UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Facebook, Inc.
Petitioner

v.

Rembrandt Social Media, L.P.
Patent Owner

IPR2014-00415
Patent 6,415,316

PATENT OWNER RESPONSE

TABLE OF CONTENTS

EXHIBITS

Exhibit	Description
REMBRANDT 2001	Summons in a Civil Action, *Rembrandt Social Media, LP v. Facebook, Inc. and AddThis, Inc.*, No. 1:13-cv-158 TSE/TRJ (E. D. Virginia)
REMBRANDT 2002	Solomon, M.B., USPS formally launches new "Priority Mail" product with next-day delivery window, DCVelocity, August 14, 2013
REMBRANDT 2003	USPS PCC Insider, July 2013
REMBRANDT 2004	USPS Priority Mail Express
REMBRANDT 2005	USPS Location finder: Menlo Park, CA
REMBRANDT 2006	FedEx Tracking for No. 797846335373 (February 6, 2014 - February 10, 2014)
REMBRANDT 2007	FedEx Service Guide September 2013
REMBRANDT 2008	FedEx Transit Times from Palo Alto, CA to Atlanta, GA
REMBRANDT 2009	FedEx Value-Added Options, Saturday Delivery
REMBRANDT 2010	FedEx Rates and Transit Times
REMBRANDT 2011	Declaration of Mark T. Jones, Ph.D.
REMBRANDT 2012	Curriculum Vitae of Mark T. Jones, Ph.D
REMBRANDT 2013	Transcript of October 3, 2014 Deposition of Edward R. Tittel

I. INTRODUCTION

The ’316 patent allows users to present diary pages over the Internet without having to set up their own websites, while giving them control over who is permitted to view particular content on the pages. Representative claim 1 presents the central disputed issues in this IPR.

The claim provides a diary server that stores, and sends to the user systems upon request, four types of information: (1) the content itself; (2) a “page design” that specifies how to present the content on the diary page; (3) “configuration information” including “privacy level information” that determines who can view particular content on the page; and (4) a “diary program” that dynamically combines the content and page design to assemble a “cohesive diary page” that is in accordance with the configuration information.

While there are several differences between the claims at issue and the prior art relied upon by Petitioner as set forth in the Preliminary Response, Patent Owner will focus here on those relating to the “privacy level” claim requirements.[1] Specifically, claim 1 as construed requires that the “privacy level information”

[1] Although the Patent Owner focuses here on the “privacy level” issues, we nevertheless maintain the arguments presented in the Preliminary Response and hereby incorporate them by reference.

(1) be sent from the server to the user system and (2) describe or specify who is permitted to view particular content on a cohesive diary page. There is no dispute about the first requirement—that the privacy level information must be sent from the server to the user system. There is a dispute about the construction of privacy level information, but both the parties and the Board agree at least that it "describes or specifies" who is "permitted to view particular content on a cohesive diary page." The only dispute is whether, as Patent Owner contends, the word "level" implies a gradation, or universe, of one or more users permitted to view particular content on the page, and not just one or more individual users within the gradation.

In its Preliminary Response Patent Owner argued, as it does now, that under any of the competing constructions the Salas prior art reference does not disclose privacy level information at all, because its "access information" does not control who can view content ***on the diary page***. Instead, Salas's "access information" controls only access ***off the diary page*** to files represented by icons on the page. In any event, Salas's "access information" is stored and used at the server and not sent to the user system as required by the claims.

In its Institution Decision the Board concluded that "on this record" Patent Owner had not proved that Salas's access information was used at the server and not sent to the user system. Respectfully, we ask that the Board reconsider both points in light of the deposition testimony of Petitioner's expert Mr. Tittel and the

Declaration (submitted herewith) of Patent Owner's expert Dr. Jones, which have materially enlarged the record. Mr. Tittel concedes that it is the server, not the user system, that consults the access information stored in its own database to determine the access rights of a user, and that Salas nowhere discloses sending access information to the user system. Dr. Jones makes the same points in his Declaration. And as we show below, the text of Salas supports the agreed upon position of the two experts. Thus, Salas falls well short of the '316 claims because its "access information" is not "privacy level information" and in any event is not sent to the user system.

Petitioner relies upon the Parker reference in combination with Salas. But Parker does not fill the gaps in Salas.

Like Salas, Parker's access control takes place at the server, not at the user system. And like Salas, Parker controls access to the files represented by icons. Mr. Tittel's only argument for the supposed relevance of Parker is that, unlike Salas, Parker modifies his icons to visually reflect the individual's access rights to the files represented by the icons. Mr. Tittel and Petitioner argue that by modifying his icons Parker is sending privacy level information to the user system. That argument is wrong.

In the first place, as Mr. Tittel agreed in his deposition, "privacy level information," properly construed, refers to "different gradations" of users who are

permitted to view content on the page. While a gradation may have only a single member, the "level" itself must be described or specified in the privacy level information, not just some individual's access independent of the level. As we discuss below, we urge the Board to modify its construction of "privacy level" information to require that the level, not just an individual with access, must be described or specified. Under that construction, the modified icons in the combined system would at most reflect the access rights of an individual user, not a "level" of users.

In any event, even under the Board's existing construction, combining Salas with Parker would not result in sending privacy level information from the server to the user system. In Parker, even when the icons are crossed out or grayed out, or supplemented by a lock symbol, they are still visible, and so their form does not control viewability of the icons themselves. And it is the icons and associated file names—not the files represented by the icons—that are argued by Petitioner to be the "content" in this analysis. At most, the combined system would be sending this "content" from the server to the user system. But sending this content does not "describe or specify" who can view the content, and thus cannot be the claimed privacy level information.

Petitioner also points to Parker's alternative of blanking out the icon altogether when the user has no access rights. But, as Petitioner argued in its

Preliminary Response, the server would have no reason to send any information to the user system if the icon was not going to be displayed at all. In its Institution Decision the Board concluded that Patent Owner "provides no support for its contention that Parker's teaching to blank out an icon results in that icon not being sent," and therefore the Board was "not persuaded that Parker's access control information cannot be used to control who can view the icon." (Decision at 19). But, here again, the record has been materially enlarged. Mr. Tittel agrees with Patent Owner that when Parker blanks out an icon the server "won't send any information at all about it." And Dr. Jones supports Mr. Tittel in his Declaration.

Finally, there would be no motivation for anyone to import either Parker's icon modification or his "blank out" alternative into Salas. Parker blanks out the icon only when a user has no access rights. But in Salas all members of an e-room have at least the right to view the files represented by the icons. For example, as Mr. Tittel agreed, all members of the three user "groups" described by Salas in one embodiment—"coordinator; reader; and participant" (14:43-44)—have at least viewing rights. Mr. Tittel declined to take a position whether in this respect the "three groups" embodiment was representative of the Salas disclosure as a whole, because he had never considered the question. But Dr. Jones explains in his Declaration that the three groups embodiment is representative in that Salas nowhere teaches that any e-room member would be denied at least permission to

view the files. The result of this is that Salas would have no reason to import Parker's "no viewing rights" icon modification because none of his members lack viewing rights. And since Parker blanks out his icons only when a member has no viewing rights, Salas would have no reason to import that alternative either.

The patentability of the challenged claims should thus be confirmed because the cited references, alone or in combination, fail to meet the privacy level limitations of the '316 claims at issue.

II. ARGUMENT

A. The Disclosure Gaps in Salas

Before turning to the two fundamental differences between the Salas reference and the claims—the gaps—we first provide a brief overview of Salas.

Salas discloses an online business workroom called an "eRoom" that allows business users to collaborate over the web on a common project. (*See* Ex. 2011, Jones Decl. ¶¶ 26-30 and 76-80.) The Salas eRoom "page" is presented in Figure 4, copied below.

