FIFTH PUBLIC MEETING
OF THE
MULTISTAKEHOLDER FORUM ON
IMPROVING THE OPERATION OF THE NOTICE AND TAKEDOWN SYSTEM

OCTOBER 28, 2014
9:06 A.M. TO 11:53 A.M.
UC BERKELEY SCHOOL OF LAW, BOALT HALL
BOOTH AUDITORIUM
215 BANCROFT WAY, BERKELEY, CA 94720

REPORTER'S TRANSCRIPT OF PROCEEDINGS

REPORTED BY ANGELICA R. GUTIERREZ
CSR #13292
MS. PERLMUTTER: So good morning, everyone.

For anyone who hasn't been here at our prior meetings, I'm Shira Perlmutter, the chief policy officer at the U.S. Patent and Trademark Office. I wanted to begin by welcoming all of you here in person and also all of you attending by webcast to this public meeting of the multistakeholder forum on the operation of the DMCA notice and takedown system.

This is our fifth public meeting and we have been alternating between PTO headquarters in Alexandria and Northern California. And I particularly wanted to say how grateful we are to Berkeley's law school for again generously hosting us at our meeting today. This has been a very fruitful partnership for us over the course of the year as we work on our various Green Paper events.

So let me just say a few words on the path of this process and where we are now at the end of October. So as you all know, the genesis of this multistakeholder forum was the Green Paper on copyright, creativity and innovation and digital economy that the Department of Commerce issued last year. And we kicked off the forum with an initial public meeting in March, many of you were there, and began quite early with a consensus that we should start
by focusing on the issue of standardization in the notice and takedown process.

Then at the next meeting in May, the working group was formed, a smaller, somewhat smaller working group with a very impressive level of interest and a very impressive level of participation from all sides. And that working group has met regularly between sessions of the full multistakeholder forum. We understand that the discussions there have continued as they started being very positive and very productive and we hear that the participants feel that the discussions have really increased the level of mutual understanding of each other's concerns and perspectives.

So the working group has been reporting to the plenary, to the full forum, at each of our meetings and this enable us to have complete transparency as this is webcast and lets the general public follow what's happening. And, of course, many of you in this room are participating yourselves in the working group so you're very involved in its activities.

Now, as we understand what's been happening in the working group, the discussions have gone down a number of paths and have evolved and at this point include some issues and approaches other than
standardization or going beyond standardization. And when the co-chairs of the working group Jim Halpert Sandra Aistars report to us later on, I believe and hope we will hear that we're making progress, that agreement is getting closer on at least some elements and hopefully we'll be able to produce a useful document of some sort by the end of the year.

We are also going to hear at today's meeting from Brianna Schofield an update on the methodology and progress of the takedown project that's underway here at Berkeley. And that will give everyone an opportunity both to understand what the project is doing and to have an opportunity to ask any questions we may have about how that work might inform our thinking here.

And, finally, we will also hear from a panel discussing their experience with trusted sender programs for sending notices. So we'll hear a bit about how these programs have been structured and how they work and he hope that these insights can take us forward in thinking about how individuals and small and medium-sized enterprises might be able to make use of these types of programs and improve their experience with the notice and takedown system.

And the last item, although not in time on the
agenda, we will discuss a little bit about what the
next steps might be, what will happen in December which
will be the last meeting of this calendar year, and
also give some idea, because I've had questions about
this, of exactly how the work of this forum, the
multistakeholder forum, relates to the other work
streams that we're pursuing under the Green Paper and
where we expect to go with each of them.

So let me just close with announcing we're
changing the agenda a bit to accommodate people's
travel schedules and so what we will do is start with
Brianna talking about the takedown project and then we
will move to Jim and Sandra's report on where the
working group project stands. And then I will talk a
bit about the next steps and the rest of the Green
Paper work before we turn to the panel as the last item
on the agenda.

So thank you very much and I'll now turn it
over to my colleague John Morris from NTIA.

MR. MORRIS: Thank you, Shira. I don't really
have much to add other than words of welcome and
appreciation for all the work that has been done and it
does sound like we've made some important progress on
what we -- what the stakeholders have bitten off first
and Shira and all of us are trying to think through and
1 think through with you how best to proceed and move
2 this whole effort forward into next year. So that's
3 something that we'll be talking with you about later
today. And so look forward to this session and thank
you very much.

MS. PERLMUTTER: Thank you. Do you need us to
move so that the slides are --

MS. SCHOFIELD: Thank you. Thanks to the
USPTO and NTIA for bringing this group together, to Jim
and Sandra for their leadership in this process. And I
know that there's been some tireless effort going on in
both the working group and the drafting group. So I
wanted to express my appreciation for that.

My name is Brianna Schofield and I'm a
research and policy fellow here at Berkeley law where I
study issues related to intersection of law and
technology. In this role one of my main projects is
studying the notice and takedown system and analyzing
how it's working in practice. So I'm pleased to be
here today to give you an overview of where we're at in
our research.

As you all know, Section 512 provides a
collaborative framework. So it provides a framework
for copyright owners to remove infringing content
online and it identifies responsibilities for online
service providers and protections for users.
There's -- as you all know, there's some questions about how this is actually working in practice and how this balance is playing out and whether it is striking the right balance currently between copyright protection and freedom of expression on the internet.

Sorry, this is -- so these questions are central to a lot of discussion about 512 that's going on now including the discussion that's happening in this room. But despite these questions, there's very little empirical evidence out there that is understanding how notice and takedown is operating in practice. So the takedown project is undertaking research that aims to update the -- some of the existing research that's out there and to provide impartial empirical data to inform conversations such as the one you're having here.

So the takedown project is led by Jennifer Urban here at UC Berkeley and Joe Karaganis at the American Assembly at Columbia University. The foundational work in this area was actually done by Jennifer Urban. She did a study in 2006 studying takedown notices submitted to Chilling Effects up through 2006. At that time there were about 900 takedown notices. So the situation and the landscape has changed dramatically since then, not least of which of the
reasons is because of the number of notices that are being exchanged at this time. If you're not aware, you should also look at recent research by Daniel Seng. Professor Seng did a study that was released last year that studied takedown notices and the Chilling Effects database through 2012. At that time there was about a half a million notices.

So the online landscape looks a lot different than it did back when some of the earlier studies were done. So we're taking -- we have a two-pronged approach to our project. The first is an analysis of machine and hand-coded notices. And the second is an in-depth survey and interview series with all the parties involved including online service providers and rights holders about their internal practices for handling notices.

Before I move on, I do want to note that this is a part of a broader research network that we've brought together. We've brought together researchers from around the world who are looking into notice and takedown issues. So we did this for a couple of reasons. The first is that there needs be a worldwide understanding of takedown, especially as 512 has been replicated informally and formally around the world to deal with issues online not limited to copyright,
notably notice and takedown is being replicated for things like privacy issues, informally for trademark issues and the like.

The second reason we felt that there was a need for a worldwide group is just that the lack of empirical data is too big of an issue for any one particular group of researchers to get their heads around. So we're working collaboratively with these researchers. We have researchers at the Haifa Center of Law and Technology in Israel, for example, at the Institute for Information Law in Amsterdam. Closer to home folks at Harvard and Stanford are looking into this and many more.

If you are interested in this, I do suggest that you do take a look at the website takedownproject.org which is listed on this slide. You'll see a list of our affiliated researchers, blurbs about their particular research interest and links to a lot of articles that have been published in this area.

So I've mentioned a couple of times that there's a lack of research and the lack of empirical data in this area. So you might reasonably ask why is this. It's -- there's two main reasons, and the first is that notice and takedown essentially involves a series of private communications. So notices and
counter-notices are not public documents by default. A handful of online service providers, as you know, do contribute their notices to the Chilling Effects database. But this is an online repository for takedown notices. But this transparency is not required and the number of online service providers that actually contribute their takedown notices are actually quite few.

The second is that notice and takedown involves non-public actions. So the decision making on all sides is not transparent. As far as I know, no online service provider publishes detailed information about the processes that they use for receiving notices and for analyzing those notices and what resulting actions that they take. On the same side, rights holders and rights enforcement services don't publish detailed information about the information that they use to detect infringement online and what decisions that they make when they're sending notices.

So because of the lack of transparency in these two areas, it's actually hard for researchers to really get below the surface and understand what's going on. So despite these challenges, we have -- this is the first part of our project. We have built a massive database with a large number of notices which
we're examining in detail. This is the quantitative portion of our research. We've built on the works that Chilling Effects has done. We've ingested six months of data from the Chilling Effects clearinghouse into our own database and we're machine and hand coding these notices.

So the profile of the database you can see here, six months of data from a chunk of time in 2013. The largest submitter by far to the Chilling Effects database is Google, predominantly for Google search notices, although there are a number of other services that -- of Google services in the databases including blogger and image search and others. There's a handful of other submitters including Twitter and a small group of other online service providers that report to Chilling Effects.

The six month period of data has about 300,000 notices in it. Those notices, because they may include more than one request, include about 108 million targeted items to be taken down. So 108 million what we call allegedly infringing materials. And those represent about 11 million unique allegedly infringed works.

So on top of the database we've built a coding engine to help analyze this data and we've trained a
team of research assistants to input information about these takedown requests. So when a coder logs into the system, they see this basic interface and the randomization engine picks one of the allegedly infringing materials identified in the notice, typically identified by a URL.

The random selection method is actually different at the URL level rather than the notice level as a whole. This is a methodology decision that we made early on because any particular notice might contain thousands of links. So we're just analyzing one specific request within that notice. That notice could then be reselected if another link comes up from that notice through the randomization engine, there could be further coding that's done on another alleged infringement within that notice.

So the coder sees this basic format. There's the coding pane on the left-hand side and on the right-hand side is the text of the original notice.

Okay. So we're focusing in here on the coding pane. This is where the coder inputs information. So there's over 700 potential inputs for each coding. So this includes collecting information in the following steps. So the first step, the coder is recording information about the notice as a whole. So this is
information about who's sending the notice, who is the
recipient of the notice. In includes information about
asking whether there's -- the notice includes the
statutory required statements, the number of links in
the notice and so on. It also includes information --
sorry the next step is information about the allegedly
infringed work. So this is the underlying copyrighted
work at issue.

Here the coder collects information and
records information about what that work is, what
category of work it is, how it's been identified in the
notice. Information about who the copyright owner is
and so on. So then they move on to step three which is
information about the allegedly infringing material.
So this is the targeted material that's being requested
to be removed.

So, again, they record information here about
what that is, how it's been identified, how much of the
allegedly infringing work appears to be copied and how
it's being used in that setting.

Then they move on and record information about
the site at which the material resides. And finally
they submit the notice and there they are given an
opportunity to sort of free form flag any interesting
issues that have cropped up in that particular coding.
So as I said, there's over 700 inputs in the course of this. That's taking our research assistants probably on average about 15 minutes to really look in detain and gather the information that they need for each particular alleged infringement that they are looking at. Some of them do take a lot longer and some of them take a little less time, but on average about 15 minutes.

Not all of those 700 inputs are use each time and some of them are actually auto populated by machine reading. Some of them require them just to look at the text of the notice which is in the interface, and some of them require them to do a little bit of outside research. For example, clicking on the link and looking at where the allegedly infringing material is.

Okay. So with this, the coding engine is designed to identify how the system is working. When we're able to release results of this, this should be able to give a good idea as to how and under what conditions takedown notices are being used as intended and correctly identifying infringing content and therefore how well the system is working to that aim.

It will also identify and quantify potential deficiencies in the system or in particular notices such as whether they provide adequate information for
an online service provider to identify or to locate the allegedly infringing material. It will also unearth claims that do not appear to be copyright claims. So as I discussed earlier, claims that might be privacy or trademark claims and the like. And we also have information that we're collecting in there which will allow us to surface alleged infringements that appear to have a strong fair use defense.

