respect to personal information in many cases constitutes an enforceable violation of Section 5 of the Federal Trade Commission Act. And the laws of many states also require vendors to keep personal information secure.

To enforce security standards, regulators need to know how vendors are performing in terms of security. Regulators have some of their own staff who can assist with security research and security audits, but they also do rely in part -- sometimes in large part -- on the work of independent researchers who help them know when vendors are failing on the security front.

So just as an example, last year, the FTC brought at least two cases -- one against Snapchat and one against Fandango -- for failing to implement reasonable security practices. And in both of those two -- both of those cases, one of the -- one of the points that the FTC cited in its complaint was that an independent researcher had informed the responsible company of a security vulnerability and that the company had failed to address it.

So not only does the FTC use the reports of security researchers to help understand how well companies are doing, it actually -- it encourages companies to develop a process for receiving and addressing reports from researchers regarding vulnerabilities as part of best practices on data security.

So just to make that crystal clear, the most prominent federal enforcer of data security recognizes that security researchers play a critical role in improving security.

So thank you again for the opportunity to speak here today this issue, and I look forward to any questions you might have.

MS. CHARLESWORTH: Thank you, Ms. Moy.

Mr. Stallman?

MR. STALLMAN: Thank you. I'm Erik Stallman from the Center For Democracy and Technology, and I want to thank the office very much for allowing me to testify today in support of the class 25 exemption.

In view of the substantial testimony that's preceded me, I will just make a few points, one that I think is directly in response to some questions that you have been raising and one that underscores a point raised by the panelists.

And the first one just has to do with

the sufficiency of 1201(j) for security testing. I think there are two reasons why that provision is insufficient. And first is the limitation to security testing that's done only with the authorization of the owner or operator of the computer, computer network, or system.

In a world of Internet-enabled devices and services that have software and firmware that might be licensed from any number of parties, it can often be very, very difficult to determine who the appropriate person to seek authorization from is.

MR. DAMLE: So I have a question about this because this is -- I've been struggling with this a little bit because it doesn't say -- it doesn't say "the owner of the software." It says "the owner of the computer."

And so the sort of prototypical example that one thinks of 1201(j) applying is: I'm a bank. I buy a bunch of servers that run Linux or Microsoft Windows or whatever. And I want to hire someone to come -- a white hat to come and test my security, but I own the computer; I own the computer network.

The fact that I don't -- may or may not

own the software that's running on that server or on the router -- the Cisco router that I've bought doesn't seem to matter because it says it's the owner of the computer or computer network.

MR. STALLMAN: Right.

MR. DAMLE: So I'm just sort of curious about that disconnect. So to take an example, if I own a cell phone, you know, I could say I own the computer that sort of constitutes the smart phone.

Why isn't sort of that the better reading of 1201(j)?

MR. STALLMAN: Well, because I think that it's unclear, like -- is it sufficient to identify one owner or one operator? I mean, you can have a system -- if your banking network is connected to a VPN and that VPN is managed by somebody else and the person who manages the VPN is the person who has introduced the vulnerability into your system, is the owner or the operator of the VPN the person at the bank? Is it the person at the -- whoever operates your ISP? Is it the person who provided -- I mean, I take your point that it's not necessarily the person who owns the software.

But particularly with connected devices you can have one -- more than one person as the owner or the operator. And it's unclear whether the statute requires -- and this isn't the definition of the factors -- need to identify one or all potential owners and operators.

MR. DAMLE: So I'm just trying to imagine a scenario -- I mean, so the VPN example is one where presumably, if I'm a company and I've hired someone to be a VPN provider for me, I can presumably go to them and say, "Look, I'm concerned about the security. Give me authorization to have someone come in and test the security."

So I'm just trying to imagine scenarios where -- because there's just a -- there are a handful of different -- there are a bunch of different types of examples. Take the medical device example.

A security researcher could buy a medical device, presumably. And presumably, that's generally what happens is that they buy the pacemaker themselves and then, on that pacemaker that they own, they're running tests against it.

MR. STALLMAN: Mm-hmm.

MR. DAMLE: And so I think a fair reading of 1201(j) would be that they're the owner of that pacemaker -- that particular pacemaker that they're testing on.

MR. STALLMAN: Mm-hmm.

MR. DAMLE: And then -- so assume with me that that -- so that's -- assume with me that that's the correct reading of 1201(j).

So what are the -- what are other examples of where -- of sort of legitimate good-faith security research that would kind of fall outside of that where you're not necessarily the owner of the computer.

MR. STALLMAN: So I'm trying to figure out your example.

MR. DAMLE: Right.

MR. STALLMAN: So in that case, it's the security researcher, the person who --

MR. DAMLE: If you purchase something --

MR. STALLMAN: Right.

MR. DAMLE: The security researcher purchases a car or a cell phone or a pacemaker --

MR. STALLMAN: Right.

MR. DAMLE: I don't know. I mean, I don't -- I think it's at least a reasonable reading of 1201(j) -- that language in 1201(j) that you're talking about that they are then the owner of the computer.

MR. STALLMAN: And, therefore, have the ability to disclose that vulnerability not just to themselves but to everyone else who might have that computer?

MR. DAMLE: Well, I don't know. That's a separate issue. The question is how they -- do they fall within the -- so they don't need -- they get the authorization themselves because they are the owner of the computer, right?

So I'm just --

MR. STALLMAN: Right.

MR. DAMLE: That element of --

MR. STALLMAN: Right. I mean, you're asking me to assume that that's a fair reading?

It is a reading. I think part of the problem with 1201(j) is that it hasn't been tested that much in litigation. And I think there are a lot of circumstances in which the security researcher would have to rely -- and this is back to my VPN example -- on the bank being, you know, a faithful custodian of their authorization when they go seek it up the chain.

And so I think there's a problem with the definition putting you potentially in the position of having to depend on the person from whom you seek authorization, also like seeking authorization from someone else and then you staying all the way down the chain within the scope of that authorization. Because the moment that you fall outside of it, you fall outside of the exemption.

MR. DAMLE: Right. And so a related question is: Is the intent of this to allow someone without the authorization of a third party -- so I'm a security researcher, and I want to test HSBC's systems -- pick another bank.

MR. STALLMAN: Mm-hmm.

MR. DAMLE: So I want to be able to test their systems to know whether they're secure.

MR. STALLMAN: Mm-hmm.

MR. DAMLE: Is the point of this exemption to allow that sort of activity without the authorization of someone else, some other third party that owns a server that I'm trying to sort of test the security of?

MR. STALLMAN: I mean, I think that that may be one point. But I think that the larger point is to have -- is a circumstance where you have something like Heartbleed, something like -- where a ubiquitous exploit that is on many systems where you don't have to go around and figure out exactly whose authorization you need to seek before performing that research.

And it's also, I think, to help the situation of what is referred to at times as the "accidental researcher."

I mean, if someone just comes across a vulnerability while they're -- while they're engaged in wholly separate research, you know, the problem -- they have no -- I mean, they're basically out of 1201(j) because they found that vulnerability before seeking authorization because they didn't know exactly what they were looking for.

I mean, part of the issue with a sufficiently robust security research exemption is that often researchers won't know precisely what they're looking for until they start looking. And if they have to stay within the confines of authorization the whole time they're searching, they may not be able to ask the questions they need to ask.

MR. DAMLE: So just to ask my question again: So the scenario that I'm positing where, you know, I'm a security researcher and I just want to test this -- the security of a -- take a website at random or take a computer network connected to the Internet at random.

Can I -- under your sort of proposal, would I be allowed to do that?

MR. STALLMAN: Well, I mean, I think it would depend why you're doing it.

MR. DAMLE: Right.

MR. STALLMAN: I mean --

MR. DAMLE: But let's say I'm -- let's say I say I'm like -- I bank at this bank or I know people that bank at this bank and I want to test that their networks are secure.

MR. STALLMAN: Right.

MR. DAMLE: Am I able to do that and fall within the proposed exemption?

MR. STALLMAN: I mean, I think that so long as your purpose was good-faith security research, yes. I think that if you're just sort of idly curious if the -- if the system is vulnerable --

MR. DAMLE: Right. Sure. Sure.

MR. STALLMAN: -- I think that's a different story.

MR. DAMLE: Okay. But so as long as I have good faith, I don't need the authorization of some third party operator of a website or a system of some sort; I can just go in and test it myself as long as I -- as long as I'm acting in good faith?

I'm just trying to understand the sort of metes and bounds of the proposal.

MR. STALLMAN: Yeah. So you're entitled to perform research without running afoul of the DMCA circumvention provision -- should not hinge entirely on your seeking authorization. That's, I think, the point of --

MR. DAMLE: Okay.

MR. STALLMAN: -- of the exception.

MR. DAMLE: Okay. Great.

MR. STALLMAN: So to move on to the other issue 1201(j) --

MS. SMITH: You know what? Can I just --

MR. STALLMAN: Sure. Go ahead.

MS. SMITH: -- follow up on that?

MR. STALLMAN: Yeah. Uh-huh.

MS. SMITH: And I think Mr. Troncoso may want to speak to it to in return to him.

MR. STALLMAN: Okay.

MS. SMITH: In the BSA's paper, they point out that the legislative history says that the scope of permissible security testing under the act should be the same as the permissible testing of a simple door lock.

MR. STALLMAN: Right.

MS. SMITH: What the person may not do is test the lock once it has been installed on someone else's door without the consent of the person whose property is protected by the lock.

And it seems like --

MR. STALLMAN: Right.

MS. SMITH: -- when you were talking with Mr. Damle, you were saying, under your proposal, there would be no authorization needed to be requested whatsoever.

Is there any way, if we were going to, you know, perhaps modify the current exemption but not allow -- you know, retain some sort of, you know, good-faith effort to get authorization in it, that we could structure that language?

MR. STALLMAN: So would it require you

to seek authorization before beginning the research? Is that what you're saying?

MS. SMITH: Yeah. I'm asking whether you can conceive of any exemption that might be more workable for the security research community that would preserve some sort of an authorization element.

MR. STALLMAN: I mean, I go back with the problem of authorization is that it is hard for the researcher to know beforehand exactly what they're looking for and to stay within its scope.

And then you have the problem of if they find something, that that authorization can be revoked or can be cabined. And so I think that's -- I mean, I understand you wanting to find some variation of 1201(j) that works, but I think definitionally, if security testing is defined as something that's done only with the authorization of the owner or the operator of the system or computer or network, that you're going to run into situations where there is needed good-faith security research that's not being done.

MS. SMITH: Right. I think the concern is that we want to stay within the confines of what the congressional, you know, intent was at the time or at least take that as good guidance.

MR. STALLMAN: Mm-hmm.

MS. SMITH: And so in Mr. Damle's example, couldn't you just ask HSBC if you were going to do research?

MR. STALLMAN: Well, I mean, you could. But what do you do about the instance where you ask and they say no?

MS. CHARLESWORTH: You'd be out of luck, I guess.

I mean, I guess, to put a sharper point on it, how do you reconcile what you're proposing with the legislative history that Ms. Smith just reviewed?

MR. STALLMAN: Well, I mean --

MS. CHARLESWORTH: And are you asking the Copyright Office to basically, you know, step away from that?

MR. STALLMAN: Well, one, I think that the environment that we live in now and the environment that we lived in when 1201(j) was enacted are different now.

And I think that the -- that overall in the legislative history that -- I mean, in the -- the House report, they said that the -- and this was where they were talking about the encryption research -- but that the goal of Section 1201 would be poorly served if these provisions have the undesirable consequence of chilling legitimate research activities in the areas of encryption.

And I think -- I mean, I understand that this analogy was made to the door lock. I think it's a very interesting analogy to apply to digital locks that can be applied and put on many different devices.

But I think that the overarching goal of the -- of Congress in providing these exemptions was to make sure that legitimate research activities could continue. And I think that the problem that we're running into now is when people are trying to conduct that research, that 1201(j) is not providing the same scope of protection that they -- that they would seek and, more importantly, that their institutions would seek and that their funders would seek and the people who would publish their research would seek.

And so you're seeing a general chilling effect with that uncertainty.

MR. DAMLE: So could I ask you something? There's mention -- so there's mention in the papers of things like nuclear power plants and mass transit systems.

Are you suggesting that the exemption should allow sort of testing of, you know, live systems that are running nuclear power plants and mass transit systems?

I'm just wondering how that kind of research -- maybe that's a question sort of for this side of the table of how that research would be conducted.

MR. STALLMAN: Yeah. I mean, I'll defer to that side of the table a little bit, but I will say that many of those systems that we think of as critical infrastructure oftentimes depend on the same type of security that's running applications and services that we think of as noncritical infrastructure.

So I would hate to have a situation where you have essentially the stewards of critical infrastructure being able to say, like, kings ex on research that affects not only their systems but systems that, you know, are in widely used customer products and applications.

MR. DAMLE: Right.

MR. STALLMAN: And by the same token, I

would hate to have a -- the ability of a person who uses just the -- you know, the weird pig voicemail thing say that this depends on the same system that runs your mass transit systems so, therefore, you can't conduct this research.

MR. DAMLE: Yeah. Although that's sort of my point, which is to say, if this can be tested -- if this can be tested by sort of off-the-shelf software, if off-the-shelf software or things that are purchasable, say, are what run these other critical systems, then you can purchase that other stuff, do the testing on that, and not allow -- not -- I mean, not have an exemption that allows you to test on sort of the live systems that are running a nuclear power plant or keeping an airplane in the air or running our mass transit systems.

MR. STALLMAN: Right.

MR. DAMLE: I mean, that's sort of the concern is that, you know, if you -- if you allow sort of the testing of live systems, then that's -- that may not be necessary is what I'm suggesting.

MR. STALLMAN: Right.

MR. DAMLE: And so that's -- that's sort

of -- maybe that's the question for the kind of the researchers.

Maybe Mr. Reid and then Mr. Bellovin. Do you have thoughts about that point?

MR. REID: Yeah. I wanted to chime in and say to the extent that the office takes that reading of (j) that you proposed, the very broad reading, to the point about alleviating chilling effects and reducing frivolous litigation, if you could put that in the record or include that as part of the conclusions in this proceeding, that would be incredibly helpful and we would be deeply appreciative if the office actually takes a position that (j) is wider than people are reading it.

It would be helpful -- it would be very helpful to know that.

Second, I wanted to take a crack at your question about (j). And I don't know if I have a good answer about the network situation.

But I think the concern that we're primarily getting after here is if you think about the little message bank. So I think one interpretation of (j) is that the computer or the computer system or whatever you want to call it there is the bank itself. And Matt went out and bought the bank and he's the owner of it, and that's, of course, the argument that we can make.

I think the concern, though, is when you look to that analogy that Ms. Smith brought up in the legislative history that the TPM that's on that system is not protecting Mr. Stanislav's property; it's protecting the computer software.

And the question is: Who owns the software?

Now, we might make the argument that we own the software because we bought it. But I'm willing to bet that the company that sells that makes the argument that they just licensed the software and that we're not the owner of it and, in fact, that software is not a computer system at all and what we're engaged in is not the act of accessing a computer system but that we're engaged in the act of accessing a copyrighted work.

And so I think that's the ambiguity that has led in the past to the office granting some clarity on this by granting an exemption.

So I think we would fully agree with your interpretation if we're in court trying to defend this. And we would absolutely push for the broadest possible interpretation of (j). But when we're trying to advise folks, we have to acknowledge it's amenable to multiple interpretations. And that's why we are seeking some clarity.

MS. CHARLESWORTH: Yeah. Just for the record, I mean, in exploring the meaning of this, we have not come to any conclusions about the meaning of (j). And I think my colleague was asking --

MR. DAMLE: I was exploring potential readings.

MS. CHARLESWORTH: Potential reading.

MR. REID: I will do my best to unhear that.

MS. CHARLESWORTH: Your point is well taken, Professor Reid. You know, we'll think about that carefully.

But in exploring the meanings, we're trying to push counsel to kind of give us your explanation.

MR. REID: Right.

MS. CHARLESWORTH: So this transcript shall not constitute a record of how we're interpreting (j). We may get there someday. We hope -- we hope to, you know, provide some clarity, obviously. But for now, we're having a discussion.

MR. REID: Well, if there's one other thing I could put out there, I would direct you to think as you're thinking about this interpretation, for the standard in 1201(a) for granting an exemption, which is the likelihood of adverse effects.

And I think what you've heard today is that there are likely adverse effects because of the uncertainty around this. So I don't think you have to come to an ironclad conclusion about what Section 1201(j) says or doesn't say in order to grant this exemption. And I don't think the office has ever done that in the past.