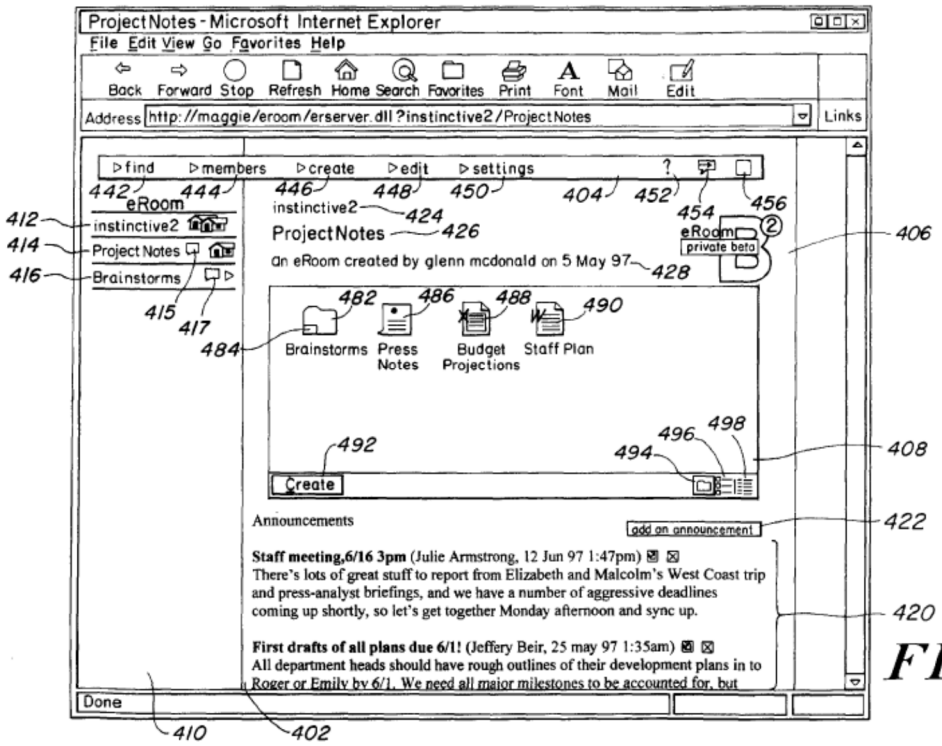
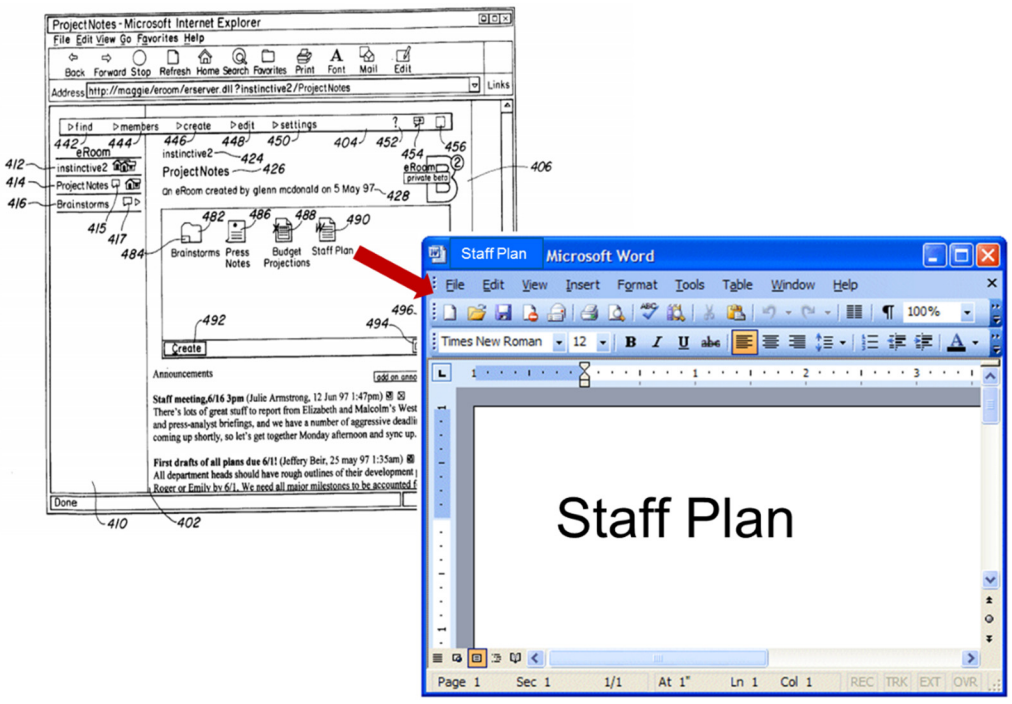


FIG. 4

(Salas, Ex. 1005, Fig. 4.) Item box 408 "collects and displays items associated with the project," such as project-related files, by presenting links to those files displayed either as large icons (shown), as small icons (not shown, but described at 6:7-9 as "small icons with identifying text to one side of the icon"), or as a list with no icons (not shown, but described at 6:9-10 "as a list"). When a user double-clicks on a file icon (within item box 408), which is a link to the file, the file is opened and displayed to the user outside of the eRoom page with the particular application that allows the file to be viewed and edited, such as Microsoft Word or Excel.[2]

[2] *See* Salas at 2:41-43 ("A file request is received from a client workstation. An

As seen in Figure 4 above, "word processing file 490," entitled "Staff Plan," is depicted with an icon that plainly represents a Microsoft Word file. Per the Salas disclosure, in response to a user double-clicking on that icon, the corresponding Microsoft Word file would be opened within the separately launched and executed Microsoft Word application, which could be used to view or edit that file. Although Salas does not include a figure depicting such an opened file, the following represents how double-clicking the "Staff Plan" icon in the eRoom would result, according to Salas, in the opening of the "Staff Plan" file separately within Microsoft Word.



application capable of viewing the file is invoked."); 12:47-66.

Salas further describes that the files (e.g., the Microsoft Word file) may have associated metadata that includes "access information such as which users may open, view, and edit the file."[3]

* * *

Salas is fundamentally different from the claimed '316 invention for two reasons. First, its access control information does not qualify as "privacy level information" under any of the proposed privacy level constructions because it does not relate to the viewability of content "on a cohesive diary page." Second, the Salas access control information—even if we assume contrary to fact that it is privacy level information—is never sent to the user system, as required by the claims.

1. The Salas "Access Information" Is Not "Privacy Level Information" Under any Proposed Construction Because It Does Not Concern Who Can View Content on a Diary Page

As seen below, everyone agrees that "privacy level information" must relate to the viewability of particular content on a cohesive diary page:

> **Petitioner's Proposal:** "configuration information that describes or specifies at least one user permitted ***to view particular content on a cohesive diary page***" (Petition at

[3] Salas at 13:52-57.

> 24, emphasis added.)
>
> **Patent Owner's Initial[4] Proposal:** "configuration information that describes or specifies which user(s) or categories of users are permitted ***to view particular content*** data ***on a cohesive diary page***" (Initial Response at 12-13, emphasis added.)
>
> **Board's Initial Decision:** "configuration information that describes or specifies at least one user or category of users permitted ***to view particular content on a cohesive diary page***.'" (Decision at 10, emphasis added.)

And as both experts agree, the viewable content on a cohesive diary page is that which has been combined with page design to form the page. The Petitioner's expert Mr. Tittel explains:

> Q. So have you gone over these different proposals for the interpretation of privacy level information?
>
> A. Yes, sir, I have.
>
> Q. Okay. And you see that they all talk about permission to view particular content on a cohesive diary

[4] The Patent Owner's current proposal, explained in Section II(B)(2)(a) below, includes the emphasized language.

page; right?

A. Yes. In fact, the language looks like it's identical in all three versions.

Q. Right. Okay. So the content on a cohesive diary page refers back to the claim and is talking about content that is combined with the page design to create the cohesive diary page; is that correct?

A. The language of the patent is that content data and a page design to specify its presentation are all included in the sending clause as well as in the assembling clause.

Q. Right. So the content that we're talking about in these claim constructions is the content that is combined with page design to assemble the cohesive diary page; correct?

A. Yes.

(Ex. 2013, Tittel Dep. 12:4–13:3.) Dr. Jones concurs. (Ex. 2011, Jones Decl. ¶¶ 21-23.) With this background in mind, making clear that "privacy level information" must relate to the content data combined with the page design to form the cohesive diary page, we now turn to Petitioner's privacy-level argument, starting with Petitioner's position on "content data" in Salas.

a. The Salas Content Data

For "content data," Petitioner relies only on the "'Announcements' and "representations of items in item box 408,"—i.e., the displayed file icons and associated file information. The Board acknowledges as much in the Institution Decision:

> For "content data including an associated time," Petitioner relies upon entries under "Announcements," and the representations of items in item box 408. Pet. 32-33. The entries are time-stamped, and the representations of items include a creation date and a modification date; both, therefore, "includ[e] an associated time," as recited. *Id.* at 33-35.

(Decision at 15.) As implied by the Petition, and as freely admitted by Petitioner's expert Mr. Tittel during his deposition, the Petitioner is not relying on the files themselves for the "content data" element of the claims. This is not surprising, as the files themselves are not combined with the page design and are not presented on the cohesive diary page. Mr. Tittel explains:

> A. … So, you know, the interesting thing about webpages is that we have links on them, and -- and the -- and for the purposes of the specific page, the -- the presence of the link represents a kind of content, but in terms of what that content can do, it represents further content that would be available to the user of that eRoom.

> Q. But it wouldn't be displayed on the page?
>
> A. No, it -- it's manifestly not present on the page. Yes, that's correct.
>
> Q. So the content -- so those files that you could access by clicking on the icons 482, 486, 488, and 490 do not represent content on the cohesive diary page; correct?
>
> A. On -- yes, sir. On the page that's on display, that's correct.