Okay. So this is the quantitative portion of our research. Where we're at now is that we've coded about two and a half thousand of these. We've started with the main population, everything that's in the Chilling Effects database. And we now are moving on to starting to build out separate tranches. So we're looking at, you know, the main population, as I said earlier, is largely Google search. So we're looking at building out separate tranches with different -- seeing if there's different characteristics for other tranches.

That might be interesting, for example, we're looking at just Google image search, we're hoping to build out a tranche that's based on characteristics of the sender. So perhaps a sender that doesn't send many notices, perhaps a sender that's only sent one or two notices within that six-month period, to see if there's
anything that is particular to different tranches of data.

So we're also in parallel with the coding now starting to try to build up a query engine and develop the questions that we're asking of this data. We are in the process of doing that now, I hope. I know everybody is eager for results from this and, believe me, I am too. We're hoping to have some results in the next few months.

To the extent that there are any online service providers in the room that don't report to Chilling Effects but may be willing to speak with me a little further, perhaps after, contact me later about sharing takedown notices with this project under these situations, we'd really love to hear from you, so please do reach out.

Okay. The second part of our research is the qualitative portion and to notice and takedown practices. So for this part of our research we have conducted extensive surveys and interviews of a lot of parties involved in the system. We have interviewed online service providers and rights holders and some trade associations and rights enforcement services. We have tried to cover a wide range of these, both small and large and those covering different markets and
different types of services offered.

We do another ask that I'll make of the room as we do have a dearth of small senders. So if anybody in this room would like to reach out to me further about ideas for approaching folks who maybe don't send a lot of notices or have a lot of interaction with the system on a regular basis, I would love to hear from them.

So here again we are working on writing up our results. I don't have anything that I can share with you today about what we're finding, but we're going through, we're analyzing, we're sorting, we're trying to figure out what we can offer to this conversation. Again, I hope that there will be something that we can offer here in the next few months.

Okay. So I will open it up to questions or comments now and I'm very interested to hear your feedback and where we might be able to add value to your conversations or any particular areas of research that you think would be valuable. And also my e-mail address is up here. Please feel free to contact me afterwards and I would be happy to discuss anything with you further.

Thank you.
MS. PERLMUTTER: Any questions?

MS. AISTARS: It's Sandra Aistars, Copyright Alliance. I have a question in terms of the types of analysis that you asked the research assistants to do, particularly when you're trying to analyze, say, whether something has a legitimate fair use defense associated with it, what types of questions are they looking at, because, you know, it's a fairly subjective legal analysis on which reasonable minds can disagree. So I'm wondering whether that's something that you have disclosed in the study.

MS. SCHOFIELD: Absolutely. When we write it up you'll have exposure to all the questions that we have asked. So it's a really good question and it's a really big challenge, Sandra, and what we've tried to do is we first of all tried to strip out as much judgment as we can so we're not asking is something -- does this look like it's a possible fair use. Instead we're asking questions like can you estimate the amount copied and they will say either, you know, 100 percent or, you know, they have variations, for example, for the amount copied.

And they are not asked specifically what we would consider like the analysis of fair use, instead they are asked to tag things about the material. So
they are asked to tag if, for example, the item appears to be contextualized with text and with surrounding information or they're asked questions like -- I'm trying to think of some good examples for you. I can't think of many off the top of my head, but it's actually breaking down the four factors and trying to get at situational characteristics that would unearth that sort of question as to whether there might be a fair use defense going on. And I can share some of those with you further.

MR. OLIAR: I'm Dotan Oliar from the University of Virginia. I was just curious, in one of your last slides you had the list of people you were talking to and analyzing and I was wondering if you are also interviewing end users and whether you're analyzing also counter-notices because they are also a target audience for those takedown notices.

MS. SCHOFIELD: Yeah, that's also a good question. So we have decided not to -- in the interview series we're not interviewing end users. It's just a category that is too wide and varied for us to really wrap our hands around and to be able to say anything about from a research perspective. So that part of the research is really examining the practices of those that are taking action within the system.
1 On the other side for the coding engine
2 portion of it, we're actually looking at
3 counter-notices there. As you probably know, they're
4 few and far between. So there's actually not very many
5 of them within the Chilling Effects database, but we
6 are looking at those.

7 MR. OLIAR: Just for a quick-follow up, so
8 maybe you could talk instead of individual users which
9 maybe is a large group, representative organizations,
10 NGOs that represent users or care about users may have a
11 good idea of what users' concerns are. And I have no
12 doubt that the number of people sending counter-notices
13 is a very small fraction of people receiving notices.
14 But still, these are the people, you know, we at least
15 care about - right? maybe the system does have some false
16 positive. But at least if we can minimize the people who
17 are unjustly hurt by the system who may not have the
18 legal knowledge or the time or may be scared and, you
19 know, may just, you know, let it go though they think
20 they may have good reasons, if we can minimize those, I
21 think that will be a good thing.

22 MS. SCHOFIELD: Absolutely. I think the idea
23 of talking to representative organizations is a good
24 idea. You know, we're also hearing issues that get at
25 this aim from both rights holders and the online
service providers who do interact with users and do
have an idea of what's going on. But I think that I
will - I'm making note of your point to talk to
organizations representing users as well, I think
that's a good idea.

MS. SEIDLER: My name is Ellen Seidler. I
have a concern about using the Chilling Effects
database as being representative of takedown notices in
general. As an independent film maker, I have sent
thousands of upon thousands of takedown notices and
only a small percentage of those have gone to Google.
So you're missing out. I know it's the only database
out there so you're sort of limited with regard to
that, but I think it's an important caveat that the
Chilling Effects database is a very limited subsection
of the millions upon millions of DMCA notices that are
sent out.

MS. SCHOFIELD: Thanks, Ellen. I absolutely
agree with that and, you know, like I mentioned, if
there's any other groups of people including senders in
the room who would be willing to discuss sharing
notices, we would be very happy to build out -- this is
part of the idea behind building out separate tranches
so that we're not swamped by what's predominantly
Google search data. But as you also mentioned, it's
what we have and it's where we're able to start because it's the data that's available.

EAST BAY RAY: I'm East Bay Ray from the Independent band Dead Kennedys. I was wondering, you said this is supposed to be a neutral study. Why is this database called Chilling Effects?

MS. SCHOFIELD: I'm sorry, I don't have any -- I had nothing to do with naming the database.

EAST BAY RAY: You don't know why then?

MS. SCHOFIELD: I cannot speculate why.

EAST BAY RAY: When did you first look at it?

MS. SCHOFIELD: When did I first look at it, probably about a year and a half ago when I embarked on this research.

EAST BAY RAY: They changed their "About," but I have a screen shot which I didn't know I had to bring. I'll have to look at the date on it. The reason it's called Chilling Effects because they were alleging, the law centers and the EFF, that people sending takedown notices were chilling free speech. And that's why it's called Chilling Effects. And my band is on there when I'm still -- you know, I was chilling free speech when it's had the different thing on it. And to me it's very 1984 that it's called Chilling Effects. I'm a legitimate copyright owner. I was put
on there as an example of chilling free speech and now they've changed what they are about so people don't know, like you, but it's still called Chilling Effects. That would be like studying black people and calling them negroes. And you're clueless to why it's called Chilling Effects.

MS. SCHOFIELD: I appreciate your point of view. It's not something that's actually within the scope or control of my research. Ours is called the coding engine, so I hope that's sufficiently neutral.

EAST BAY RAY: What I'm trying demonstrate is bias because the whole principle of safe harbor is supposed to be based on neutrality. And when there's bias, then the whole concept of safe harbor gets a little wobbly. Thank you.

MS. PERLMUTTER: I would urge seconding Brianna's suggestion that anyone who has data, whether it's rights holders who are sending notices or ISPs that are receiving them, provide them to the project to the extent that's possible because obviously as Brianna said, the broader the scope of the data they can look at, the more valuable the results will be. So certainly add my suggestion to that.

Let me suggest that we move on and we will now go to the report of the working group from Sandra
1 Aistars and Jim Halpert.
2
3 MR. HALPERT: Well, we apologize for this. We probably should describe the state of play here and then we hope to be able to show you just representative snapshot of what the text looks like at this moment. But I think we'd just better start, I don't see any other -- given the time constraint, I don't see any other way to do it.

4 MS. AISTARS: There's a document that was we circulated to the working group list this morning by Rebecca Jones from my office that I think everyone who's in the meeting room from the working group should have. And that same document was made available to the USPTO at the same time and as we did after the last plenary session, we'll just do a quick scrub of it to make sure it doesn't have, you know, typos or errors or missing pages or something crazy like that. And then USPTO can post that to their website as they did after the last plenary session so that those who are watching on the webcast, those who aren't on the web distribution list for the working group all have a copy of where things stand and what the state of play currently is.

5 If we get it in a way that we can display it on screen, that will be great but otherwise we'll just
walk through and describe the provisions that we're working on right now. When you do see the document, what you will see is a document that is largely clean text and there are certain areas that are bracketed that are still under discussion. There are also areas that are highlighted in yellow. Those yellow areas represent the sections where we had the most active discussion in yesterday's working group meeting.

And so those are areas where we were doing active drafting on the fly where we were capturing the group's discussions. But the group itself has not had a chance to review either Jim's or my notes on the topic. So those are truly active sections of the document. But the entire document as a whole is a discussion draft and once we get through this whole process and we've got a solid draft that has everything in it, we'll still need to do a scrub and make sure that everything works the way it's supposed to work and that there aren't any unattended issues in the document. So you should consider the entire document as, you know, as a discussion draft still being, you know, still being negotiated by the parties.

But I think at this point in time is fairly complete, represents all the areas that we're discussing and represents I think a lot of forward
progress since the last time we met and there were just big empty chunks in a lot of the sections that we were talking about, so...

MR. HALPERT: There's a lot of progress in flushing out issues. So if you read through this document, whereas there were gaping holes as of the September 10th meeting at the Patent and Trademark Office, now there's at least text with a few highlighted, yellow highlighted gaps where we may try to insert new concepts.

But we basically have been all the way through the document with I think three sets of drafting group meetings between September 10 and today and a working group meeting yesterday afternoon, which many of the people in this room attended, and as a result of that I think most -- almost all the issues have been aired and people are working constructively to find middle ground to address them. And the -- if we are able to continue at this pace, we should have a draft to go out for comment in the -- certainly by December that has been, you know, reviewed thoroughly so that it's consistent and we have ironed out the language, ideally simplified language from what you see now because negotiated texts tend to be a little overwritten but.

With that we hope to be able to report at the
next meeting with a draft that then the public can
review and comment on and that the full participants in
these plenary meetings, anybody should -- who's
interested should attend or should connect in by phone
and you should have by the next meeting, I'm hopeful,
the opportunity to review a full text and we look
forward to comment on that when it's ready for comment.

MS. AISTARS: Right. So let's just walk
through, the form of the document remains as it was.
We've set out several categories of practices, good
practices, bad practices and situational practices and
those are identified both for people who send notices
and people who receive notices. And in terms of people
who receive notices in various respects they are broken
into practices that apply to service providers who work
using web forums versus service providers who work
using e-mail to receive notices because some of the
practices will vary.

So, Jim, why don't you start and while Jim
will walk through the areas that apply to service
providers and I'll walk through the ones that apply to
notice senders. And we're happy to take any comments
on things that might not be clear.

MR. HALPERT: So the first of the good
practice is to make -- for service providers is to make
the DMCA takedown notice and counter-notice mechanisms
easy to find and easy to understand so that both
notifiers don't have to hunt or go -- aren't burdened
trying to find the material, the same thing for
counter-notifiers. And also the process is described
in a way that it's easy to use and there are a series
of examples. And typically the way we've been resolving
these good practices is to provide a list of such as's
that provide examples of ways to accomplish the goal
that are not exclusive but that give guidance to
review -- to readers who are not well versed in this
process and are coming to it for the first time. Some
concrete ideas about how they might accomplish the good
practice.