So if your conclusion looking at this is that it's amenable to a couple of different readings but that security researchers are going to be chilled by the fact that it's not clear, then you need to grant the exemption. And that's what the office has done in the past, and we'd encourage you to do so again this time.

MS. CHARLESWORTH: Okay. Back to -- oh. Professor Bellovin.

MR. BELLOVIN: I was just going to follow up on what Professor Reid said and perhaps explain it in a slightly different way.

As I read Section (j), it is -- the scenario contemplated is "I'm an employee of, say, a bank. I want to protect my own computer system." Attacking some other bank, that may or may not be a violation of the Computer Fraud and Abuse Act. No one here on this side of the table is advocating doing that irresponsibly. That's not the issue.

But if it's my bank, if I find a flaw, yeah, I might be able to take protective measures or I might not, depending on what the situation is. Even the most sophisticated users would have a very hard time remediating a flaw in something like an iPhone, which is a very closed system.

But what we are talking about as security researchers is not the very narrow question of who owns a particular device but vulnerabilities not in the device but in the software -- which, as Professor Reid noted, we arguably do not even own, according to the license agreements we have to click through every time we open up a toy box or something -- and it's -- the issue is not so much the flaw in our particular copy but the flaw in the class of copies, of which there may be hundreds of millions out there, and which manufacturers often don't want -- they may or may not want to hear about it. They certainly don't want anybody else to hear about it.

And that is where the chilling effect is taking place, not by copy, where if the flaw is serious enough I will just not use it, but everybody else, the hundreds of millions of other instances of that software out there that are all owned by the manufacturer and licensed to consumers and companies that have to be protected. That is what we're trying to solve the problem of.

MS. CHARLESWORTH: Okay. Thank you, Professor.

Mr. Stallman, were you --

MR. STALLMAN: I just had one more point on 1201(j), and then I'll leave the rest for questioning.

But the other deficiency with it is references to violation of other applicable laws, specifically including 18 U.S.C. 1030.

In our reply comments, we included a statement on legal impediments to cybersecurity research that was signed by 35 noted security research experts. An additional 14, I think, have signed on to that comment now just because it was around and they were interested in it.

And so I would like to submit that for the record.

But the general point is that, because Section 1201(j) includes these other provisions like the CFAA, like the Wiretap Act, like the Stored Communications Act, which are themselves uncertain with respect to whether or not research violates those statutes, 1201(j) has the unfortunate effect of sort of compounding and amplifying the uncertainty and the legal risks that already exist in this law.

And I don't think it's a satisfying answer to say that, well, just because there's other, you know, legal murkiness around this issue we shouldn't address this one because I think this is -- this is one opportunity that the office can remove one of the -- the most significant impediments but also send a clear signal that this is -- this is an area that other -- that the Congress and other agencies should be looking at.

MS. CHARLESWORTH: Mr. Stallman, on the

updated exhibit, is that the exact same comment?

MR. STALLMAN: Yes, it is.

MS. CHARLESWORTH: It just has additional signatures?

MR. STALLMAN: Additional signatures, yes.

MS. CHARLESWORTH: So people previously have had an opportunity to --

MR. STALLMAN: Yes.

MS. CHARLESWORTH: -- see the comment?

MR. STALLMAN: Yes.

MS. CHARLESWORTH: Okay.

MR. STALLMAN: The text is entirely unchanged.

MS. CHARLESWORTH: All right. Well, we'll -- because it's the same text, we'll accept that as Exhibit 11.

MR. STALLMAN: Thank you.

MS. CHARLESWORTH: Has it been marked, Steve? Okay.

(Whereupon, Exhibit No. 11 was marked for identification.)

MS. CHARLESWORTH: So that will go into the record with the additional signers.

MR. STALLMAN: Thank you.

MS. CHARLESWORTH: Thank you.

Okay. This is -- this is a very long panel. I see Mr. -- don't get overly excited.

We were wondering if people might like truly a five -- when I say "five-minute," a five-minute break just to stretch their legs before we begin with the opposition.

And, you know, people are nodding yes. So it is -- what time do you -- my watch is -- 11:15. So if we can come back at 11:20, and we'll resume the discussion.

Thank you.

(Whereupon, a short recess was held.)

MS. CHARLESWORTH: Okay. We're back with class 25, software and security research. And I'm going to turn to -- now to Mr. Troncoso.

MR. TRONCOSO: Thank you. Proponents characterize class 25 as an exemption to enable good-faith security testing, and we totally support this goal. I also wanted to agree with something that Professor Green said in his opening statement, that we really are surrounded by the good guys and we have a big interest in working with the academic and independent research communities to advance security interests.

However, we also need to recognize the fact that any possible exemption that is granted in the course of this proceeding also has the potential to be exploited by the bad guys. And so I just wanted to frame my comments with that.

BSA members recognize that user trust is indispensable and that that trust must be earned. BSA members also recognize the importance of collaborating with the independent research community, and they do so every day.

BSA members are, however, extremely worried about one particular aspect of this class, the specific authorization for researchers to make disclosures about vulnerabilities based upon the researcher's sole judgment before the software developer has had an opportunity to remedy the problem.

It's a sad fact that bad actors are relentlessly searching for vulnerabilities that they can profit off of from the software that all of us rely on in our daily lives. We believe specifically authorizing zero-day disclosure practices through this rulemaking may well enable exploitation of vulnerabilities to engage in identify theft, financial fraud, and other serious threats to our nation's critical infrastructure.

The objective of this proceeding must be to promote security research in a manner that is -- that thwarts those malefactors without creating unintended consequences.

Both Congress and the administration are in the midst of vigorous debates on these very issues. Congress is currently considering legislation on information-sharing proposals aimed at creating incentives for parties to share threat and vulnerability data both with private parties and the government.

BSA strongly supports enactment of these bills.

At the center of the congressional debate is how best to create those incentives principally by limiting liability without unintended consequences. The Obama administration is also considering important policy initiatives on vulnerability information disclosures.

The Department of Commerce recently announced that it is considering implementing export controls on the tools used to hack systems to discover vulnerabilities. The Commerce concern is, again, about balance; how to responsibly disseminate tools while guarding against their falling into the hands of persons with bad intentions.

Nearly 20 years ago, Congress struggled with these same considerations when enacting the DMCA. Congress enacted exceptions to the circumvention prohibitions to promote security research but included careful checks and balances on the ability of people to make ill use of these exceptions.

Proponents of class 25 argue that ambiguity within these statutory exemptions are having chilling effects on the very type of research they were intended to promote. Were proponents merely seeking narrow classification to these provisions, we would not oppose their efforts.

However, proposed class 25 does much more than that. The reality is that proponents are seeking an exemption that is both broader than existing statutory exemptions but which contain none of the important safeguards that Congress deemed important.

Consistent with congressional intent, as reflected in the DMCA's current statutory exceptions, we believe that class 25 should be amended to permit circumvention only when the software has been lawfully obtained, the researcher has made a good-faith effort to obtain authorization from the owner of the system or network, circumvention is carried out solely for the purpose of good-faith testing, and the information derived from the testing is used primarily to promote the security of the software and maintained in a manner that does not facilitate copyright infringement or any other violation of applicable law, including the CFAA.

Most importantly, the disclosure of vulnerability information must be done judiciously consistent with the facts of the specific situation in ways that avoid unintended consequences.

We believe that judicious disclosure requires vulnerability information to be first shared with the entity best placed to fix it, namely the developer, and with enough time to cure the problem before it is disclosed more broadly.

The concurrent disclosure standard proponents advocate would exacerbate the risk to the public by affording bad actors a window of opportunity to exploit vulnerabilities before they've been patched.

This isn't a speculative concern. Unfortunately, there is already a thriving market for black market -- in the black market for security research regarding zero-day vulnerabilities.

Should you determine that a broad security exemption is warranted, we urge that you tailor the class in a manner that is consistent with congressional intent and that you are mindful of the broader national cybersecurity policy debate that is now under way in Congress and within the administration.

Most importantly, the goal must be to help good-faith researchers here today and not inadvertently to help bad actors.

Happy to answer any questions that you have.

MS. CHARLESWORTH: So on -- on the disclosure, we've heard a lot about that. I mean, what -- if we were to -- you know, the congressional standard, as you know -- or the standard that's in 1201(j) is that -- the complaint is that it's too opened-ended.

MR. TRONCOSO: Mm-hmm.

MS. CHARLESWORTH: You know, you're looking back. I mean, do you have any specific proposals in terms of how to address -- when you say, you know, "notify the manufacturer first," is there a time constraint before you can disseminate? Or how would you -- if you -- if you were going to address this in an exemption, how exactly would you do that?

MR. TRONCOSO: Mm-hmm. Well, I mean, I think, as a preliminary matter, you would first need to make the determination that there has been a substantive chilling effect on these research activities. And there's a lot of research going on.

Obviously, I take everyone at their word. I think that, on the edges, there certainly is some chilling. But I think if you look at the market right now, BSA-member companies have a big interest in partnering with the independent research community. And many of them are actively trying to incentivize that by offering rewards, either financial or reputational, to those who provide information about security vulnerabilities but do so in a responsible manner.

And typically, that just means providing the vendor with enough time to issue a patch before the security researcher makes that -- makes a public disclosure about the specifics of that vulnerability.

MS. CHARLESWORTH: And how much time is that?

MR. TRONCOSO: You know, there is not really a set time. And I'm sorry I can't give you an easy answer on that.

The reality is that every vulnerability is different, and the fix to every vulnerability may take a different amount of time.

You know, particularly with enterprise software, when our member companies are evaluating patches to vulnerabilities that have been identified, they need to spend a lot of time with that patch to ensure that it's not going to create some other type of vulnerability down the line. And because enterprises are so complex and system upon system upon system, that can just take a lot of time.

Some patches are easy to -- easy to get out, but others aren't. So I think that we'd be probably uncomfortable with a fixed deadline for, you know, disclosure for those reasons.

MS. CHARLESWORTH: Do your companies -- I mean, you sort of spoke about this a little bit. But, I mean, how -- how many of your members -- or what percentage of them actually authorize security research? Do you know?

MR. TRONCOSO: I don't know the exact number. I know that the trend is for software companies to do that, but I don't know how many do in a sort of official capacity. Some of them probably also work sort of more behind the scenes.

But there's certainly many of them that have, you know, very visible programs that are advertised on their websites about that.

MS. CHARLESWORTH: Okay.

MS. SMITH: Do your members have any specific concern about the dissemination or discovery of trade secrets in security research that's unauthorized?

MR. TRONCOSO: I think, absolutely, that would be a concern of our member companies.

MS. SMITH: Okay. I mean, have you seen any specifically? Because I think you said you would be okay with the exemption if it was narrowed from the proposal?

MR. TRONCOSO: Mm-hmm.

MS. SMITH: But I'm wondering if -- you know, how could we address this concern or how realistic, you know, or palpable is this concern?

MR. TRONCOSO: I mean, I think that you would want to build in sort of the standard that I had referred to earlier, that it couldn't involve any other violation of applicable law. And so that would apply to sort of disclosure of trade secrets as well.

MS. SMITH: Okay. So that would satisfy the concern?

MR. TRONCOSO: That particular concern.

MS. CHARLESWORTH: Okay. Mr. Lightsey?

MR. LIGHTSEY: Yes. Thank you. Good morning.

I'll just begin by noting that my comments are directed solely with regard to any impact that the proposed class might have on the automobile industry. I don't purport to address anything beyond the impact on automobiles.

So today GM vehicles include, on average, 30 purpose-built electronic-control units, or ECUs, that control functions in the automobile ranging from the radio to vital engine and safety functions.

These ECUs control functions like engine controls, braking, speed, steering, air bags, and other very important features for the safety of the occupants in the vehicle.

These ECUs -- the software in these ECUs is protected by technological protection measures, or TPMs, that, if circumvented, could present real and present concerns for the safety of the occupants of the vehicle as well as the compliance of the vehicle with regulatory and environmental requirements.

So TPMs play a vital role in the overall security and safety design of the vehicle.

Now, with regard to the chilling effect, particularly in the automobile industry, the proponents have not presented any evidence that there has been any chilling effect whatsoever. In fact, to the contrary.

And that's because the automobile industry is -- has every incentive to encourage responsible security research and does so. We have, as we said in the class 22 proceeding, relationships with various independent security researchers, academics institutions. We participate in various industry forum, including SAE and others. We attend meetings of the security research industry, such as the Black Hat conference and the DEF CON conference. We do -- we do every -- we engage in various efforts with DARPA.

And so we certainly do our part to encourage responsible security research into the software in our systems.

And our concern is that, if the broad exemption, as proposed, is granted, that the ability for automobile manufacturers to control that research and to have the opportunity to fix vulnerabilities before they're widely disclosed would be severely limited and could thus create safety concerns.

Thank you very much.

MS. CHARLESWORTH: Thank you.

Mr. Troncoso, I had a question that I neglected to ask you earlier.

In some of your papers, in your filing or the filing, I think, of BSA, it mentioned that the research should be limited to vulnerabilities caused by access controls.

Do you -- can you comment on that? And

is that -- I didn't hear you say that just now.

MR. TRONCOSO: Yeah. I think that when -- we were talking about the fact -- those are the only extensions, as far as I know, that the Copyright Office has granted in the past, that they were sort of narrowing tailored to specific types of access controls that were creating security vulnerabilities.

But the class that we're looking at here is extraordinarily broad and would apply to virtually any type of software.

So, you know, I would need to go -- I don't have the filing in front of me. But I --

MS. CHARLESWORTH: But is it your position that -- I mean, at least in one of the -- one part of your papers, I think I saw that you were okay with a narrow exemption in this area, but it should be limited to vulnerabilities caused by access controls.

Am I -- is that an incorrect understanding of your position?

MR. TRONCOSO: No. We would certainly be comfortable with a narrow exemption like that.

MS. CHARLESWORTH: Right. But are you saying you -- there's no version of an exemption that could be broader than that that you'd be comfortable with?

Because that's a fairly -- that's a fairly significant limitation.

MR. TRONCOSO: Okay. Fair enough.

I think that our overriding concern is about the disclosure issue, and that's certainly what is motivating our participation in this proceeding.

And to the extent that that can be addressed and that congressional sort of intent underlying the existing statutory exemptions can be integrated, we would be comfortable with an exemption.

MS. CHARLESWORTH: An exemption that was broader than just vulnerabilities that are specific to the access controls themselves?

MR. TRONCOSO: That's correct.

MS. CHARLESWORTH: Okay. Thank you for that clarification.

Okay. Going back to the disclosure issue -- well, I think there are a few issues that we've identified. One is this sort of issue of the specter of, you know, are you looking at a consumer good -- like the piggy mailbox this morning were you can kind of take it and look at and it work with it in a way that's probably not that risky, hopefully, to anyone else?

You know, or are you talking about nuclear power plants, I mean, that specter where you'd be hacking into, like -- or a plane's operating system as the plane is operating?

And I'd really be curious to know from the researchers, I mean, how to think about that issue and address it in practical terms.

I mean, I don't think there's a huge record here of needing to, you know, look at live nuclear power plants and things. But, I mean, I don't want to -- obviously, that's also a security concern, and I don't want to say it's not.

But, I mean, how should the office be thinking about this question and the concern that, say, publishing research about how to break into a system where the breach of -- where the breach could be catastrophic, let's say, or very serious for the public?

I mean, how should we think about that?

Is that -- Dr. Green? Did you want to comment on that?

MR. GREEN: Sure. So I think there are two issues here.

One is: Should you be performing security testing or research on live, active systems?

That's obviously something that can be very dangerous, and you should use extreme restraint with that.

However, there are other laws that directly apply to that. For example, the CFAA is a law that is, as far as I can see, specifically designed to deal with a case of people accessing online systems in unauthorized ways. So I have never viewed the DMCA as being something that specifically applies to that case. Of course, I'm not a lawyer. That's just my interpretation as a researcher.

Now, having said that, there are -- certainly, there are things that -- I mean, the question then is: Is it something that you should be allowed to do? Is it something that we should be -- should we be using Section 1201 as a way to prevent people from doing research on these types of systems? Does that benefit us as a society?

I think the answer is that clearly it

does not benefit us because, you know, we have access to a -- we know that there are a number of systems, such as control systems, that, whether you're accessing them in real time or whether you're accessing separate copies, the results of the experimentation can lead to vulnerabilities that cause major safety issues in things like nuclear power plants.

So the value of performing that research and, you know, properly disclosing and getting those vulnerabilities fixed is very, very high.

MS. CHARLESWORTH: I mean, I can agree with you there. But, I mean, I saw a news report recently about someone who allegedly -- I hear laughter -- hacked into -- but it's not funny to me since I spend a lot of time on airplanes -- hacked into a live, operating airplane system.