(Ex. 2013, Tittel Dep. at 18:14-19:5.) This is of course because the files are opened and displayed not as web pages by the browser but instead by the relevant file application, such as Microsoft Word or Microsoft Excel, as Salas makes clear.[5]

Mr. Tittel further admitted that the files themselves are not combined with the page design in Salas, which necessarily follows from the fact that the files themselves are not presented on the displayed eRoom page:

> Q. … Now, the actual files that 482, 486, and 488 and 490 would lead you to if you clicked on those icons, those files are not combined with the page design in Salas. Do you agree?

[5] *See* Salas at 2:41-43 ("A file request is received from a client workstation. An application capable of viewing the file is invoked."); 12:47-66; Jones Decl. ¶ 23.

> A. The -- there are links to those files in -- in that, but the contents of those files are not combined.

(Ex. 2013, Tittel Dep. at 22:25-23:6.)

With the alleged content data now clear, we turn to whether Salas discloses the claimed "privacy level information." As explained below, it does not.

b. The Supposed Salas Privacy Level Information

In response to the Petition, the Board was convinced that "on the present record" Salas teaches "privacy level information" in two ways. Each is addressed below, along with citations to new evidence and thus a much broader record than when the Institution Decision issued.

First, the Board pointed to the "access information" file metadata in Salas, which indicates "which users may open, *view*, and edit the file." (*See* Decision at 16; Salas at 13:54-55 (Board's emphasis).) But that access information pertains to the files themselves, as Salas makes clear and as Mr. Tittel confirmed during his deposition:

> Q … So if you could now, in the Salas patent, take a look at Column 13.
>
> A. Yes, sir.
>
> Q. Lines 54 and 55.

File metadata may include: the name of the file; the size of the file; the date the file was created; the date the file was last modified; access information such as which users may open, view, and edit the file; and information regarding the edit status of the file, such as whether an edit lock has been set by a user.

A. Yes, sir.

Q. Do you see the reference to access information such as which users may open, view, and edit the file?

A. Yes, sir.

Q. You see that? That word "file" is referring to the files that you could -- that you're linked to by the icons in Figure 4; is that correct?

A. Yes, with one interesting exception, and that is that the contents of the brainstorms folder -- never mind. I withdraw my remark. I'm sorry.

Q. So the answer is yes?

A. Yes. The answer is yes.

(Ex. 2013, Tittel Dep. at 23:8-24:1, exhibit excerpt added inline.) And the files themselves are not the claimed content data, as explained above. Accordingly, the file metadata "access information" in Salas cannot be the "privacy level information" required by the claims because it does not concern the viewability of content data presented on the cohesive diary page. (Jones Decl. ¶ 24.) Instead, this

metadata pertains only to the viewability of the Salas eRoom files themselves, which are viewed *outside* of an eRoom page. (*Id*.)

Second, the Board pointed to other file metadata such as the "filename, creation date, modified date, and which application should be used to open and edit the file" as meeting the privacy level information element of the claims:

> Moreover, the file metadata "determines what information will be displayed to a user who is viewing a cohesive diary page" by determining the appearance of icons, small icons, or lists in item box 408. For example, Salas teaches that the visual appearance of items in item list box 408 is based upon file metadata such as filename, creation date, modified date, and which application should be used to open and edit the file. See, e.g., Ex. 1005, Fig. 4, 6:4-13.

(Decision at 16-17.) But none of that metadata has anything to do with privacy controls. (Jones Decl. ¶ 25.) It does not "describe or specify" one or more users who are "permitted to view particular content on a cohesive diary page"—which everyone agrees is a privacy level requirement.[6] (*Id*.) That metadata is instead

[6] As explained in detail in Section II(B)(2)(a) below, the only dispute over the meaning of "privacy level information" in the claims is whether, as Patent Owner contends, the word "level" implies a gradation, or universe, of one or

simply information displayed to a permitted user in different ways, depending on the option (494, 496, or 498) that the user has selected:

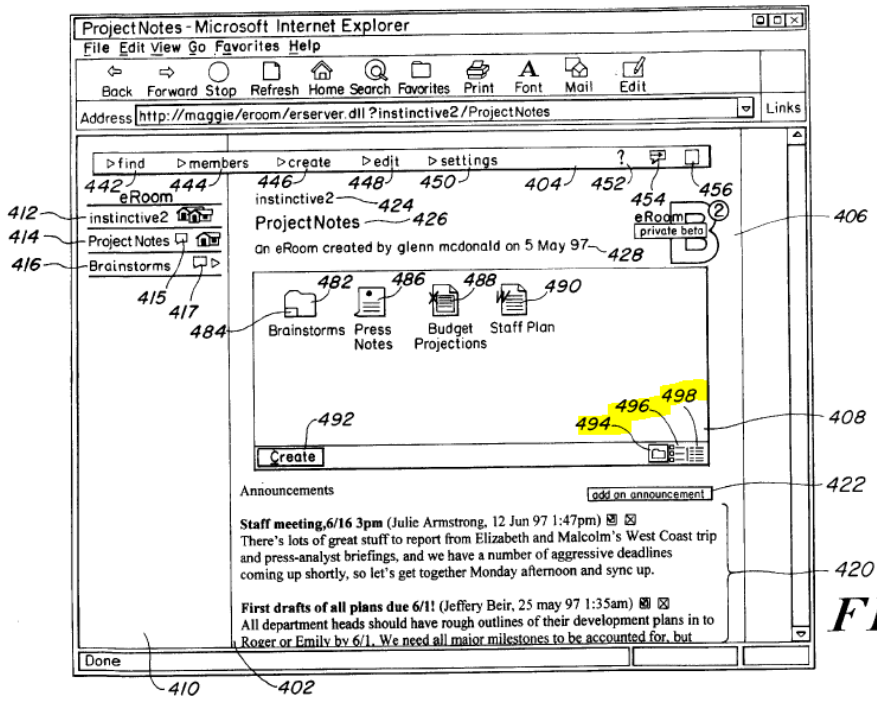


FIG. 4

(Ex.1005, Salas Figure 4, highlights added.)

For these reasons alone, the "access information" in Salas does not meet claimed privacy level information. But even if it did, that information is never sent to the client workstations in Salas, as the Salas disclosure itself makes clear as we explain below.

---

more users permitted to view particular content on the page, and not just one or more individual users within the gradation.

2. The Salas "Access Information" Is Used Only at the Server and Not Sent to the Client Workstations

Salas is clear that "access control" information is stored in a database at the server:

> The server database 20 stores various tables which contain information about eRooms, members, *access controls*, and other data objects.

(Ex.1005, Salas at 3:49-51, emphasis added; Jones Decl. ¶ 31.) The claims, however, require that privacy level information *be sent* from the server to the user system. The relevant question thus becomes: Does Salas disclose sending its server-side access control information to the client? The answer is "no" for the reasons that follow.

In considering the arguments made by Petitioner and Patent Owner on this question, the Board noted in the Institution Decision that "on this record, we are not persuaded by Patent Owner's argument that the access checks described [in Salas] are necessarily performed on eRoom server 14." (Decision at 17-18.) The record has been substantially enlarged since this decision, however, in particular with respect to the synchronization, editing, creating, and modifying of project files as described in Salas columns 11-13. This is the very disclosure that the Petitioner cited in support of its argument that Salas discloses sending access information to the client workstations (see Petition at 40-41) and that the Board

relied upon in rejecting the Patent Owner's previous arguments (Decision at 17-18). But the record now includes sworn deposition testimony from *Petitioner's own expert* that this disclosure (1) repeatedly teaches server-side rights checking and (2) nowhere teaches sending access control information to the client workstations. The record further includes the Declaration of Patent Owner's expert, Dr. Jones, who agrees with Mr. Tittel on the meaning of this critical Salas disclosure. Given the enlarged record, as explained in detail below, the Patent Owner respectfully requests that the Board reconsider.

a. The Salas Synchronization Technique

The centerpiece of Petitioner's argument that the Salas disclosure supposedly "makes clear that this privacy level information is transmitted to the client workstation (12) prior to the display of the eRoom page" is the Salas "synchronization technique" that is described in column 11 and the top of column 12. (Petition at 40-41.) We thus begin there.

Column 11 makes clear that the synchronization is done "to ensure that the objects from the local database and locally stored files are not stale before inserting them into the eRoom template." (Salas 11:14-16; Jones Decl. ¶ 32-33.) In operation, when an "object needs to be synchronized, the updated object may be requested from the server[.]" (Salas 11:32-33; Jones Decl. ¶ 32-33.) And in response to this request from the client workstation:

> The server 14 transmits to the client workstation 12' any data objects ***to which the user has appropriate access rights*** that also have a modification tag value greater than the modification tag value sent with the synchronization request.