The second transparency element here is to
provide clear plain English explanations consistent
with the DMCA requirements of who can submit a notice,
what information should be submitted to comply with
DMCA requirements and what additional information can
facilitate the removal of alleged infringing content.
Later in the document we describe when requesting
additional information beyond the DMCA requirements, it
can be an appropriate process and some considerations
of where that could be inappropriate requesting a lot
of additional information that's not required. But
here we just flag that as a good practice.

We also talk about implementing processes for receiving notices that are commensurate with the level of good faith claims of instances of infringement -- this language has been changed a little bit overnight and we haven't vetted the language completely -- sought to be submitted by rights owners. So the idea is to make it easier for rights owners to submit information including multiple URLs being submitted at one time, use of e-mail or use of a web form that can accommodate multiple URLs, or through uploading text files and then offering, where appropriate, we go into this again in the contextual practices at the end, methods for submitting larger volumes of notices. And those -- that's something that we will touch on later.

And then also having -- there's a suggestion that additional efficiency may be achieved by establishing a standard document structure for e-mail or for uploaded text files so that the information can be submitted in a regular way by notifiers and it's also easier for the service provider to handle as the service provider reviews the submissions.

MS. AISTARS: It's worth noting that we have had discussions within the working group and the drafting group early on to explore what those sorts of
examples of, you know, standardized document structures or e-mail structures might look like and that's something we may return to and revisit to offer up as examples or appendixes to the documents so that people don't have to figure it out for themselves.

MR. HALPERT: And this would be a task to turn to after we get the good and bad practices document out for comment. The idea behind this would be not to prescribe a specific form that should be used but to offer a sample that -- or a series of samples that different rights owners and service providers might want to refer to as the develop their own or might just want to pick up and use themselves.

And then there's also a recommendation for compliant notices, notices that meet the DMCA requirements to provide a confirmation of receipt of a notice or a counter-notice that includes a method to identify the notice or counter-notice in further communications. The concern had been that notices would sometimes go into some black box and there would be no way to refer back to it to find out what had happened to the notice. And here there are examples of a copy of a completed web form or a confirming e-mail saying what had happened in response to the notice.

A fifth good practice is explaining to
submitters that DMCA notices and counter-notices are only accepted for copyright infringement claims, where applicable, and that there are legal sanctions that apply for some knowing and material misrepresentations in DMCA notices. This is to discourage the submission of irrelevant or noncompliant notices that can clog the practice -- clog and slow down process.

Then there is a bracketed item that was just raised, this was a suggestion from an AT&T lawyer who commented on this, that there should be some good practice with regard to reinstating in a timely fashion material that was improperly or inaccurately identified as infringing in DMCA notice and as to which a counter-notice was submitted. So that's sort of a replacing back online good practice.

We then are looking for any suggestion, this is -- these are just general good practices for service providers with regard to notice and takedown. And we're asking if there are -- and you'll see in the document and highlighted in yellow whether there are suggestions for syntax for e-mails or sample e-mails that would make processing e-mail notices more -- easier both for notifiers and for recipients. So if there are service providers out there that handle a lot of e-mail notices, you guys may want to suggest and
I would appreciate receiving suggestions on good practices in that regard.

Then for web form submission, which a number of service providers use as a way to increase efficient internal processing of submissions, all the same good general practices would apply as to service providers. And then the further good practice specific to web forms are to have clearly labeled fields marking which information is mandatory because required by the DMCA and which fields are requested to enable better processing of the notice.

Another is to provide sample text or help buttons and instructions to help explain what information is being requested so that the notifier, particularly smaller notifiers, understand what this is and what they are being asked to do.

And then the -- there is a further suggestion to employ industry standard features that promote efficient submission of forms such as avoiding server-side settings that disable auto complete features that -- and employing practices similar to those used for online sales transactions as a standard matter wherever possible to retain properly entered data so that the notifier doesn't have to go retype information multiple times. And the idea is here to
promote efficient submission on the notifier's side but using practices that are common for internet sites generally and e-commerce in particular which typically have -- for purchases have people filling out forms.

A fifth recommended -- or web form good practice or fourth I should say because there's the one catch-all for all the other good practices that are just generally applicable, is to explain why a notice or counter-notice submission is rejected to allow the sender to efficiently correct the submission and resubmit.

There has been on the service provider side concern about junk providers of very, very large numbers of notices who know what they are doing, and I think we'll need to qualify this a little bit to say, look, if there's a noncompliant notice, it's good to go out the first time and say correct this, but that may not be necessary or appropriate where the sender knows perfectly well that they are not complying with the, say the mandatory elements of the notice and the duty to respond to that, to willfully inaccurate notice sender, may be an inefficient waste of time. But the idea is for submitters who are acting in good faith, notifiers, to tell them why their notice was rejected so they can fix it.
And then the further good practice is well, having these efficient intake processes also to implement reasonable measures to deter fraudulent, erroneous or abusive submissions which are a source of significant inefficiency.

So that's the list. I don't know if anybody has any comments on further good practices for service providers with regard to receipt of notices, but this is the list that we have come up with. Feel free to e-mail me and Sandra and anyone else with suggestions of other good practices. These are the ones that the group has worked through and is pretty close as a drafting group matter to having language to share publically. There are parts of the draft that need more work.

Any comments thus far?

Sandra, do you want to take over good practices for notice senders?

MS. AISTARS: Sure. Just to give context, both on how the good practices for the notice recipients and good practice for notice senders came about, a lot of this reflects discussion amongst the group participants about what is going on in the marketplace that works, what are the good practices that the members of the online service provider
community are already employing, why are they employing these sorts of good practices. And so the list that Jim reflects to you reflects a lot of things that members of the working group, you know, felt important to include as good practices because it's something that they feel provides for efficiency in receiving notices from notice senders.

And similarly the good general practices for notice senders also reflect things that notice senders are doing generally in the marketplace to comply with obligations that are imposed upon them and to ensure that they are living up to the requirements of the DMCA and that they're sending good notices. The idea amongst all of the working group participants is that, you know, most of the people who are participating are fairly experienced in sending or receiving notices and are able to flag the problems that happen on both sides in this process.

And so the document attempts to help put forward practices and guidance for folks who might not have the same depth of experience as the working group participants do and to collect in a place things that people should be thinking about as they send notices or as they receive notices.

So in terms of good general practices for
notice senders, the first practice identified is a good faith submission of all of the information that's required by Section 512© and it's been flagged by online service providers that often their operations are slowed down by receiving incomplete notices or notices that are inaccurate or don't comply with all of the requirements. And so making sure that people realize that they are asked for this information for a reason.

Submitting takedown notices requested as section -- sorry -- we got a little -- right. So another issue that was flagged in our discussions is that in certain instances online service providers receive takedown notice requests that are framed as Section 512 notices but they are really not referring to copyright infringement or unauthorized use of copyrighted works, but they are, in fact, relating to things like trademark issues or violation of community guidelines or something of that nature. So a good practice would be to ensure that you're submitting your notices only regarding copyright matters.

MR. HALPERT: I'd add one clarification. It would be okay to submit other things, other complaints to service providers. No implication to say don't submit things. But don't style a request relating to
defamation or trademark infringement as a copyright notice and takedown request because that's going to be confusing and will slow down the process.

MS. AISTARS: Right. One topic that we've had a good bit of discussion about is how to ensure that notices that are submitted are both pointing to the online location at which the alleged unauthorized material is residing and that that's accurate information that the online service provider can act on. And also that the material that you're pointing to is actually being used in an unauthorized fashion that's not authorized by the copyright owner, its agent or the law.

And so we have had discussions in the group to try and provide guidance, not just in terms of providing kind of an overarching request that people take, you know, good faith efforts to do this, but actually we've outlined a variety of steps that we know of that people are taking in the marketplace today that we think are effective in helping to ensure that you're pointing to information that is actually located where you say it's located and that it's actually, you know, an unauthorized use.

So some of those are identified and this is particularly important where automated tools are being
used, but the way that the language is drafted, it
applies both to instances where somebody is sending
notices on an individual basis where a human being is
involved sending each and every one of the notices as
well as to situations where automated tools are being
used.

So the overall guidance is that before
submitting a takedown notice it's good practice to take
measures that are reasonable under the circumstances to
ascertain the online location at which the alleged
infringing material resides and to appropriately
consider whether the use of the material identified in
the notice in the manner complained of is unauthorized
by the copyright owner, its agent or the law.

And then when you're using automated tools of
various types to search for and send the notices, there
are a variety of practices, some of which include
conducting a human review of the site to which notices
will be directed to ascertain whether the site is
particularly likely or unlikely to be hosting or
linking to material that infringes copyright so that
you're directing notices at sites that, for instance,
are unlicensed sites or are sites dedicated to
infringement rather than ones that you've authorized to
use your materials.
Establishing search parameters to the copyright owner or its agent that you believe will efficiently identify the unauthorized files while, you know, minimizing the inadvertent inclusion of authorized files. And in addition to using things like keywords and titles of the copyrighted work, using additional metadata where you can to help indicate -- to help narrow the types of files that you're turning up.

So things like the size of the content file might be useful in identifying the location and the unauthorized use of file in these circumstances. Regularly conducting spot checks to evaluate whether the search parameters that you've set are actually returning the expected results and adjusting the search parameters as you need to in order to provide more accurate results.

And then other practice suggested is in the instance where there is information provided by the service provider that your notice systems are generating significant numbers of notices that are inaccurate to identify the online location or that are producing files that are actually not pointing to unauthorized uses, to work with the service provider and make good faith efforts to try to correct the
issue.

So these are all practices that we've, you know, we've discussed, they're currently highlighted for further discussion and review. But I think we're in pretty good shape with those in terms of practices that we're aware of and that we recommend.

MR. HALPERT: And to be clear for the internet users in the audience and tuning in over the phone and watching a webcast, if this is actually being webcast live, which would be kind of cool. This provision is also intended to address uses not simply that are not authorized by the copyright owner but also uses that are non-infringing generally.

So the -- rather than trying to spell out what is fair use in a document like this that would be very -- would require pages and pages and pages and would still be a case-by-case analysis, the focus here is to address issues of licensed works and of uses, for example, of remixes that are transformative works and whatever it would be under the question of whether the use is authorized by the law or not.

And the -- but we're addressing this not as a separate fair use section which would be too difficult, frankly, and too long, but rather treating this question of whether the notices are really relating to
infringement as an accuracy question. So in this
there's a fair amount of back and forth to come up with
the right words, but this is something where we hope to
obtain agreement of the rights owners of internet user
representatives and service provider representatives
and continue to work on this language you see in the
current snapshot.

But we've made a lot of progress in the past
roughly three weeks and are hopeful of getting an
agreement that's balanced and reflects all the different
interest here.

Oh, sure, there may be some -- there have been
some suggestions about a way to be able to tell on the
face of the notice or to have more information about
whether the notifier really is -- or what general type
of rights owner the notifier is acting on behalf of,
not the individual artist, but if there's a company or
something who's hired the notifier in an agency
situation. And this is complicated for a variety of
different reasons, but there's a placeholder bracket
for further discussions on that.

And there have been suggestions about drawing
on educational materials to educate users about online
infringement as well as potentially some education to
users if the rights owner wanted to that would be
available online, could be linked to from a notice, for example, or from the service provider site giving internet users some informative information so that the notice and takedown process is also an educative process rather than simply the mechanical posting and removal and then reposting of content.

MS. AISTARS: And I think for both of these, those aren't likely to be issues that would be reflected in text in a document like this but rather something where the working group members would come to some suggestion that we would make to the larger community as to, you know, how or whether to approach the issues and there are other groups that we might suggest working with if the group agrees that they are important to approach.

MR. HALPERT: This could be a potential further workstream for the -- if the people involved in the multistakeholder group think that it's worthwhile.

MS. AISTARS: So moving to bad practices -- that's the service providers, okay.

MR. HALPERT: So what may be most -- these good practice are examples. What may be of greatest potential significance in how this was applied or ever referenced by a quarter or other entity is also to have
a list of bad practices, both to discourage people
coming to this in good faith and also to identify some
practices that really raise serious potential obstacles
to the efficiency of the notice and takedown process
and the integrity of that process.

