LIBRARY OF CONGRESS

UNITED STATES COPYRIGHT OFFICE

SIXTH TRIENNIAL 1201 RULEMAKING HEARINGS

Friday,

May 29, 2015

Library of Congress

Mumford Room

Washington, D.C.

Reported by: Christine Allen,
Capital Reporting Company

A P P E A R A N C E S

UNITED STATES COPYRIGHT OFFICE:

JACQUELINE C. CHARLESWORTH
MICHELLE CHOE
SY DAMLE
JOHN RILEY
STEVE RUWE
REGAN SMITH

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINSITRATION:

JOHN MORRIS

P R O C E E D I N G S

(9:03 a.m)

PROPOSED CLASS 27:
SOFTWARE-NETWORKED MEDICAL
DEVICES

MS. CHARLESWORTH: Good morning, everyone. Welcome to the last of the seven hearing days of the Sixth Triennial Rulemaking proceeding. You can say you were there.

I see some repeat customers and some new faces. I'm Jacqueline Charlesworth, General Counsel of the U.S. Copyright Office. I along with my colleagues here will be presiding over this hearing, which concerns networked medical devices. I am going to just ask them to quickly go down the line and introduce themselves.

MS. CHOE: Michelle Choe, Ringer Fellow.

MS. SMITH: Regan Smith, Assistant General Counsel.

MR. DAMLE: Sy Damle, Deputy General Counsel.

MR. RUWE: Steve Ruwe, Assistant General Counsel.

MR. RILEY: John Riley, Attorney Advisor.

MR. MORRIS: John Morris with NTIA. While I have the mike, can I just express my appreciation from NTIA to the Copyright Office for the courtesy of allowing us to participate in the couple weeks of hearings. It's been very helpful for us to be able to ask some questions, so thank you.

MS. CHARLESWORTH: Good. We will always take appreciation, so thank you, Mr. Morris. As I've explained before, the purpose of these hearings is not so much to go over what you have already submitted in writing, which we have all read carefully, but to kind of focus on the issues that seem most contentious or most in dispute, as well as factual areas where perhaps we have questions or the record may not be as complete as we would like it to be, and finally, a lot of times we are looking at sort of the scope of the exemption and how broad or narrow, how to tailor it to the uses in question.

With that in mind, the format we have been following is we will have you start with an opening statement, and I will warn you we often do interrupt with questions, and end up usually with a very good discussion, and we will sort of

discuss the issues that way.

Once we sort of get through that, if people have things to add or something comes up, you want to comment on it, if you tip your placard up, we will call on you and allow you to respond.

Before we get into the actual discussion, just a couple of things. We are only supposed to have four mikes on at a time, so it is helpful if you can turn it off when you are not talking. We try not to talk over one another. I try to call on people rather than have a free form discussion.

With that said, if you could quickly tell me who you are and the interest you represent, and then we will go back to Mr. West and he can begin with the opening remarks. Dr. West, excuse me.

MR. SELLARS: Actually, let me clarify one point. My name is Andrew Sellars. I am from the Harvard Law School Cyberlaw Clinic representing a coalition of medical device researchers, including Mr. West. I should clarify Mr. West is not a doctor. I think that was a mistake. He has a Bachelor's Degree and is a computer researcher and software engineer.

MS. CHARLESWORTH: Well, we promoted you.

MR. SELLARS: I'm sure he appreciates the promotion.

MS. CHARLESWORTH: I was right when I said "Mr." to begin with. Mr. West, if you want to introduce yourself. I think we sort of heard who you are, but just for the record.

MR. WEST: My name is Ben West. I'm an independent researcher.

MR. SELLARS: My name is Andrew Sellars. As I said before, I'm attorney for Mr. West, Mr. Jerome Radliffe, Mr. Hugo Campos, and Ms. Karen Sandler, who are the coalition of medical device researchers that are petitioning for this exemption.

As we said in our comment --

MS. CHARLESWORTH: Sorry. I just wanted everyone to introduce themselves first for the record. I take it you want to go first, Mr. Sellars.

MR. SELLARS: If that's possible, yes, thank you.

MR. SIY: Sherwin Siy, Public Knowledge.

MS. MOY: Laura Moy, New America's Open

Technology Institute.

MS. CHARLESWORTH: Okay. You may now have the floor, Mr. Sellars.

MR. SELLARS: Thank you, Ms. Charlesworth and members of the panel, good morning. The exemption that the coalition are seeking here is designed to ensure that research that is already being conducted into medical devices is allowed to continue now that these devices, largely at the suggestion of independent research, have begun to adopt technological protection measures governing access to their source code and data outputs.

I would like to actually begin with Mr. West, who with this panel's permission, would like to read a brief statement sort of describing his own research and how it is implicated by technological protection measures, if that is okay.

MS. CHARLESWORTH: Yes, that's fine.

MR. WEST: Hi, my name is Ben West. I have type I diabetes and I use a variety of medical devices such as continuous glucose monitors and insulin pumps. I'm a software engineer. While I was living and working in San

Francisco, I learned that my CGM and my pump contained a wealth of information that was very important to pursuing my therapy.

However, the information provided by these devices is sometimes delayed or even sometimes unavailable. I started looking closely at these devices starting around 2009 or 2008, the information that they store and the ways in which they operate.

My continuous glucose monitor is a two part system. There is a small sensor that I insert under my skin and I replace it every seven days, and there is a handheld receiving computer which displays the current glucose value along with 6, 9, and 12 hour trends.

The sensor transmits a new sensor value every five minutes, and the handheld receiving computer shows the last value with an overall trend.

My collaborators and I are a group of like- minded patients, or often parents of patients. We used a variety of reverse engineering techniques to analyze the data that is stored in this handheld computer. The vendor's own software is used to retrieve up to three

months of data from the device, so we used a combination of hardware and software USB sniffers to create a transcript of the interactions that the vendor typically has with these devices.

After studying these transcripts along with our other research, the community as a whole was able to obtain valuable information that is sometimes not shown to the -- it is information that is available on the device but not always shown or available to the patient.

An example of this is the handheld computer does not show the delta or the difference between my current glucose number and the previous one from five minutes ago. Using our knowledge of the protocol to fetch the data from the handheld computer, we were able to provide patients with not only the glucose and the trend, which is usually provided, but also the delta from this and the previous readings.

We've gone a step further to provide software that conveniently shows this information on mobile phones.

MR. DAMLE: I'm sorry to interrupt. I'm just sort of curious, if you can explain why it is important to have that additional piece of data or

why that is useful to you. That would just be helpful for us to know.

MR. WEST: Sure. There is a display that has the current glucose number. Depending on what that number is, I may need to take action. I may need to leave the room or go get glucose or go take medicine. Because it is changing all the time, it's really, really important to get a good idea of where it has been and where it's going. Being able to tell the last one was -1, I've only changed one point in the last five minutes, versus I've changed 10 points in the last five minutes. That's a very important cue for what I need to do.

MS. CHARLESWORTH: Does the trend just say up or down?

MR. WEST: Yes.

MS. CHARLESWORTH: I see. It's not a numerical value?