(Salas 11:52-54, emphasis added.) Because the server only sends objects to which the user has appropriate access rights, the access checking must necessarily be done at the server, as Mr. Tittel admitted:

> Q. Now, in your report, you rely on what I'll refer to as the synchronization discussion?
>
> A. Yes, sir.
>
> Q. That runs through Columns 11 and 12 as evidence that access information is sent down to the user database, the local database?
>
> A. Yes, sir.[7]
>
> * * *
>
> Q. . . . So that synchronization request is sent to the server?
>
> A. Yes, it is.

[7] Ex. 2013, Tittel Dep. at 40:2-8.

> Q. Okay. And then the server sends back to the client any data objects to which the user has appropriate access rights?
>
> A. Yes, that's correct.
>
> Q. And so the server must be making that judgment as to whether the client workstation has appropriate access rights, and it's going to send only those data objects to which the user has appropriate access rights; isn't that right?
>
> A. That's what the language of the patent says.
>
> Q. Right. And so that activity that I just described is happening at the server after it receives a synchronization request; correct?
>
> A. That is what the language of the patent says.[8]

(Ex. 2013, Tittel Dep. at 44:2-22.) Dr. Jones concurs. (Jones Decl. ¶ 34.)

Petitioner points to the continued discussion of the synchronization process at the top of column 12, where Salas discloses that "local database metadata has been updated" (12:1-3) and suggests that this teaches updating *all* metadata including the access rights metadata. The Petitioner states:

[8] Ex. 2013, Tittel Dep. at 44:2-22.

> This synchronization results in the file metadata – which includes the access rights discussed above – being transmitted to the user system. "Once synchronization has been accomplished and local database metadata has been updated, the appropriate data objects are inserted into the eRoom . . . ." (*Id.*, 12:1-3.)

(Petition at 40-41.) But neither Dr. Jones nor Mr. Tittel agree with Petitioner.

Dr. Jones explains that updating "local database metadata" refers only to the modification tag that is so important to the Salas synchronization technique, as explained in column 11. (Jones Decl. ¶ 35-36.) Dr. Jones further explains that the mere statement that "local database metadata has been updated" teaches nothing about what specific metadata has been sent to the client workstation, whether it even includes *file* metadata, let alone the only file metadata relevant to Petitioner's argument: access information. (Jones Decl. ¶ 36.) In fact, as Dr. Jones explains, the previous unambiguous disclosure in column 11 that access rights are necessarily checked at the server *before* the objects are sent makes clear that whatever metadata is sent, it does not include access information. (Jones Decl. ¶ 37.) And Mr. Tittel agreed that there is no discussion—in words or in substance—of updating *access information* file metadata in this passage:

> Q. … And then at the top of Column 12, it says, "Once synchronization has been accomplished and local database metadata has been updated," et cetera, et cetera;

right?

A. Yes.

Q. And the updating of the local database metadata that they're talking about there is the updating of the modification tag; right?

MR. WEINSTEIN: Object to the form.

THE WITNESS: It -- it doesn't say that explicitly.

Q. . . . But in context, that is what it's talking about, don't you think?

A. The preceding topic addressed both the new received modification tag value, but it also talks about the received data objects, and data objects have metadata associated with them. So it's not clear to me that the only thing that's changing is a modification tag count.

Q. Okay. But there's certainly no indication there that access information is being updated?

MR. WEINSTEIN: Object to the form.

Q. . . . Isn't that right?

A. The words access information is being updated do not appear in that paragraph.

Q. And the substance of updating access information is

not appearing there either; isn't that correct?

MR. WEINSTEIN: Object to the form.

THE WITNESS: There is no discussion of the updating of access information in that paragraph.

(Ex. 2013, Tittel Dep. at 49:24-51:7.) And because there is no discussion of updating access information in that paragraph, those of skill would not interpret updating "local database metadata" as teaching sending of access information. (Jones Decl. ¶ 38.)

Indeed, to interpret this "updating" passage as including the updating of access information would imply that access data was already present in the user system and in need of updating. But there is no suggestion in the synchronization discussions that, even though the access check takes place at the server, a duplicate of the access information is also (needlessly) stored at the user system. (Jones Decl. ¶ 39.) Nor is there any indication that the access rights change during the described synchronization process and would thus have any need to be updated. (*Id*.)

Thus, the file synchronization discussion in Salas, far from supporting Petitioner's argument, actually supports Patent Owner's position—that access information is used at the server to check access rights and never sent to the client workstation—a point which is further evidenced by the Salas file edit-lock

technique explained in column 12 immediately following the synchronization discussion.

b. The Salas Edit-Lock Technique

With respect to the edit-lock technique, the Board stated that Figure 6[9] and its description in the specification failed to support (on the then-current record) the Patent Owner's view that this disclosure describes access-rights checking at the server and not the user system:

> Patent Owner argues that the access check depicted in Figure 6 and described in column 12 of Salas "takes place at the server, not at the user system" (Prelim. Resp. 20), but Figure 6 is described as "a flowchart of the steps taken by a client workstation" (Ex. 1005, 3:4-5), and the paragraph in question begins by describing "the first step taken by the background daemon." On this record, we are not persuaded by Patent Owner's argument that the access checks described are necessarily performed on eRoom server . . . .

(Decision at 17.)

[9] "FIG. 6 is a flowchart of the steps taken by a client workstation to allow users of the system to edit files[.]" (Salas at 3:4-5.)

It is true, as the Board notes, that the procedure illustrated in Figure 6 begins at the client workstations with the step (602) of checking "for local availability of file. Step (604) illustrated in the Figure—launching the "indicated application" for a downloaded file—is also performed by the client workstation. But column 12 includes a detailed description of several steps that take place *in between* the client steps of checking locally for the file (step 602) and launching the appropriate application after the file has been downloaded (step 604)—and it is now undisputed that those additional steps, which include an edit-lock check, an access-rights check, and if appropriate an edit-lock set, all take place at the server.

The first of these server-side steps is to check for an edit-lock after the first step at the client is complete:

> If the file is not present or is stale, then it must be downloaded from the server 14. The file is checked to determine whether another client workstation 12 has caused an edit lock to be set on the file indicating that the file is being edited. This may take the form of a database query for the object ID associated with the file which returns at least the metadata associated with the file indicating presence or absence of an edit lock.

(Salas 12:27-31.) And as Mr. Tittel explained, that edit-lock check takes place at the server:

> Q. [T]here has to be a check to see whether there's an edit lock?
>
> A. Yes.
>
> Q. That's what it says?
>
> A. That's correct.
>
> Q. And that's at Column 12, lines 28 to 31?
>
> A. Correct.
>
> Q. And [then] it says, "This may take the form of a database query to the object ID associated with the file which returns at least the metadata associated with the file indicating presence or absence of an edit lock." Do you see that?
>
> A. Yes.
>
> Q. Now, what is your position on where that edit lock check is taking place? Is it at the local workstation or is it at the server?
>
> A. It's at the server.

(Ex. 2013, Tittel Dep. at 54:9-55:1.) Dr. Jones agrees. (Jones Decl. ¶¶ 40-42.)

Immediately after this edit-lock check, Salas states that "[i]f no edit lock has been set for a requested file, the access rights of the requesting user are checked."

(Salas at 12:34-36.) This check, too, takes place at server and not the client—again as both experts agree. Mr. Tittel admitted:

> Q. . . . Now, next here, "If no edit lock has been set for a requested file, the access rights of the requesting user are checked." Do you see that?
>
> A. Yes, sir.
>
> Q. That's at the server, too; right?
>
> A. Yes, sir.

(Ex. 2013, Tittel Dep. at 55:7-11.) Again, Dr. Jones agrees. (Jones Decl. ¶ 43.) And as both experts further agree, when an edit lock is required because the user has the appropriate access rights and has indicated editing will occur, that "edit lock is set before the file is downloaded[.]" (Salas at 12:40-41.) This edit lock, too, is set at the server:

> Q. "If the user has appropriate access rights, i.e., can edit if the user has indicated editing will occur or can view if the user has indicated only viewing will occur, the user will be allowed to retrieve the file."
>
> That's happening at the server as well; correct?
>
> A. Yes.
>
> Q. Okay. In the case of a user that indicated editing will occur and edit lock is set before the file is downloaded,

that's happening at the server as well; correct?

A. Yes.

(Ex. 2013, Tittel Dep. 55:14-56:2; *see also* Ex. 2011, Jones Decl. ¶ 44.) It is only *after* these server-side actions are taken that the file is downloaded to the client and second client-side step (604) of launching the appropriate application occurs at the client with respect to the downloaded file. (*See* Ex. 1005, Salas at 12:47-49; Jones Decl. ¶ 45.) That brings us to the Salas disclosure concerning how the downloaded file is opened by the client workstation.