So for service providers, we thought about a
series of these and Sandra -- the Copyright Alliance
did a good job of presenting a bunch of these at the
first meeting at Berkeley. They did a report showing
what some actors were up to. And the first was hiding
intentionally the procedure for submitting a 512© or
512(d) takedown notice or counter-notice.

Sandra had wonderful slides showing how hard
it was to find the designated agent on a bunch of sites
or having paid advertisements people have to click
through, that sort of very slimy stuff. That ranks
you're Letterman and you're coming up with the top, I
guess, five. That struck us as the first one to put
in.

The second one was requiring -- this is sort
of similar, notice and counter-notice -- or
counter-notice submitters to watch advertising or
provide anything of value as a precondition to
submitting a notice or counter-notice claim like
registering or having to do other things online, which
just further gums up the process and is inappropriate. Then the third one, this one we still need to work on the language a little more, but using arbitrary mechanisms that are designed to make the notice and takedown process inefficient or difficult. The classic example is the use of multiple Captcha codes where if you make a mistake, you'll have to start again and resubmit the information. Having cool down periods between submissions of notices or counter-notices that are deployed in a manner that really are intended to very much slow down the notice submission process.

On the other hand, and using other sorts of arbitrary mechanisms that are intended to significantly hamper the ability of a rights owner to send or multiple rights owners to send notices, sufficient to address the scale of infringement on the site.

And then we also will have in here a notice -- a reference back to the situational or contextual practices at the end about security measures. We've already identified security measures as a good practice and the question is how they are used and they not be wielded intentionally as a way to slow down submission of compliant notices.

And then our number 4 on this list, and actually we only have four right now and maybe there
will be some others added. Using stigmatizing or
intimidating language which risks and we might add is
designed to chill submission of legitimate takedown
requests or legitimate counter-notices. This is
something where the group has to go over this and come
up with precise language, but we heard a lot about and
even heard a little bit from East Bay Ray earlier about
the abuse that some rights owners, Ellen Seidler spoke
to this too at Berkeley the last time we were here,
abuse that notifiers, particularly individual notifiers
have to undergo when they submit what's a legitimate
takedown notice about an infringing use of their work.

So those were the bad practices. And, again,
if there are others that you think, even if you have
not been involved in the working group or in the
drafting group that you think ought to be included,
please send them by e-mail to me and Sandra and we'll
make sure that they are addressed in the process.

Then for service providers, specifically when
e-mail is the submission mechanism, we're asking
whether there are any bad practices particular to
e-mail. We have asked this for about three months,
haven't heard anything, but if you know of any, please
do send them to us and we're delighted to use them.

Same thing for bad practices with regard to web forms
specifically. And, again, we may have some particular things for that -- that particular interface seems to raise some more issues and if you have suggestions, please send them along.

We'll also be adding if we can get a hold of Ron Yokubaitis both good and bad practices with respect to Usenet, but again that's just a gap right now.

Sandra.

MS. AISTARS: Yeah. So then moving to bad general practices for notice senders, we are discussing actively issues related to how to properly direct notices, particularly 512© notices, to the right entities. And I think we still need to bottom out exactly on how we address that, but the idea is that if you know that the allegedly infringing material or the activity doesn't reside on the service provider's system or networks within the meaning of 512© and you have -- the entity who you're directing the notice to really has no way of addressing the issue that you're raising, you should not be directing notices to that entity.

There's enough discussion as to, you know, entities who are hosting providers and, you know, where and when it's appropriate to direct notices to those entities and I think we still need to further discuss
that before -- before bottoming out on language on that issue. But that's an issue that is tagged for discussion here.

MR. HALPERT: The distinction here is between entities that actually host the online location, website, whatever it is and an entity of underlying infrastructure who's basically providing the power and maybe the connectivity of the location but doesn't have the ability to take down material.

We need to think about an appropriate balance there where the rights owner who's not getting a response from the actual website host who's in a position to take the material down will under some circumstances want to contact the provider of a huge data center capacity and we need to figure out what would be an appropriate description of a bad practice. There are notifiers who send millions of -- up to a million notices when they are frustrated that the individual website hosts are not responding to the data center operator and that's clearly inappropriate, but we have to sort of parse through at what point it becomes inappropriate to do that. Sorry.

MS. AISTARS: Right. As I said, it's an open discussion because the countervailing issue that needs to be considered is, you know, not cutting off the
ability for people to kind of work their way up the
chain if there is a legitimate connection between the
content and the notice being sent.

I see Vicki has a comment that she wants to make.

MS. SHECKLER: Vicki Sheckler with Recording Industry. Jim, as you know, we do have an issue with that concept. We do believe that 512© applies not only to the website operator but also to the hosting provider underneath. We understand that there are some instances where we need to work out an arrangement to deal with that. But just for the record, we do feel strongly that it is appropriate for everyone that claims 512© safe harbor status to be able to take notice and then process it. Thank you.

MS. AISTARS: So moving to further bad practices that have been identified. A lot of these are kind of parallels to what we have identified as, you know, good practices. For instance, sending notices only reflecting copyright matters and sending notices only when you're actually entitled to send notices on behalf of a particular actor. The flip side of that which has been identified as a bad practice here is falsely asserting that the notifier is authorized to act on behalf of the owner of an
exclusive right that's being asserted or similarly submitting invalid takedown notice requests for harassing or retaliatory purposes that don't have anything to do with copyright issues such as trying to silence a critic or with the goal of disrupting the business of a competitor. Those are all things that we've identified as bad practices.

We have also clearly set out, again, as a flip side to the good practice identified earlier that it's a bad practice to submit a DMCA takedown notice to assert rights other than copyright rights.

We have also set out as a bad practice a practice of repeatedly submitting 512 notices regarding URLs where the rights holder knows that the allegedly infringing material or the hyperlink has been reposted by the service provider in response to a valid counter-notice that, you know, contains all the elements that are set forth in 512(g)(3).

We're having a further discussion with the group on how to deal with issues where it's not that the notice has been or that the content has been reposted because of a valid counter-notice but rather that the content has repopulated automatically because it's a set of nested links. And in that latter case, at least certain members of the group feel that it's
appropriate to -- certainly appropriate to send additional notices and that it may additionally be appropriate to find a way to take action to remove those nested links based on the initial notice that's received if that's something that's within the structure of the site to do.

    But, again, that's something that's kind of an open discussion item that we're trying to figure out kind of the scope of what that might entail. So it's just highlighted with bracketed language.

    Kind of again the flip of what was asserted as a good practice, you know, the failure to take efforts to ensure that you have a good faith belief that you're dealing a copyrighted work, that the work is actually, you know, able to be found at the location that you're directing the online service provider to and that it's actually work that is being used in an unauthorized fashion and -- let's see.

    And the last couple are kind of elaborating on those points. Failing to specify that the notice sender has a good faith belief that the use of the material is not authorized by the copyright owner, its agent or the law and failing to specify that the notice, in the notice, the 512© notice, which works are infringed or where the infringing work or the
hyperlink is located on the service provider's system or network so that it can be removed.

MR. HALPERT: These are all going to providing enough information so that the service provider knows what to do and knows what the work relates to and how to find it. But there are some people who don't want to go to that trouble and they submit a notice. And so this is describing that as a bad practice.

On to the situational practices. These are the ones that for which there's often a very good reason to do something, but not in all cases. So they are balanced and there are three topics that we've designated or four topics that we've designated as for possible situational practices treatment, and many of them are dealt with or alluded to above but those are fleshed out here.

One is trusted submitter program, the idea being that here the senders have a good record of submitting accurate notices. They want to submit a lot of them, they are authenticated each time, and where it's practicable for a service provider to implement that sort of program, it can yield significant efficiencies. We go on to list some of the features that these programs may require -- or may include rather than may require.
By way of example of how to run one, you're going to hear more from providers and users of trusted sender programs after we sit down. So we will yield the floor shortly for that and you can hear more about it.

But the idea is to offer this as not something that needs to be done, but it's a process that can yield some significant efficiencies and the thrust of this document is to encourage efficiencies. So we go through both the -- we allude to some of the reasons why service providers might want to offer them up and then why rights owners might want to use them.

Second consideration, this is in yellow, I guess.

Do you want to cover this one?

MS. AISTARS: This was in yellow simply because it was discussed yesterday. But it's acknowledgment and status reporting. So in good practices we've identified already that it's a practice for service providers to provide confirmation of receipt of a notice and to provide the notice sender some method to identify the notice so that they can communicate better with the online service provider about particular notices that they have sent and they know, you know, what the online service provider is
referring to in further communications that might occurred.

This is a further elaboration on that point that where a service provider has the resources to make it practicable, if they can take additional measures such as providing a record of all of the URLs that they received from the submitter and providing the submitter with a record of the action that the online service provider has taken with respect to notice, that could provide additional efficiencies in the notice sending and receipt process in terms of ensuring that there's an accurate and complete exchange of information and that there aren't additional follow-up requests coming from the notice sender that the online service provider has to act on. So we have laid that out as an additional good step that people can take, you know, under the circumstances, you know, circumstances permitting.

The points that Jim alluded to as we were discussing the good practice of providing an acknowledgment is also captured here, the fact that if you are an entity who is sending repeated notices that don't meet the 512(C)(3) requirements and you appear to be doing so for harassing reasons or illegitimate reasons, those sorts of notices don't necessarily merit
a response. It's not good for the online service
provider, it's not good for legitimate notice senders.
It gums up the works for everybody and, you know,
deters attention away, deflects attention away from
action on legitimate notices. And so it might be
reasonable to provide an explanation and a -- of the
deficiency, you know, the first time that you get such
a notice. But if you've got an entity that just
persists in sending you kind of, you know, harassing
notices that are deficient and harassing notices, you
know, that is something to take into account when
thinking about whether to take these additional steps.

MR. HALPERT: It might encourage them if they
got a response each time they sent a notice. And then
in terms of requesting additional information, again,
like this acknowledgment, situational practice, this is
alluded to above and then fleshed out here saying
that -- requesting additional information that
describes the work or a link to the legitimate version
of the work can improve efficiency in some contexts,
particularly where the title information alone is not
sufficiently descriptive of the work to allow the
service provider to identify it.

This can happen with photographs, for example,
copyrighted works are available at the same URL and the service provider simply with the URL isn't going to be able to find the specific works complained about, obviously if it's all of them that may be different, but where there are particular ones that are alleged to be infringing, the service provider really will -- to be able to act on the notice will likely need some additional information.

So this is a scenario where requesting additional information is a good -- is considered to be a situationally perhaps good or situationally to be a good practice.

With respect to these optional pieces of information, the service provider should consider whether informing notifiers that the information would encourage efficient submissions or aid in identifying works in question, it is going to be helpful to have that additional explanation of why this is required. And then there's, on the other hand, consideration that you don't want to request additional information where the notifier has already provided enough information to identify the work in question.

So there's a fine line here where there's not enough information to identify the work -- for the service provider to identify the work, and then this is
a good practice. When there already is enough
information, it may well not be a good practice. So we
tried to reflect that balance in the draft and the idea
is probably to add some examples of this to be --
without being exhaustive, but just to give examples for
readers to understand where this additional
information -- these additional information requests
may be helpful and promote efficiency.

Ideally we will boil this down. Right now
this is pretty wordy. But to give people an idea of
the circumstances under which this may be a real plus
for efficiency.

MS. AISTARS: Right. One area where this
tends to come up is where a notice sender is requested
to provide a link to a place online where an official,
you know, original authorized copy of the work can be
found and that often isn't something that is actually
available online. In some cases, for instance, if
that's like the answer key to test results or -- that
are -- or to tests, that's not something that's going
to be posted online.

So obviously it's a situational thing and, you
know, care needs to be taken in how you ask for
additional information and when you ask for it, and so
that's what we're trying to reflect here.
MR. HALPERT: Yeah. The draft may wind up with some of these examples reflected so that readers can -- without parsing tons of text can understand this more immediately.

Then finally to Captcha codes. This has required a lot of work and it is still not done.