MR. WEST: Right.

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

MR. WEST: We provide this information through a mobile -- a wearable software suite, so we put this on mobile phones and wearable devices. This has allowed families to regain common

liberties. For example, we regularly hear from patients who tell us their diabetic children are now able to attend school or miss less school because of the remote monitoring.

This is not something you can do with just the device, you have to get the data off the device and then transmit it somewhere else where it can be remotely displayed.

MS. CHARLESWORTH: Can you explain how it impacts the school day or why they wouldn't be able to attend school, how this would permit that?

MR. WEST: Sure. There is often a sense that you are okay for the next three hours roughly, but beyond three hours, it's very difficult to predict. There needs to be action every three hours, and because you're taking insulin, too much insulin could lead to death or very nasty things.

For a parent to send their child to school with this very dangerous situation, the schools are not always prepared to handle that situation. This allows the parent from work or from home to monitor and keep in touch with the people that are taking care of that child.

Because of that, these are often

scenarios where the child -- they are making a decision to not go to school or to not go on walks with the grandparents or not go to sleepovers because the people that are providing the care don't have the needed facilities to handle it.

The remote monitoring piece allows the parent or someone else to keep track of what's going on remotely. That enables the choice to say okay, we are going to go to school, we are going to go on this first walk with grandpa alone, those types of activities.

MS. CHARLESWORTH: Would the child in your scenario also have a device or a phone with them where they would be able to see, for example, the trend or the information, so is the concern that the child still needs adult supervision in terms of interpreting the data? The child would have information with them, right, at school?

MR. WEST: Yes. Typically, children younger than 14 or so typically do not perform the therapy. It's usually someone else that's helping them perform the therapy. That means the children are usually not monitoring this to enact therapy on their own.

MS. CHARLESWORTH: I'm sorry. I don't

mean to belabor this point too much. When they go to school, do they take a phone or device that is the monitor --

MR. WEST: Yes.

MS. CHARLESWORTH: And then maybe show it to the school nurse? I guess I'm trying to understand the need for remote access versus whatever is with the child at the time.

MR. WEST: Yes, so typically what happens is -- this is my rig. What will happen is we will provide a child with this exact thing, and we will put it in their book bag or even in a spy belt, which is just a belt. That stays with them. Someone else is providing the interpretation and telling them what to do.

MS. CHARLESWORTH: Okay.

MR. WEST: And coordinating the care. For example, if the child goes low during school, a parent at work can call the school and tell them you need to get my kid out of gym class and give them some sugar because they have too much insulin.

MS. CHARLESWORTH: Do you know of any specific children who have taken advantage of that technology or who were not able to go to school

because they did not have the technology?

MR. WEST: Yes. We have a Facebook group called "CGM in the Cloud." This group was created last year. We now have 12,000 members that are in this group, around 4,000 of those people have adopted this kind of system. It's proving to be very, very popular, very, very much in demand, and it is very much meeting a need.

MS. CHARLESWORTH: Thank you. That's very helpful. You can continue with your remarks.

MR. WEST: Thank you. Good questions. This is only possible through the remote monitoring that our research has allowed. Access to this information can also be used to assess the confidence or the quality of the glucose estimate shown on the device. It is showing me a number but how good is that number. Is it stale. Is it accurate. Is it inaccurate.

For a variety of reasons, the glucose estimate on the devices can be incorrect. For some causes such as a new insertion, new sensor insertion, or if I'm dehydrated, the receiver can stop showing glucose estimates altogether. It might show three question marks instead of numbers.

Yet, there is still data available from the sensor and from the device. Once again, our research has been able to get that raw data out of the device and we are able to make use of it, where otherwise you would get no data at all.

Even when no glucose estimate is provided, the metadata from the sensory hardware itself can be used to accurately estimate glucose levels.

In addition, even when glucose estimates are provided, they may be inaccurate. Our research uncovered that patients may receive inaccurate or false readings when pressure is applied to the sensor. For example, when someone sleeps on a sensor. In these events, the raw sensor data can be used to identify when the glucose estimate is incorrect or even when the sensor is beginning to fail.

I was able to do these things because the device is unencrypted on models that are currently available on the market. However, I've learned the next version of the device that I will use for my insulin pump does have encryption. This device is already sold overseas, and will soon replace similar devices in the United States.

The vendor is Medtronic.

I'm asking for this exemption so that the work we have been doing to improve the quality of life for people with diabetes can continue.

MR. DAMLE: I have a somewhat technical question about how you were able to sort of make this work for you. Is all you are doing pulling data off the device? Are you changing the software of the device in any way, or are you only sort of looking at what the readouts are and pulling them off and then doing something with it?

MR. WEST: Good question. Right now, our design behind all of this is to read only. We are not affecting the behavior, we are not changing anything on the device. In fact, we have gone to great lengths to make sure that our usage of this device matches exactly what the vendors themselves do to audit what happens on that device.

MR. DAMLE: That raises an interesting question, I think, for the lawyers, which is why an exemption would be necessary if all that is being accessed is data. Mr. Sellars?

MR. SELLARS: Sure, I'd be happy to address that. The reason why the exemption is

necessary is because on many devices that are on the market today and on more that are coming out in the near future, even accessing the data itself would mean circumventing a technological protection measure.

As we noted in our exemption, some of these devices, the data outputs would be protected under copyright and some would not. I don't think AdvaMed disputes us on that point. It would largely depend upon the selection and arrangement of the information itself.

As we also mentioned in our comments, Mr. West is one of four researchers that are doing different forms of medical device research that are all related to analyzing the source code or data outputs of devices. Some of this research is done as a matter of personal safety and monitoring. A lot of information that is critical to a patient's care is inside of a device and is sometimes not made available to the patient.

Sometimes the symptoms of things, such as a cardiac event, can be indistinguishable from other day to day occurrences, such as dizziness or fatigue. If I'm dizzy, I'm not going to be sure if I have allergies, I missed breakfast, or I'm

having a cardiac episode. My device knows but in many cases it wouldn't necessarily let me know.

MR. RUWE: Would the device that Mr. West was addressing -- is that going to address cardiac arrest symptoms? I think what Sy's question was about, at least I'd like to ask if he wasn't asking, is the information that Mr. West was addressing in the glucose monitor, is that the sort of data that anyone is asserting copyright ownership on or copyrightability of?

MR. SELLARS: The statements of AdvaMed and the National Association of Manufacturers indicate they are asserting ownership in things including sequel databases and other ways in which this data might be ranged.

I would also note in some devices, the data is not streamed in real time, it's dispatched, and when there is a dispatch of data, there is often a greater affordance for an arrangement or selection of particular information. Also, sometimes this data will include metadata about the patient, including who their primary care physician is, who they are, their date of birth, and other information that might be relevant to their care.

MR. RUWE: Is there any detail of the type of data in the readout that Mr. West just addressed?

MR. SELLARS: AdvaMed asserts that a copyright exists there. In many cases, it's not clear until you actually do the reverse engineering whether or not a work would be protectable, and of course, as we all know, reasonable courts can disagree on the edge here.