Salas explains that the client workstation knows which application to launch in order to open and view the file (step 604) in one of three ways: (1) using what's called the OLE standard; (2) considering the file suffix; or (3) reading the "file metadata which is transmitted together with the file and indicates which application should be used to open and edit the file." (Salas at 12:49-55; Jones Decl. ¶ 46.) While it is true that the third option is to use "file metadata" sent to the client from the server, as the specification makes clear and as Dr. Jones explains, the file metadata being sent here is not "access information" but instead information that "indicates which application should be used to open and edit the file." (Jones Decl. ¶ 47.) Salas does not teach sending access information to the client here. (*Id*.) The Petitioner's expert agrees:

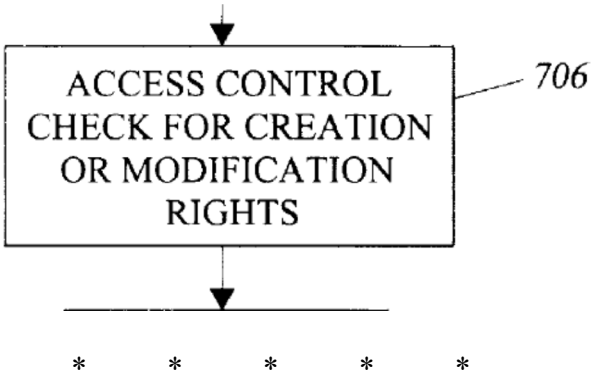
> Q. Okay. And the metadata that it's talking about sending down with the file in the third option --
>
> A. Yes.
>
> Q. -- is metadata that indicates what application should be used to open and edit the file; correct?
>
> A. Yes.
>
> Q. There's no discussion there of sending access control metadata down to the server – or down to the client; correct?
>
> MR. WEINSTEIN: Object to the form. Go ahead.
>
> THE WITNESS: I -- I don't see in the words that we're discussing any mention of access control.

(Ex. 2013, Tittel Dep. at 57:20-58:9.)

The upshot of the Salas edit-lock technique is that access rights information is stored and used at the server, and never sent to the client. (Jones Decl. ¶ 48.) So too with respect to the following and final disclosure of these three critical columns, where Salas explains the technique for creating and modifying files.

c. The Salas File Creation and Modification Technique

The Salas description of how eRoom users create or modify a file begins at column 13, line 10, by introducing the discussion of Figure 7[10] and the "intuitive drag and drop method" to upload new or modified files from the client to server. (Jones Decl. ¶ 49.) By dragging and dropping a new or modified file on the eRoom page, a client-side program (ActiveX control or background daemon) is activated to manage the upload process and the steps that it takes in this process are identified in Figure 7. (*Id*.) The Salas disclosure here makes clear that the third step taken by that client-side program is to check the access rights of the user and that this is done *over the network*:



[10] "FIG. 7 is a flowchart of the steps taken by the client workstation to allow users of the system to upload files to a server using a "drag-and-drop" interface[.]" (Salas at 3:6-8.)

> The user's access rights are checked to ensure that the user possesses "create" or "modification" rights for the page to which the user desires to upload the file (step 706) and the file to be uploaded is stored to local mass storage (step 708). Access rights may be checked *over the network* in many ways.

(Salas Figure 7 and 13:27-32, emphasis added; Jones Decl. ¶ 49.) This disclosure is significant. As Dr. Jones explains, it demonstrates without question that the access information is not on the client workstation because the server never sends them there. (Jones Decl. ¶ 50.) If this information were sent to the client and resident there, this "over the network" disclosure would be not just superfluous, but *wrong*. (*Id*.) For his part, Mr. Tittel agreed with the Patent Owner's view of this critical passage:

> Q. And then the next sentence, in the next paragraph, "The user's access rights are checked to ensure that the user possesses, create, or modification rights for the page to which the user desires to upload the file, step 706. And the file to be uploaded is stored to local mass storage, step 708." Do you see that?
>
> A. Yes, sir.
>
> Q. Okay. So there has to be now a check of the access rights; correct?

A. Yes.

Q. All right. And it says that, "The access rights may be checked over the network in many ways." Do you see that?

A. Yes.

Q. Why are the access rights being checked over the network?

A. This is a distributed system. That means that it is a system that involves actors that are in different locations. In a situation where information has to be resolved about what operations are allowed, we want to communicate from the client to the server.

So there has to be a shared view of what kinds of communications are going to be allowed.

Q. Right.

A. And, again, for reasons of concurrency control, network access controls typically reside in either some kind of a directory services database or in some kind of network account database. And that involves communication with some kind of a server across the network.

Q. Okay. So the user workstation -- well, let's put it this way: The ActiveX control or the background daemon,

> which is resident -- well, that's resident at the user workstation; correct?
>
> A. Yes.
>
> Q. Okay. And so it, namely the ActiveX control or the background daemon, has to go over the network to find out whether the appropriate access rights exist, and it does that by going over the network to the server which has that access control information; isn't that correct?
>
> MR. WEINSTEIN: Object to the form.
>
> THE WITNESS: Yes, that is correct.

(Ex. 2013, Tittel Dep. at 59:11-61:10.) As Dr. Jones explains, Mr. Tittel is correct to observe that "network access controls typically reside in either some kind of a directory services database or in some kind of network account database" and that because these controls reside on the server there must be "communication with some kind of a server across the network." (Jones Decl. ¶ 51.) Dr. Jones further explains that the only reasonable result of this observation in the context of this Salas disclosure is that the access information is not on the client workstation because the server never sends it there. (*Id*.) The remaining file creation and modification discussion provides yet further supporting evidence for this understanding of Salas.

Salas next explains what happens "[i]f the user has the appropriate rights" to create or modify the file. As seen in the passage below, and as Dr. Jones explains, this Salas disclosure makes clear that the file metadata is created and stored at the server and not the client. (Jones Decl. ¶ 52.)

> If the user has the appropriate rights, then a command is sent to the server to create a new file (step 710). This step may be skipped if the user is modifying a file instead of 40 creating a new file. However, creation of a new file allows the server to provide a degree of fault tolerance and version control, if those features are desired. If ***the server*** has been instructed to create a new file, ***a new object is created containing metadata*** associated with the data file and the file 45 is transmitted to the server 14 using HTTP (step 712). If a file modification is occurring, ***the server 14 updates the metadata*** contained by the data object associated with the file and the file is transmitted to the server 14 using HTTP (step 712). The ***server 14 associates the uploaded file with 50 the newly-created data object***.

(Ex. 1005, Salas at 13:38-51, emphasis added.) Thus for a file creation, *the server* creates a "new object . . . containing metadata associated with the data file" and stores it on the server. For a modification, "*the server* 14 updates the metadata contained by the data object associated with the file." In both cases, "*[t]he server*

14 associates the uploaded file" with the metadata. (Jones Decl. ¶ 53.)

Mr. Tittel, again, agrees:

> Q. …. So then moving to the next paragraph where it says, "If the user has the appropriate rights, then a command is sent to the server to create a new file, step 710."
>
> Do you see that?
>
> A. Yes, sir.
>
> Q. And that command is being sent by the ActiveX control or the background daemon; right?
>
> A. Yes. The command comes from the runtime environment on the client side.[11]
>
> * * *
>
> Q. And then moving down to line 43, "If the server has been instructed to create a new file, a new object is created containing metadata associated with the data file," and that new object is being created by the server; right?
>
> A. Yes.

[11] Ex. 2013, Tittel Dep. at 63:7-63:16.

Q. And the file is transmitted to the server using HTTP in step 712; right? And the transmission of the file itself is carried -- is carried out by the ActiveX control or the background daemon; right?

A. Yes.

Q. Okay. And then it says, "If a file modification is occurring, server 14 updates the metadata contained by the data object associated with the file." Do you see that?

A. Yes.

Q. So the server is updating the metadata contained in that data object, which is resident at the server; right?

A. Yes.

Q. And the file is then transmitted to the server using the HTTP step. Okay? You see that?

A. Yes, sir.

Q. Okay. And then the server associates the uploaded file with the newly created data object, and that means that the server has received the file, it's got that newly created data object with the new metadata in it, and the server associates those two things with each other; is that correct?

A. Yes.

(Ex. 2013, Tittel Dep. at 63:20-65:3.) And, again, the upshot is that access control information is stored and used at the server, and never sent to the client. (Jones Decl. ¶ 54.)