And now they may be doing it for a good -- for what they perceive to be good purposes. But, you know, aside from the fact that, you know -- well, I mean, a security researcher is also not a perfect person. As smart as you all are, I mean, you could also make a mistake when you take over the airplane to operate -- I mean, this is getting -- it sounds a little absurd, but if I believe the report, someone did that.

And, yes, on the one hand, exposed a flaw. But on the other hand, if I were riding on that plane, I would -- would not -- I mean, I would be uncomfortable knowing that it was being piloted by someone who, you know, may know less about piloting an airplane than the pilot.

So anyway, I'm just wondering -- I mean, are you saying -- would you be willing to limit this so that -- at least for purposes of 1201 where we're talking about not live systems and maybe that question should be debated in Congress in terms of how to perform security research on nuclear power plants and things of that nature?

MR. GREEN: So I'm going to leave the legal aspects of that response to my colleague here. But I am going to say just -- I think I speak for all of the security researchers here when I say that that story is not something that we endorse.

MS. CHARLESWORTH: Thank you. That's good to know.

MR. GREEN: No ethical researcher should be working on live systems like that, and we -- if it happened, we're very unhappy about it.

MS. CHARLESWORTH: Okay. Thank you for that.

MR. REID: And I just wanted to chime in too and say, in addition to distinguishing that particular story, I think the vast majority of the research that we're talking about here and, indeed, I think all of the research that we care about is responsible work that's aimed at fixing problems like these in a safe way.

And so I think the anecdote of that story shouldn't -- I hope won't color the office's judgment too much on this.

The other thing I would throw out here is --

MS. CHARLESWORTH: Well, wait a second. But you're just -- I mean, that's just circular. It's saying, "Well, we want an exemption that allows ethical stuff, and we don't think that's ethical." But, you know -- but, I mean, I said this in L.A. in a different context. I mean, we're trying to -- part of our job here is, if we -- if we do go forward and grant some sort of exemption, there needs to be enough information and enough sort of -- a little bit of line-drawing in there so that you're notifying the public of what they can and can't do.

MR. REID: Sure.

MS. CHARLESWORTH: And also, I think, assuaging fears to some extent of people who might be worried that it would be used in ways that were, say, dangerous. I mean, I -- you know, so I -- saying -- you know, often we get that response. It's just we're saying it should be lawful. We're saying it should be ethical.

But at the same time, we're looking at the record here and we're trying to consider some potential limitations or narrowing so that people feel that the exemption would be one that's consistent with congressional intent and the goals of the proceeding.

So if you could maybe speak a little bit more -- I mean, so I'm -- basically, it's like, "Are we willing to get rid of -- to exclude live systems from this exemption?"

I don't think there's much of a record -- I will say that -- and to support the idea that you would need that and, you know -- I'd be interested to know whether that's something that the researchers could concede may not be necessary at least at this moment in time for this exemption that's sought.

MR. REID: I mean, I guess the -- the other thing that I'd urge you to consider is that however this gets treated in this proceeding, whether you choose to include live systems or not to include live systems, as Professor Green mentioned, there are a number of other laws that deal with this sort of thing. And I think a lot of the collateral concerns that folks have raised -- you know, tampering with vehicles, tampering with medical devices, tampering with live airplanes -- are illegal under a whole bunch of laws.

And I think the question you ought to be asking yourselves is: Are we -- is the DMCA the last line of defense to protect airplanes? Are we relying on copyright law to protect the security of airplanes?

MS. CHARLESWORTH: Apparently so, according to some.

MR. REID: Because I think, as a matter of policy, A, we're not. And, B, if we were, that would be -- that would be deeply troublesome. And, C, we're getting so far away from the reason the DMCA was enacted, which is to protect the commercial exploitation of copyrighted works from copyright infringement.

There's nothing that I could tell in the report about the airline incident that indicated anything about copyrighted software. There's nothing about a technological protection measure. There's nothing about circumvention. And in the affidavit from the FBI, there's no citation to the DMCA or any provision of the Copyright Act. There's a citation to Section 1030.

So I think, to the extent that there are concerns about this, there are a number of other both legal and policy venues in which they can be addressed. And I don't think the office needs to be worried about enabling behavior that's illegal under other -- under other laws because there's still -- the behavior is still going to be illegal under those other laws.

And I think what we're trying to get at here is there are complicated contours to this discussion, and there are discussions that should happen in other venues. Obviously, folks have raised concerns about the EPA and the FDA and that sort of thing. And I think we're in support of having those discussions at those venues and in the context of those laws and policies.

But I think what we're trying to press for here is that copyright law is not the place to do it and that you don't need to and that the DMCA and Section 1201 don't require you to.

MS. CHARLESWORTH: Okay. Thank you.

Professor Bellovin?

MR. BELLOVIN: I want to thank you for focusing on copyright laws, about half of what I was going to say. I would -- the only thing I would add in that vein is we are here precisely because we want to make certain that we're in compliance with the law. We are very much concerned with avoiding breaking laws. It's exactly why we want this exemption. We don't want to violate the copyright law. We don't want to violate the CFAA. We don't want to violate the airplane hijacking laws.

As a -- you know -- but just returning to the purely technical issue of copyright infringement. It is almost never a concern -- in fact, I'm hard-pressed to think of any example where copyright infringement becomes a concern unless you have a copy of the system.

If this guy who allegedly tried to hack

into an airplane in flight -- thank God. I fly a lot. I don't like hearing this either.

In order to be able copy, say, Boeing's software -- which would be copyright infringement -- he first had to hack into something. As a pragmatic matter, if I am testing a system for security flaws in a way that could possibly involve copying, I have to have the physical thing in my possession because that's where the code is. That's where the copyrighted material is.

You know, this is not a CFAA exemption request. That may be a good thing. I have opinions on that, but I'm not going to go into it.

But as a pragmatic matter, infringing copyright, circumventing a protection on copyright, circumventing a technological measure that's protecting copyright pretty much requires that it be your device because that's how you have access to the code or the circuit boards or whatever that is the actual copyrighted material.

And it --

MS. CHARLESWORTH: Well -- I'm sorry. You're so much more skilled in this area than I am. But couldn't you hack into someone's system through the Internet?

MR. BELLOVIN: But then you have to hack in first. You have to first violate the CFAA to get at the system before you can get at the copyrighted material. The larger violation there is the hacking.

And I think a more probable case, certainly one we have seen, is not involving the DMCA, but I'm going to hack into a company in order to steal their source code, their trade secrets, what have you. And this is not protected by the sort of technological measures that the DMCA bars circumvention of. This is protected by ordinary computer security controls and enterprise security controls and firewalls to keep bad guys out of my system.

It's not -- you know, the DMCA was intended to protect devices that contained code or books or what have you that has been legitimately purchased that you're trying to prevent extraction of, reproduction of in violation of the Copyright Act. It's not intended to be a CFAA supplement.

And, again, as a technical matter, that's rarely the way. You have to go break something else if it's somebody else's system, violate the CFAA before you can get to the copyrighted code. And that's rarely the way that copyrighted or otherwise protected material is stolen because of a hack.

MS. CHARLESWORTH: Okay. Thank you.

Professor Matwyshyn?

MS. MATWYSHYN: Just very briefly, the exact facts of the incident that you're referencing are still somewhat in dispute. And so time will give us a better sense of exactly what happened.

But at present, I think the lack of support for such conduct that you're seeing from the researchers representative, large portions of the security community are absolutely not rallying around the conduct of this individual.

MS. CHARLESWORTH: Well, I would hope not.

MS. MATWYSHYN: They are not. I give you my assurance. This is a deeply troubling turn of events.

So the norms of the security research community are not in line with this type of conduct.

MS. CHARLESWORTH: Yeah.

MS. MATWYSHYN: And in that type of a

situation, the homicide laws are the first line of defense. And that is the severity of the problem.

And so the -- whether a TPM was circumvented in the process of killing hundreds of innocent people, we hopefully will never need to inquire on that scale.

MS. CHARLESWORTH: Okay. Yes. I mean, I appreciate all the comments about, you know, the relationship between copyright law or the lack thereof and what we're talking about.

But because of the way the law is written, these are -- I said this in L.A. too -- these are the issues that have come to the table, and so we have to consider them.

And, Professor Blaze, your turn.

MR. BLAZE: So first of all, I mean, let me add my voice to the chorus that condemns tampering with live safety, critical systems. I think nobody -- nobody advocates that here. And I -- certainly not I.

And as a frequent flyer, I was as horrified as anyone at the possibility of this sort of tampering, although all the facts are quite murky at this point.

I wanted to return to the other issue

that you had asked us to talk about, which was disclosure.

You know, I want to not give short shrift to the -- the purpose of disclosure is not -- is partly to help have these security vulnerabilities that might be discovered repaired. But there's a second and, I think, equally important purpose, which is warning consumers against defective products.

For example, in the -- I'm not quite sure what it's called -- this odd little mailbox pig.

MS. CHARLESWORTH: Exhibit 10, I think.

MR. BLAZE: Yeah. The mailbox voicemail pig.

You know, certainly, if I were a parent with one of these devices, I think, you know, even before it's fixed, if this had vulnerabilities that could expose my child to danger, I would want to know about that and remove it. And disclosure to the public is really the only way to achieve that even if it's at the expense of some embarrassment to the vendor.

So I want to make sure that we give adequate consideration to the benefit of the security research and scientific process, not merely considering the stakeholder as being the developer of the software but also the users of the technology more broadly.

MS. CHARLESWORTH: Thank you.

Mr. Lightsey?

MR. LIGHTSEY: Yes. I'd just like to say, once again, with regard to the automobile industry, there's been absolutely no evidence of any chilling effect on security research.

And given the dramatic consequences that we're concerned about here in terms of people's safety and lives, we feel very strongly that the proponents have not met any burden that they might have of showing a need for an exemption here.

And by simply saying, "Well, there are other laws and regulations and regulatory bodies out there that address these concerns," it is not sufficient in this context as well.

We feel that the DMCA is a relevant protection, and we encourage the ability to engage with the security -- responsible security researchers and to have the opportunity to fix the vulnerabilities that they can find.

Thank you.

MS. CHARLESWORTH: Thank you, Mr. Lightsey.

Mr. Troncoso?

MR. TRONCOSO: Returning back to everyone's favorite pink little pig example, I just wanted to point out -- thank you -- Mr. Stanislav, when he explained sort of what happened to him as he was researching that vulnerability, if I recall correctly, he explained that he reached out first to the manufacturer and, you know, notwithstanding the bluster that sort of he may have received at first, ultimately he was able to work with the manufacturer to ensure that that vulnerability was fixed. And he didn't -- and Mr. Stanislav did not disclose the information about that vulnerability until after it was fixed.

And I think that that sort of gets to the -- to the norm that we're seeing even amongst the researchers in this room that, you know, it is consistent with what software companies' interests are, which is protecting consumers from these vulnerabilities.

And I'll also point out that, in Professor Green's filing -- his initial filing -- and his sort of research addendum at the end of his filing, he indicates that he always provides disclosure to software companies before disclosing vulnerabilities to the public. And that really is a key issue for us and one that is critical to safety of the public.

Thanks.

MS. CHARLESWORTH: Thank you.

Professor Green, do you want to respond to that and whatever else you had to say?

MR. GREEN: Sure. I'd like to say that I always attempt to provide disclosure to software companies. In some cases, it's not possible. And I gave an example of a vulnerability where there were thousands of websites and we simply couldn't notify everybody.

The other issue I'd like to bring up with disclosure is that sometimes you notify -- you disclose somebody -- a software company of an issue, and they are not able to properly remediate it, tell you that there's no fix, or they tell you that the fix that they can provide will take a year.

At that point, you have the obligation as a researcher to look at the end users, the consumers affected. And that has to affect your calculation quite a bit.

For example, Android telephone -- this is one. But Android telephones are rarely updated by carriers. So if you notify Google of a vulnerability, they will make a patch. But the probability that it actually gets out to consumers is very low -- to most consumers. Ninety percent of consumers can be vulnerable a year later.

So you have to make a lot of calculation about how you disclose things based on what's right for consumers and not what's right for software companies.

MS. CHARLESWORTH: Okay. I think it was Professor -- oh, I'm sorry. Mr. -- yeah. I couldn't -- sideways to me.

MR. STANISLAV: The pig keeps getting in my way.

So to your point, sir, the three minutes I had to explain my situation for multiple things was -- I was a little short.

In the case of this specific device -- and also this device as well -- in order to disclose these issues --

MS. CHARLESWORTH: And that's -- sorry. For the record, we're talking -- are those both now in Exhibit 10, the devices?

Oh, okay. All right. Exhibit 12? Yes.

MR. STANISLAV: With both items in Exhibit 12 then. Both of these were reported through the help desk system of that -- of the organizations because there was no front door for me to access. I had to go through multiple days just to convince the help desk employees that these were issues I needed help with and to triage them up the chain to someone who could address them directly.

I actually had a help desk ticket closed on me for this specific camera device and had to reopen a new help desk ticket just to continue dialogue.

Specifically, however, with this device, the only reason that these issues finally got solved after about a -- offhand, about a month and a half -- was because my company at the time was going to disclose the vulnerability through public channels because there were no -- there was no progress on getting these issues solved.

At that point, a reporter reached out to the vendor. The vendor said they had never heard from a researcher about any issues. And then I received a reply from the CEO of this company that same day on the e-mail thread I had been having with her addressing, "Oh, maybe we should have a phone call to discuss this issue if you are still pursuing it."

MS. CHARLESWORTH: And that's the pig device?

MR. STANISLAV: Yes.

MS. CHARLESWORTH: Okay.

MR. STANISLAV: So I certainly -- there are many great vendors out there. The BSA represents many of the vendors that do work really well with security researchers. Microsoft being one of them, for sure.

However, these companies represent the companies that most of the products you are buying are from. They are not from the tier-one providers.

The Internet of things is generated from innovators, from entrepreneurs, from people on crowdfunding sites like Kickstarter. These people do not have large legal teams that understand complex legal situations. They will fight back with whatever means they have to shut you up to not make them look bad.

MS. CHARLESWORTH: Okay. Now Professor Matwyshyn and Professor Bellovin.

MS. MATWYSHYN: Just a brief comment on the point of the cars that was raised.

So, indeed, car companies such as Tesla are implementing the state-of-the-art security processes in place. However, there's unfortunately a large degree of variation in security processes across car manufacturers.

And because, for example, some car manufacturers have not yet fully staffed out their security teams and have a large number of job openings for security personnel, for example, on their websites, it would certainly be beneficial for them to engage with the security community more aggressively.

And Tesla, for example, is on the face of things, ISO-compliant. They have not opposed our approach. And, in fact, they are bringing a car to DEF CON, one of the major computer security conferences, and asking participants to engage with the car and to find flaws in the car. That is the best practice for security in the auto industry.

And if every car company was on the

level of Tesla, we would not be concerned about that industry in particular. And the security researchers are very concerned about that industry in particular.

MS. CHARLESWORTH: Professor Bellovin?

MR. BELLOVIN: One of the issues with notification -- and I certainly am in favor of notification. I have done it myself in the times I have found vulnerabilities -- is whether or not the vendor would have the legal right to block or delay publication. This actually interacts in a bad way with university policies.

I may not accept a grant, for example -- this is university policy, not personal policy. I may not accept a grant that gives the funding agency or some outside party the right to block publication. The university sees this as a very fundamental matter of academic freedom that nobody else do it. And it's university policy.

And it's actually mirrored in an odd place in the law having to do with the export laws on technology. What is export? There's something called "deemed export." You cannot teach foreign nationals certain things under certain conditions. That's in technologies, including perhaps encryption.

But one of the things that it says in the law last time I looked -- and this was about eight years ago -- was that fundamental research is okay, but -- and what defines fundamental research? One of the criteria is: Can somebody else block publication?

If someone else can block publication, than it is not considered fundamental and the export control rules can't apply, which causes other very serious chilling effects for academics, including criminal sanctions for violating these export control laws, which are a very major concern in the country today. Mostly not on this grey area, but it is, indeed, a concern.

So the university is very careful to avoid anything that lets somebody else block publication. I cannot do grant-funded research that, with a contract, gives somebody else the right, precisely to preserve academic freedom and also to protect me and my students under the export laws.

MS. CHARLESWORTH: Professor Blaze?

MR. BLAZE: I'm sorry. I'm losing my voice a little bit.

The -- I wanted to give an example along the lines that Professor Bellovin was discussing.