As this Office has noted in prior rulemakings, when there is an edge case about a state of the existence of a work, they should proceed to the merits of the exemption.

MR. RUWE: Also, Mr. West, just to clarify, the ways in which you are enabling real time monitoring, is that only accessing the data coming off the sensor itself, or does that also involve accessing the monitor, the vendor's monitor and data that may reside there?

MR. WEST: It's both. We have several projects, offshoots, and variants, and we do all those things.

MR. RUWE: Thank you.

MS. CHARLESWORTH: Are you able under your technology -- I take it there are things that

show up on your screen, on the device that you held up, but are you able to do sort of an audit or a printout? What other features, going back to are you printing out something that looks like a report at any point, with columns or headings? How are the data presented?

MR. WEST: What we are doing with it is putting it on wearable devices that are glanceable, so I actually -- one of the pieces that we have is this Pebble watch. We are able to put the numbers on our watch. This does a number of things for me, including the ability to just glance at my wrist and then move on with whatever else I need to do.

As a result, I don't have to stop whatever it is I was doing to press a button on this device and then maybe do something and then go back to work. Let's say I'm an hourly employee at McDonald's. If this device is constantly causing me to stop working so I can test and take care of this device, that's time I don't do work necessarily, or with this, I can glance at my wrist, and then if nothing needs to be done, I haven't wasted any time.

MS. CHARLESWORTH: Your technology does

not generate something, what I would call a printout or spreadsheet or tabulation of data? It's individual pieces of data that are transmitted to like a watch or mobile device?

MR. WEST: We also store all the information that we collect in a database, and that database is owned and controlled by the user. Does that answer that?

MS. CHARLESWORTH: Does it replicate -- do you think that replicates a database that the vendor also has? We're trying to figure out sort of the copyright status of the data. In other words, when you generated a database, did you design the selection/arrangement of how the data are presented?

MR. WEST: I see. The device has a database in it already, so we are pulling out the records from that, and then we are duplicating those records and storing them in our own database. Our database -- we're just using an off the shelf open source database.

MS. CHARLESWORTH: You pull the data from whatever the database arrangement is of the vendor, you are pulling that off through the device --

MR. WEST: Through the device.

MS. CHARLESWORTH: Then you are creating your own new database using that data and you have decided how to organize the new database?

MR. WEST: Correct.

MS. CHARLESWORTH: Mr. Sellars?

MR. SELLARS: I'd just like to follow on this point very briefly. As we noted in the initial comment, extracting data from a database that is itself unprotectable and putting it into your own database is fair use of the work, as the Assessment Technologies of Wisconsin case versus Wire Data indicates, that the data itself is unprotectable. Extracting it from a protectable expression for other uses is a fair use of that. It is actually not infringing use of that in a copy that might be made in order to perform that extraction in-house is likely a fair use, which was in dicta in that case.

If I could address the other members of the coalition very briefly, I think it would be useful to shade in some of the other uses that are being argued for here, amongst the other members of the coalition include Mr. Jerome Radcliffe, whose research has been done into the security of

these systems, in particular, insulin pumps and continuous glucose monitors.

As the opponents themselves stipulate, the research that was done by Mr. Radcliffe and other researchers like him has already spurred reform in the manufacture of these devices, both the Intellectual Property Owners Association and AdvaMed indicate that reforms were made to these devices after, and the key word being "after," these vulnerabilities were disclosed by Mr. Radcliffe.

His research has also been instrumental in how the Government Accountability Office and in turn the FDA have been regulating these devices. The 2012 GAO study that has spurred a lot of FDA's current reform on cybersecurity cites Mr. Radcliffe extensively as well as several other independent researchers.

Additionally, we have Mr. Hugo Campos. Mr. Campos has hypertrophic cardiomyopathy, which is a thickened heart muscle, that can make it difficult at times to pump blood. His research into safety and security is more of a personal nature. He knows from his own research into the field that cardiac events can be triggered by

things such as diet or environment, other different triggers of that nature.

While the device is recording largely at all times whether or not particular impedance of the heart or other heart activity, it often does not share that data with patients until they go in for a check-up. Based on insurance, that often can be 60 to 90 days later.

If I told you that what you had for lunch on February 28 could have killed you and you should not eat it again, I don't know about you, I would be in a lot of trouble because I do not remember what I had for lunch on February 28. That was 90 days ago.

What Hugo has been working to do has been to get better access to the data that is already on the device that is often being dispatched off the device on a much more regular basis, often daily, in order to learn more about his heart activity on a day to day basis because things like what he eats or where he goes or what he does can often be triggers for cardiac events.

Finally, the fourth and final member of the coalition is Ms. Karen Sandler. She is a lawyer and a software expert and does research

into the security of devices at the software level. She along with my co-panelist, Laura Moy, published a study entitled "Killed by Code," which goes into a lot of the vulnerabilities in software to date, and what can be done to spur reform.

I'd like to point out, and something that I think is often missed in the discussion of medical device security itself, is while for our own sort of romantic reasons, we always look toward the espionage or the hackers or the sort of interesting forms of vulnerability and intrusion, what Ms. Sandler and Ms. Moy's research has shown is what tends to affect patient lives most is not this sort of stuff, it's bad code. It is design flaws. It is software miscommunication, power management issues, device restarting and not telling anyone and then not functioning as it is supposed to.

We cited in our comment the study of Professor Homa Alemzadeh who looked at recall history of devices and found hundreds of recalls per year for software issues on medical devices, and estimates the number of deaths attributable is also in the hundreds.

While I think attention has been given a

lot to the potential for vulnerability intrusion, and indeed, that is a valid concern, there is a more fundamental concern here which is that the devices simply aren't working as they should be, and as all fields of software research know, having more people conducting studies and testing these vulnerabilities to simulate their environments and use it to detect whether or not there are problems overall always tends to improve the health of these devices.

I would also just finally note that we are in an area of regulatory overlap here, that in addition to the Copyright Office, the FCC, the FDA, the Department of Homeland Security, all have a regulatory role in the medical device space, and as has been said many times before by this Office, and as a matter of good practice, the primary responsibility for this rulemaking should be to inquire as to whether or not the implementation of access control measures is diminishing the ability of individuals to make non-infringing uses.

On the questions of copyright and piracy, the opposition commenters offer next to nothing to suggest that there would be an issue here in terms of piracy.

As we noted in our comment as well, software is never going to replace the need for one of these devices itself. You can't look at the source code of a pacemaker instead of getting a pacemaker. It is essential to your care. The therapy it provides on a utilitarian level and the inseparability of the hardware and software means it is impossible to conceive of a circumstance where access to the data, data outputs, and source code would actually affect the sale of these devices, and in turn, these works.

Indeed, as this Office has previously noted, having robust security and verification of security actually can improve the sale of works themselves because now you can say I, independent researcher, looked at the Medtronic insulin pump, I audited it for errors, I found none. I trust this device.

That, I think, in my mind, improves the commerciality of the works.