* * *

We now turn to the suggestion that, with respect to sending the file metadata in Salas, it is an all-or-nothing situation. The Petitioner argues that just because *some* file metadata is sent to the client workstation—like filename, creation date, modification date, and which application to use—it *all* must be sent. At his deposition, Mr. Tittel seemed to extend this argument by proffering a "mirroring" theory whereby the system maintains a "consistent database structure between the client and server." (Ex. 2013, Tittel Dep. at 42:21-24 and 45:21-46:5.) At bottom, this argument and its "mirroring" extension are efforts to create the appearance in Salas of something that is not actually there: sending access information from the server to the client workstation and storing it there.

We know that this disclosure is not in Salas for several reasons.

First and foremost, as detailed above, *every single action* described in Salas as being related to the access information happens *at the server*, as both experts agree. Both experts also agree on the interpretation of the very important "over the network" disclosure described in Section II(A)(2)(c) above. That disclosure proves that the Salas file access information is not sent to or stored on the client

workstations and thus that shows without question that Petitioner's "mirroring" theory is wrong. (Jones Decl. ¶ 57)

Second, there is no reason to send the access information metadata to the client workstations in Salas given that it is created, stored, modified, and used at the server. And when Mr. Tittel was asked why one would send the access information in light of these disclosures, he gave simply his conclusion (mirroring) as being required when a Salas user creates an object for the first time:

> Q. . . . So we know that the access information is stored at the server, and we know that the server is checking to see which data objects the client has appropriate access rights for.
>
> And so what would be the point of sending the access rights information down to the client?
>
> MR. WEINSTEIN: Object to the form.
>
> THE WITNESS: The point would be that it maintains a consistent database structure between client and server, and the point further would be that there -- there has to be some communication of access information from client to server as well as from server to client, particularly in the case when the client creates an object for the first time, and on the next synchronization request the existence and the metadata for that object is sent from the client to the server.

(Ex. 2013, Tittel Dep at 45:14-46:5.) But the Salas file creation disclosure appears in column 13 and—as Mr. Tittel himself later agreed in the deposition — demonstrates that the opposite is true. As explained in Section II(A)(2)(c) above, when creating a file in the Salas system the file metadata is created by the server, stored at the server, used by the server, and never set to the client workstation. (Jones Decl. ¶ 58.)

Third, as Dr. Jones explains, "database mirroring" is a term of art, meaning keeping exact copy of a database in a second location for backup purposes and we know that Salas does not do that based on two additional disclosures. (Jones Decl. ¶ 59.) Salas makes clear that the client has only a subset of the server's database and thus is not the same as the server's database:

> The database 20' stored on the client workstation 12' contains ***a relevant subset*** of the data objects stored by the server 14. That is, the database 20 stored by the server 14 typically will contain more information about a particular project than the database 20' stored by the client workstation 12'.

(Salas 4:31-36, emphasis added.) Salas also teaches that some tables may be stored on the client workstation but not the server. Salas discusses an "unread" table used to indicate things that have been modified since the user read them last:

> However, the database 20' stored on the client

> workstation 12' may contain tables ***which are not stored by the server database 20***. For example, a client workstation 12 may store in its database an "unread" table which indicates which objects have been modified since the user of the client workstation 12' has last accessed those objects. An unread table may include a member identification field and a modification tag indicating the last modification date and time of an object.

(Salas 4:37-46, emphasis added.) As Dr. Jones explains, these two counter-examples make clear not just that "mirroring" is not required by the Salas system but that the opposite of mirroring is expressly disclosed. (Jones Decl. ¶ 59-60.) Taken together, these disclosures make clear that in Salas the asymmetry in information storage is bi-directional: the server stores more information than the client and vice versa. (*Id.* ¶ 60.) That is not mirroring. (*Id*.)

Finally, on top of all that, Mr. Tittel freely admitted at his deposition that Salas lacked an explicit disclosure of storing file access information in the client database (thus mirroring the server database) and that he was therefore "reading in" that disclosure to account for "what database professionals refer to as concurrency controls":

> Q. . . . . Is there any place where Salas says that access controls are stored in the client database?

A. ***I don't see any place where he says that explicitly***, but my understanding, as a person of skill in the art, is that as it says in Column 11 starting at line 12, because multiple users may concurrently and even simultaneously perform work on a project, that means we have to have what database professionals refer to as concurrency controls in place in order for the system to work properly.

And you'll notice that Salas spends some time discussing in the patent how edit locks are managed so that we don't find ourselves in the situation of having multiple writers to the same file at the same time, which, in database terms, is a huge no-no. . . .

. . . So I would assert that in order to provide proper concurrency controls, that the local database that the person working on a client machine, as described in that paragraph I was looking for earlier, he mentions three different groups into which users can be divided, coordinator, reader, and participant, a participant he go -- defines further as a person that may access the eRoom and may edit the objects and files contained in the eRoom as well as upload new objects and files to the eRoom. The local user couldn't do that properly if they didn't have local access controls that mirrored, or in some cases, anticipated for the case of new objects, the contents of the master database on the server

(Ex. 2013, Tittel Dep. at 38:21-40:1.) But Salas explicitly addresses concurrency

controls in its edit-lock and synchronization discussions, as the reference itself makes clear and as Dr. Jones explains. (Jones Decl. ¶ 61-62.) Thus, to those of skill in the art, the Salas reference already provides proper "concurrency controls," making Mr. Tittel's reading into Salas a mirroring requirement unwarranted.

* * *

We now turn to Parker.

B. Parker Does Not Fill the Salas Gaps

Petitioner relies upon the Parker reference in combination with Salas, but Parker does not fill the gaps in Salas. We begin the Parker discussion with a brief overview of its disclosure, and Petitioner's argument.

Parker discloses a file administration system where, like in Salas, the icons and filenames are the relevant "content data," not the files themselves. (*See* Jones Decl. ¶¶ 63-67.) Also, like in Salas, the access privileges or rights in Parker are checked at the server and not at the client. Parker states that:

> [U]ser's access privileges may then be saved to a file, to be *consulted by the file service* ***to determine*** whether that user has sufficient access privileges to one of the ***server*** files or folders.

(Ex. 1011, Paker 2:12-15, emphasis added.) As Dr. Jones explains, that "file service" clearly operates on the file server and is the only such file service disclosed in the Parker reference. (Jones Decl. ¶ 67.) And as Mr. Tittel admitted,

this access privilege determination disclosure, must occur on the server:

> Q. Where it says, "Determine whether that user." Where is the act of determining whether the user has sufficient access privileges take place?
>
> A. It -- it occurs at the file system where the request for the file is serviced no matter where it may be located.
>
> If the user is asking for a local file, it will be satisfied locally. If the user is asking for a file on another system, it will be satisfied by the file service on that system.
>
> Q. Okay. Well, now, that last sentence there is talking about access privileges to one of the *server* files or folder. Do you see that?
>
> A. Yes, sir. In that case, the logical extension of what I've just said would be that it would be determined on the server.

(Ex. 2013, Tittel Dep. 74:13-75:7.)

Parker describes examples where the file icons and filenames are, depending on user access level, either (1) modified by ghosting, graying out, or adding an additional lock or unlock icon or (2) "hidden altogether." (Ex. 1011, Parker at 11:40-47.) Petitioner relies on Parker for its feature of incorporating into displayed

file icons and filenames an indication of whether the viewing user to whom the icon is displayed has the right to access the file pointed to by that icon:

> It would have been obvious to one of ordinary skill in the art to add, to the eRoom system of Salas, the user interface technique of Parker in which an item is displayed normally (if access is allowed) or "in a ghosted state," "greyed out, shaded, or hidden altogether" (Parker, 11:44- 47), depending on the viewing user's access privileges. This would predictably result in the eRoom system of Salas in which the ActiveX control running in the web browser obtains the file metadata identifying the access privileges of the user (Salas, 13:52-57), and then uses it to generate the eRoom page with an item box (408) listing each file with a visual indication consistent with the viewing user's access privileges (e.g. fully visible, ghosted, grayed out, with a "lock icon," etc.).

(Petition at 46.) The Board recognized that "Petitioner relies upon Parker for further teaching the modification of icons based on a user's access privileges, which Salas describes as being included in file metadata" and was then "not persuaded by the Patent Owner's argument that Salas's file metadata in combination with the teaching of Parker does not control what appears on the page." (Decision at 17.) The Patent Owner respectfully asks the Board to

reconsider.

1. The Salas/Parker Combination Fails to Disclose or Suggest Sending "Privacy Level Information" under any Proposed Construction

The proposed combination of Salas and Parker fails to disclose sending "privacy level information" from the server to the user system under any of the proposed constructions. (*See* Jones Decl. ¶¶ 68-73).

