UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Facebook, Inc.
Petitioner

v.

Rembrandt Social Media, L.P.,
Patent Owner

U.S. Patent No. 6,415,316 B1
Filing Date: September 1, 1998
Issue Date: July 2, 2002

Title: METHOD AND APPARATUS FOR IMPLEMENTING A WEB PAGE DIARY

SECOND DECLARATION OF EDWARD R. ("ED") TITTEL

Inter Partes Review No. 2014-00415

Table of Contents

Page

I, Edward R. ("Ed") Tittel, declare as follows:

I. INTRODUCTION

1. I previously submitted an original declaration dated February 6, 2014 (Ex. 1002, "First Tittel Declaration") setting forth my qualifications and experience. In the interest of brevity, I refer to that information rather than repeat it again here. (First Tittel Decl., Ex. 1002, ¶¶ 1-9.) My previous declaration also included a definition of a person of ordinary skill in the art. (*Id.* ¶ 13.) The patent owner has agreed with that definition, and I adhere to it here.

2. I have been asked to prepare this second declaration to respond to certain points raised in the "Declaration of Mark T. Jones" ("Jones Declaration," Ex. 2011), which is dated October 14, 2014. In preparing this second declaration, in addition to the materials that I previously reviewed (listed in Paragraphs 10 and 11 of my earlier declaration), I have also reviewed

- the "Decision" by the Patent Trial and Appeal Board ("Board") instituting *inter partes* review on July 7, 2014 (Paper 9);
- the "Patent Owner Response" dated October 14, 2014;
- the transcript of Dr. Jones's deposition taken in this proceeding on January 16, 2015 (which I understand will be submitted to the Board as Exhibit 1016 by Petitioner).

II. CONSTRUCTION OF "PRIVACY LEVEL INFORMATION"

3. With the exception of the "privacy level information" features in the two independent claims (*i.e.* claims 1 and 17), Dr. Jones does not appear to dispute that the prior art that I described in my first declaration discloses or suggests all limitations of claims 1, 4, 17, 18 and 26. Many of the patent owner's arguments about this feature, however, appear to depend on a narrower interpretation of "privacy level information" that I believe is unwarranted.

A. "Privacy Level Information" Need Not Specify a "Universe" of Users

4. Dr. Jones contends that the term "privacy level information" in the '316 patent should be understood as "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." (Jones Decl. ¶ 15.) This interpretation differs from the one adopted by the Board's July 7, 2014 Decision in that it imposes the additional requirement that "privacy level information" specify "the universe" of users permitted to view diary page content.

5. Dr. Jones contends that his proposed narrower interpretation is consistent with how one of ordinary skill in art would understand the disclosures of the '316 patent. (Jones Decl. ¶¶ 15-17.) I respectfully disagree with Dr. Jones

on this point. In my opinion, the interpretation adopted by the Board is more consistent with how one of ordinary skill in the art would interpret the claims.

6. I have found nothing in the specification that requires that "privacy level information" identify a "universe of one or more users." The specification does not use the word "universe" (or any variant of that word) in any of its discussions of privacy level features. Nor does the specification impose any conditions on how privacy levels must be implemented. The specification instead discusses the "privacy concept" features in exceedingly broad terms, and by reference to a single individual rather than a "universe" of users:

> In the described embodiment, the diary may enforce privacy-rules on any part or level of the book, i.e., book, section, page, individual content entry. Other embodiments may implement other levels of privacy rules, and multiple implementations of this privacy concept are possible. In various implementations, privacy enforcement may be either advisory or mandatory. Different authentication and verification schemes may be employed to identify the user attempting to access the book. <u>If a user does not have sufficient permission to view an object in a diary, the diary may not make the object visible to the user, i.e., the user does not even know that the object exists, or it may present the object using an alternate representation</u>.

('316, 5:55-67 (underlining added).) I have underlined a portion of the text above to emphasize the fact that "privacy level information" can pertain to a single user attempting to view a diary page. "If a user does not have sufficient permission to view an object in a diary," the patent explains, the diary may conceal the object or "may present the object using an alternate representation." ('316, 5:63-67.) Nothing in the specification requires that "privacy level information" specify a "universe" of users, or excludes "privacy level information" from describing the access rights of a single individual user.