MS. CHARLESWORTH: Okay. A couple of questions. You mentioned the FDA issue. There is a fair amount in the record to suggest that many of the devices you would be seeking to circumvent or that the software resides on devices that are

in fact fairly heavily regulated, certified, reviewed by the FDA, that I think the suggestion is some of these changes or actions could somehow bring them out of compliance or risk bringing them out of compliance.

It's true that is not a copyright issue, but it certainly is sort of a significant issue. I hear you saying it is not a copyright issue, but what about the bigger, sort of the substance of the concern, which is that these devices or that these activities may not be consistent with the FDA's view of the matter?

MR. SELLARS: Certainly. I would say that while I agree the opposition commenters did indeed say that, they offered no substantiation to that point whatsoever. Indeed, as we stated at the outset, what the opponents fundamentally miss is that this research is happening now. This is the state of affairs.

This is the way in which it is normally done, that there is independent research, and the FDA not only tolerates it, they promote it. They hold hearings where they invite independent researchers to come in. They rely upon their research in order to help better improve their own

regulation of these devices. They actively solicit contributions when a person discovers a vulnerability, there is a mechanism that the FDA makes available to report those vulnerabilities or those other issues.

Same with the Department of Homeland Security when a cybersecurity issue is found on a device, there is a mechanism by which the Department of Homeland Security allows people to contact them and help them coordinate a response to that issue.

I would say the history of the research that is done on this device completely refutes the suggestion that the FDA would not approve of this. My indication is they quite clearly would.

MR. RUWE: How would you react to us limiting the exemption in a way that tied the exemption to reporting and working within programs of those other agencies?

MR. SELLARS: Sure. I understand there has been a suggestion in a few of the exemptions, including on vehicles and in the general security exemption, to limit the grant of an exemption here only if you disclose the vulnerabilities that are discovered to certain outlets, either to the

vendors themselves or to certain agencies.

While I agree that the standard course of disclosure is to go to the vendor first when there is an issue, there are absolutely times when it is appropriate instead to go to someone else, including to another agency or perhaps to the press itself.

When there is a vulnerability that is not related to something a hacker could use to intrude, if it is instead just a design flaw, there is absolutely no reason why you couldn't just tell the world that there is a problem with this device and you shouldn't use it.

We have also in our history a sad tradition of medical companies knowing about vulnerabilities in devices and not telling the public until there is a serious issue. We cite a few specific examples including the Therac-25 incident, which involved the linear accelerator. We cited Professors Nancy Leveson and Clark Turner's study on that particular vulnerability.

There is also an issue with Guidant pacemakers where a hardware problem in Guidant was known for at least three years by the manufacturer but they did not tell doctors that they knew of

the problem until a 21 year old man died as a result of that failure and the New York Times in turn conducted an investigation and uncovered the fact that Guidant knew about this issue.

As recently as this year, we have had Wired produce several studies about Hospira infusion pumps that have known vulnerabilities to them, and that Hospira knew about them, and it wasn't until Wired said they were going to publish the story about this issue that they actually issued the notification there was a problem there.

While the medical companies, I'm sure, wish to be proactive in responding to issues, they are at times unfortunately reactive. I think it would be bad policy to adopt a limit to the disclosure.

I also think it raises serious First Amendment concerns. Under the unconstitutional conditions doctrine, it raises First Amendment issues whenever a government entity premises a benefit, even a discretionary benefit, on a speech based restriction, and restricting the audience of speech is a restriction of speech, as the 10th Circuit said in U.S. West vs. FCC.

I think that raises serious First

Amendment concerns if you limit the audience of what you can tell someone after you conduct a field of research.

MR. RILEY: Is this exemption designed or do you envision the exemption being able to pull data from these devices, data that could otherwise be used or subject to test data exclusivity laws for data that is going to be submitted to regulatory agencies? Like the device or whatever devices related to a medicine where it is pending approval.

MR. SELLARS: I think the experience of this research shows there are issues that come up post-market as well as pre-market when it comes to devices being issued. As you indicate, the FDA, when a new device enters a market, has a couple of different regulatory options before them.

If a device is sufficiently similar to a device already in the field, they allow for simple notification of the device entering into the market and the new features. If it is a sufficiently novel or dangerous device, instead they go through pre- market approval, where as you note, there are studies that are conducted often at the funding of the manufacturers themselves,

and as we know, there are also studies that show funded studies by industry tend to favor the industry outcomes. They have a bias there.

I would also note that a lot of the issues that have been found, including by Mr. Radcliffe, are on devices that are already in the market, that are already functioning. New information about them is coming to light.

MR. MORRIS: May I jump in?

MS. CHARLESWORTH: Absolutely.

MR. MORRIS: Mr. Sellars, let me just kind of understand what the exemption is trying to facilitate. I've heard a number of different security problems and different use of data, but are you trying to facilitate or any of your clients trying to do research that would lead to the modification of the software in the device that then goes out and kind of is used on a continuing basis?

We have obviously had discussions about automobiles, and I think in those situations, the people actually want to modify the software, and the device of the automobile runs slightly differently.

I'm unclear whether that is something

you and your clients are trying to achieve.

MR. SELLARS: No. The exemption here is seeking to access the source code and data outputs of the device, not to modify the software that is in the devices. I think there is a suggestion that frankly I find a bit absurd, that people would be doing some of this vulnerability testing on devices used in patient care.

The normal course is that when you are developing a technology that compliments a device or you are trying to access information about how the device is functioning, you use explanted devices. That is the normal course.

MS. CHARLESWORTH: You anticipated the question I was about to ask. There are sort of two branches to your request. One is data readouts from actual patients, like Mr. West here, and then the other branch is sort of the security and vulnerability testing. As you just said, you just reiterated something I think I saw in your comments, which is it would be explanted devices that would not be used again for real patients.

Is that your proposal?

MR. SELLARS: That is the proposal. I would note, however, the two exemptions are quite

linked together. As Mr. West's comments earlier noted, when you are accessing device data about a patient's health, you are often also learning about how the device itself is functioning.

As Mr. West indicated, there is an error that exists in continuous glucose monitors today, which is what he knows as the pressure error, if you lean on a sensor, it malfunctions, it produces bad data.

While there are research done both in terms of individual patients and on the aggregate, one can often inform the other together. In terms of the vulnerability testing, that is done on explanted devices.

MS. CHARLESWORTH: Right. I see them as somewhat distinct requests, although they are blended together in the proposal, because the scope of the devices or the actual devices in one case would be presumably being used by actual patients and in the other case, it is sort of the opposite would be true, they would not be in use by a lot of patients.

I think there was another concern about the fact that once they had been tested, they would then go back into clinical use.

MR. SELLARS: My understanding is that once a device has been tested, it is no longer sterile and can't be used in implantation. I know some studies by Kevin Fu at the Archimedes Research Center at the University of Michigan that have discussed some of the difficulty you have when testing devices to simulate human activity because once a device is out of its packaging, my understanding is you can no longer use that device in patient care.

MS. CHARLESWORTH: Steve? You're good? Did I ask your question?

MR. RUWE: (Off microphone.)

MS. CHARLESWORTH: Great minds think alike. Mr. Siy?