MS. AISTARS: Yeah. So this is kind of going back and forth I guess more broadly than just Captcha codes because we all recognize that, you know, we're talking about Captcha codes now but, you know, security tools and technology tools evolve very quickly and so we may be talking about something completely different a few months from now. But generally the use of security measures as we've recognized in the document is something that's important for people who provide online services for a variety of reasons.

So we've recognized it as, you know, a good practice in the document. But, nevertheless, the entities that send notices, whether they're entities who employ automated takedown systems or whether they're individuals who have to send notices manually, have identified that even the use of, in the instance of Captchas, even the use of single Captcha code can be challenging when sending large volumes of notices on the one hand through automated tools or when you're an
individual and you have to deal with a large number of sites sending, you know, one -- sending a notice about one URL per site.

And so while we've described it as a good practice to use security tools, on the other hand, we have described it also as a bad practice to use security tools in an arbitrary fashion in a manner that's intended to make the submission process more difficult.

We're also recognizing in this kind of situational language that, you know, even when you're not trying to make the sending of notices difficult, just the nature of these tools can present a challenge and that's something the group recognizes is an issue and that there are various ways that people may consider workarounds, whether those are using trusted sender programs where you're already pre-authenticating somebody and so you don't need to employ those tools, in a particular trusted sender program, or whether you're allowing the submission of a large number of URLs using just the single Captcha code to try and alleviate that burden or whether you're allowing recourse to other modes of sending notices such as by e-mail.

So those are just examples of workarounds that
we identified as possibilities. And, again, the this
is language and kind of an illustration of the state of
discussion as of yesterday around whatever 5:00,
6 o'clock Pacific.

MR. HALPERT: And what you see is not agreed
language, but we're continuing to work on the security
measure side to come up with language that reflects
legitimate need for security measures on many sites
while suggesting ways to work around potential
obstacles.

So that's the current state of play and we're
going to continue to work hard and we hope have
something for you at the next meeting.

MS. PERLMUTTER: Let me ask, we're running
slightly behind but not terribly. That was an
extremely substantive and informative description of
what's been happening in the working group. I know I'm
personally encouraged and excited by all of the
thinking and effort that's gone into this by so many
people, including many of you in the room.

We did want to give the opportunity for anyone
in the room who isn't in the working group and also
anyone who's participating remotely to ask any
questions or make any comments before we take a short
break and move on to the next topic on the agenda. If
anyone has anything they would like to say, please take
this opportunity while Jim and Sandra are standing here
to answer questions.

Yes, Corynne.

MS. MCSHERRY: I got an e-mail from someone
would who would like to call in.

MS. PERLMUTTER: Hollis, do you --

MS. ROBINSON: Yes. For any anybody who's on
the phone or wants to call in, the number is
1(888)453-9955 and the passcode is 6039037.

MS. PERLMUTTER: And that information is
available on our website as well if anyone didn't get
it all as Hollis read it.

MS. MCSHERRY: I think the operator has to do
something.

MS. ROBINSON: All they have to do is press.

MS. PERLMUTTER: Sorry. I think we usually
say this at every event and we've probably started to
get complacent and think that everyone knows.

MS. ROBINSON: For those on the phone, if you
just hit star one and the operator will assist you and I
do see we have two questions right now.

MR. NEILL: Good morning, everybody. This is
Art from New Media Rights in San Diego. I just had a
couple of comments and some questions as well. And of
course I'm just kind of looking at this this morning, so bear with me on some of the language.

So I think that one of the suggestions that I would have is in the good practices for notice senders, I would ask you all to think about including something, especially when you start talking about including language about automatic notifications and things like that. When you're talking about such a high volume of notices, we do see at New Media Rights, we work with a lot of individuals on both sides, who both send notice takedowns as well as there's been counter-notices.

And one of the problems is when people get content taken down, it can be difficult to get the content restored and sometimes it's very, very helpful and I think a very good practice by notice senders where they have learned that that material was authorized by the copyright owner, that they actually gave a license. Or that it actually was authorized by law to go ahead and take steps to help restore that content. And some folks do and some folks don't.

But anyway that's a good practice that I would suggest. That's more of a comment.

My question is also in that space of good practice -- I believe in the good practices for notice senders. The paragraph, and it's not a numbered
paragraph, I don't think, so I don't have the number, but maybe it is. Particularly, it's that paragraph that starts particularly where automated takedown notices will be sent to a site based on metadata, that particular paragraph. Some of the metadata that's cited is keywords, titles, file size, et cetera, and then it says conducting a human review of the site, you know, is a good practice. I was just wondering, what does a proper human review look like? I mean, I don't know what the -- I wasn't clear what that meant there, conducting a human review of the site to which notices will be directed to ascertain whether the site is particularly likely or unlikely to be hosting or linking to material that infringes copyright.

It sounds like -- I'm just trying to understand how specific, is that looking at the overall site or is that looking at to see if there are specific, actually specific infringing works on the site or just that the site can host infringing work?

What does that mean, I guess.

MS. AISTARS: So I mean this is language as we said that is still being discussed by the group and that was, you know, just actively put forward yesterday for discussion. So I don't want to speak for the full group on it. You know, the idea here was that, you
know, you don't want to be sending notices to sites, for instance, that appear to be kind of wholly dedicated to, say, film criticism and, you know, they are not -- you know, they are not engaged in, you know -- you know, uploading entire copies of movies or anything like that. And so you need to really identify what the source, you know, what the target of your -- of your notice sending is before you start sending it.

Similarly, it's a common practice among notice senders, especially when working with vendors, to provide lists of, you know, like white list sites of sites that are sites where licensed versions of their work are authorized to appear. And so those are the sorts of things that you want to, you know, exclude right away before, you know, starting an enforcement practice against a particular site.

But, in general, all of these practices here are listed, both here and in other places in the documents, are listed as examples that are, you know, given as guidance to people to think about, not as something that is intended to spell out, you know, you need to take these, you know, four, five steps and, you know, in every instance, you know, every member of the working, you know, agrees completely that, you know, this is exactly, you know, how we will conduct our
review, you know, before beginning.

So it's intended to be kind of helpful and illustrative rather than something that outlines absolute obligations or tries to prescribe something in an area that is ever changing. I think the tools also are improving in -- that people use and are improving in ways that actually, you know, may make -- you know, may make the human review in certain instances, you know, less useful. It also depends on the type of site you're dealing with. I mean, some sites you can't actually access the files, you know, when you're first approaching the site. So I think it's all --

MR. HALPERT: Contextual.

MS. AISTARS: -- contextual if you're dealing, you know, with a cyber locker, say, where the, you know, the links are not readily available from the, you know, front page of the site and so forth. So that's why the, you know, the overall introduction attempts to put all of this into the reasonable, you know, circumstances and the context that you're operating in in any given case.

MS. PERLMUTTER: We have a comment from the audience and then let's go to the other comment on the phone.

MR. SHEFFNER: Ben Sheffner with the Motion
Picture Association. I just want to build on Sandra's answer and she addressed some of this towards the end of her answer. But to address the caller's question, the kind of human review that would be appropriate is going to depend entirely on the nature of the site. As Sandra mentioned, there are cyber lockers which host vast amounts of infringing material where you won't be able to see anything past the home page of the site which doesn't even really display any of the infringing material itself.

There's other sites where it might have millions of pages that you could potentially review, but I don't think anybody is suggesting that it would be appropriate to review all of them. The idea is that before sending notices based solely on metadata, things like keywords or title or file size, et cetera, you should get some sense of the site. It's that kind of searching and sending of automated notices is more appropriate for a site that has vast amounts and vast percentage of infringing material is overwhelming as opposed to sites where you might just have relatively rare occurrences of unauthorized or infringing material and it may not be as appropriate to use simple meta database searches and that kind of thing.

So, again, to emphasize the kind of review
that would be appropriate is going to vary vastly depending on specifics of the site.

MS. PERLMUTTER: Thank you. Let's go to the other question from the at-home audience.

MR. HALPERT: There was someone else who was in the queue?

THE OPERATOR: Three people. We have three questions in the phone queue, yes.

MS. PERLMUTTER: Why don't we take all three in order.

THE OPERATOR: Okay. Our next question comes from Teri Karobonik.

MS. KAROBONIK: Hi, this is Teri from New Media Rights. I think one of the things that we should really consider going forward as we talk about particularly good general practices for notice senders, under three is that a lot of the times it's, in fact, not the copyright holder but a third-party agent who is hired to do nothing but send takedown notices. So I do think that's something we should at least mention and bring up in the guidelines as something that needs be considered some general oversight since working on the user side and also speaking to folks who use services like these, a lot them are independent creators. Some of them are more scrupulous or less scrupulous than others.
So putting in some sort of language recognizing some sort of oversight of these groups just to make sure that the notices being sent on creators' behalf are actually legitimate. And if notice senders -- or if creators are noticing some pushback and a lot of the notices seem inaccurate, that's something that really needs to -- that the creator really needs think about going forward.

MS. AISTARS: So the document is drafted not to make distinctions between notice senders, whether they are an individual or an agent acting on behalf of an individual. I think in the context of a document where you're talking about, you know, pure efficiency seeking additional legal obligations on I think you said independent individual artists, seems to be --

MS. KAROBONIK: I think more of a general best practice when you're hiring an agent to work on your behalf. And maybe it boils down to good business sense, and many of the creators we work with already do this. But to keep in mind if you're hiring folks that aren't going a good job for you, maybe that's something that as a best general industry best practice, you should really think about going forward that maybe this isn't the company for you.

Since as working on the small creator side,
this is a new cottage industry where there isn't a lot of regulation, there isn't a lot of guidance at the moment. But folks are really are voting with their feet for these services. So I think providing some sort of general very basic guidance that, hey, you know, if you're going to hire someone to do your enforcement for you, you should make sure they are actually acting in your best interest.

MS. PERLMUTTER: Thank you. I think it's something that the working group can have a conversation about at its next meeting.

MR. HALPERT: Yeah, thanks Teri.

MS. PERLMUTTER: There's two more on the phone who is next?

THE OPERATOR: Our next question comes from Andrew Bridges.

MR. BRIDGES: Hi. Thank you all for this. I'm sorry I can't be there today. I wanted to raise a point that I didn't see in the draft this morning, and that is problems of the reality of bad faith notice construction and delivery by some copyright holders, particularly those who want to litigate large statutory damages claims over the question of whether notices are sufficient to --

MR. HALPERT: Can you speak a little louder,
MR. BRIDGES: Okay. I'll do my best. I wanted to address the question of the reality of bad faith notice construction and the delivery by some copyright holders in order to set up large statutory damages claims where the issue in the litigation is the adequacy of the DMCA notices. Let me give several specific examples. For example, I'm aware of --

MR. HALPERT: Andrew, let me stop you for a second.

Do you have a suggestion with regard to the language that are not -- if you can frame these in relation to whether the language addresses the issue currently or not because a big part of the bad faith practices for notifiers is designed to address this. And so please do cite the examples, but also give us direction if you think it's not addressed by the current draft.

MR. BRIDGES: Well, I did not see this addressed in the -- these types of issues addressed in the document, maybe I missed something. But, for example, the sending of, let's say, 15-page faxes late at night on holiday weekends with no fax cover sheet, no numbering of the pages, no headers, no dates, no return address on the first page. A number of major, major service providers have no records of receiving
faxes that some copyright holders claim that they have sent. The use of screen captures of non-machine-readable images as an alternative to capturing and cutting and pasting machine-readable text so that human transcription would be required by the service provider instead of working with machine-readable text.

Things like that where there are delivery mechanisms that appear to be designed specifically to impede the automated handling of notices and to introduce error in the processing and handling of notices. Maybe I missed it, but I didn't not see those types of --

MR. HALPERT: Those are not in there, Andrew. Do you have another one?