In 2007, when I did research into vulnerabilities in electronic voting systems -- which were the systems used to conduct national elections throughout our country and were clearly a very critical thing -- we very specifically, -- we, first of all, found sweeping vulnerabilities across every system that was tested that could be exploited to affect the outcome of an election by somebody who had fairly limited access.

MS. CHARLESWORTH: Sorry. That was authorized research, right?

MR. BLAZE: It was not authorized by the vendors, but it was authorized by the -- by customers, the state governments that had approved them. The voting machine vendors were not -- didn't -- didn't contract with us to do this but rather the users of the voting machines contracted with us.

MS. CHARLESWORTH: And did the vendors ever pursue you at all over that?

MR. BLAZE: Well, we had a certain shield over us. We were indemnified under state law, and there was some contractual back-and-forth with the voting machine vendors that I wasn't myself privy to that allowed the state governments to indemnify us.

So it falls into a bit of a grey area there.

But we -- one of the issues we addressed was the question of whether we would give the voting machine vendors advance notice to allow them to fix it. And we, in this particular example -- although we normally do try to give -- in my community, ordinarily will try to give notice to the -- to the vendors.

In this case, we felt that allowing the end users to remediate immediately through procedural changes that we would -- that we recommended outweighed the benefits of not notifying the users and allowing the vendors more time to repair things that would actually take them longer than the next election to fix.

MS. CHARLESWORTH: So let me just -- I just want to understand.

So did you notify the state authorities so they could --

MR. BLAZE: So the state authorities --

MS. CHARLESWORTH: -- do a workaround?

MR. BLAZE: So the reports were published. The state authorities were notified, and the vendors were notified all simultaneously.

MS. CHARLESWORTH: Right. But the vendors knew you were doing the research generally?

MR. BLAZE: The vendors were aware that we were doing the research but didn't see our results until they were made public.

MS. CHARLESWORTH: Okay.

Ms. Moy?

MS. MOY: Yes. Thanks.

I just wanted to chime in quickly and just emphasize again the importance of disclosing not only so that the vulnerability can be remedied but so that consumers who are in the market for a product of the nature of the product that has a vulnerability can make an informed decision about which product is best for them.

If a -- if a vendor can stall publication of the vulnerability for six months or a year while it addresses that vulnerability but continue to market the product in the meantime without patching that vulnerability, I think that

that's an enormous problem and one that -- and one that has major implications for consumers who are in the market who deserve to know about that.

MS. CHARLESWORTH: Can I ask you a question?

MS. MOY: Mm-hmm.

MS. CHARLESWORTH: Could some of that -- the need for consumers to know be addressed by sort of a high-level communication that this has a security problem without getting into the details of how you would, you know, hack the system to do something bad with it?

MS. MOY: I'm sure that that would probably address the problem for some consumers. I would say not all.

I mean, there are certainly going to be cases where the nature of the vulnerability is an important consideration. I mean, it would be difficult to know without looking at it on a case-by-case basis. But just talking about, you know, the -- for example, the BMW vulnerability that was -- that was publicized in January of this year that was a vulnerability with the remote unlocking -- with the remote unlocking function.

I think that there are details there

that might be important to certain consumers. Some of the public reports that I read said that it couldn't be used -- that vulnerability couldn't be exploited to unlock other people's cars; it could only be exploited to unlock your own. I don't know if that's true. I don't know if that's the case.

But, you know, I'm sure that there are consumers who would read reports like that and make a decision for themself about whether or not they're willing to take on the risk of purchasing a product with that known vulnerability addressed.

MS. CHARLESWORTH: But the report -- I mean, in that, you're saying there's some detail, there's some information --

MS. MOY: Mm-hmm.

MS. CHARLESWORTH: -- about what it is. Obviously it isn't step-by-step instructions on how to hack the BMW system; is that correct?

In other words, why would your -- why would an ordinary consumer need to know that?

MS. MOY: Well, I mean, ordinary consumers include people who have -- who have an understanding of how the technology works. Right?

I mean, we -- yeah, many consumers --

for example, myself, I would not be able to know even by reading a technical explaining of how -- of how the vulnerability can be exploited, I wouldn't be able to do it.

But someone like Professor Green or Professor Bellovin would understand, and that information might be important to them and to others that -- you know, to others like them, also to others who might read materials that they would write on the subject.

MS. CHARLESWORTH: But what I'm trying to get at is, as Mr. Troncoso's concern, right, that by publishing the detail of how to exploit a vulnerability, you are enabling that -- the claim is you're enabling a certain group of people who might not otherwise have known about it or done that to do it -- bad guys. Not really sophisticated ones who are out there all the time but the kind of -- you know, and that -- but to know -- to warn consumers, you don't need -- I mean, I would think in the ordinary case, you could concede that a consumer, you know, who says, "Oh, my gosh. There is a problem with the BMW," then is on notice and can take additional steps, if they want, to find out more about it or -- you know, or at least talk to BMW about it.

But in the ordinary course, why would you need to have step-by-step instructions on how to exploit the vulnerability? And why would that even be a good thing?

MS. MOY: Well, part of what I'm saying also, though, is that the -- the detailed description of what the vulnerability is would be important to provide information to those who can translate what the -- the nature of the vulnerability and the severity of the risk to everyday consumers as well.

MS. CHARLESWORTH: But -- I mean, you're -- I'm really struggling with this.

MS. MOY: Mm-hmm.

MS. CHARLESWORTH: If I were buying a car -- I'm like you. I'm not someone who's that sophisticated -- and someone said this -- let's take the pig example -- "This pig allows people to intercept communications with your child," and then I can decide whether I want to take it back to Toys"R"Us and demand a refund. I can decide -- I mean, why do I need to know this specific as your typical consumer -- typical consumer, why do I need to know the specific reason or way that you exploit that system? I mean, why -- why does that need to --

MS. MOY: But let me respond -- to that with another question and say: How is it that you know at that high level who's going to translate the -- who's going to translate the nature of the vulnerability for the -- for the consumer?

MS. CHARLESWORTH: Okay. Mr. Stanislav is going to write an article, and he's going to say, you know, "I tried to" -- you know, I don't know the -- all the -- you've mentioned the scenario.

But I mean, the company, let's say, refuses to fix it. And for whatever reasons, he decides to publish an article or to alert news outlets and says, "This toy has a big problem. It allows people potentially to hack in and intercept communications with your child, and you should get the word out there because people should be informed consumers and should know that if they're buying this toy."

That's how I would know. I wouldn't need to know the specific line-by-line instructions on how to hack into the system or the toy in order to make a decision whether I wanted my child to continue to have that toy.

MS. MOY: So isn't --

MS. CHARLESWORTH: And I --

MS. MOY: Sorry.

MS. CHARLESWORTH: I mean, can you -- can you concede that?

MS. MOY: I mean, I --

MS. CHARLESWORTH: Why is that so hard to concede?

MS. MOY: It's -- well, the -- I -- as I said, I think that that would -- that would satisfy it for a lot of consumers. I think that there are still some for whom that would not be sufficient information.

I also --

MS. CHARLESWORTH: Why?

MS. MOY: -- am having a --

MS. CHARLESWORTH: Why?

MS. MOY: -- hard time envisioning -- sorry. I'm just -- I'm also having --

MR. STANISLAV: I can address that if you want. I have an answer for that.

MS. CHARLESWORTH: Okay. Well, I want

to -- I want to have Ms. Moy explain why, and then -- and then you can address that.

MS. MOY: Well, the problem is that I am not a consumer like Mr. Stanislav. Right? I mean, the -- I can tell you that that would be sufficient for me, but I can tell you that I think that it would be insufficient for other consumers who are at a different level of sophistication than I am.

In addition, I'm having a difficult time from a legal perspective envisioning what -- how you would cabin an exemption in such a way that there were disclosure allowed but not with the particular level of technical detail that would facilitate replication of the vulnerability and -- I mean, which I think is another -- that is -- that is also at the heart of the problem here. Right? I mean, what we're describing is maybe a legal distinction that I think would be very difficult to put into an actual exemption.

MS. CHARLESWORTH: Well, I mean, I think Congress was driving at this a little bit in (j). And it says it's solely to promote the security of the owner or operator of the computer or computer system or computer network and shared directly -- I mean, in other words, I think part of the policy that I'm seeing in there was the idea that you weren't necessarily advising the world how to do this, but it was -- you were doing the research in a way that didn't enable malicious actors.

I mean, I -- you know, it's not stated expressly, but that's -- again, that's what

Congress -- Congress here looked at -- we're all -- we're hearing the same thing: This is complicated. There's a lot of -- Congress kind of put this test in here and one of the factors, I think, is sort of looking at whether you use the research responsibly and whether it was disclosed responsibly and so forth.

So I think you can -- you could -- I could write a law that did that. I could

MS. MOY: Yeah. I mean, I also --

MS. CHARLESWORTH: -- but --

MS. MOY: I also -- as a consumer, I would want to -- I would also want to read others' analysis of how bad the vulnerability is and also -- not only how bad is the vulnerability -- is the specific vulnerability but what are the implications for the way that this company approaches security. Right?

I mean, is it a vulnerability that a company -- even a company implementing reasonable security practices could have built into a system and -- or is it something that represents a major oversight? And I -- I would want to know the -- I would want to see the analysis of parties that I trust who are capable of translating the technical details into a -- into a report, perhaps a journalistic report or an academic report, that I can read as a consumer and determine for myself whether or not I'm willing to take on that risk and whether or not I'm willing to trust the company to address security concerns sufficiently in the future.

MS. CHARLESWORTH: I mean, do you think a high-level disclosure is better than no disclosure? In other words, a high-level one that didn't have the specific instructions in terms of how to exploit the vulnerability versus no disclosure?

MS. MOY: I mean, if those are the options that consumers are given, then yes. I think more information for consumers in the marketplace is generally a good thing.

But, again, I don't think that that would -- I don't think that that would get to all of the reasons that we want to see disclosure of vulnerabilities.

MS. CHARLESWORTH: Okay. Thank you, Ms. Moy.

I think, Mr. Stanislav, you had a specific response.

Then we'll -- then we'll circle around the room again.

MR. STANISLAV: Yeah, very briefly.

So two things. One being: I pulled up an article at the time of the research in Exhibit 12 of the web camera. The CTO at the time was quoted as saying that my research was inaccurate and misleading -- and had misleading information. I've since presented the research on this publicly at many security conferences and also software engineering conferences. I have the proof to back it up.

And so when a story like this comes out and the vendor says that I am lying, I have the proof to show consumers what their actual risks are.

The second part of that is prevention. Whether it's a firewall manufacturer, a router manufacturer, an anti-virus company, if they do not know the specific details of the vulnerability, they cannot protect the consumer in the meantime until the vendor gets a release patch out, whether it's five days or five years or never.

MS. CHARLESWORTH: Okay. Thank you, Mr. Stanislav.

MR. STANISLAV: Thank you.

MS. CHARLESWORTH: Mr. Sayler?

MR. SAYLER: So just building on this a little bit. I mean, if we go back to the example of the blog post Mr. Stanislav writes with the high-level disclosure, you know, targeted at consumers, I mean, I would argue that the technical disclosure is hugely important.

And it's not necessarily for the individual consumers; it's for people like me that are now going to go read that blog post and go, "Well, this toy is maybe not unique. It's using a microchip that other people have probably bought, and this issue may exist in a wide range of toys. I'm going to go out to Toys"R"Us. I'm going to buy myself, you know, 20 toys. And I'm going to replicate what he did on all of them to see where else this vulnerability may exist so that I can then disclose those to those manufacturers and to those consumers."

I mean, the ability to duplicate and replicate research is hugely important. And maybe not to the average consumer, but it requires public disclosure in order for those of us in the community who do that kind of work to replicate and undertake those kind of -- those kind of efforts.

Getting back to Mr. Troncoso's point a little bit about not wanting to increase the number of zero days. So, you know, zero day being a bug that no one knows about yet and thus that an adversary can potentially exploit before someone has a chance to patch it.

He mentioned the black markets where exploits are traded, and that is an unfortunate reality of the world. And I think, unfortunately, many of the flaws that security researchers discover might very well already be available on the black market. Right? We're not necessarily the first to discover it. We're just the first to discover them and tell the world about them.

You know, if I had a half a million dollars and I wanted to go buy one of these, I might be able to do it already. So I don't necessarily think we're increasing the number of zero days by allowing certain forms of public disclosure. I think it's more an issue of the bad guys may very well already know about a lot of these, and the disclosure allows the good guys to find out about them and see how bad they actually are.

MS. CHARLESWORTH: Well, that's the argument. And the argument on the other side is: There's a certain number of them that people may not know about, and you'll be educating them. That's the concern.

MR. SAYLER: Yeah. And, I mean, then there's a balance here. Right? The question becomes: Is it okay to maybe have some people who are going to find out about this via your public disclosure, but in response you're going to protect millions of end users who now know there's a piece of software they should no longer use?

I mean, this gets at the very complexities of this whole disclosure question, and I think the reason for some of our pushback on this is it is so complex and it's extraordinarily hard to codify in a specific written exemption how to do this properly.

And to some extent -- I mean, yeah, maybe we are saying it would be great if we could just rely on individual security researchers, you know, practicing good faith -- whatever that means -- research, that they will do this properly. And I guess I don't have a great response for, you know, what happens when they don't.

But I think the benefits of allowing them that latitude far outweigh the downsides that the adversaries might use by exploiting these kind of exemptions.

MS. CHARLESWORTH: Okay. Let's see. We have -- okay -- a few more minutes.

I want to go -- I'm going to start -- I'm going to go around this way because Mr. Lightsey's had his placard up. But I will get to everyone.

This will be kind of, I think, the last round of comments that we'll have time for.

Mr. Lightsey?

MR. LIGHTSEY: Yeah, just very briefly,

just to protect the record. I will say that, on behalf of GM, cybersecurity is certainly something that we take very seriously. And we have an extensive organization under a senior leader at GM who's responsible for that.

As I indicated in California, it's a subject that's reported quarterly to our board of directors. This certainly has the highest attention of GM management.

On behalf of the industry, I can say that the industry has committed to a set of privacy principles voluntarily. One of the those principles commits to maintain reasonable security to protect people's information.

And as indicated, you know, that's certainly something we understand is enforceable under Section 5 of the FTC.

And then, finally, we are also engaged in putting together a cyberthreat sharing organization where the entire industry will participate and share cyberthreat information.

Thank you.

MS. CHARLESWORTH: Thank you.

Mr. Troncoso?

MR. TRONCOSO: I just wanted to make a

couple of points. Earlier the issue was raised about the potential for software companies to just decide we're not going to fix a problem that you've notified us about.

But I would just sort of point to the fact that we do have regulators in place to handle situations exactly like this. So if security researchers are encountering pushback from software companies who are just outright unwilling to fix problems that they've been notified about, I would urge them to go to the FTC, for instance, and have the issue resolved that way.

And then sort of circling back now to the zero-day issue --

MS. CHARLESWORTH: Can I -- can you pause for a moment?

MR. TRONCOSO: Yeah.

MS. CHARLESWORTH: What would the -- I mean, tell me more about the FTC process.

MR. TRONCOSO: Laura -- Ms. Moy brought this up in her testimony. She indicated that the FTC has been willing to prosecute -- or not prosecute -- but to bring enforcement actions against companies who are not employing sufficient safety standards in their products and that they've done so in this specific space of security vulnerabilities.

So I think that that's sort of where I was going with that. I don't have more specific information than what was presented, though.

On the second issue of the zero-day vulnerability concerns, I think that building in a requirement to disclose vulnerabilities to the vendor of the software is critical to ensuring that there are not perverse incentives for researchers to keep their research hidden so that it's more valuable on the grey and black markets.

Of course, we're not talking about the researchers in this room, of course. We're talking about the potential for this exemption to be exploited by researchers who are not in this room, who are the sort of bad actors that we have concerns about.

MS. CHARLESWORTH: Thank you.

Let's see. Yes.

MR. STALLMAN: I'll be quite brief. Just to respond to that issue, I don't know that we have great visibility into the -- into the black and grey markets for security exploits, but I think it definitely is the case that part of the value of the exploits that are trafficked in is their secrecy, is the fact that they are -- they are unknown.

And so publication, I think, is one way to quickly make what might be a previously existing but unknown to the -- to the broader research community vulnerability swiftly lose its value as something that should be trafficked in the black market.

So I think that's a reason to encourage more disclosure and more -- sorry -- more publication and disclosure.

MS. CHARLESWORTH: Thank you, Mr. Stallman.

Professor Blaze?

MR. BLAZE: So thank you. I'll be very brief.

So two points. First of all, there is a bright-line difference between the legitimate scientific research community and the black-market criminals, which is that we publish our work and we're required to publish our work because that's what the scientific method demands.