MR. SIY: Thank you. I think I just wanted to touch on a few points that were discussed earlier. One of them was with regard to the copyrightable works issue. I know some of the discussion earlier was about whether or not the data structures and the formats themselves were copyrightable.

I think certainly AdvaMed and some of the opponents have made the case that some of them would be, as Mr. Sellars pointed out, fair

uses or uses of the uncopyrightable elements of those things.

I do want to stress there are also copyrightable works contained within the software of the device itself, and those works are frequently going to be accessed if not necessarily copied under Section 106 through the use of any of these uses.

Also, in the course of security testing on explanted devices, copies may be made and ran in temporary storage and to the question earlier, modifications might be made in the course of that testing.

MS. CHARLESWORTH: That's helpful. Thank you. Did you have anything else?

MR. SIY: No, I think I will yield my time.

MS. CHARLESWORTH: Actually, as long as we are on the law, you have a fair use claim here. What are the other sources of law you would be relying on to access those works if any or the data compilations?

MR. SIY: Sure. Plain access itself would not be an infringing use. Access that led to or acquired essential step copies would of

course fall under Section 117, access and use that required modifications would also fall under Section 117, to the extent those might not even apply in the hypothetical situation, which I don't believe we are facing here, that the software itself is not held to be owned by the patient, I think fair use applies incredibly strongly in this case.

MS. CHARLESWORTH: What is the position in terms of you mentioned the ownership issue, do you know what the practice is? Maybe Mr. Sellars can address this in terms of what the manufacturers say in terms of who owns the software.

MR. SELLARS: Certainly. Of course, in terms of intellectual property ownership of the software, they, of course, own it. In terms of chattel ownership of the device itself, we uncovered no evidence to suggest anything other than the patient being the chattel owner of the device, and the opponents asserted no ownership claims to the contrary.

MS. CHARLESWORTH: They are not asserting -- when you get a glucose monitor, is there a license?

MR. SELLARS: My understanding is that there is no license that is signed at that time.

MS. CHARLESWORTH: Signed or --

MR. SELLARS: Or given. There is no license in my understanding. Our research did not uncover any license.

MS. CHARLESWORTH: It sounds like there is not a practice which is prevalent with a lot of other consumer goods of the manufacturer saying you are using the software and the device that are under a license.

MR. SELLARS: Yes, and I think that also speaks to their being no real after market use of these devices other than the research we have discussed here, nor is there a reasonable way of suggesting that a person could ever lose ownership of something like a pacemaker.

MS. CHARLESWORTH: What about going back to the permanent exemptions in 1201, do any of those help the reverse engineering? You want to address some of that?

MR. SIY: I think Mr. Sellars' written submission covers this very nicely. Again, these might apply in certain cases, but they do not cover the field of the exemptions being requested,

and therefore, at best would be an incomplete solution for some of the uses for some of the devices.

MS. CHARLESWORTH: Okay. Anything further?

(No response.)

MS. CHARLESWORTH: Ms. Moy, did you want to speak?

MS. MOY: Yes. Thank you again for having this hearing and for allowing me to speak here. It's difficult to add anything really large and substantive to what has already been said so eloquently, so I will try to keep my comments this morning brief and just make a few points.

First, as others have commented and as we have said extensively in the record in written comments from multiple parties, vulnerabilities have to be discovered so they can be fixed. There is no other way to do it.

We know through a large body of research and writing on this topic that there are serious vulnerabilities in medical devices, both the types of software bugs that Ms. Sandler and I and a couple of other authors wrote about in our 2010 paper, "Killed by Code," as well as

vulnerabilities that have to do with security.

Device manufacturers are doing really great work making life saving devices, and they work very hard to make the devices as safe as they possibly can, but code inevitably has bugs. It is practically impossible if not actually impossible for manufacturers to eliminate all the bugs before devices go on the market.

Bugs in medical device software and firmware could lead to serious injury or even death for patients through things like delivery of inappropriate shock or inappropriate dosage of insulin, other types of incidents we have heard about.

In addition, problems of medical device software and firmware could expose patients' private records, and this is something we both write about in our 2010 paper and have also discussed in comments.

We know that medical identity theft is a serious threat right now, and accordingly medical records have been the target of a number of really high profile breaches that we have all heard about in the news over the last year. Vendors of medical software and devices are struggling to

protect against that threat.

We have to assist researchers in finding these vulnerabilities as soon as possible so they can be addressed, preferably before bugs either lead to harm to patients or before security vulnerabilities lead to the loss of private data.

MS. CHARLESWORTH: On that point, one of the claims made in the opposition papers is that allowing this sort of circumvention in some cases could lead to like inappropriate access to third party medical records.

In other words, let's say you have a device that is running off a central software system and you circumvent and you kind of get into other patients' records, I don't know if that is something you can address or the others, but is that first of all a real possibility, and second, if it is, how would we address that in the exemption?

MS. MOY: I'll just say briefly that I have seen nothing to suggest that when researchers are working with these devices that they are looking at somehow a manufacturer's database of records, records of multiple patients, but I would also defer to my colleagues who know more about

this than I do.

MR. SELLARS: Certainly. The best paper I'm aware of that addresses these concerns is one by Daniel Halperin and Kevin Fu and others that addresses the vulnerabilities in pacemakers. This is one of the leading papers on the disclosure of vulnerabilities. He noted there were also privacy concerns.

My understanding based on his paper is it was largely about the privacy of the individual whose data was being transmitted, that this data is fairly unidirectional, it goes to the server, and he did not uncover any way by which you could use the medical device to access the computer servers of a Medtronic or Biotronic or Boston Scientific or someone else.

I would also note that the opposition commenters produced no evidence of such a way being possible.

Finally, I would also note again this is an area of regulatory overlap. If you are using a device to access another's server without authorization and thereby obtaining information, that raises concerns under the Computer Fraud and Abuse Act, 18 U.S.C. Section 1039(a)(2).

I think other laws could fill in the gap for bad actors in that scenario.

MS. CHARLESWORTH: Just as a factual matter, you sort of addressed this a little bit, is it possible -- are you saying it is not possible to go through an individual medical device and access a central server where other patients' data may be housed? Is that just an impossibility? I don't think you are seeking that. I get that. I'm just wondering whether certain types of circumvention might actually allow you to do that.

MR. SELLARS: I have not uncovered a circumstance where that would be possible. It seems like this information is unidirectional, as I said.

MS. MOY: Yes, that is also what I have read in my research. The Halperin paper that Mr. Sellars just referenced illustrated that implantable devices, some implantable devices at least were broadcasting the patient's information in the clear, the patient's name, medical record number, perhaps doctor name.

The reason for that is when the patient goes to the hospital, if the patient experiences a

type of event or requires urgent medical assistance, the device can easily be identified, that the patient can be identified, and that service, whatever medical assistance can be provided to that patient.

That was the context in which there was some access to sensitive patient information. It was about, as Mr. Sellars said, the individual's device broadcasting information in an unidirectional manner.

MS. CHARLESWORTH: Okay.

MR. RUWE: There have been some concerns about negative effects from being able to trigger a device to transmit data beyond the ways in which the data would be transmitted by design, and this was battery concerns. Would it be appropriate to restrict access to data that is being transmitted by design?