MR. BRIDGES: No, that's mainly it. It's bad faxes that are either illegible where the copyright owner won't replace them or faxes that are transmitted in a way that seem designed to provoke mishandling of the faxes upon receipt. These are just some examples. I wouldn't give more. But they are reality. These are featured in at least half a dozen, maybe a dozen cases I'm aware of with attorney's fees in the million of dollars and statutory damages claims in the billions of dollars.

MS. AISTARS: One place where we do -- it
doesn't address these specific examples, but one place where we do at least have a placeholder where I think we can make progress on this is where we refer to providing either standardized kind of submission formats or e-mail text formats that we want people to follow. So perhaps drilling down a little bit more on those areas with the group would be helpful to try and ensure that we are putting forward good examples of how to do things properly as well as just saying how not to do things.

MS. PERLMUTTER: If it would be useful, Andrew, maybe you can join in the next working group meeting or have additional conversations with the working group or the chairs to give some more of these examples.

MR. HALPERT: Yeah, that would be very helpful. Thank you.

MR. BRIDGES: Thank you, I'll be happy to do that.

MS. PERLMUTTER: And I think we had a third caller in the queue.

THE OPERATOR: Yes. Our final question in the queue right now comes from Rowena Cherry.

MS. CHERRY: Yes, and I wanted to ask -- three things I wanted to ask about. When you go to some of
these sites where you've received an alert that they've
got your stuff and you look for the metadata and you
see your title and you see it's supposed to be by you
and you look at the file size and it seems appropriate,
but the only way to absolutely make sure that it is
what it says it is is to download it. And I don't know
how many people are too afraid of malware on these
pirate sites to actually go ahead and download it.

What can be done for copyright owners there?
You don't want to send a bad request, but on the other
hand, you don't want to lose your work in progress by
potentially downloading something that could be very,
very harm full, in deed, to your livelihood and
computer and so forth.

And then also I think we touched on torrents,
but what is a copyright owner supposed to do if you are
one of, you know, 200 e-books, for instance, on a
certain torrent or in a large file where you don't own
the total collection, but you own an element inside the
collection?

And my third question was, what are people
supposed to do about Ebay because obviously it's one of
the bad practices sites and the sellers, how can you
educate them when right now they are being told --
there are people reselling rights, there are people
right now selling the rights to resell 29 Jeffrey
Archer books and 65 Dean Koontz books and a whole
collection of Robert Ludlum works. And is Ebay a bad
actor in this because there seems to be no way to
educate sellers on the site.

Thank you very much. Those are my three
questions.

MR. HALPERT: I'll take the third one. The
first sale doctrine remains the law in the United
States and Ebay is emphatically not a bad actor, has a
very well-functioning notice and takedown program.
There may be a business discussion that you would like
to have with Ebay about this, but there's nothing in
the law right now that would prevent somebody from
reselling books. There aren't -- this isn't like
scalping tickets in some -- concerts event tickets in
some parts of the country.

So I don't think -- I don't believe that what
they would be doing -- what was occurring on their
platform would necessarily be the subject of
infringement and so may be out of scope for our work.

MS. PERLMUTTER: I think the other question is
the extent to which that involves problems with the
operation notice and takedown system. So if there were
those kinds of issues for any content that is
infringing, then obviously we would want to address it
through looking at how the notice and takedown system
is working.

MR. HALPERT: Right.

MS. AISTARS: I think with respect to the
first two issues that Rowena raises and the challenges
that copyright owners face, particularly individuals
face in sending notices and investigating where
material is located and ensuring that they're sending
an accurate notice, those are points, you know, well
taken and things that we have been trying to reflect in
the drafting and some of the reasons, you know, why the
language that you see highlighted in the best practices
section is highlighted and has been, you know, somewhat
challenging to come to agreement on because everyone in
the working group certainly, you know, operates, you
know, applying best practices and doing the best that
they can and at the same time is aware that there are
challenges beyond those that we can address ourselves
even applying, you know, the good faith of everybody in
the group.

So we're trying to keep the language cabined
such that there is no obligation placed on a rights
holder to, you know, take action such as, you know,
investigating to the degree that you would have to
download a file and check it or click on it or whatever
and put yourself and your computer at risk in order to
be able to send a DMCA notice and similarly, you know,
not putting you in a position where you have to, you
know, do a sophisticated level of legal analysis on
every affirmative defense that might arise prior to
sending a notice. So those are all issues that we are
aware of and contemplating.

MS. PERLMUTTER: Let me just interrupt
momentarily with a message from your sponsor which is
that we're now about half an hour behind on the schedule.
So what I would like to do, I see there are three
people lined up to make comments or ask questions. If
I can ask each of them to be brief and then I would
suggest if people are willing that we forego a break
and work through so that we can get to our panel this
afternoon. Obviously anyone should feel free to take a
break on their own. So if that's acceptable, then
let's continue. And I see Keith --

MR. KUPFERSCHMID: It's Keith Kupfershmid from
SIIA. I will be only about 30 seconds here. I want to
address the caller's question about Ebay. We work
very, very closely with them and one of the things I
think they do well certainly is they do have a whole
section of Ebay where they post educational material.
So we, for instance, have posted on Ebay site
information about the first sale defense as Jim
mentioned about things like OEM software and academic
software and what you can and cannot do with them. So
there is a section there and frankly it would be great
if other ISPs sort of followed that model.

MR. OLIAH: Dotan Oliar from UVA Law. I have
a question that's a bit more general about improving
the procedures for the notice and takedown.

Section 512 requires users -- requires copyright owners
to submit their notice and state a good faith belief
that the material is infringing, but users who are in a
position to file a counter-notice need to state their
legal position under penalty of perjury. So I was
wondering whether there has been any study given to
whether users can meet this heightened burden of
stating a legal position under penalty of perjury and
whether any changes to these procedures should be made.

MS. PERLMUTTER: Just to say, you know, among
the parameters of this particular process is that we're
not discussing any changes in the law. We're just
looking at how we can improve the operation of the
existing system. So we haven't been addressing that at
this point. Not to say it's not a valuable issue to be
discussed.
MR. OLIAR: Right. Yeah, I assume that it goes beyond the --

MS. PERLMUTTER: Yeah, thank you.

MS. MCSHERRY: But actually I think I can say a little bit to that part of the discussion, as everybody knows, has been a conversation about whether we want to include some practices with respect to counter-notices and making sure that counter-notices are accurate, too, which I think is a very valid thing to do.

I'm sorry, this is Corynne McSherry from the Electronic Frontier foundation.

I want to make a suggestion that it seems to me that we are at a point where we may want to invite thoughts from the larger community who isn't able to attend or be on the call with respect to this document. And I'd like to suggest, I know we are still in process, but I'm a little worried that if we wait until December to circulate something, then the document may feel sort of fully baked without sufficient opportunity for public comment.

So there's, you know, we have wonderful new technologies these days for soliciting comments from folks and input from people. So I think we should consider procedurally what's the best way to get wider
public comment.

MR. HALPERT: Corynne, I think that this is very valuable and important. I think this document needs to be considerably simplified before it's fair to send it out for public comment because people who are not lawyers at this point are going to have a hard time with the document. And once we have done that work, which presupposes, though, a certain amount of other -- of ironing out a few of the remaining issues, then that's the most productive time to do it; otherwise, the overwhelming reaction to it will be why are there 15 lines of text here, I don't understand them.

And I think we may be able to work in the working group, and I suggest this as one of our tasks, to simplify this document once the issues, for example, the issue of service provider good practices has been done for a while. I think we should go through that language and make it simpler and easier to understand. Once we do that with different sections of this, it, you know, subject others views, I don't know that there's any problem sending out parts of it before the whole thing is done.

But I don't want to send out language that's inconsistent because people will be annoyed by that. Or language just that's too legalesey so that people
who aren't lawyers really have a hard time participating in the process and it imposes on their time, those are just quick reactions. But I do agree with you that this needs absolutely to go out for further --

MS. PERLMUTTER: We have already, I understand, hosted a prior version as a draft. I think anything that's been discussed which is a public forum is certainly open for people to ask to see. And we do want to post on our website things that people can see and comment on in any way that they wish to as soon as possible. So we will post whatever the working group gives us as being something that can be presented. It will not be any kind of formal government request for comments, but just merely an opportunity for people to see it and make whatever comment they might wish to do.

This is a good segue I think into the general question of what next steps are. So just to say, and I don't mean to cut you off, to put on the table that the last meeting of this full group that we currently have scheduled is December 10th, am I correct? December 15th in our office in Alexandria. So we need to be thinking a bit about what happens between now and then and thereafter.

We had been promising and intending and
pushing and hoping to have some output by the end of the year and I think with all the work that's been done and all the substantive results that have been achieved so far even though there's still work to be done and even though I realize it's not a definitive agreement, there's something that is worth putting forward in some form by the end of the year, some statement of good and bad practices and hopefully some sort of samples or standard forms, documents or e-mails that people could choose to use if they see fit.

So we certainly want to urge both thought about what can be put forward in what format before December 15 and after December 15. And then obviously the main topic at that next meeting on December 15 will then be what next. Is there more work that would be available on the same issues. How do we handle the additional issues that were raised in the Green Paper and the comments that were submitted on this topic on the takedown notice and takedown topic. Are there other things still to be explored or not. And also does this forum think that a continued conversation would be useful or desirable on any other issues that you may wish to continue having conversations about.

So we will set aside most of the December 15th meeting for that conversation which
doesn't fully answer your question, but just to give
some context.

MR. HALPERT: And that probably does
presuppose our having something circulated in advance
of that, meaning if we can do it to have some
exposition so that -- it's hard to do this work without
deadlines, but maybe we should aim to have something
circulated a week before, if we can, so that there can
be more concerted feedback and more folks can
participate by phone or otherwise.

MS. PERLMUTTER: That would be good.

MS. AISTARS: I think what we have now
actually has at least, you know, full text for all of
the sections reflected in some fashion. So it's not
like there are gaps that are totally left, you know,
unfilled. So I think people can start collecting
comments from their respective communities as we speak
and filtering those into the drafting committee's work
and the working group's work even before we get to
December 15th. And I'd urge people to do that because
I think that's just much more efficient than waiting
until the plenary group and then, you know, realizing
that there's something we haven't thought about and
haven't reflected in the documents and it sets off a
cascade of three or four other related issues that
people haven't thought about.

  MR. HALPERT:  We received some really helpful feedback just on the phone today, for example.

  MS. MCSHERRY:  I'll sit down after this, I promise. But one idea might be if there are -- the working group could consider, if there are one or two sort of specific issues that we would like to solicit input on, thinking about whether there's a forum for doing that as opposed to circulating the entire document for comment, which I agree as it currently stands might be kind of confusing, but -- for the general public. But if there are one or two issues where we would like to solicit input and collect it, you know, that might an in between thing that we could do. So I'll just make that suggestion. We can talk about it further.

  MS. PERLMUTTER:  Thank you.

  EAST BAY RAY:  This is East Bay Ray again. I just had one comment on the document. I guess in -- I think we have to look at in the group, on I guess like September 30 or something, but there's a music site called Groove Shark which federal judges ruled against and then a couple of weeks later I have a printout of the code of one of the ad networks that is run by an ISP is back placing ads on it. I think the document --
might have to add a section about ISPs that have an ad network because then they start having a financial interest.

And, you know, Groove Shark has been, you know, judged at this moment to be in violation. They don't a safe harbor at the moment. So, anyway, I think we need to differentiate between an ISP and an ad network.

MS. PERLMUTTER: Yes. There certainly has been work done by ad networks and best practices that they've looked into relating to their functions.

Just one other word from our side which is, you know, I think what we need is to be able to produce something that is useful by the end of the year without necessarily trying to make it the most comprehensive statement that includes every possible issue one can think of. There will be opportunities to move on and discuss other issues as well. So please bear in mind that we would like to see if there's something that can be produced now to show that all your hard work has accomplished something in 2014 and then we can talk about how to structure an ongoing conversation about other related issues or whatever seems appropriate going forward at whatever pace you all choose.

MR. HALPERT: Thanks, everybody.
MS. PERLMUTTER: Thank you very much. Very helpful and interesting conversation. A lot of interesting ideas. We will now call up the panel to discuss the issue of trusted sender programs, which I think will also relate to the ongoing work of the working group as well.