So this -- you know, disclosure is

simply -- public disclosure is simply part of our process.

You asked about a compromise type of disclosure to the public in which you describe the existence of a vulnerability without describing how to exploit that. And I -- when I think about how I would implement that, I can think of some examples in which it might be possible to tell somebody that here's how you can tell that you're vulnerable. Here's what you can do to remediate the vulnerability without giving you enough detail to exploit it.

But I can think of many, many others in which that would be sufficient information to trivially derive what the details are, that the existence and the way of telling whether or not it applies to you is tantamount to revealing how to -- how to exploit it.

So I'm not sure that a meaningful line can be drawn there unless -- and I think the people on that side of the table would agree -- unless we ask people to make very, very broad statements like, you know, "Well, there's a terrible life-threatening problem with GM cars, and I can't tell you what it is." You know, I think -- you know, being able to say, "This model GM car has this type of problem with the brakes" is much more valuable to everybody concerned.

MS. CHARLESWORTH: Right. But, I mean, what I'm driving at -- and, you know, it's -- saying something has a problem with the brakes, the software isn't performing correctly, you know, is different from saying, "There's a vulnerability here. And here's how you exploit it" and line-by-line instructions.

I mean, do you -- don't you ever make those distinctions in your writing?

MR. BLAZE: Sure. And sometimes it's possible --

MS. CHARLESWORTH: I mean --

MR. BLAZE: -- you know, and I'm certainly not going to suggest that it's never possible to do that. In some cases, the technical details for exploiting it are much -- involve very, very specific things.

But in other cases -- in other cases, they aren't. So, for example -- and, you know, I'm speaking totally hypothetically here. I don't actually own a car, let alone a GM car.

You know, it may be that there are many models of cars, some of them are vulnerable, some of them aren't. And the vulnerability is that, if you turn the turn signal to the left three times, it causes the brakes to stop working. And that's -- you know, and the only way to tell whether the car that you've got has that vulnerability is to try it. And there's no other way to describe this vulnerability except with information that's tantamount.

And it's going to vary across the spectrum from that to cases where you could obscure it. And I don't think we can draw a generally applicable line that would meaningfully separate the two.

MS. CHARLESWORTH: Okay. But just to -- just a quick question. I mean, when you publish your research --

MR. BLAZE: Mm-hmm.

MS. CHARLESWORTH: -- I assume in some situations, I mean, you refrain from giving detailed information. I mean, does that ever happen -- about how to hack a system because you think maybe it actually might be harmful?

MR. BLAZE: Absolutely. And it depends

on -- and really the test is whether or not, in order to explain what the vulnerability is and in order to explain what the problem is so that others can learn from it and so that people can protect themselves against it, you know, is it necessary to include details that will allow its exploitation?

And sometimes the answer is: Well, the exploitation involves doing a lot of very, very specific, detailed steps that are -- you know, that aren't essential to understanding it. But in other cases, everything essential to understand it gives you enough information to exploit it. And then in still other cases, we're somewhere in the middle where, you know, you're doing 90 percent of the engineering of the exploitation and leaving 10 percent out. But a determined person could figure it out.

And it's going to vary across that whole spectrum.

MS. CHARLESWORTH: And when you say that's -- the test is -- I mean, do you think that's a widely shared view in the academic security community? Or is that a generally held --

MR. BLAZE: I think --

MS. CHARLESWORTH: -- view?

MR. BLAZE: Sure. And with the understanding that essential property of the scientific process is we publish papers that are reproducible that others can test and that others can -- and that others can build upon.

So we also have that other demand on us that the readers of the scientific papers that I write need to be able to reproduce and verify my work.

But even separate from that, I think the test of unnecessarily providing aid and comfort to people who would do this for no good is not something that any of us want to do.

MS. CHARLESWORTH: Okay. Thank you, Professor.

Professor Matwyshyn?

MS. MATWYSHYN: Thank you.

Just to follow up, there's a whole array of mitigation measures that the researchers can talk with us about, that researchers regularly engage in in the course of their disclosure processes already.

Sometimes it's leaving out essential

detail. Sometimes it's changing the timing of a disclosure. But there's a bundle of tools that researchers use currently as best practices, as norms within their own self-governance in the way that they engage with and disclose.

MS. CHARLESWORTH: Are those written down anywhere? Or is it just sort of in the air?

MS. MATWYSHYN: It is -- well, the researchers are better positioned to talk about this. But in general, they are in there because they are contingent upon the nature of the reproducibility.

MS. CHARLESWORTH: So there are no written -- are there any? I mean, are there any written best practices?

MS. MATWYSHYN: The closest are the ISO standards.

MS. CHARLESWORTH: Which really -- okay. Thank you.

MS. MATWYSHYN: So two more quick points. On the point of the zero-day vulnerability markets and markets in vulnerabilities generally, from the researcher perspective, the researcher faces a decision. That's why this proceeding is so important.

The researcher is in possession of knowledge of a vulnerability. That researcher gets to choose at present: Do I sell this vulnerability and make a quick buck and wash my hands of it; or do I undertake the laborious and personally risky process of attempting to contact vendors, have them potentially threaten me with the DMCA, engage in months of conversations trying to convince people there is a problem when they might not believe me, and then --

MS. CHARLESWORTH: Are you saying there's an overlap in those communities, the people who would --

MS. MATWYSHYN: There's a choice.

MS. CHARLESWORTH: There's a choice. But, I mean, aren't we talking about good-faith people here who would not be selling --

MS. MATWYSHYN: But -- so -- but in the grey areas, the --

MS. CHARLESWORTH: But --

MS. MATWYSHYN: So the market in zero days is not currently criminal, and the U.S.

government in particular purchases zero days regularly.

So researchers frequently feel that they have a choice with these most elite vulnerabilities. But the majority of vulnerabilities are not that sophisticated. They're commonly known vulnerabilities that have simply not been patched.

And so frequently a discovery will happen when a researcher is using a product and noticed that this product has not patched this ten-year-old vulnerability that has been widely known for a long time. And then we want those researchers to contact the company, and we don't want something like the DMCA to prevent the researcher from doing this act of public service and assisting the company in correcting this flaw.

And, finally, on the point of the FTC, I served as the FTC senior policy adviser on privacy and security last year. So the way that the FTC engages with security -- it performs an incredibly valuable function, but it is an agency with limited resources. And so although it has engaged in over 50 enforcement actions on security and reasonable security standard implementation by companies, there hasn't a formal intake mechanism for consumers to report problems other than consumer sentinel or for security researchers to report problems through a trusted type of hotline.

Such a hotline for security researchers does not currently exist at the FTC, and the FTC cannot act as the mediating vector for DMCA threats from vendors. And so the FTC's role is not quite apposite here with respect to our DMCA questions.

MS. CHARLESWORTH: Well, okay. I mean, you said something that was somewhat disturbing to me, and I -- I questioned you a little bit. But I mean -- and maybe this is sort of a side conversation.

But you're suggesting that the people we're trying to grant the exemption to -- or who would benefit from this exemption, if they don't get it, could -- might sell research on the black market? I mean, I hope I misunderstood that.

MS. MATWYSHYN: So there is a -- this is -- the zero-day market is a very small sliver of what we're talking about here.

MS. CHARLESWORTH: But is it --

MS. MATWYSHYN: A very small sliver.

MS. CHARLESWORTH: How does it play into this? I mean, you're --

MS. MATWYSHYN: A zero-day vulnerability

is one type of flaw that can exist.

MS. CHARLESWORTH: No, I understand --

MS. MATWYSHYN: And so in the absence of a regulatory regime for zero-day vulnerabilities broadly, which we don't currently have --

MS. CHARLESWORTH: But we have 1201, which says you can't -- you can't circumvent -- I mean, in other words, you're assuming someone has discovered a zero-day vulnerability.

MS. MATWYSHYN: Right.

MS. CHARLESWORTH: With circumvention or without? I mean, have they already broken the law or have they not? I mean --

MS. MATWYSHYN: If in the course of the discovery of the vulnerability they may have circumvented, we want them to report it to the company and to the public.

MS. CHARLESWORTH: Right.

MS. MATWYSHYN: We want to encourage --

MS. CHARLESWORTH: But if they've already circumvented in violation of 1201, why do they care -- I mean -- I guess, why would --

MS. MATWYSHYN: So the act of disclosure exposes a researcher to risk.

MS. CHARLESWORTH: So you're saying that

the -- those -- there are researchers that -- you're asserting that there are researchers who, without this exemption, will take their research and sell it on the black market?

MS. MATWYSHYN: We don't want that to happen.

MS. CHARLESWORTH: We don't, but --

MS. MATWYSHYN: We want to nudge everyone toward disclosure.

MS. CHARLESWORTH: But do you have any evidence that that has actually happened, that people who -- I mean, it's just a -- it's a disturbing -- it's kind of a disturbing argument here.

MR. BELLOVIN: Well, I don't know if -- I don't know enough of the facts to say if it was a choice. But Charlie Miller, who's one of the foremost researchers to automotive vulnerabilities -- he's an ex-NSA hacker, from his own description, and has stated in interviews that he has found a vulnerability of sufficient interest to some unnamed U.S. government agency, that he sold it for some unspecified but high-five figures value to the U.S. government.

So here's someone who is finding and

publishing vulnerabilities who's also sold an interesting vulnerability to some part of the U.S.

intelligence community.

I don't know any more details than that and, of course, he's not going to say.

MS. CHARLESWORTH: Professor Bellovin -- well, both -- Professor Matwyshyn, I think you finished your final comments there.

Professor Bellovin, did you have anything else to add?

MR. BELLOVIN: I would add I served as chief technologist to the Federal Trade Commission for a year, and I will second what she said: It does not have the resources to act as an intermediary in most of these cases.

In particular, it is not a consumer protection agency in the case of resolving individual cases of a bogus DMCA takedown threat, for example, or "Don't do this research." It's not the purpose of the agency.

Most of what I was going to say was already said by Professor Blaze.

I would say that security researchers, from just very vague information, just disclosure of the very vague information is enough to reveal the really interesting parts.

So take automobiles. The automobile hacking case that I'm most familiar with involved vulnerabilities in the wireless tire pressure monitoring system. You know, it never would have occurred to me to go look into that.

Once I knew that there was an attack there, it probably would have taken me only a few weeks to recreate the work that -- for any competent security researcher to recreate the work once they were pointed in that direction.

"There's a security vulnerability in the tire pressure monitor wireless system." That statement alone is enough for the serious enemies -- and those are the ones I'm most concerned about -- to do it. You don't need the details at that point. Asking the question -- the right question is often the very hardest part of this kind of research, and it's very hard to say -- you know, should this vulnerability have said, you know, "Get rid of it. It's dangerous"? Well, do the batteries overheat if it's rechargeable batteries? Do I worry about a three-year-old pulling this off, or do I worry about a software flaw?

Different remediation measures for

consumers are indicated in each of those three.

When I hear there's a software flaw in this, it would not take me long at all to find it, to recreate it. Knowing to look there was the hard part.

MS. CHARLESWORTH: Okay. Again, referencing the famous Exhibit 12.

Okay. We're coming down to the wire here.

Mr. Sayler, are you going to defer to Professor Reid?

MR. REID: So I just wanted to chime in and underscore Professor Bellovin's point about remedies because I think it's not just about the understanding -- although I think -- about understanding the vulnerability and explaining the vulnerability. It's about, in some circumstances, consumers being able to take an actual remedial action. And sometimes explaining that takes some detail.

So we might look at Exhibit 12 and say, "You know what? There's a piece of crappy software in there, and you should just throw this thing away if you own it because it's not worth the trouble to fix it."

But if I say the same thing to you about your car, you're going to say, "Well, wait a minute. I paid a lot of money for my car, and I can't just go throw my car away. Tell me more about it. Tell me how it fix it."

And if you look at how the auto industry handles other kinds of problems -- so I just Googled, because I own a Honda Element, and we got a recall notice about the air bag in it.

I just Googled it, and the first article that came up is a 30-page article explaining every detail about the vulnerability, every factory where the vulnerable air bags came from, everything that led to the air bags potentially having a problem.

I can look up my VIN number. I can plug it into a web page, and I can find out if my car has a problem. I can schedule an appointment to fix it.

And then I looked up similarly --

MS. CHARLESWORTH: Excuse me. Is that a software vulnerability or --

MR. REID: No. I'm just trying to draw an analogy to --

MS. CHARLESWORTH: Okay.

MR. REID: -- nonsoftware vulnerabilities.

MS. CHARLESWORTH: But that's not a software issue?

MR. REID: If I -- if I type in "can hackers hack my car," which is -- if you start typing "can hackers," the first thing that comes up on Google is "control my car," all I get is a scary "60 Minutes" video where somebody sitting in the back, Lesley Stahl sitting in the front, and her car is going all over the place and she's kind of freaking out.

And it says, "What can I do about it?" And it says, "For now, not much."

And I think the difference here, if you want to look at it, is that we've got the DMCA in one instance and not in the other. And researchers need to be able to disclose more in a lot of circumstances to explain to consumers exactly what's going on here and to apply the kinds of pressure that Ms. Moy talked about.

So I just wanted to underscore the point of consumer remedies can be really important when we're talking about the granularity of the disclosure.

MS. CHARLESWORTH: Thank you, Professor.

And, Mr. Sayler, you have your sign up, but you were done?

MR. SAYLER: Yeah.

MS. CHARLESWORTH: Okay. So I'm going to just ask -- quickly poll my colleagues here to see -- Mr. Ruwe has one more question.

MR. RUWE: Mr. Stanislav, what was the name of your former employer, the one that you worked for when you identified the concern regarding the pig?

MR. STANISLAV: Duo Security.

MR. RUWE: And what were their primary services?

MR. STANISLAV: Two-factor authentication, security for authentication.

MR. RUWE: All right. Thanks.

MS. CHARLESWORTH: Okay. Ms. Smith?

MS. SMITH: Professor Matwyshyn, you said that the norms of the community are perhaps best written out in the ISO standards.

And, you know, something concerning me today is there's a lot of talk about these norms and respecting the norms, not to hack a plane when it's moving; or in patients, not to test a medical device that's already implanted into a patient.

Is there anything in the standards that, you know -- or similar standards that has not been shared with the office or that could -- or any type of standards into what makes a security researcher a security researcher?

MS. MATWYSHYN: So security researchers, in the opinion of the community about themselves, is driven by the nature of the conduct of the individual. Someone who discloses flaws for the purpose of improving the security of our society and works to better the vulnerable systems that currently put us all at risk, that is a security researcher.

The ISO standards are a moving target. They're evolving. The discussions continue. And the two individuals who lead the process have stated that they are happy to directly consider any issues that the panel feels should be discussed with the community participating in the ISO standard and to attempt to contemplate those issues in the next round of the iteration of the two ISO standards that we reference in our exemption request.

MS. SMITH: So do the ISO standards or

anywhere else have a definition of "security researcher," like what you said? Did that come from something?

MS. MATWYSHYN: So the ISO standards are driven by the corporate end of addressing the processes for security vulnerability intake, the internal mechanisms, and the relationship with researchers. So the ISO standards refer to that side of the equation.

From the companies that are ISO-compliant, I believe their perspective would be that anyone who comes to them with a piece of research that demonstrates an actual vulnerability in their product is a security researcher for their purposes. They have provided useful information for improving the quality of the product and the integrity of the code that is embedded in the products that the company is making.

And so when a company such as Facebook or Google awards a bug bounty to someone who brings this type of problem to the table, by bringing that problem to the table and the problem being replicated and being deemed genuine, that triggers the award of the bug bounty and you are, hence, a security researcher.

MS. SMITH: Because you brought it forward?

MS. MATWYSHYN: Mm-hmm.

MS. CHARLESWORTH: I was just going to ask: Why aren't those standards public?

MS. MATWYSHYN: The ISO standards?

MS. CHARLESWORTH: Mm-hmm.

MS. MATWYSHYN: So that is something else that the two individuals chairing the committees mentioned that they would affirmatively raise and push for, to open up the standards and to make them public.

But ISO is an organization that has traditionally been closed. They issue standards in a whole variety of corporate contexts, very high credibility organization. And so traditionally their standards have been closed, but in this case, because of the tremendous social value that would be implicated by an exemption that, for example, relied on them, they are amenable to requesting that the standards be opened. And hopefully they will receive permission from the organization.

MS. CHARLESWORTH: I mean, it's a little

-- I mean, if we were going to go down that route, it's a little hard to draft a law that's based on something no one can see.