MS. MOY: We can answer that question, but do you mind if I also finish my opening remarks?

MS. CHARLESWORTH: We didn't realize, so please.

MS. MOY: Do you want to move with that question first, and then I can come back.

MS. CHARLESWORTH: Why don't you answer Mr. Ruwe's question, and then please, by all means, finish your opening remarks.

MS. MOY: Okay. Sorry. Your question was about battery drainage?

MR. RUWE: And other negative effects from triggering the data transmission beyond the ways in which the manufacturer had designed the data to be transmitted.

MS. MOY: As Mr. Sellars was saying and as we were discussing in response to a previous question, research with individual devices that are implantable devices are typically done on an explanted device. Battery drainage is not really a concern.

In fact, performing the type of research that security researchers are doing so that vulnerabilities can be addressed is something that can prevent battery drainage in the future from exploitation of vulnerabilities. If someone is accessing your device without your knowledge, an implanted device, because they are taking advantage of a vulnerability to read information about the patient without the patient's knowledge, that is something that could lead to inappropriate

battery drainage and hopefully security research that is done that allows manufacturers to address such a vulnerability before it is exploited could avoid that type of problem.

MS. CHARLESWORTH: There was another claim on the data prong of this that pinging a device a lot would drain the battery. In other words, if you were gathering data more frequently than had been intended by the manufacturer, you might inadvertently, let's say, drain the battery. Do any of you have a thought on that? Mr. Sellars?

MR. SELLARS: Sure. First, I would note that concern is primarily with devices that are implanted instead of attached to the body. Continuous glucose monitors and insulin pumps, the batteries used I believe are AAA batteries or AA batteries. They are replaceable batteries in any event. The battery concern is nonexistent there.

Mr. West's testimony showed ways in which getting additional information off the device could be quite relevant to a patient's care.

Turning to the question of pacemakers, the research that has been done to date largely

concerns using passive interception of data as it is being transmitted. There are devices called interrogators of devices that allow for that. Those are manufactured by the vendors and are largely left in hospitals and environments, and typically in order to get interrogation of information, you would have to speak with the doctor and make an appointment, and your insurance would have to cover it.

MS. CHARLESWORTH: I'm sorry. I'm certainly not a medical device researcher.

MR. SELLARS: Neither am I.

MS. CHARLESWORTH: A mere copyright lawyer struggling with some of this. That didn't quite answer my question. It answered it with respect to the glucose monitor. You can just change the batteries. A pacemaker, limited battery life, very hard to replace the battery. You circumvent a TPM, and you are again sort of -- you make your own interrogator, you are interrogating the device much more frequently that was contemplated by the manufacturer.

As I understand the claim, that could drain the battery in a way that wasn't expected by the patient or wasn't intended by the doctor

overseeing the care.

How would you address that concern?

MR. SELLARS: It's hard to say the precise concern, as Ms. Moy pointed out, there is research that show that repeated or continuous interrogation of a device would drain a battery. I would also note that the doctor, as you mentioned, often this sort of patient access to data is done in collaboration with a doctor. That is to say a doctor is not always privileged with special access to the data or they have to get it through particular channels, through Biotronic or Medtronic, or one of the other vendors.

Often these sorts of experimentations, these ideas, ways in which to get better access to data are not done without a doctor's consultation. They are done with a doctor's consultation. Of course, a doctor can apprise them of the risks in going forward as indeed all doctors do.

In our revision to the exemption language in the reply comment we deliberately included the term "informed consent," which we meant to be a signal back to tort law and the theory of informed consent there, where a patient would be apprised of the risks of an operation

before going forward, and then affirmative consent would be sought before conducting any sort of access to patient data.

MS. CHARLESWORTH: Right. I would say one of the sort of pitches here, as I understood it, is you wouldn't have to go to the doctor to get this data, that you would have immediate access to it.

MR. SELLARS: I think that is a distinction between the project you are undertaking versus the particular day to day access of data. When you decide you are going to try and get better access to your data, I think it is quite natural for a person to talk to their doctor saying hey, I'm concerned about cardiac events, I know there are ways by which I can get better access to my data than what the device provides for me, and then would go forward from there.

I think most of us when we engage in something that we think complicates our health, we talk to our doctors.

MS. CHARLESWORTH: I would go to my local hacker for that.

(Laughter.)

MS. CHARLESWORTH: Honestly, if it became something you just knew you could do. As I understood it, that was one of the advantages, you didn't have to wait three months for your appointment with a doctor.

MR. SELLARS: I think Mr. West can speak to this better than I can.

MS. CHARLESWORTH: Mr. West?

MR. WEST: My take is if you're going to build an interrogator that does this thing with the battery, you can't do that inadvertently. You can't do that by accident. In order to build an interrogator that is going to manipulate the battery and get it to talk back to you, you must know it does that to the battery.

MS. CHARLESWORTH: You might know that. A layperson --

MR. WEST: What I'm saying is for someone who is going to create a new interrogator device, in order to successfully create that device, they must know that it does that thing to the battery. That is what they have to build it to do.

Does that make sense?

MS. CHARLESWORTH: I understand the

person building -- I think the concern that was raised in the opposition, and of course, they are not here today to present it in their own words, was just that in that case, you are dealing with an implanted device in a real person, and that real person may not realize reading their data frequently or somehow going through that process could be draining their battery in a dangerous way. That's the concern as I understood it.

We're not the FDA here obviously, but we are trying to understand sort of all the parameters that are going into this exemption. I don't know if you have further thoughts.

MR. WEST: Under that circumstance, it seems like it would be important for the patient to be correctly informed like when they are getting the device installed, about the risks of what might happen.

MS. CHARLESWORTH: Who would be doing that informing?

MR. WEST: Whoever is installing the device or who is selling the device.

MR. SELLARS: I would also note, if I may, that there is nothing stopping this activity from happening today, and it is not happening.

There is no evidence brought by AdvaMed to suggest that is happening.

As to devices that do not have encryption on there today, it is possible to create an interrogator that would allow you to do that. We are not seeing evidence of that actually happening. What we are seeing is people building tools that allow for the passive interception or better access to data.

As Mr. Siy noted in a blog post he wrote for Public Knowledge, the device often will be accompanied with a monitoring base station that will be transmitting this on a daily basis instead of the 90 days I mentioned earlier.

I would find a lot of the concerns indeed raised by the opposition commenters completely unfounded. They are pretending as if this activity isn't happening yet and this is the only hurdle that is preventing it from happening.

As to unencrypted devices, this is happening now, and there are not the risks that are being presented by the opposition commenters.

MR. RUWE: Did I misunderstand, as far as what you are seeking, what uses are being employed, would it be appropriate for us to limit

the exemption to the monitoring of passive, for passive monitoring of implanted devices? Would that be problematic?

MR. SIY: I believe it would be. I think the opposition by AdvaMed merely suggests a hypothetical drain in certain uses. I think that drawing a bright line rule -- if we are concerned about battery life, drawing a bright line rule based upon what is being transmitted and the characteristics of transmission rather than the characteristics of the battery, it seems to me a poor fit.