The critical point here is that the relevant "content" is only what is displayed on the diary page, namely the icons, file names, lock symbols, and the like. (*Id*. ¶ 69.) The underlying files represented by the icons are not "content" because they are not ever displayed on the diary page. (*Id*.) So "privacy level information" for the Salas/Parker combination must "describe or specify" who can view the icons, file names, and lock symbols. (*Id.*) Parker's technique of modifying the icons to indicate access rights to the underlying files does not say anything about who can view the icons, file names, or lock symbols. (*Id*. ¶ 70.) To the extent that these items are sent from the server to the user system they simply represent the sending of content. (*Id*.) But sending that content fails to meet the "privacy level information" requirement to "describe or specify" who can view that content. For that reason alone, the Salas/Parker combination falls short of satisfying the claim requirement of sending "privacy level information" from the server to the user system.

The fact that Parker also proposes blanking out the icon altogether if the user has no right to view the underlying file does not help Petitioner. Mr. Tittel testified that the blank out would occur only if the user had no access rights at all, and that in that instance the server would simply not send any information at all:

> Q. But if the server decides [in Parker] that the client has no rights, at all, for a particular file or a particular folder, then it won't send any instructions [] to the client with respect to that file; isn't that right?
>
> A. It won't send any information about it at all.

(Ex. 2013, Tittel Dep. at 79:22-80:3.) Dr. Jones agrees that if the icon is to be blanked out it would make no sense to send any information. (Jones Decl. ¶ 72.)

The Board stated in its Institution Decision that Patent Owner "provides no support for its contention that Parker's teaching to blank out an icon results in that icon not being sent." The record has now been enlarged to provide that support.

2. The Salas/Parker Combination Does Not Teach Sending "Privacy Level Information," as Properly Construed

In addition to arguing that the combination of Salas and Parker would not result in a system that sends privacy level information to the client workstation under any of the competing constructions, the Patent Owner also urges the Board to reconsider the construction of privacy level information because the Patent

Owner's proposed construction reflects a further distinction between the claims at issue and the Salas/Parker combination.

a. The Proper Construction of "Privacy Level Information" Must Account for the Word "Level," which Implies a Gradation or Universe of Users

Whether the construction of "privacy level information" properly accounts for the claim term "level" is the sole claim construction dispute in this IPR. As the record to date makes clear, the parties do not dispute that "privacy level information" governs who is permitted *to view* particular content on a cohesive diary page. Nor do they dispute that the "privacy level information" *must be sent* from the diary server to the user system, as other language in the claim explicitly requires. Nor is it disputed that the "privacy level information" must itself *describe or specify* those who are "permitted to view particular content on a cohesive diary page."

These agreements were reflected in the Board's Institution Decision, which stated:

> On this record, and for purposes of this Decision, we construe "privacy level information" to mean "configuration information that describes or specifies at least one user or category of users permitted to view particular content on a cohesive diary page."

(Decision at 10.) This preliminary construction also reflects the Board's rejection

(on the then-current record) of the Patent Owner's proposed construction as being "overly narrow" to the extent that it precluded "specifying an individual user[.]" (*Id*.)

The Patent Owner believes that the district court's original construction that it urged be adopted by the Board in the Preliminary Response, with the words "which user(s)," both (1) permitted specifying an individual user (when that user was the only user with viewing rights) and (2) properly accounted for the claim term "level." In light of the Board's "overly narrow" comments, however, and in an effort to make the "level" requirement more explicit in the construction itself, the Patent Owner now urges the following construction for "privacy level information":

> "configuration information that describes or specifies the universe of one or more users or categories of users permitted to view particular content on a cohesive diary page"

This construction does two things. First, it unquestionably permits a level or universe of one single user, which as the Board correctly concluded is not precluded by the Specification. In fact, the Specification expressly describes an "owner" privacy level depicted as a single profile head in Figure 4(e) that is understood by both experts as disclosing a privacy level with a single member: the owner himself. (Ex. 1001, '316 patent, Figure 4(d) and 10:36-41; Ex. 2013 Tittel

Dep at 10:12-18; Jones Decl. ¶ 16.) Second, unlike the Board's preliminary construction (and the Petitioner's proposed construction), it accounts for the claim term "level."

Simply put, the Board's preliminary construction is too broad because it covers information that merely specifies whether a particular individual user has access to certain content, and does not specify a level of access—the universe of users that have access to certain content. That type of individual-access information concerning one user within a broader set of permitted users is really just a password system, and the'316 specification plainly distinguishes between passwords and privacy levels. It states that "passwords" and "privacy levels" are each a type of "configuration information." (Ex. 1001, 9:2-4.) And it further describes the difference between the two. Passwords are used to determine whether individual users are authorized to access aspects of the diary page, while privacy levels specify a universe of users permitted to view content:

> "Button 438 allows any user to change the privacy level on which the diary is operating, provided that the user is able to authenticate himself at the desired level. Authentication is preferably performed by requiring the user to enter a password required to change the privacy level to a certain level" (Ex. 1001 at 10:29-33.)
>
> "User settings are stored as configuration data, which

includes the passwords required for users to access the different privacy levels." (*Id.* at 17:21-23.)

In other disclosures, in particular those emphasized below, the Specification makes perfectly clear that "privacy level information" is more than merely whether an individual user is authorized to see content. It is instead a particular universe of users.

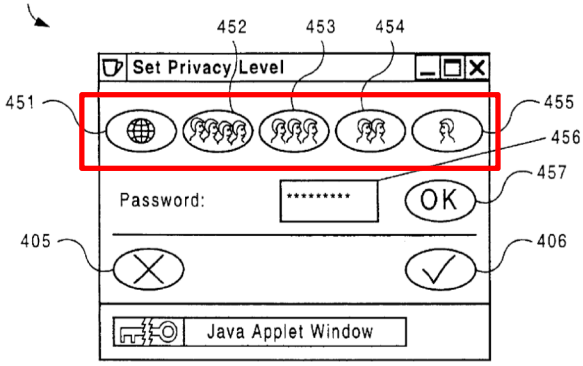


Figure 4(d)

2. Privacy Level of a Diary Page

Button **438** allows any user to change the privacy level on which the diary is operating, provided that the user is able to authenticate himself at the desired level. Authentication is preferably performed by requiring the user to enter a password required to change the privacy level to a certain level. In the described embodiment, clicking or otherwise selecting this button displays window **450** of FIG. **4**(*d*).

FIG. **4**(*d*) shows a window **450** or similar navigational element for the privacy function of button **438**. Window **450** allows a user of the diary to set a privacy level at which the diary is operating of: world, friend, close friend, best friend, and owner via respective buttons **451**, **452**, **453**, **454**, and **455**. Any user can change the privacy level, provided that he is able to authenticate himself, e.g., via a password supplied in area **456**. This window determines which sections and which objects will be visible during browsing through the diary. If the user selects the owner privacy level (button **455**) and can supply a correct password in area **457**, after clicking OK button **456**, buttons **440**, **442**, **444**, and **446** of FIG. **4**(*a*) become available to the owner. Otherwise these buttons are grayed out. Use of button **440** will pop-up a new window containing the advanced diary operations such as, e.g., moving or copying objects from one section to another. The passwords for a particular user's diary pages are stored as configuration information in that user's diary information **114**.

(Ex. 1001, Figure 4(d); 10:28-54; emphasis added.) All the examples of privacy levels in the specification—"world," "friend," "close friend," "best friend," and "owner"— reflect a universe, or level, of permitted viewers. (Ex. 1001, '316 patent 10:36-41; Fig. 4d.) And in still other disclosures, the Specification describes that privacy levels are used by the diary owner to control what is shown to "various

classes of persons" viewing the owner's diary, and that such control is effected by checking whether the privacy level assigned by the diary owner to particular content is "lower than or equal to" the privacy level of the viewer*:*

> [T]he owner of the diary can control what is presented to *various classes of persons* via his diary. The owner can identify various pages, sections, or content objects as having a certain privacy level. When a diary applet executing in the browser receives information for the user's diary, the diary applet generates HTML only for those portions of the diary that have a *privacy level lower than or equal to the privacy level of the viewer who is viewing the diary*. Thus, it is possible that the diary applet will generate different HTML pages for an owner and for a random stranger who each ask to view the same diary page on their respective browsers. The person viewing a diary page can only view that content marked *as appropriate for him and other people at his privacy level*. The diary applet of the described embodiment asks for a password to determine a privacy level of a person. The correct password values are part of the configuration information for a diary.[12]

[12] Ex. 1001, '316 patent at 18:8-29 (emphasis added).

And this "lower than or equal to" aspect of the '316 privacy levels makes clear that they progress in terms of restrictiveness in stages, degrees, or gradations, each higher level or grade more restrictive than the next in terms of who can view the diary content, ending with the most restrictive level, the owner himself. In this way, these Specification disclosures simply make express what is unquestionably implied by the claim term "level." As Mr. Tittel explained during his recent deposition, the term level itself implies a "gradation":

> What do you understand the word "level" to imply?
>
> A. I understand the word "level" to mean that there are different ***gradations*** of privacy level that can be selected by the user.