Let me just say that I unfortunately have to catch a plane. I will be leaving in 15, 20 minutes. Go until noon and the rest of the office and NTIA will be here.

MS. BLANK: Unless everyone planning on taking an assumed identity. I don't have for everybody because we kind of put this together. So if you want to take one that suits you or keep one that's up here; otherwise, we'll just have to introduce ourselves as we go. I guess I'm not going to try to be Shira Perlmutter, so I'll be myself.

And I apologize for those who we have no tags for. This is the section on trusted senders as you saw from your agenda. We thought that it would be helpful to invite members of our group here who are in the camp that send the notices and especially those who sometimes use third-party vendors because we refer to that occasionally in our discussions, but we haven't had any in the room, so we can at least get some
insight. And also we have Fred von Lohmann who appears on every panel that we ever have. And he's going to talk a little bit how Google came to have the program they have and a little bit how it works and whatever else may be relevant.

Now, since I haven't had much of an opportunity to speak to my panelists in advance, I'm going to look to them to help me out. I really think it would be helpful if we sort of started with really just a few minutes because we are now going to show how we can catch up on an agenda. And I'd still like to end on time.

So if you could give me a few minutes on how does your organization -- we'll skip over Fred for a moment. How does your organization use vendors and/or trusted sender programs, when did you start and why. Now, I understand that not all of you use in the same way, which is why I want to go down the line a little bit. So let's start that and then I'll ask Fred to give sort of an initial comment about his company's program and we'll go from there.

Ed.

MR. MCCOYD: I'm with the Association of American Publishers. We're the national trade association of the book publishing industry. Our
members directly hire in the case when they use commercial vendors to do their monitoring of the internet for infringement and sending of takedown notices. They have direct relationships with the vendors. So AAP, unlike some of the other trade associations, doesn't provide that as a service.

However, we do talk to our members about who they are using and recently we canvassed them as to how many had access to Google's trusted submitter program for its search platform. And it turned out that quite a few of them were getting access through a vendor that they use for notice and takedown called Digimarc. When Digimarc finds downloadable infringing files hosted on sites such as cyber lockers, it will send a takedown notice to the hosting site but will simultaneously use Google's trusted copyright removal program to send a request to Google to have links to those hosted infringements removed from Google search results. And their experiences with that have been very positive. They've spoken very favorably about it.

There's also another vendor called Mark Monitor which does the same thing for another one of our large publishing members.

And, finally, several publishers in our membership have access to a service called a copyright
infringement portal which is administered by the publisher's association in the UK and which our members have discounted access to pursuant to an arrangement we've entered with the UK publisher's association. And the portal also has access to TCRP and reports good things about it.

And finally, Covington and Burling law firm has a vending arm in its London office which does monitoring and takedown notification, and they have access to trusted sender programs at the online marketplaces Ebay and Taobao, for example. So not all of our member publishers have access through third-party vendors to trusted submitter programs. We did ask them whether they would be interested in broader access and they said they would.

And, furthermore, even the publishers that have such access through venders don't -- some publishers use vendors pretty much exclusively for their monitoring and takedown. Some do everything in-house, particularly smaller and medium-sized publishers that don't have the resources to pay for such vendors. And then some do a combination. So, for example, the vendor will specialize in finding and doing takedown on downloadable files, but then the publisher's in-house team will handle things like the
entire book is posted in HTML on a web page or also linking sites which aggregate links to files hosted elsewhere.

So the members said yes, we would be interested in getting broader access to trusted submitter programs; however, AAP wouldn't be -- if AAP did have an opportunity to be a facilitator for more publishers to get access, we'd love to do that. But if it involves our office being an administrator of the day-to-day -- handling the day-to-day submission of the links and other data, we would need more resources to do so. So we would have to see whether the member publishers would be willing to pay additional fees to staff us to do that or for us to hire a third party to help us.

But if the administration is something that individual publishers, large and small, could handle, then we were thinking perhaps we could play a more limited facilitating role.

MS. BLANK: Thanks, Ed. Vicky.

MS. SHECKLER: Hi, I'm Vicky with Recording Industry Association of America. We represent the major record labels in the United States. We along with our sister trade associations do the bulk of the web-based noticing in house and don't necessarily use
outside vendors for that type of work. Occasionally we'll use outside vendors. We're continuously assessing the benefits of outside vendors, but today we do most of it in-house.

MR. KUPFERSCHMID: I'm Keith Kupferschmid, I'm with the Software and Information Industry Association. It's fairly easy I think when you hear the Motion Picture Association and the recording industry and the AAP, the book publishers, to sort of realize, okay, I get it, I know who they represent. For us, not so much.

We represent sort of what I would like to consider the serious side of copyright, not the entertainment side. And so we represent software companies and information companies. And as you might imagine, each of them -- I mean, I think we do have about 800 member companies. And they range from very large companies like an Oracle or IBM to very, very, very small companies.

And depending on the size of the company you're talking about, they may or may not have the resources to do it themselves. They may ask us for assistance. They may ask us to do everything. And so it really does range for us in terms of what we do and who we use and how we use different services depending
on, frankly, the size of the company and the resources that are available.

We do have large members that do similar I think to what you heard from Ed that do their own automated and manual searching. Even those large companies will use us on occasion or maybe regularly depending on the company to do very what I would called targeted investigations or targeted searches. They might rely on us, for instance, to do enforcement on Craigslist or Taobao or something specifically focused like that.

The -- I guess if I can bring up the F word for a second, fair use. We don't -- we handle clear cases of piracy where entire works are being taken down or being infringed. And if there are instances where maybe portions of a work -- this doesn't really happen in software but mostly for our content companies. Where portions of are work being used, that's something that they would handle themselves. So we're looking for just real clearcut egregious cases.

And as part of that, I mean, it shouldn't come as a surprise, we've used third-party vendors for at least 15 years now and I can name them all but we don't have the time because we've bounced around from vendor to vendor. We also use -- we engage in sort of these
trusted sender programs. I mean, we don't really define that, so I'll define it rather broadly in terms of sort of a special relationship that we have with the ISP that allows us to more efficiently send them notices and get material taken down.

The groups or the trusted sender programs our companies work with is Ebay, Google, Amazon, Craigslist and Taobao. We understand a benefit of those programs is the fact, of course, that there are enough bad apples out there, so if you establish this trusted sender program, you're hoping that, of course, you won't get those bad apples in the program. So we understand that benefit.

We truly believe that these type of trusted sender programs are the future, not just in DMCA takedowns, but we saw this issue come up in the Marrakesh treaty discussions recently, in the ICANN discussions that are going on with accreditation of privacy and proxy services. It's a way to distinguish sort of the good guys who are willing to swear on a stack of bibles that they're doing the right thing and they know how to identify infringement from the people who might be misusing the copyright law for those purposes.

MR. SHEFFNER: I'm Ben Sheffner with the
1 Motion Picture Association of America. We represent
2 the six major motion picture studios here in the U.S.
3 And it's interesting to hear the sort of different
4 practices of different trade associations, and I think
5 one thing to keep in mind is that the practices do
6 indeed differ.

7 Our model is a bit closer to the AAP actually
8 than the RIAA in that the MPAA does not itself or
9 through vendors send large numbers of DMCA notices
10 either under section 512© or (D). Our six studios
11 all handle that individually. Mostly they use vendors,
12 but some do quite a bit of in-house. So the MPAA is
13 not directly sort of overseeing the large scale
14 takedowns by our members.

15 In terms of trusted sender programs, we think
16 they are a good thing. There are not a lot of them.
17 Of the major sites here in the U.S. that I'm aware of
18 that are actually employing these, Google and various
19 of its platforms and then Ebay through its VeRO program.
20 We think they're a good thing. We think they're very
21 helpful for both notice senders and recipients and we'd
22 like to see more of them.

23 Just to give people who may not be familiar
24 with what these trusted sender programs are or sort of
25 how they operate or how you sign up for one, I like to
use the analogy of the Pre program of TSA when you go through security at the airport. Essentially what you have to do is you fill out a big form and you give TSA all this information and they run you through these databases, make sure you're not a terrorist, make sure you don't have a history of hijacking airplanes. And then you go in for a very brief interview and they give you basically a number. And once you have that number, you're routed into the special line at security. And essentially some of the normal security measures like having take off your shoes and taking your laptop out of your bag, you don't have to do that anymore and you can basically go through a fast lane. In other words, they've sort of prechecked you out so that you can be processed more efficiently.

These trusted sender programs have a lot in common. They essentially check you out, make sure they know who you are, make sure that you're sort of a legitimate company that has a history of sending legitimate notices and then you may be able to bypass certain of the hurdles that are normal -- that sending notices normally entails, whether it's using Captchas or filling out various forms to sort of tell the notice recipient, the service provider who you are. And it can make the process a lot more efficient.
Another thing that these trusted sender programs can do is sort of facilitate machine-to-machine transactions which we think are really the future of notice sending and receiving. Things like the use of APIs, other sort of machine-to-machine communications, those obviously take a little bit of work to set up to be -- the machines need to be able to talk to each other. It's not something generally that somebody who does this one off can do. Again, the use of such technology we think greatly improves efficiency as often facilitated through these kinds of arrangements.

MS. BLANK: Thank you. And it is interesting to hear how different each organization is in its handling of sending notices whether it's on behalf of their members or not.

Fred, time for you. If you could help us understand how Google came to develop its system, which I understand is a very massive system, and maybe you can outline that for us also and where you think this process is going.

MR. VON LOHMANN: Sure. Happy to do so. I will say, for the record, I have never asked Ben to remove his shoes. Entirely not the case. But actually I think Ben did a great job describing the basic
concept of the trusted submitter programs, at least the
ones that Google operates.

Today we have trusted submitter programs for
search, for You Tube for Blogger and for Picasa, among
our services. As has been mentioned, there are similar
programs that other large online service providers have
also created.

At Google this really started in 2010 when,
you know, we were thinking how can we improve the
efficiency of the process. And we were seeing that a
lot of our resources were used attending to notices
that were submitted by sometimes individuals, sometimes
companies, vendors, who were not clear about the
process who ended up filing incomplete notices, notices
that were misdirected. That ended up taking a lot of
our internal effort.

And it was our suspicion at the time that
probably, you know, to use the old 80/20 rule, probably
80 percent of the notices that we were getting were
probably coming from 20 percent or fewer of the
submitters. And for those that were sophisticated,
reliable repeat players, that there must be something
we could do to essentially facilitate their submission
without getting them trapped in the queue behind some
of the notices that were more prone to being incomplete
or otherwise invalid or erroneous.

So that was the intuition that started our effort. And, in fact, now four years later, we have actually seen that intuition more than confirmed. Today I actually was just checking with some of our folks. We have just under 100 individuals or 100 entities, I guess I should say, that are part of the trusted submitter program for web search. And those hundred odd submitters submit well above -- well in excess of 95 percent of all the notices that we receive for search are from those hundred entities. So it was much more than 80/20. It turned out to be more like 95/1.

And I think my -- the feedback that I received from rights holders and vendors that use the trusted submitter program has been generally quite positive. We at Google have been quite grateful in developing these programs we've worked with content owners in the development program when we launched the original trusted submitter program for web search back in 2011, we did so in cooperation with folks from the content communities. So that's been very helpful.

MS. BLANK: Let me interrupt you. I want to have a teaching moment. So what I'm hearing from you, though, is that there was a problem on both sides. The
notice senders couldn't get their notices in because they were getting trapped and then you guys were getting swamped. Now we have a solution that has benefited both sides.

MR. VON LOHMANN: I think that's absolutely right. Again, I can't speak for everyone but certainly for Google, the trusted submitter programs have been very helpful for the particular problems that we were facing on the services where we had the largest volume of notices.

MS. BLANK: Just out of curiosity, the 100 participants, what kind of sizes do they run? Are they the very large companies or small companies?