In fact, as Mr. West has pointed out, many of the problems that we are seeking to address here come from the fact that information -- - that insufficient information is being received through the existing process as dictated by the manufacturer.

MR. MORRIS: Can I follow up on the hypothetical in the opposition and perhaps ask Mr. West in his capacity as an actual patient, is there a scenario, in a hypothetical, where say there is a glucose monitor that gets fully implanted, that expects to have a 10 year battery life, but using your technique to gather

additional data, it might only have an eight year battery life, so that means he might have to have an additional surgery an extra couple of years early.

Do you envision there could be scenarios where a patient could decide the extra information is worth having the surgery to your shorter than the 10 year battery life?

Ultimately, are there scenarios where the information that the manufacturer is not originally offering but you are offering would be a decision the patient might want to make?

MR. WEST: I think that is conceivable, yes. I think it is also conceivable that someone could come up with an auditing technique that is tweaked such that actually it makes the device last longer. That is an equally likely possibility, not just by auditing this device using my crazy method it could shorten the life, but the other thing it could do just as equally, just as a hypothetical, is extend the life, or as you mentioned, provide much, much better value that may make it worth it.

MS. CHARLESWORTH: Mr. Sellars? I do want to get back to Ms. Moy.

MR. SELLARS: Certainly. Very briefly, I would say also just to build upon what Mr. West just said, the personalization of care is an area of national concern right now. It was part of the President's State of the Union Address, this idea of precision medicine, this idea of personalizing and customizing care is very much in accordance with other branches of government in terms of national policies, that we are finding that better health outcomes are coming when we consider the patient more as an individual, and these sorts of techniques can benefit that as well.

I am happy to turn it over to Ms. Moy.

MS. CHARLESWORTH: Thank you. Ms. Moy, back to you.

MS. MOY: Sure. I just have two more quick points to make. My second point is vulnerability should be disclosed, that doctors and patients considering devices can incorporate the considerations both about the integrity of the code and security considerations into their decision making.

I would argue that medical professionals and patients have a right to as much information we can provide as possible about the safety and

security features of the devices they might be considering, especially for surgical implantation, and robust security research will help medical professionals and patients make informed choices.

There was one opposition commenter who noted that information about security research of these devices or just research in general about these devices could affect the cost/benefit analysis being performed by doctors and patients.

That is probably as it should be. If I'm considering an ICD and I have a choice between a St. Jude device and a Medtronic device, and there is a recent news article that suggests the St. Jude device is delivering inappropriate shocks that have led to death, that is an important piece of information for me as a patient that I would want to incorporate into my decision making as I decide along with my doctor which device to adopt.

That is something that Karen Sandler herself was considering when she and I wrote this paper in part, following up on her decision to get an implantable device, and she really wanted to take a look at the code so she could make an informed decision about which device to get, and that was really what sparked her research into

this area.

My third and final point is just that vulnerabilities should be disclosed to help the FDA gauge how well the device review and approval process is doing at ferreting out serious problems before devices go on the market.

As Mr. Sellars has pointed out, the FDA has in fact solicited input from the security research community. The security research community is doing important research now that informs the process at the FDA, and in part, the reason that the FDA has been taking additional steps in the recent past to enhance medical device cybersecurity is a response to the very important work of independent medical device researchers in this area.

Thanks again for the opportunity to speak about this. I am happy to answer any questions.

MS. CHARLESWORTH: On that last point, the record suggested that a lot of -- I think it has been mentioned here -- a lot of devices actually don't currently have TPMs, a lot of FDA regulated devices. As you now mentioned, the FDA has sort of stepped up its interest in this area.

Can you sort of give me an overview of like how many of the devices that would be covered by your proposed exemption actually are currently subject to TPMs? I think you suggested the suggestion is that many more will be in the near future and how probable that is. I don't know if Ms. Moy is in the best position, Mr. Sellars. Any of you.

MR. SELLARS: I would be happy to address that. In pages six through eight of my initial comment, we highlight a few specific examples from the vendors themselves. Unfortunately, often we are relying on the vendors themselves to state whether or not they have these things because we are still trying to build additional research here.

Some research that is included in Appendix B to our comment discloses other specific examples. It is very hard for me to give you a percentage. I just don't know.

In terms of future adoption, in October the FDA issued new guidance for cybersecurity in devices which strongly encourages encryption, and my understanding from talking to people who work in the space, when the FDA strongly encourages

something, that becomes de facto law because they go through approval through the FDA.

It is not simple speculation or conjecture. We have the FDA now looking at the cybersecurity of devices as they are being approved.

MS. CHARLESWORTH: Mr. West?

MR. WEST: I currently use a Medtronic pump, the next pump that will come on the market from Medtronic has encryption built into it. For someone like me, this means that I will be losing access to the data on that device.

MS. CHARLESWORTH: Thank you. Do my colleagues have any more questions?

(No response.)

MS. CHARLESWORTH: Mr. Siy?

MR. SIY: Thanks. I just wanted to make one final comment, with regard to the overlapping jurisdiction question, and I think to the extent that the Copyright Office might be considering policy considerations with regard to health, privacy, battery life and things like that, as Mr. Sellars and Mr. West pointed out, these things, this research is already happening, and as they also said, the TPMs are coming.

With the increasing adoption of those TPMs, that is what is altering the status quo, and that is what is increasingly creating the need for the exemption. In other words, I think what is changing here -- what is happening is the status quo is being altered to at least maintain that in the best interest of the patients and the researchers and requires the granting of the exemption.

MS. CHARLESWORTH: Thank you very much. Thank you, panelists. This was a particularly interesting proposal, and an area I hadn't thought much about before. I really appreciate you being here today.

We are going to take a break before our final panel. The last panel of the day is literary works, assistive technologies. We are ending a little bit early. We will stay on track for 10:45. We will be back here for Proposed Class 9.

Thank you again. We will see some of you perhaps later.

(Recess.)

PROPOSED CLASS 9: LITERARY WORKS DISTRIBUTED

ELECTRONICALLY ASSISTIVE TECHNOLOGIES

MS. CHARLESWORTH: Order in the court. I think this is our smallest and final panel of the Sixth Triennial Rulemaking proceeding. Thank you for coming.

We are going to be considering Proposed Class 9, literary works distributed electronically, assistive technologies. Both of our panelists have been here before, so I will spare you the long version of the introduction.

We will state our names for the record, and then we will have you do that. If you want to proceed with your remarks, we will be grateful to hear them.

I'm Jacqueline Charlesworth, General Counsel of the Copyright Office. I and my colleagues will be presiding over this hearing.

MS. CHOE: Michelle Choe, Ringer Fellow.

MS. SMITH: Regan Smith, Assistant General Counsel.

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

MR. RUWE: Steve Ruwe, Assistant General Counsel.

MR. RILEY: John Riley, Attorney

Advisor.

MR. MORRIS: John Morris with NTIA.

MR. REID: I'm Blake Reid. I'm here on behalf of the Samuelson-Glushko Technology Law and Policy Clinic and our partners at the American Foundation for the Blind, the American Council for the Blind, and the American Association of People With Disabilities.