MS. MATWYSHYN: Exactly. And so that's why, in the last round of filing, we distilled the main criteria that are embodied in those ISO standards. And so that is an alternative framing that addresses that closed system problem.

MS. CHARLESWORTH: Thank you.

MR. REID: Could I chime in very quickly? And just to your point, I wanted to tie back to something Mr. Troncoso said earlier, which was something that a security researcher is not is someone who's intending to invoke the exemption to commit copyright infringement.

And I think, as we reflected in our filing, we would be comfortable with a limitation that makes clear that it's got to be for noninfringing purposes. We think the statute is expressly geared towards that.

And I think, to the extent you're looking for a limitation that you could work in, it's probably in all of the exemptions that you're granting.

MS. CHARLESWORTH: Well, it's in the law

already. Right?

MR. REID: Right. We agree.

MS. SMITH: Or what was or not in violation of any other applicable law, which is in the current exemption?

MR. REID: I mean, just in the interest of time, I'll defer to the discussion we had earlier on that.

MS. CHARLESWORTH: Yes. I think, Mr. Cheney, you were leaning forward. You're leaning back now?

Okay. Well, I -- yes, Professor?

MS. MATWYSHYN: Just very quickly on the last question. I think that that would unfortunately be a suboptimal framing because many of the problems that currently exist with respect to chilling research suboptimally intertwines the DMCA with other statutes which are problematized in their own nature.

So, for example, the computer fraud and abuse side has three circuits, what's on it. We don't want this approach in addressing the challenges that currently exist under the DMCA for security researchers to fall victim to the flaws of other regimes that aren't built into the system.

MS. CHARLESWORTH: Okay. Can I just say something?

We will not be granting an exemption that somehow suggests that you can violate other laws. I just -- I'm going to say that for the record.

Professor Reid?

MR. REID: We're okay with that.

MS. CHARLESWORTH: Okay. Thank you.

Professor Bellovin?

MR. BELLOVIN: One last quick point. One reason why there's not any strong formal consensus on the vulnerability reporting mechanism is, well, twofold.

One, as Professor Blaze said -- Professor Green said, it's often very hard to understand how best to disclose something, so it's always -- there are very often going to be grey areas.

But the second and more germane one in this context is a fear of vendors not acting in good faith. Many -- as we have seen, there is a chilling effect even when it does not seem to be a copyright concern. There is a concern that many vendors will act this way. Rightly or wrongly, we have seen enough instances where no copyright concerns have actually been implicated, but the DMCA has been used as a club.

And that has led many people to reject the notion of a consensus saying, "I will use my best judgment, and I will not coordinate, not sign onto a policy that gives somebody else the power to act incorrectly."

MS. CHARLESWORTH: Okay. We've run over. So I'm going to close this panel.

This was a very illuminating discussion, and we really appreciate the strong turnout, particularly from the academic community. It's clear that you have deeply held feelings about this, and it's a tricky issue. It's an important issue. And we will -- I'm guessing we may well issue some additional -- some specific questions for you based on the discussion we had today. I'm not sure exactly when that will be, but you will have another opportunity to respond to those, everyone here, before we come up with our recommendation.

So thank you.

I think -- what time should we

reconvene? Let's see. 1:45...

I guess we -- I think people probably can have -- there's a cafeteria right down the hall. So I think we will try and get back on schedule, 1:45, for panel -- for the panel on unlocking, classes 11 to 12. See we'll see those of you who are involved with that back here at 1:45.

(Whereupon, a short recess was held.)

MS. CHARLESWORTH: Welcome back to those of you who were here before, and welcome to any newcomers. This is the Sixth Triennial Rulemaking Proceeding under Section 1201 of the Copyright Act.

My name is Jacqueline Charlesworth. I'm the General Counsel of the Copyright Office.

And I'm going to -- I'm going to go down the line and have my colleagues introduce themselves.

MS. CHOE: Hi. Michelle Choe at the Copyright Office.

MS. SMITH: Regan Smith, Assistant General Counsel.

MR. DAMLE: I'm Sy Damle. I'm Deputy General Counsel.

MR. RUWE: Steve Ruwe, Assistant General Counsel.

MR. RILEY: John Riley, Attorney-Advisor.

MS. CHENEY: And I'm Stacy Cheney, Senior Attorney at NTIA, U.S. Department of Commerce.

MS. CHARLESWORTH: Okay. So you have -- are there more of us than you? I don't know. Maybe it's a tie. Okay.

So as some of you may have heard from earlier today, the point of the hearings is really to kind of home in on the issues that are sort of a little bit in dispute, maybe murky areas where we have questions. And we do let everyone have a brief opening statement.

But in making your remarks, I would encourage you to focus on the issues where there may not be full agreement or the law perhaps is unclear.

We do frequently interrupt with questions. So be prepared on that.

And, you know, we are familiar with your written comments. So there's no need to sort of review sort of your high-level comments if you've already submitted them in writing because we did carefully read them.

We try not to talk over one another. Your remarks are being recorded by the court reporter. And if you're -- I don't -- are there any exhibits with this one?

So we don't have to worry about that.

If you want to add to the conversation, tip your placard up, and we will get back to you so that you can respond or add an additional comment as you see fit.

And for the record, this is proposed classes 11 and 12, unlocking wireless telephone handsets and tablets.

So before we launch into the opening statements, I'm told I'm going to have to -- this is going to be very -- I'm going to go from right to left in this one. I'm used to going from left to right.

So we'll start with you -- I can't read your name -- Mr. Mackey? No. To your left, who is sitting next -- he's not a real person, or is he -- no, he's -- are you going to be participating on the record?

MR. MACKEY: Yes.

MS. CHARLESWORTH: Okay. What -- we'll start with you. If you could just briefly give your name and your affiliation or the interest you have in the proceeding.

We'll go from right to left, and then we'll start at your end and have you make your opening remarks.

MR. MACKEY: All right. Good afternoon. My name is Aaron Mackey. I'm with the Institute for Public Representation at Georgetown University Law Center. And I'm Of Counsel to Consumers Union in their proposed exemption.

MS. CHARLESWORTH: Great. Thank you.

MR. SLOVER: I'm George Slover, Senior Policy Counsel for Consumers Union.

MR. LAZARUS: Mike Lazarus, an attorney for Telecommunications Law Professionals. And we represent Competitive Carriers Association.

MR. HARRIS: Hi. Good afternoon. Eric Harris with ISRI, the Institute of Scrap Recycling Industries. And I'm Associate Counsel and Director of Government and International Affairs.

MR. WEISSENBERG: Good afternoon. Brian Weissenberg, a law student at Stanford Law School, involved in the IP and Innovation Clinic there, representing ISRI.

MS. LONG: Hi. I'm Donna Long. I'm also a law student at the Stanford IP and Innovation Clinic. And also with us here at the table is Professor Phil Malone. He's the director of the IP and Innovation Clinic, and he won't be speaking today. He's just chaperoning us.

MS. CHARLESWORTH: Well, it's good to know everyone is well chaperoned.

Hello, Professor Malone.

Okay. So, Mr. Slover, does that mean you're kicking us off? Okay.

MR. SLOVER: Good afternoon. Consumers Union, the advocacy arm of "Consumer Reports," is pleased to be here to support our proposed exemptions to allow consumers to unlock telephone handsets and tablets so they can be connected to other wireless networks and thereby extend their useful lives, save money, and increase competition and innovation.

We've introduced ourselves already, so I'll skip that.

We note that no one filed an opposition to our proposed exemption for tablets, and the one party who filed an exemption in opposition to our proposed exemption for handsets, TracFone, has now joined with the Competitive Carriers Association in support of a differently drawn exemption.

We're encouraged at the efforts to reach a consensus.

Today I will talk about why we have written the exemption the way we have identically for handsets and tablets as they are functionally equivalent for this purpose and why we think our way is better than the other ways put forward.

We will also be happy to answer any questions you might have for us.

But first I will briefly recount the reasons why we believe these exemptions are warranted, reasons that are more fully set forth in our petition comments and reply comments.

To start with, this exemption has been approved twice before in 2006 and 2010. And when it was phased out in 2012, a public uproar led to the President and Congress calling for its restoration and the resulting bipartisan enactment of legislation reinstating in and directing the

Copyright Office to consider expanding it to include tablets.

The exemption we propose is modeled closely on what Congress enacted last summer with the expanse to tablets that Congress envisioned.

Second and perhaps more fundamentally, mobile device unlocking has no business getting caught up in the DMCA's prohibition on circumvention, convenient as it may be for certain wireless carrier business models.

As the Copyright Office has noted, unlocking a mobile device has nothing to do with copyright infringement in any meaningful sense. Unlocking is about being able to use equipment the consumer has legally purchased.

As we explain in our written submissions, the focus for copyright analysis is properly on the network-connecting software in these devices. The locking software is important only because it obstructs access to the functioning software.

Even if the network-connecting software is copyrightable, which is by no means clear, it is not being copied in a copyright sense when the device is connected to another network. It is either being engaged or it is being bypassed. And the only possible copying of the locking software would be for the very limited purpose of getting out of its way.

Any incidental copying or adaptation of either locking or network-connecting software is protected under Section 117 as an essential step in making the phone or tablet function.

In the Unlocking Act, Congress removed any issue regarding whether the owner of the device also has to own the copy of the software to get the protection of Section 117. Using the DMCA to enforce the law prevents consumers from making full legitimate use of the phone or tablet they've purchased. It strikes at the heart of the fundamental rights of ownership that have been a cornerstone of our law for centuries.

It arbitrarily cuts short the useful life of perfectly good devices, adds to unnecessary waste, removes affordable alternatives for cost-minded consumers, and props up anti-competitive business models that restrict consumer choices. It harms consumers on both the selling and the buying side.

As we and others have established,

that's precisely what happened when there was no exemption. And that, in a nutshell, is the harm we are seeking to remedy.

MR. DAMLE: I just have -- I'm sorry to interrupt you.

MR. SLOVER: Yes. Go ahead.

MR. DAMLE: I have a couple of questions, but I'll start with one just to establish for the record why you believe the unlocking policies of the carriers are insufficient for you.

MR. SLOVER: Well, you mean the voluntary --

MR. DAMLE: Yeah, the voluntary policies, right.

MR. SLOVER: Well, first of all, because they are voluntary, which means they could be changed at any time. So they're no substitute for a right.

Secondly because there are restrictions and conditions. You basically work through a process with your current carrier to unlock the phone. So that eliminates some of the flexibility for consumers who would prefer not to deal with their previous carrier, would rather turn over the phone in a locked state and have somebody else do the unlocking.

And, you know, because it can be changed, you know, it's kind of -- over time, the voluntary policies came to fruition when everybody was kind of poised to see the legislation enacted into law and probably with an eye to creating a good record for that and during the time when there was no exemption, at least one of the carriers significantly restricted its policy.

So we think there's no substitute for having a guaranteed right.

MR. DAMLE: Which carrier was it that restricted the --

MR. SLOVER: It was AT&T.

MR. DAMLE: Okay. All right. So moving on to sort of the kind of dispute that remains among at least the people that are arrayed here as between -- as I understand it, there's just sort of a dispute about the scope of any exemption we should grant.

So one question I have for you is: one thing I didn't see in your proposal was a limitation to used cell phones and tablets, which is something that we have in the existing exemption. It says that it has to be a used wireless telephone handset.

And so is that -- is that something -- is that purposeful? Are you meaning to allow circumvention of new handsets now?

So I wonder if you could address that.

MR. SLOVER: Sure. And I was going to -- I was just about to get to sort of --

MR. DAMLE: Okay.

MR. SLOVER: -- why our exemption is different --

MR. DAMLE: Sorry. I'm jumping ahead.

MR. SLOVER: -- from the others.

No. That's okay.

And I -- maybe I can explain it more fully once I get to that point.

But my answer to you is a couple of things. One, imposing conditions or restrictions on the right to unlock makes it difficult from an ordinary consumer's perspective. Because what that means is here's a proof requirement. You've got to be confident that you can prove this in order to be protected from potential civil and criminal liability.

And I think it's going to be difficult

for a consumer to know whether a phone has been used or how it's been used in the past. All they're going to know is that they've got a phone that they've obtained, as far as they know, from a lawful avenue and they want to unlock it and use it on a new network.

So that's one thing.

The other thing is that there's one situation where at least one of the definitions of "used" is that it's been previously activated on a wireless network. And so even if you could satisfy the proof requirements, there's one situation where we think consumers should have the latitude to part with a phone before that happens. And that's a situation where, under the contract that I've got now, you -- you get a phone for a certain period of time and then you're allowed, when you renew your contract, to get a new phone. And that's one of the incentives for renewing.

Well, maybe you're a guy like me who's 60 years old, and most of what you do is use your phone to make calls and send e-mails, and your teenager or your teenage nephew really likes the full array of what the newest phone can do.

So rather than upgrade yourself to that

new phone, you're just going to keep using the one that you've been using. But you essentially get the new phone for free as part of the package. So it doesn't make sense to give it up. So you take it and you pass it on to your nephew.

MS. CHARLESWORTH: Is that -- I'm sorry. But my experience, you know, is that usually you're under contract, you go in with your old phone under the contract, you have to hand that one in and you get a new one that's another subsidized phone under the contract.

I mean, I'm not familiar -- are you saying there are actual -- and there may be. So it's -- you know, but what kind of -- when would you encounter a situation where you were -- had both phones and the second one wasn't being subsidized?

MR. SLOVER: You mean the new phone wasn't --

MS. CHARLESWORTH: Well, I'm saying, if I have -- if I -- I mean, correct me where I'm wrong in this scenario.

I have, say, an iPhone 5. I want an iPhone 6. I believe, if I went to my carrier and took my iPhone 5 in and said I want a 6, they'd say, "Yeah, you can have this. You've finished your contract for the 5, but give us the 5 back" or at least the 6 would then be subsidized and under contract.

I'm just -- I'm just curious to know from anyone on the panel whether there are -- and, you know -- whether there are scenarios were you would end up with a new, unsubsidized phone that hadn't been activated with the carrier.

MR. SLOVER: Well, it might --

MS. CHARLESWORTH: The scenario you're talking about, which is not familiar to me.

MR. SLOVER: It might very well be subsidized. And the times that we've done this before as a family, they have been subsidized.

It's a hidden subsidy that's part of the -- of the monthly payment that we make.

MS. CHARLESWORTH: Right.

MR. SLOVER: And there are new models now -- new kinds of service contracts that have evolved in the last year or two or three that have a different arrangement where the subsidy is more transparent. But they still have the ones where it's not transparent.

And in those situations, if you -- I

mean, you could say, "Well, thanks. But I don't need a phone." But that wouldn't change your monthly payment.

I mean, it would under some of the new ones. But in some of the old ones, it doesn't change it.

So what we think consumers should be able to do is to say, "Okay. I'm going to take that phone that you're requiring me to pay for. I'm going to take it. But I don't want to use it."

MS. CHARLESWORTH: Is it under contract?

MR. SLOVER: "I'll let somebody else use it."

MS. CHARLESWORTH: Is the new phone under contract in your scenario?

MR. SLOVER: It's a service agreement.

MS. CHARLESWORTH: Right. So it's a -- presumably, it's a subsidized phone. So you're saying -- I mean, then do you go and pay off the contract? How does that work? What's your obligation to the carrier vis-a-vis the new phone?

MR. SLOVER: Well, your obligation is under the contract. You've --

MS. CHARLESWORTH: So you can --

MR. SLOVER: -- agreed to have service with that carrier for a two-year period or however long it is.

MS. CHARLESWORTH: Right.

MR. SLOVER: And if you don't continue the service for that period of time, there's an early termination fee.

There are contractual obligations that don't have to do with the lock on the phone.

MS. CHARLESWORTH: But would they let you walk out of the store with a phone that they didn't activate to their network? I mean, if I were -- and this is -- I mean, if you're AT&T and you're handing out a subsidized phone, why would -- why would your policy permit you to hand it out without activating it, which is -- we're going back to the definition of "used" here, which you objected to.

But, I mean, it seems it me that the policy -- most policies -- and, again, people can feel free to dispute this -- that if it's a subsidized phone, they're probably not handing you a phone that they're not activating and letting you walk out of the store, even if you're under contract.

MR. SLOVER: Well, if that's the kind of deal that they want to offer, then that's the deal that they should offer. And other carriers may offer a different deal.

MS. CHARLESWORTH: But do they? That's what -- we're trying to find out what they actually do because you're objecting to the definition of "used," and the bigger issue here is the -- you know, we have comments from TracFone. They're not here today. But the bulk situation where people are buying up phones, subsidized phones -- and I want to hear more about this too -- and then reselling them in a way that's -- at least TracFone thinks is inequitable.