MR. VON LOHMANN: I think it's -- it covers a pretty wide range. From our perspective, the two characteristics that we're looking for when we receive applications for the program are, number 1, reliability, a demonstrated track record of good quality notices. We make it very clear to members of the trusted submitter programs that this is aimed at clear copyright violations to really encourage the use of this channel for, as was mentioned earlier, clear examples of infringement rather than edge cases that probably do require a little more review. And volume as the other factor.
The existing -- we attempt to build our public tools as much as possible to allow easy submission of relatively low volumes of notices. So the sort of special features of the trusted submitter program really only make sense if you are going to be submitting in volumes that the default public web form is not going to be able to handle.

So that's sort of the criteria we use. And probably the most important thing, I mean, as you point out, it really is a win-win. And from our perspective, one of the great advantages to creating a trusted submitter program was to create an incentive for good behavior on the part of submitters.

And, in fact, while the vast majority of those who have chosen to participate in the trusted submitter program have been very good, have continued to be very reliable. There have been a few bad apples in that batch who sent repeated bad notices despite warnings, despite efforts to communicate with them, to explain, to try to work through what the issues were. And we have had to kick people out of the trusted submitter program.

And from our perspective it creates a very healthy set of incentives that keeps submission quality high. In fact, I've been thanked by some rights
holders insofar as it has kept the vendor community's quality higher. It keeps the vendors, the enforcement vendors, it keeps them on the ball which is something that both copyright owners and service providers both want. They want their vendors -- everyone wants the vendors to be doing a high quality job.

So, yeah, I think that has been, at least in our experience, it has been a win on both sides.

MS. BLANK: Vicki, you look like you want to ask a question.

MS. SHECKLER: I would like to comment. We do very much appreciate what Google has done with the trusted submitter program with search, but I'd like to put it in context for you. In roughly the past two years, which is when we have been doing this to scale, RIAA alone has sent Google roughly 58 million infringements to de-index in that time. And that's for roughly 300 sites, more or less. It could be like 350, something like that. That suggests that there's a problem with this system.

You may have heard last Friday the Taylor Swift 1989 album leaked. RIAA and its sister organizations have sent over 3000 infringement notices, about that, since Friday. I looked this morning, I easily found 22 links to that album from unauthorized
sources. So while the trusted submitter program is great and very much appreciated, we very much appreciate the new efforts that Google has undertaken to go with that program to help demote some pirate sites and that seems to be working well, we very much appreciate that, I'd like to remind us about the context that we're talking about here and that that is one of the reasons you hear us talk so much about efficacy as well as efficiency.

MR. VON LOHMANN: And, of course, this process that we -- that the PTO has convened here has been about the DMCA process and ways in which that process can be improved. And Google continues to receive as efficiently as possible and act on as expeditiously as we can the notices that we receive. We do not control the web. We cannot stop people all over the web from posting materials that they shouldn't post and we welcome working together with rights holders to identify and remove those from search results when we can. But the DMCA process clearly anticipates the submission of notices and the expeditious action on the part of service providers. And that is exactly what Google has consistently done and what the trusted submitter program is intended to make better.

MS. BLANK: Let me veer off in a slightly different direction for a moment. Keith, you said that
you use vendors to send out notices. Do you participate in any trusted submitter-type programs?

MR. KUPFERSCHMID: Sure, we do. We have various trusted submitter programs that we work with. You know, I mentioned before Ebay and Google. We also have our own sort of not trusted submitter program, but we've created a program somewhat similar that has had its benefits which is on -- that we use on Ebay which is to certify resellers, software resellers.

And really what these resellers do, we give them sort of a certification mark that they would put on that auction site and that helps them with their customers, the people who are going to look for software where they see the certification and they go okay, well, they've been certified by SIA. What that means is they're not selling pirated software, OEM or academic software.

And there's benefits to them for doing that, right. They can draw more traffic or more customers to their particular auction. And there's obviously benefits to us also because then we can hopefully somewhat, I think, what like, for instance, Google is doing and other trusted program do, sort of define, divide the good actors from the bad actors here. And that program that we run or have run does something I
think very similar.

So the benefits of trusted submitter or trusted sender program I think are significant and it would be good to see I think a lot more ISPs take that up; in other words, to improve the efficiency of the DMCA notice and takedown process because I think it benefits everyone. As Fred mentioned, he's found that it's a win-win, I think it is a win-win.

MS. BLANK: When you work with your vendors for sending notices, do you have some kind -- what's your method for making sure they remain good vendors and not run afoul, say, of trusted submitter criteria?

MR. KUPFERSCHMID: I think this is - While I'll just speak for myself, and throw it open to other people, in terms of the vendors that we use or don't use. What we do is we just do just like anyone we do business with, we investigate them first and, you know, through word of mouth and through other means and find out, you know, we're actually looking at one vendor right now that we thought pretty good things of and then I heard some things the other day that maybe called that into question.

And so it's just -- honestly it's just good business practices. I don't think it's anything
specific to vendors. Anyone you do business with, you want to make sure you're doing business with someone who's, you know, ethical in doing business in the right way, whatever that business is.

MS. SHECKLER: I would add to what Keith was saying that it's always good to do diligence on your vendors and to run a trial program as a sender we regularly run trials with our senders before sending any notices from any vendor so that we can assess the quality of them.

MR. SCHEFFNER: And I would raise another example. It's a little bit outside the scope of what we're talking about today, but I think it's highly relevant, which is about our enforcement of peer-to-peer. We the MPAA and the RIAA are involved in something called the copyright alert system which is a voluntary initiative we entered into with a number of the major ISPs here in the US to send notices to identify infringement going on with peer-to-peer networks, then have our vendors send notices to the ISPs who pass along what we refer to as copyright alerts to the individual users.

We have a vendor, MarkMonitor, which scans these peer-to-peer networks and then based -- it does -- it goes through the whole sort of verification
protocol and then they send along notices. No one calls this a trusted sender program, but that's essentially what it is. They -- you know, we and our vendor and ISPs who are the recipients of these notices have worked out the protocols. It's done through machine-to-machine communication using this protocol that we mentioned early on called ACNS, the Automated Copyright Notification System. And it essentially allows for -- facilitates the communication between -- directly machine-to-machine between the vendor and the ISPs.

We think it's worked pretty well in terms of its sort of technical operation. ACNS was not designed just for peer-to-peer. We think it's easily adaptable to the 512© and potentially (D) context as well. And actually one thing that we would like to come out of this process is to sort of include a modified version of ACNS just to use as an example of the kind of scalable machine-to-machine communication that we think facilitates efficiency.

But I would echo a point that Vicki just made a few minutes ago and which I've made at previous of these meetings, which is efficiency is great, we should all be in favor of efficiency. Certainly no one is against that. But efficiency alone does not solve the
underlying problem. I mean, the fact that they've sent hundreds of millions of notices, we've sent tens of millions of notices -- our members have sent tens of millions of notices is in some ways a success story because, yes, there's these processes in place to process all of this stuff, all of these notices. But in another way it's a failure because it shows that there's massive amounts of infringement that isn't really solved by this process.

MR. VON LOHMANN: Turning to Jenny's original question, I think one very part of assisting in the diligence of vendors is the publication of transparency reports. And Google has a published a transparency report that allows any copyright owner to go and evaluate the record of any of the vendors who have sent us takedown notices. Every notice is documented in the transparency report. You can see what percentage of those URLs that were reported were rejected, how many of them were not rejected. And that, you know, and in my mind that gives you something more to go on in terms of diligence and monitoring the effectiveness of your vendors than simply their word or how they happen to be when you originally did a contract with them.

So, of course, in addition to the transparency report, when we do receive faulty notices from
submitters who are members of the trusted submitter
program, we reach out and try to have a conversation
and say something seems to have gone awry here, and
often that allows the vendor or the rights holder in
that case to fix the issue, which, of course, is the
best outcome for everyone. So there's communication
and transparency as well that's important.

MR. MCCOYD: If I could just add to some of
the points just made. Publishers are not currently
participating in the copyright alert system which was
established by other industries, but we conducted some
or we arranged for some pilots a while back for our
members to use MarkMonitor as well as another vendor
called Irdeto to take advantage of relationships that
those vendors had established with telecoms to -- for
the internet access providers to voluntarily forward
notices to their subscribers who were detected engaging
in infringement of the publisher's titles via
peer-to-peer and some direct publisher-to-vendor
relationships emerged out of that. And that was both
for telecoms within the U.S. as well as those willing
to collaborate, those abroad willing to collaborate
with the vendors.

On the transparency piece, we are very
supportive of collecting data as Fred just mentioned
and was also reported in the presentation given this morning. One issue that we've taken note of is on Chilling Effects, when the service provider forwards its notice, at least as far as we can see, the full links that were reported are included. So -- and I know Sandra has mentioned as part of the technical working group's discussions in the past, looking at transparency as a whole and seeing, for example, if automated measures can be implemented to redact a portion of the link because in some instances if you search for a popular book title, on the first page of results you will occasionally see a Chilling Effects, a link to a Chilling Effects page. And if the person is resourceful enough to click through and copy and past links in the notice, they will come across some infringements which are still live. So just a potential future piece of work that I'd like to posit.

MS. BLANK: Thank you. This time went very quickly. Somehow I thought it would feel like we had more time. But I want to thank everybody for being available today to talk about this issue. I think we have more to talk about and I think that it will come up naturally as our process continues. And at this point I would like to ask John Morris from NTIA to come and say some final remarks for us.
MR. MORRIS: Reclaim my identity.

Thanks, Jennifer. Really just a closing thank you. I mean, I think -- Shira and I thought that this was an extremely constructive meeting that -- I mean, obviously the work that -- Jim and Sandra have been leading the work that all of you have been doing, has made an enormous amount of progress. And then the participation both on the phone and in person with a lot of new ideas and new things for the stakeholder group to really grapple with were very, very helpful. And this panel I thought was also very helpful.

So really nothing more to add other than to encourage you to keep up the good work. Extend a specific thanks again to Jim and Sandra and thanks to all of you. I think we're done.

MS. BLANK: We're done.

MR. MORRIS: So we're done. Thank you very much for coming out and we'll see you December 5 -- we'll see some of you December 15 or on the webcast. So thanks very much for coming.

MR. PETERS: What time?

MR. MORRIS: I have no idea. Sometime. It will start later than 7 a.m. and it will end before 7 p.m., I'm sure of that. I have no idea. I don't know. Hopefully we'll be able to figure out that soon.
MS. BLANK: Well get that soon, definitely.

MR. MORRIS: Thank you very much.

(Proceeding concluded at 11:53 a.m.)
CERTIFIED SHORTHAND REPORTER'S CERTIFICATE

STATE OF CALIFORNIA       )
COUNTY OF CONTRA COSTA    ) ss.

I, ANGELICA R. GUTIERREZ, hereby certify:

I am a duly qualified Certified Shorthand Reporter in the State of California, holder of Certificate Number CSR 132925 issued by the Court Reporter's Board of California and which is in full force and effect. (Civ. Proc. 2025.320 (a))

I am authorized to administer oaths or affirmations pursuant to California Code of Civil Procedure, Section 2093 (b) and prior to being examined, the witness was first placed under oath or affirmation by me. (Civ. Proc. 2025.320, 2025.540)

I am the officer that stenographically recorded the testimony in the foregoing proceedings and the foregoing transcript is a full true record of the testimony given. (Civ. Proc. 2025.540 (a))

I have not and shall not offer to provide any services or products to any party's attorney nor party who is financing all or part of the action without first offering same to all parties or their attorneys attending the deposition and making same available at the same time to all parties or their attorneys. (Civ. Proc.
2025.320(b))

I shall not provide any service or product consisting of the deposition officer's notations or comments regarding the demeanor of any witness, attorney or party present at the deposition to any attorney or party present at the deposition or third party who is financing all or part of the action, nor shall I collect any personal identifying information about the witness as a service or product to be provided to a party or third party who is financing all or part of the action. (Civ. Proc. 2025.320 ©)

DATED November 6, 2014