Just quickly before Jonathan introduces himself, I wanted to pass on the regrets of Mark Richert from the American Foundation for the Blind. He was supposed to join us today. He is actually in Alabama giving the commencement address at the Birmingham School of the Blind. A weather system blew through and delayed his flight. He is deeply sorry he cannot be here. We will do our best to fill in in his stead.

MS. CHARLESWORTH: I am sorry he couldn't make it. I hope he gets safely home. Thank you, Mr. Reid. Mr. Band?

MR. BAND: I'm Jonathan Band. I'm here on behalf of the Library Copyright Alliance.

MS. CHARLESWORTH: Okay. Mr. Reid, you may proceed.

MR. REID: Thank you. We appreciate the

opportunity to speak one more time and apologies that we have to be the closing act here. I know you have seen a lot of us this week.

You have also seen a lot of contentious exemptions this week and strong arguments on both sides, and a lot of really complicated issues. I learned an awful lot just watching. We hope this exemption is one of the simplest and one of the easiest decisions you have to make. It is very basic.

It guarantees the right of people who are blind or visually impaired to read books. That is a civil and a human right and it underscores the ability to access information and participate in a democratic society.

I think the good news is it is also very uncontroversial. We are asking for a straight across renewal of an exemption that the Office has recommended and the Librarian has granted several times in the past. We are not asking for any modifications from the last round.

It is largely unopposed and you even heard from the American Association of Publishers who notwithstanding some reservations supports the exemption.

The circumstances of the exemption have not changed except for marginally from last time. It is still necessary for folks to do circumvention, both on an individual and on an authorized entity level. It is still necessary to enable assisted technologies.

I think we have even more evidence, although I don't think it was ever in controversy, that the use we are talking about is non-infringing, after the HathiTrust case last year, and there is still very limited availability and issues with advertising of non-circumventing alternatives like eBooks made available in an accessible format, audio books, and that sort of thing.

The only changed circumstance I think is really material is the Marrakesh Treaty, for which we think at least at a minimum the granting of this exemption is necessary to put the United States in compliance with that treaty.

In short, we really hope you will grant the exemption. I am happy to answer any questions you have. That is all I have.

MS. CHARLESWORTH: Before we get into any questions or move on to Mr. Band, I just

wanted to thank you and your students for helping to make a record in this particular class. It has been very helpful. The written material has been helpful to help establish a need for an exemption here.

Mr. Band?

MR. BAND: I will be really brief. Blake said basically everything I wanted to say, just two points. One, no one is opposing this exemption. The second point, just to reiterate the Marrakesh Treaty point. I certainly hope the United States ratifies the treaty within the next three years, and we would need to have this exemption in place to comply with the treaty. I think that alone would be an adequate basis for renewal of the exemption.

MS. CHARLESWORTH: On that point, on the Marrakesh point, can you elaborate a little bit on the question of the relationship between this exemption and the treaty?

MR. BAND: The treaty has a provision, I believe it is Article VII, that indicates countries need to have a way for people who are blind or authorized entities have to have a way to circumvent technological protection measures in

order to take advantage of any exception under the treaty.

That would map directly on this exemption. It would be better obviously if it was a statutory exception so that you would not have to renew it every three years, but since that is beyond the power of this body, we would have the exemption to enable someone to circumvent in order to take advantage of an exception consistent with the treaty.

MS. CHARLESWORTH: Okay. Thank you, Mr. Band. Do any of my colleagues have any questions?

MS. CHOE: Yes. This is for both of you. The Association of American Publishers in their comments mentioned the EPUB 3 and HTML 5 formats. If you could provide more information about those formats and how they work or don't work as alternatives.

MR. REID: Sure. This actually goes into a broader point that I was hoping to make, which is that we are actually very hopeful those formats, EPUB 3 in particular, will some day see widespread adoption in the industry and actually provide a non- circumventing alternative. In fact, I am hopeful that in our lifetimes, unlike

the other exemptions that I have spoken on behalf of this week, that some day I will be able to send you guys a letter and say we are not seeking renewal of this exemption because all of the books that are being put out by the publishers are coming out in EPUB 3 format, it's accessible, it interoperates with screen readers and text-to-speech functionality, and Braille displays.

I think there is some hope that the publishing industry will move in that direction, and I think as AAP pointed out, the unfortunate reality is we are not there yet, and I don't think we are going to get there in the next three years.

It may be a very different story three years down the line, but at this point, adoption by publishers has been inconsistent. The availability of titles in those formats and the interoperability of titles that are purchased on particular platforms, with particular readers, still isn't there.

I guess all I can say is stay tuned. I hope to have a different answer to that question next time around. We are not there yet.

MR. BAND: I will just add that even if we come to a point three years from now, six years

from now, where all new books coming out, eBooks coming out, meet that standard, you still will always have the problem with Legacy books.

I think we would still have to be seeking an exemption for Legacy eBooks because not everything is going to be up to that technology.

MR. REID: It is worth noting that addressing the sort of access to the archive is going to be a really hard problem to address because every year that goes by, the books are not coming out in those formats, we are also creating a volume of books that doesn't exist in an accessible format.

There are also a number of other challenges related to accessibility, like the user interfaces on devices like tablets and phones on which people are reading these books. The technology has a long way to go.

I really would encourage you guys -- I'm sorry Mark was not able to be here today -- if you have a relative or family member or friend who is blind or visually impaired, ask them to go through the process of how they use a tablet or E-reader to read a book even when it is made available in an accessible format.

You will think that it is broken first. You will hear this computerized voice talking really fast, and you will start hearing the book being read. Think of Siri reading a very long book to you. This is not an ideal solution.

I think the technology has a long way to go. I also want to emphasize this exemption isn't going to fix everything about eBook accessibility, and I want to make sure that we don't claim that it does. At least at this point, it is a really helpful Band-Aid for folks who are looking to either engage in self help or looking to make books available, for example, to their students or to their clients at an authorized entity.

That is why we are asking for renewal.

MS. CHARLESWORTH: Okay. Any further questions?

(No response.)

MS. CHARLESWORTH: Congratulations. This has been the shortest panel, and a good way to wrap up these hearings. Thank you both very much for being here on behalf of your clients today.

This will conclude the Sixth Triennial Rulemaking hearings. We are getting out a little

early. We can have a nice lunch. It is Friday. Thank you all again and to those who watched from the audience for being here today.

(Whereupon, at 10:59 a.m., the proceedings were adjourned.)

CERTIFICATE OF NOTARY PUBLIC

I, CHRISTINE ALLEN, the officer before whom the foregoing proceeding was taken, do hereby certify that the proceedings were recorded by me and thereafter reduced to typewriting under my direction; that said proceedings are a true and accurate record to the best of my knowledge, skills, and ability; that I am neither counsel for, related to, nor employed by any of the parties to the action in which this was taken; and, further, that I am not a relative or employee of any counsel or attorney employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

_____
CHRISTINE ALLEN
Notary Public in and for the
DISTRICT OF COLUMBIA

Q