But you're positing a scenario where you could -- you're disputing a definition based on a scenario that I'm not sure exists in the real world. And so that's what I'm trying to understand, that you could walk out of -- as an individual consumer, you could walk out of AT&T with a contract phone that hadn't been activated.

MR. SLOVER: Well, what we're -- what we're hoping will be the result is that there will be flexibility in the kinds of contracts that can be made available to consumers and the kinds of ways that they can get phones and that there's not a barrier that doesn't need to be there that says, you know --

MS. CHARLESWORTH: Well, there --

MR. SLOVER: -- we're prohibited under the DMCA, as its been interpreted, from allowing you to walk out of here with a phone that hasn't been activated.

MS. CHARLESWORTH: They would just let you buy an unlocked phone, right? You would pay the $700.

I mean, that would be the answer -- there is a -- I mean, a lot of -- some carriers do let you do that.

In other words, if they're going to let you walk out of the store with a phone that's, you know -- I mean, they can sell you an unlocked phone, and then there's not a concern about fulfilling your contract and all that.

So that -- you know, they can do that regardless of Section 1201 today.

MR. SLOVER: Right. Those that want to can offer that.

But if they're going to lower the price of the monthly service contract in connection with that, then that would be something that a consumer could weigh the pros and cons of which way to go.

But if the consumer sees an advantage to being on an extended contract, they know they're going stay with the same carrier because they've been with that carrier for years and they like that carrier, they should be able to keep their old phone. And the deal that they've signed up for should not require them to pay for a phone that they don't want just because they are constrained from passing that phone along to somebody else.

MS. CHARLESWORTH: Okay.

MR. DAMLE: So just to be clear, I mean, you object to the current exemption, as it was reinstated by -- I mean, you don't think the current exemption, as was reinstated by Congress, is sufficient?

MR. SLOVER: We think, as a practical matter, most of the phones that are going to be involved here are going to be used phones. But we -- in advocating before Congress and in advocating in past triennial reviews, we have urged that the exemption not be limited to used phones.

So our position is the same as it's

been.

MR. DAMLE: Okay.

MS. CHARLESWORTH: And how do you respond to the TracFone concern?

MR. SLOVER: Well, we are not in favor of illegal bulk trafficking, and we're not talking about illegal bulk trafficking here. We're talking about something that an individual consumer would do with the phones that they obtain for themselves or for their immediate family members on a contract that they've entered into with a carrier.

MS. CHARLESWORTH: Can I just go back to your scenario? Because under your -- let's say you purchase a phone from -- you get your new phone from AT&T and you in your head think, "I -- you know, I'll pay off my contract, but I'm going to -- I want to unlock this and switch it right away. I'm going to go from AT&T to the next store."

You could have AT&T activate it and then not -- I mean, in other words, you could easily fall under the "used" definition if you simply have it activated by AT&T before you walk next door and have a new carrier unlock it and activate on their network.

So that's why I'm not -- I mean, it's just not that hard -- I mean, that's -- since you're getting the phone right there anyway, there's really no particular burden in doing that if you want to meet the "used" definition.

But the reason that people have proposed that definition, as I understand it, is to help prevent or at least exclude the kind of bulk trafficking scenario, which is a concern in the record.

So there's sort of that -- as I -- and they can speak to that more directly than I can. But that's the -- that's what they're responding to. So, like, I just don't really see the -- I don't -- I don't see why this is so limiting to, you know -- to consumers who want to switch even if they're, frankly, going to break their contract.

MR. SLOVER: Well, I think working through the hypotheticals that you've laid out...

I've got an iPhone 5. I have the opportunity to get an iPhone 6 or I have an opportunity for virtually nothing to get an iPhone 5S when I go back in. And I decide that the iPhone 5S is not that much better than the iPhone 5, so I'm going to keep the one that I've got.

But I'm basically being offered a free iPhone 5S. So I would like to give that to my nephew who lives in a different city. And he's going to hook it up with somebody different. It's going to be on a different account than mine.

So what the hypothetical that you're describing would be is that I would get the phone from AT&T, I would hook it up, I would transfer all of my data and my phone number and everything to my new iPhone 5S, and then I would go back in the next day and say, "I want you to transfer everything back into my old phone."

So theoretically that could happen. It wouldn't be all that hard.

MS. CHARLESWORTH: And your new --

MR. SLOVER: But why should the consumer have to do that if the end result is the same?

MS. CHARLESWORTH: So how would you propose to address the bulk issue differently?

I mean, in other words, assuming that's a legitimate concern that people are misusing -- might misuse the exemption or whatever TracFone -- you know it's their concern. But it has been a perennial concern, this -- I mean, how would you address it?

MR. SLOVER: So Consumers Union definitely agrees that it's a legitimate concern.

I think the question here is: is it a copyright concern?

So from the bulk unlocking perspective and what the problems are there, TracFone has a number of alternative legal remedies at its disposal that its used.

And from our perspective, the question really is: Should the average consumer continue to have DMCA liability?

MS. CHARLESWORTH: Well, I mean, is it a copyright concern that the person has to go to AT&T and switch the data back?

I mean, a lot of this stuff is not really -- you know, a lot of the things we talk about or the value of recycled phones and whether their price is different because you can unlock them -- you can say they're not copyright concerns, but they're all part of this -- this particular exemption that we're talking -- I mean, they're concerns that are raised.

I understand there may be other legal

avenues. But, like, let's assume that they think that 1201 is an important factor in this, which they clearly do.

I mean, is there a way you could write the exemption to exclude that behavior that you would be willing to agree to? Because the other parties have come to, I think, some version of an understanding on this.

MR. SLOVER: Well, I don't want to speak for the other parties as well --

MS. CHARLESWORTH: No.

MR. SLOVER: -- because I -- what I've noticed, I think there is still a difference between what CCA and TracFone have proposed versus what ISRI has proposed with the "used" exemption with the addition of the term "used" as well.

So I think that there's some issues there.

MS. CHARLESWORTH: Okay. Well, why don't we move on and hear from the other parties.

Mr. Lazarus?

MR. LAZARUS: Okay. So we represent Competitive Carriers Association. We will significantly scale back our open and just sort of try and get to a couple of paragraphs.

We -- Competitive Carriers Association is the nation's leading association for competitive wireless providers and stakeholders across the country. CCA's membership includes more than a hundred wireless providers ranging from small rural providers serving fewer than 5,000 subscribers to regional and national providers serving millions of customers.

As a result, CCA has a keen interest in ensuring that all wireless subscribers have access to cutting-edge handsets and wireless devices available today for use on networks of their choice.

CCA believes that the use of wireless devices to connect to different wireless networks represents a noninfringing use and not granting an exemption will likely result in adverse harm to consumers both in the present day as well as within the next three years.

Accordingly, CCA strongly supports an exemption allowing consumers to unlock all of their devices that connect to wireless telecommunications networks in order -- in order to associate such devices with the network of their choosing, which CCA originally proposed via four different petitions before this office and comments in the record.

This protection should apply not only to handsets and tablets but to all wireless devices that have the potential to connect to a telecommunications or information services network.

Because this proceeding is forward-looking, an exemption should allow consumers the ability to unlock any relevant device and not be subservient to the will of one carrier or manufacturer.

In addition, as directed by Congress, the exemption should not limit who may provide assistance to unlock a device and, therefore, should allow an agent of the consumer, whether it be a person or a different wireless provider, to perform the unlocking procedure, just as a locksmith may unlock an individual's car or home when they do not have the necessary key.

Now, while there has been near universal support for an exemption of this nature, one party did express limited support, seeking additional protections related to subsidies, TracFone.

Although CCA believes that its original

proposed exemption is consistent with the Copyright Office's mandates concerning circumvention, in light of the Register of Copyright's recent testimony before the Committee on the Judiciary where she expressed a desire for Section 1201 to be amended to provide that existing exemptions will be presumptively renewed during the ensuing triennial period in cases in which there is no opposition, CCA worked diligently with the sole opponent, TracFone, to its proposed exemption to reach a compromise on a modified proposed exemption.

These modifications will continue to properly enable users to take control over the use of their wireless devices and permit them the choice of which network they will be connected to while also helping to ensure that such an exemption may not be easily exploited by traffickers and to steal subsidies pursuant to contracts.

MS. CHARLESWORTH: Okay. And can you explain, just to home in on the issue -- be specific for the record about how you -- the part of your proposal that protects against bulk unlocking and why -- and how it does that?

MR. LAZARUS: Sure. So what we tried to do is come up with a formulation similar to what I would call the contract law formulation.

A number of our member carriers have subsidies. You can buy a phone from them for a two-year contract. You can buy a phone from them via a device installment plan. So we're not blind to that concern.

And what we tried to build into this exemption was the idea that, for the original owner, that you would not be able to go unlock your phone unless you adhered to the -- to the terms of the contract that you had. So essentially, you walk into AT&T, you buy a phone for two years -- under a two-year contract. In month three, you shouldn't necessarily be able to just go get your phone unlocked.

So that's how we tried to bridge the gap with TracFone.

Now, what we also don't believe -- so when you go into -- as far as liability is concerned, we do believe that we should follow what Congress asked this office to do, which is essentially, if you take that phone and bring it into a particular carrier, that carrier should be able to unlock it. We don't think there should be any liability surrounding that.

Any liability should hold to the -- what I would call the original owner and their original obligations to their original carrier.

MR. DAMLE: So I just want to sort of test a few points here.

MR. LAZARUS: Mm-hmm.

MR. DAMLE: One is -- well, you mentioned that it's a two-year contract. There are often termination fees that you can pay to get out from your contract.

MR. LAZARUS: Sure.

MR. DAMLE: I take it that, if someone pays the termination fee -- they're leaving the state, they're leaving the country, they don't want to -- they just want to terminate their contract and take their phone.

MR. LAZARUS: Yep. Absolutely. I think that's built into our proposed exemption already. It's really -- once you pay off the ETF, the early termination fee, your obligations to the original carrier terminate.

So at that point, you should be able to take your phone and unlock it wherever you want.

MR. DAMLE: Okay. So one of the concerns that ISRI has raised -- I don't want to put words in their mouth -- but as I understand it, that it's unclear who the owner is.

So if I own a phone and then -- if I buy a phone sort of on eBay and it's locked, I don't necessarily know where -- whether the original owner has satisfied all of their obligations to the -- to that carrier that the phone is locked to.

So do you have -- do you have a response to that concern? Is there --

MR. LAZARUS: Well, we --

MR. DAMLE: Is there a solution to that concern?

MR. LAZARUS: We were concerned with the original owner.

MR. DAMLE: Right.

MR. LAZARUS: So as far as we're concerned, if it goes to a second -- a second owner at that point, we don't think that owner should have to track down, you know, what has been going on, you know, two owners before, three owners before. Right?

So it's essentially a good-faith

obligation attached to the original owner.

MR. DAMLE: Right.

MR. LAZARUS: So we're not in -- I don't view us as in disagreement. I think we all view this the same way.

That second owner should just be able to go get their phone unlocked without having to worry about, "Okay. There were three owners before. Do we have to try and figure out what happened there?"

MR. DAMLE: Okay. So -- okay. So a slightly -- so let's say I want to give it to a family member. I want to give my phone to the family -- to a family member.

MR. LAZARUS: Mm-hmm.

MR. DAMLE: Say it's not a member of my immediate family; it's my nephew. What about in that scenario? I mean, is the subsequent owner in that scenario required to satisfy the contract?

I mean, I'm giving you hypotheticals to test the limits of --

MR. LAZARUS: Sure. I think in that particular situation -- we don't have a particular view on it. I think -- again, once -- we're trying to avoid a situation where you do have to worry about an obviously much closer call -- you know, if the dad buys the phone and gives it to -- you know, a husband buys the phone and gives it to the wife, for instance. Can she get around her contract?

We would view that as no. Most of our member carriers would view that particular situation as no.

But, again, I think we view that more as a contract claim, more as a contract matter rather than necessarily a DMCA matter.

MR. DAMLE: So if we were to make clear -- just going back to sort of the -- like, you know, the arm's length kind of scenario.

MR. LAZARUS: Mm-hmm.

MR. DAMLE: If we were to make clear that subsequent owners would not be required to assess whether the original owner has satisfied or -- his or her contract obligations or whether those contract obligations are waived, you would be fine --

MR. LAZARUS: Absolutely. Yes.

MR. DAMLE: Okay. That's helpful. Thanks.

MS. CHARLESWORTH: Did you have anything

else, Mr. Lazarus?

MR. LAZARUS: No.

MS. CHARLESWORTH: You're good for now?

MR. LAZARUS: I am.

MS. CHARLESWORTH: Mr. Harris?

MR. HARRIS: Thank you very much. I'm appearing today in support of ISRI's proposed exemption for class 11, unlocking the wireless telephone headsets.

I want to make two introductory remarks and then turn the presentation over to our two law student counsel.

ISRI is a trade association representing more than 1600 processors, brokers, and industrial consumers of scrap commodities. However, among our members are recyclers of used phones and tablets. These are the companies that lawfully acquire used, unwanted phones from individual and corporate owners, refurbish these phones, and resell them back into the marketplace.

The work of recyclers provides important public and economic benefits by enhancing the value that consumers can receive when they sell the used phones, increasing the number and variety of used phones available for other consumers to purchase and ensuring greater competition in the wireless device and carrier marketplaces.

In order to achieve these benefits, recyclers like our members need to be able to unlock in bulk the phones they legally obtain. We need a clear exemption to Section 1201 that removes concerns about potential DMCA liability, the risk of which is substantial in the current law.

Only one party, as we've discussed, TracFone, has objected to our and the other proponents' proposed unlocking exemptions out of concerns that the exemptions will permit illegal phone trafficking.

Let me be clear. ISRI's members do not engage in phone trafficking, and we do not in any way condone such trafficking.

MS. CHARLESWORTH: Can I ask you a question? I mean, I've always had -- this is -- there seems to be a couple different versions of -- I don't know if they're all trafficking, in your view.

MR. HARRIS: Right.

MS. CHARLESWORTH: But what TracFone was describing was people, as I understood it, going to a -- buy subsidized -- or phones that are intended for -- to be locked to a carrier off of a shelf at a discounted price, essentially subsidized.

MR. HARRIS: Right.

MS. CHARLESWORTH: And then instead of, you know, accessing that carrier or -- you know, they sell them somewhere else with the -- you know, and sort of an arbitrage on the phones.

Is that a -- is that a scenario that you're familiar with? And can you comment on that?

And then there was a sort of second scenario. I'll just -- it will be a two-part question where there seemed to be sort of truly a black market in phones that were meant to, say, go to carriers for subsidized plans but somehow fell into the wrong hands.

And I'm just curious to know more about

-- about the sort of that -- those issues:

trafficking and the stuff that TracFone was talking about.

MR. HARRIS: Sure. As to the first question, I mean, we'll take their word for it.

That's not our concern. That's not our issue.

And we concede the notion that applying the exemption for used devices really addresses almost all of our concerns.

Our members don't deal in recycling new phones or phones that you buy at a store. That's just not the business model. That's not what they do. That's not what we're here to advocate on behalf of.

As far as the black market or illicit trade of phones in the alternative, also that's not the behavior that we're advocating for. We're looking at legitimate contractual relationships where a recycler will go and purchase that phone or that tablet from either a consumer or a business entity. And then they own those phones and they want to refurbish them and do what they need to do to resell them back in the market.

And that's all under a very transparent, you know, very legally valid contractual type of arrangement.

MS. CHARLESWORTH: Do you think there needs to be a definition of "used" in the exemption? Or is "used" sufficient, from your point of view, to explain what's exempted?

MR. HARRIS: Well, I think certainly a definition could be helpful depending on what it is. Certainly, we're comfortable with what appears to be where that definition is going.

MS. CHARLESWORTH: Meaning saying it had been -- what is it? -- "lawfully acquired and activated on the wireless telecommunications network of a carrier"?

MR. HARRIS: Yeah. That language would be fine for us.

MS. CHARLESWORTH: That would work for you?

MR. HARRIS: That would work.

MS. CHARLESWORTH: Okay.

MR. DAMLE: Sorry. And the language -- so I think that may have been language that you had put forward at one point.

But the language proposed by CCA and TracFone in their reply comments, do you have any thoughts about that language?

MR. HARRIS: As far as the "original owner" concept or --

MS. CHARLESWORTH: Well, it's more tied to fulfilling --

MR. DAMLE: Fulfilling the contract.

MS. CHARLESWORTH: -- the contract.

MR. DAMLE: Not being used for unlawful purpose, theft and fraud -- the device was not obtained by theft or fraud.