(Ex. 2013, Tittel Dep. at 9:17-21, emphasis added.) Dr. Jones agrees. (Jones Decl. ¶ 17.) And as the Specification makes clear, each gradation is a different group of people, each grade more restrictive than the next in terms of who can view particular diary content, as Mr. Tittel explained:

> Q. And each gradation is a group of different people?
>
> A. Well, in the most literal way of answering your question, each one of those little bubbles there would represent a different gradation, and we start off on the left-hand side with a symbol for the world, which I would presume to mean everyone in the world, and then we

> have another level where we have four heads, which in looking at the language of the patent, I would guess would mean friend, and then the bubble with three heads would be the close friend, and the bubble with two heads would be best friend, and then the bubble with the head facing the other way, I believe refers to the owner himself or herself, as the case may be.
>
> Q. So the owner level would have just one person in it, which would be the owner himself; right?
>
> A. That is the implication of both the singular tense for the word "owner" and the visual representation that appears in Figure 4D.

(Ex. 2013, Tittel Dep. at 9:22-10:17.) Again, Dr. Jones agrees. (Jones Decl. ¶ 17.) Thus both experts agree that a "privacy *level*" is the universe of users (e.g., public, friends, best friends, owner) permitted to view particular content. It follows that "privacy level *information*" must describe or specify the level itself.

For these reasons, the Patent Owner respectfully urges the Board to modify its preliminary construction of the "privacy level information" limitation, in light of the now-supplemented record, to require that the level itself be described or specified, not just an individual with access. Without that, the construction improperly and erroneously reads the "level" term out of the limitation. *Aspex Eyewear, Inc. v. Marchon Eyewear, Inc.*, 672 F.3d 1335, 1348 (Fed. Cir. 2012)

(reversing a construction of the limitation "rearwardly directed free end" because it "effectively reads the term 'free' out of the limitation.")

b. The Salas/Parker Combination at Most Discloses Sending Individual Access Information and Not Privacy *Level* Information

The Patent Owner urges the Board to modify is construction of "privacy level information" to require that the level, not just an individual with access, must be described or specified. By contrast, Parker's icon modifications and icon blank outs reflect only the access rights of a particular individual. Thus, when "privacy level information" is correctly construed, the Petitioner's Salas-Parker combination fails to meet the claim requirement that the privacy level information be sent from the server to the user system. (Jones Decl. ¶ 74.)

As demonstrated in Section II(A)(2) above, the supposed "privacy level information" in Salas is *never sent* from the server to the client. To fill this gap, Parker must thus disclose sending privacy level information. It does not. Modifying the icons and associated filenames or even blanking them out does not amount to sending "privacy *level* information" to the user under the proper construction. As Dr. Jones explains, at most the Parker icon modifications or blanking have to do only with the access rights of an individual user and have nothing to do with the universe of users that have access to any particular piece of content. (Jones Decl. ¶ 74.)

C. There Is No Motivation To Combine Salas and Parker—And Substantial Reasons *Not* To Combine Them

Finally, even if Parker sent information that described or specified users that had view permission, there would be no motivation to add that feature to Salas because in Salas every member of the e-room has viewing permission, both of the underlying files and the icons themselves. (Jones Decl. ¶¶ 75-83.) Dr. Jones explains:

> 76. Salas does not teach any role in which a member of an eRoom does not have the right to read all of the content in the eRoom. The preferred embodiment of Salas describes three roles: coordinator, reader, and participant. Salas, of course, isn't necessarily limited to these three roles. However, not only does Salas not describe other roles, the access control mechanism and eRoom interface pages are specific to these roles because they are appropriate for the problem faced by Salas. . . . Hypothetical eRoom member roles such as partial readers would be both inconsistent with the problem of Salas and Salas's solution to that problem.

(Jones Decl. ¶ 76; *see also* ¶¶26-30.) Here is what Salas says about the three eRoom user roles:

> In some embodiments, users may be divided into ***three separate groups***: coordinator; reader; and participant. In this embodiment, a coordinator can add members to the

> eRoom and may supersede any rights granted to users. A reader is someone who has access to the eRoom solely to view the content of that eRoom while a participant is a user that may access the eRoom and may edit the objects and files contained in the eRoom as well as upload new objects and files to the eRoom.

(Salas at 14:42-50.) As Dr. Jones explains, in this scheme, if a user is a "reader" in a particular eRoom, then that user can view everything in the eRoom, but not modify or add content. If a user is a "participant" then that user can view all content in the eRoom as well as add and modify content. If a user is a "coordinator" in a particular eRoom, then that user has the additional right to add new members to the room.[13] (Jones Decl. ¶¶ 77-78; Salas 3:49-57 and 14:37-54.)

Dr. Jones further explains how those of skill would understand that the "other embodiments" implied by the opening phrase in this passage are other embodiments where all the eRoom users can *at least* read all the content, such as where the users are divided not into three groups but just two: coordinator and participant. (Jones Decl. ¶ 79.) Those of skill would not understand the "other

[13] Salas also names an Observer role without description (Salas 3:55), but this would, based on its name, appear to be the same as a reader role.

embodiments" to imply embodiments were some of the users were not permitted to read some of the content. (*Id*.) That would defeat the entire purpose of Salas. (Jones Decl. ¶ 79; *see also* ¶ 76.) Petitioner seems to agree:

> Salas makes clear, therefore, that the system *allows the user to view the list of files in the project* but the user may be [sic, not be granted] certain types of access to the file.

(Petition at 43.) And although not expressly admitted, the Petitioner seems to suggest here that Salas is all about *types* of eRoom user access and not about access *per se*. Dr. Jones agrees with that suggestion. (Jones Decl. ¶ 80.) He agrees with that suggestion not only because that is how those of skill would understand the express Salas disclosures identified above, but also because giving every eRoom member at least viewing access to all the project files simply makes good sense given the very purpose of the Salas system. (*Id*.) The Salas system provides "a collaborative work environment over a network" (Salas 1:7-8) that facilitates "a two-way exchange of information and project data between team members" (Salas 1:59-60) so that team members can work together on a common project:

> The present invention relates to methods and systems for providing a networked, collaborative work environment. In particular, the systems and methods described below allow a group of users to share work and files, engage in discussions related to a common project, and otherwise

> collaborate. For example, users interact with Web browsers executing on their client workstations to access Web pages that allow them to: participate in ongoing discussions; create new discussions about project topics; upload files to a common area associated with the Web page; download files and edit files that have been uploaded to the Web page by others members of the project team; and create new pages of various types and link them to existing ones.

(Salas 1:66-2:11.) In a collaborative work-based system like that, there is good reason to share everything and no good reasons to hide anything. (Jones Decl. ¶ 76.) Unlike for an on-line personal diary. Unlike in the system described in the '316 patent. And unlike the claims at issue in this IPR, each of which requires (1) "privacy level information" that configures the diary page by determining what will be displayed to a particular user and what will not be displayed and (2) sending that privacy level information to the user's system

As such, the skilled artisan would simply not be motivated to add the Parker disclosure to the Salas collaborative work environment system. (Jones Decl. ¶¶ 81-83.) Indeed, at most Parker would provide motivation to use modified icons and filenames to indicate who has *edit rights* in addition to the view rights that all eRoom users have, but sending ***edit*** rights information does not satisfy the claim

requirement of sending privacy level information that describes who can ***view*** the relevant content.

III. CONCLUSION

For the foregoing reasons and those presented in the Preliminary Response, the Patent Owner respectfully requests that the Board reject the Petitioner's arguments and confirm the patentability of the '316 claims at issue in this IPR.

Respectfully submitted,

Date: October 14, 2014

/John S. Goetz/
John S. Goetz
Reg. No. 54,867

Fish & Richardson P.C.
3200 RBC Plaza
60 South Street
Minneapolis, MN 55402
Telephone: (212) 641-2277
Facsimile: (202) 783-2331

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on October 14, 2014, a complete and entire copy of this Patent Owner's Preliminary Response was provided via e-mail, to the Petitioner by serving the correspondence e-mail addresses of record as follows:

Heidi L Keefe
Mark R. Weinstein
COOLEY LLP
ATTN: Patent Group
1299 Pennsylvania Ave., NW, Suite 700
Washington, DC 20004

Email: hkeefe@cooley.com
Email: mweinstein@cooley.com
Email: zpatdcdocketing@cooley.com

/Jessica K. Detko/
Jessica K. Detko
Fish & Richardson P.C.
3200 RBC Plaza
60 South Sixth Street
Minneapolis, MN 55402
(612) 337-2516