MR. HARRIS: Yeah. I mean, and -- my colleagues here will get -- will get into this as well.

MR. DAMLE: Okay. Fair enough.

MR. HARRIS: So maybe I'll punt to them. But I do think that overall there is a path that we can move forward here that would certainly address our issues.

MS. CHARLESWORTH: Okay. Thank you, Mr. Harris.

Mr. Weissenberg?

Ms. Long?

MS. LONG: Hi. So we understand that TracFone's initial proposal as well as TracFone and CCA's compromise both contain a requirement saying that you have to -- the original owner has fulfilled the contract obligations or recouped -- allowed the carrier to recoup any subsidy it may have provided in the handset price.

But for ISRI's members, that language

would be impractical. It would make it impossible for them to unlock the phones they receive because ISRI is not the original owner. They're a subsequent owner, and they acquire the phone lawfully, but they have no way of figuring out whether the original owner has satisfied its contract obligations.

MR. DAMLE: So the colloquy that I had with Mr. Lazarus where I suggested we might be able to kind of clarify that subsequent owners would not have that obligation, would that satisfy your concern?

MS. LONG: Yes.

MS. CHARLESWORTH: Okay. You can continue.

Ms. Long, did you have anything further to add or --

MS. LONG: That's all I have.

MS. CHARLESWORTH: Okay. And, Mr. Weissenberg, did you want to say anything for the record?

MR. WEISSENBERG: Good afternoon and thank you again for allowing us to testify before you today.

Again, my name is Brian Weissenberg, and

I'm a Stanford law student at the Stanford IP and Innovation Clinic, representing Petitioner ISRI.

In my short time, I want to make two brief but important points about the Unlocking Act which was enacted in 2014 and which helps guide the unlocking portion of this rulemaking.

First, as Mr. Slover already discussed a bit, the Unlocking Act demonstrates that Congress and the President believe that any copyright concerns should yield to the pro-consumer benefits of unlocking one's phone and moving it onto a different carrier.

While ISRI submitted a full and careful Section 117 analysis and fair-use analysis in our initial comment, we believe that analysis is ultimately unnecessary because the Unlocking Act expressly allows unlocking by owners of mobile devices regardless of whether they own the underlying copies of software on those phones.

The act specified and the Copyright Office itself affirmed in its notice of inquiry that future unlocking exemptions will apply to phone owners, not owners of the copies of the software.

But second and most importantly, we

believe the Unlocking Act itself also allows bulk unlocking.

As just discussed, the Unlocking Act specifically allows device owners to unlock their phones. Recyclers are the lawful owners of those mobile devices they receive and seek to unlock.

This is also confirmed in the legislative history of the Unlocking Act.

Now, you may recall that at one point there was a clause in the bill that mentioned bulk unlocking in a way that many were concerned might be interpreted to deny unlocking benefits to bulk unlockers.

But after much debate, that language was ultimately removed and does not appear in the Unlocking Act that was signed into law by President Obama.

But what's more telling is that, even when that language was in the bill, Representative Goodlatte, the bill's primary sponsor, expressly stated that the clause, quote, "is not intended to impair unlocking by legitimate recyclers or resellers," unquote.

But instead that language was targeted at phone traffickers. So Congress made clear that this act was intended to protect phone recyclers like ISRI's members. In other words, we resell used phones just like a used bookstore sells used books, which the Librarian of Congress in 2010 stated would be a protected commercial activity.

Now, although we believe bulk unlocking is covered by the Unlocking Act, we also believe it is vital that such unlocking be explicitly permitted in any new exemption to avoid any ambiguity and uncertainty for recyclers.

Finally, I want to note Mr. Harris's reminders that only one party, TracFone, opposes the unlocking exemptions and add the important fact that even TracFone says in its filing that it supports an unlocking exemption so long as that exemption expressly excludes any provision that could be exploited by illegal traffickers to steal subsidies and harm consumers.

So, really, the only real disagreement at this stage of the rulemaking should be over the precise scope and wording of an unlocking exemption.

Now my colleague, Donna Long, will answer that question describing how our proposed exemption is carefully drafted so it will not exempt illegal phone trafficking.

Thank you.

MS. CHARLESWORTH: Ms. Long?

MS. LONG: Hi. I'm Donna Long. I'm with the Stanford IP and Innovation Clinic. We're representing ISRI.

So I have two quick points about our trafficking discussion so far.

First of all, TracFone has available and regularly uses a variety of noncopyright legal claims to stop traffickers and seeks recovery for any harm that it would suffer from trafficking.

So the DMCA is not only inappropriate but unnecessary for the trafficking concern.

MS. CHARLESWORTH: But can I just -- I mean, isn't it true that they also have successfully used the DMCA, 1201, to address trafficking issues?

MS. LONG: Yes. They have successfully filed lawsuits with the DMCA as well as up to 10 or 12 other claims that they've won on all of them.

MS. CHARLESWORTH: Right. But they -- okay. Continue.

MS. LONG: And second, I wanted to

emphasize that ISRI's proposed language was carefully crafted so that it could not be construed to permit phone trafficking. Our language would only allow unlocking of used phones and, as we said, that means phones that have been lawfully acquired and activated on the wireless telecommunications network of a carrier.

So TracFone's new phones that are being unlocked in the process of this legal trafficking would never fall within the scope of that language.

As TracFone has described in its trafficking litigation, the scenario that they are trying to address is where trafficked phones are bought at a retail outlet then resold new without ever being activated on a network. And, therefore, trafficked phones would never fit the definition that ISRI has proposed about "used."

MS. CHARLESWORTH: Okay. Did you have a question, Mr. --

MR. DAMLE: I hit the bell. Sorry about that.

So I actually wanted to go back to Mr. Lazarus, if that's okay.

MS. CHARLESWORTH: No. No. Go ahead,

Mr. Damle.

MR. DAMLE: So one question I had -- just looking through the elements of your proposed language, one question I had is why it's necessary to include -- to specifically exclude devices obtained by theft or fraud. I mean, that's something that we don't have in our current exemption, and maybe this is not a position that you've been taking and this may have been from TracFone.

But I'm sort of curious if you can just sort of explain the reasoning behind putting that explicitly in the exemption.

MR. LAZARUS: Sure. And as you note, this was part of a -- sort of a negotiated way --

MR. DAMLE: That's what I --

MR. LAZARUS: -- to get TracFone to --

MR. DAMLE: Yes.

MR. LAZARUS: -- to not be opposed in this proceeding.

I mean, I think most wireless carriers, for the most part, are actually able to tell whether or not a phone has been stolen before they reactivate it on their network. I know some of the carriers are able to do that.

So, again, it was part of the negotiated settlement, and we didn't view it as -- again, if you're looking at some of TracFone's concerns, you know, theft is one of their main concerns. So...

MR. DAMLE: Okay. And go back to the sort of subsequent owner point. You can imagine a scenario -- again, going back to eBay -- where an innocent purchaser buys a -- buys a cell phone from eBay or one of ISRI's members -- you know, Gazelle or something.

MR. LAZARUS: Sure.

MR. DAMLE: Gets a cell phone and doesn't know whether it's been stolen or not.

MR. LAZARUS: Mm-hmm.

MR. DAMLE: So do you have the same position with respect to that situation?

MR. LAZARUS: CCA does, yes.

MR. DAMLE: And do you know if TracFone --

MR. LAZARUS: I don't think I'm in a position to speak for TracFone.

MR. DAMLE: Okay. All right. And then, again, the same thing with respect to the specification that it's for -- that it not be for "any unlawful purpose."

Can you give me a sense of sort of what the unlawful purposes are? Is it, again, just criminal trafficking of --

MR. LAZARUS: That's exactly right.

MR. DAMLE: Okay.

MR. LAZARUS: Again, trying to fit a negotiated settlement that -- or a negotiated proposal that would fit what CCA was looking for and try to resolve some of TracFone's concerns in this proceeding. And the idea that it would be for unlawful purpose, I think, might have come from their original proposal as well.

MR. DAMLE: Okay. And is it your view that the proposal, as you've drafted it, is meant to cover bulk unlocking of used cell phones? Is that something that you've -- of used cell phones, not new ones.

MR. LAZARUS: I think, if you look at it as drafted, I don't think the language difference, if you look at -- you know, what we were concerned about was -- again, sort of the contract principle of, okay, you buy a cell phone from one of our members, you know, them trying to break their contract. That's not what seems to be going on with the formulation that ISRI is looking for.

MR. DAMLE: Right.

MR. LAZARUS: So I don't think there's that much disagreement between the two. And I don't think we were trying to get at stopping what I would call legalized bulk unlocking.

MR. DAMLE: Right. Okay. All right. That's helpful.

MS. CHARLESWORTH: Mr. Slover?

MR. SLOVER: Yes. I just wanted to clarify that the point that Mr. Lazarus has brought up and that your colloquy engaged in, the difference between the original owner of the phone who got it in connection with the contract with the carrier and subsequent owners who don't have a clear knowledge -- a firsthand knowledge of how the phone was originally acquired, I think, is very important.

That was not clear to us as we read any of the proposals. If that's clarified, that takes care of, from our perspective, a big part of our concern, which was how are you -- how is the consumer who acquires this from eBay or even a bulk unlocker going to know the provenance of the phone, tracing it all the way back to its origin.

So I think that would be very helpful.

We detailed in the statement that I was going to give and that I didn't finish some of the things that we saw as preferential in our proposal to the others. And one of them was about the problems of proof that would be required of a consumer, particularly one of the subsequent consumers.

With your permission, I'd like to offer it in writing after the proceeding just so that you can see what I would have said. And then, if we have a chance to follow up on that, if you're taking additional written statements, we'd expand on that.

MS. CHARLESWORTH: Well, I think -- we hadn't planned on another full round of comments.

Are you saying -- what is it -- is there something you want to share with us here in terms of what you would have said?

MR. SLOVER: Well, in a nutshell --

MS. CHARLESWORTH: Because, to be honest, I mean, you know, when -- you know, we'd have to reopen -- you know, and in limited cases, we may ask targeted questions. So I won't rule out the possibility we would ask a limited question afterwards that would address some of these issues.

But I think if you have something to say on that issue, I would recommend that you say it now.

MR. SLOVER: Okay. Well, this is -- I will.

This is the first that we are hearing about the possibility of distinguishing between the consumers and how they would be affected.

We'd hope to have a chance to consider that more fully. It sounds like a promising idea, but it's hard to do that on the fly.

But the main thing that I wanted to -- that was in my earlier statement that I'd like to say is that the proof requirements of, you know, whether a phone is going to be used for an unlawful purpose -- you know, how is an ordinary consumer going to know what's lawful and what's unlawful?

You know, it's -- the way that it's written, it says "including abusing a subsidy," but it's -- you know, including but not limited to.

So it could be anything. And so that's why we think the cleaner proposal, like we've done or like ISRI has done, is superior to one that loads up too many conditions which really turn into proof requirements for an ordinary consumer to be comfortable that they're complying with the law.

MS. CHARLESWORTH: Okay. Mr. Weissenberg?

MR. WEISSENBERG: Just one quick comment. ISRI agrees with Mr. Lazarus and Mr. Slover that the responsibility for those subsidies should lie with the original owner.

But to the extent that the Copyright Office adopts another definition that we propose, we just ask that they make it very explicitly clear that it applies to lawful bulk recyclers like us, so -- to leave out any ambiguity.

Thank you.

MS. CHARLESWORTH: Okay. Do we have any further questions?

Mr. Cheney?

MS. CHENEY: Yes. We haven't talked about the sort of mail-order phones that are available sort of through secondary -- not directly from carriers, such as Overstock and others that you can go onto their website and you can purchase -- you can select it from different carriers.

Is that covered as well under what you've proposed in these possible exemptions where they might get the phone and then you have to call after you receive it to actually connect to the -- to activate and you're not activated -- the phone is not activated when you receive it in the mail, but it's activated once you call and activate it after you've received it.

Is this covered in this situation?

MR. LAZARUS: Yes. I would think -- I think it's covered by our formulation. I think the idea -- just use Amazon as an example. You can buy an unlocked phone through Amazon or you can buy a locked phone through Amazon tied to a particular wireless network.

MS. CHENEY: Right.

MR. LAZARUS: And so it's whatever choice you would make. But I think that would be covered by our formulation.

MS. CHENEY: Is it covered by Consumer Union?

MR. SLOVER: It would be covered by ours because ours extends the protection to the owner of the device.

MS. CHARLESWORTH: Does that answer your question, Ms. Cheney?

MS. CHENEY: Yeah.

MS. CHARLESWORTH: Mr. Damle?

MR. DAMLE: So I just wanted to clarify something about the tablet unlocking proposals and that -- that those -- I just want to be clear whether or not your proposals would limit those to also used tablets, not new tablets.

Is there an issue -- like, is that -- I assume the answer is yes, but --

MS. CHARLESWORTH: So you'd treat them in the parallel fashion?

MR. DAMLE: Right.

MR. DAMLE: Mr. -- we're getting nods. So, Mr. Weissenberg, do you want to speak on behalf of ISRI?

MR. WEISSENBERG: Yes. ISRI is -- we're seeking an exemption for used devices. That's correct.

MS. CHARLESWORTH: Okay.

MR. WEISSENBERG: Yes.

MR. DAMLE: And Mr. Lazarus?

MR. LAZARUS: Yes. We would be fine

with this applying to both.

MR. DAMLE: And Mr. Slover?

MR. SLOVER: We do want the same exemption to apply to all devices that fit within the same function. And we would hope that you would consider the one situation that we described where we think there should be the option for either if the market already is there or the market were to evolve so that the consumer has the choice to pass along the new phone.

MS. CHARLESWORTH: Right. But -- I'm sorry. But just again, I mean, I think -- I'm not aware that any carriers would, under that scenario, let you walk out of the showroom with a subsidized phone that they hadn't activated. Are you?

MR. SLOVER: Well, one of the -- no, I'm not. But one of the problems with the exemption in the past is that it has rigidified the business models and discouraged competition and innovation in the way that phones are being offered.

And so we think that the less restrictions that are imposed on the exemption now, the more it allows for the market to evolve competitively and for there to be more choices for consumers.

MS. CHARLESWORTH: Okay. Thank you. Okay. Mr. Riley?

MR. RILEY: I have a question for Consumers Union.

Mr. Slover, earlier you stated that you advocated before Congress to draft an exemption that did not include that "used" language. Yet Congress, when they introduced the Unlocking Consumer Choice in Wireless Competition Act, did revert to the earlier exemption that did have that "used" language.

How are we to treat that? Is that Congress's intent, or do you have some other explanation as to why they rejected your advocacy on that issue?

MR. SLOVER: Well, my familiarity -- and I was working pretty closely with the people on both the House and the Senate side -- but what they wanted to do was to reinstate the 2010 exemption as it was. And they were loathe to step into the position of dictating changes, particularly for an interim period.

The one exception that they made was owner of the device versus the owner of the copy of the software.

So I don't think it's a pronouncement necessarily that it should be that way because they left it open to the Librarian to decide whether to extend the exemption, you know, in the next triennial proceeding rather than dictating that it should be.

MS. CHARLESWORTH: Okay. Thank you.

We all happy?

So do we get out of school early? Yes.

Thank you, everyone, for attending and commenting on the unlocking exemptions.

We're going to wrap up for today. For those of you who come back tomorrow, I think we start again at 9:00 a.m. Is that correct? And tomorrow with proposed class 1, which is audiovisual work.

So thank you again, and we look forward to seeing some of you tomorrow.

(Whereupon, at 2:46 p.m., the 1201
Rulemaking Process Public
Roundtable was concluded.)

CERTIFICATE OF NOTARY PUBLIC

I, CHRISTINE ALLEN, the officer before whom the foregoing deposition was taken, do hereby certify that the witness whose testimony appears in the foregoing deposition was duly sworn by me; that the testimony of said witness was recorded by me and thereafter reduced to typewriting under my direction; that said deposition is a true record of the testimony given by said witness; that I am neither counsel for, related to, nor employed by any of the parties to the action in which this deposition was taken; and, further, that I am not a relative or employee of any counsel or attorney employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Christine E. Allen

DISTRICT OF COLUMBIA

____
CHRISTINE ALLEN
Notary Public in and for the
DISTRICT OF COLUMBIA

My commission expires:

Notary Registration No.:

CERTIFICATE OF TRANSCRIBER

I, JANE MOLARO, do hereby certify that this transcript was prepared from audio to the best of my ability. I am neither counsel for, nor party to this action nor am I interested in the outcome of this action.

Jane T Molar

____
June 5, 2015

____
JANE MOLARO

Page 21

Page 26

Page 42

Page 45

Page 48