7. The patent owner points to the disclosures in the specification relating to Figure 4(d), which shows a user interface for allowing a diary owner to set a privacy level with respect to a diary page. ('316, 10:28-54.) One of ordinary skill in the art would have found these disclosures irrelevant to the meaning of "privacy level information" in the claims. This is because Figure 4(d) and its accompanying description in the written description describe how a diary owner sets the configuration information and privacy levels for a diary page – not the subsequent assembly and display of the diary page by a viewing user.

8. The process of setting the privacy level for a diary page is not recited anywhere in the claims. The claims instead focus on the assembly and display of a diary page "in accordance with the configuration information." For example, claim

1 recites the steps of sending "a diary program," sending "diary information," and then "assembling the cohesive diary page . . . to be displayed by the diary program running in the browser." ('316, 23:56-60 (claim 1).) By the time the "assembling" step in claim 1 occurs, the "privacy level" has already been set by the diary page owner. The process of setting that privacy level is not specified in the claims. In my opinion, therefore, the privacy level interface in Figure 4(d) is not informative about the type or kind of "privacy level information" that must actually be transmitted to the user system when a diary page is subsequently assembled and displayed on an individual user system.

9. I respectfully note that Dr. Jones has overlooked the fact that claims 1 and 17 are written entirely from the perspective of assembling a diary page for an individual user system viewing the page. ('316, claims 1 and 17 (assembling a cohesive diary page for a single "user system").) The claim steps do not require assembly of a diary page for any "user system" other than the one recited in the claim.

10. For example, suppose "User X" is attempting to access a diary page. The diary server would only need to send privacy level information relating to "User X" to his or her user system in order to properly complete the "assembly"

step. There is no reason for the diary server to send privacy level information for "User Y" or any other user other than "User X."

11. Dr. Jones states that the word "level" implies the existence of some type of "gradation," and taking that word in isolation, I agree. (Jones Decl., ¶ 17.) But I disagree with the next sentence of his declaration, where he states that "each gradation is a different group of people, each grade more restrictive than the next in terms of who can view particular diary content." (*Id.*) This argument misreads the claim language, which merely requires sending "privacy **level** information," with the word "level" in singular form. The singular use of the word "level" is consistent with an "assembly" step that is concerned about assembling and displaying a diary page for only one user system.

12. Although the diary server may maintain information about multiple privacy levels, the claims do not require that the diary server send information about multiple privacy levels to the user system, and as I mentioned above, there is no reason for it to do so. In fact, for consumers of access information, as in the case of a user of the diary server, the only access information that matters is the information pertaining to that user him- or herself. In my opinion, therefore, Dr. Jones's assertion that "privacy level information" may pertain to a "universe" of users is incorrect.

B. "Privacy Level Information" Does Not Require Client-Side Filtering

13. One other point about "privacy level information" requires only brief comment. Dr. Jones's declaration repeatedly emphasizes that in the prior art Salas and Parker references, the actual filtering of the content – the identification of those content items the user is allowed to view – takes place on the server and not at the user system. (Jones Decl., for example, at ¶¶ 31, 34, 67.)

14. To the extent Dr. Jones was suggesting that this argument distinguishes Salas and Parker from the claims of the '316 patent, I respectfully disagree. The claims do not on their face require "privacy level information" be used by the user system to prevent the display of (filter) content. The claims on their face only require (1) that the diary server send "privacy level information" to the user system; and (2) that the user system assemble the cohesive diary page "in accordance with" that information. This language under its broadest reasonable construction (which I understand is the standard for interpreting claims in *inter partes* review) simply requires assembly of a diary page that is *consistent with* the privacy level information. It does not under this standard require that content selection and filtering take place at the user system. Dr. Jones appears to agree, as he testified at his deposition:

Q: Does the language of claim 1 impose any requirement that the user system use the privacy information to determine what content, if any, the user is permitted to see?

MR. GOETZ: Same objections.

THE WITNESS: No, I don't believe it does.

(Jones Depo., Ex. 1016, at 11:25-12:7.)

III. THE COMBINATION OF SALAS AND PARKER DISCLOSE SENDING "PRIVACY LEVEL INFORMATION" TO THE USER SYSTEM AND ASSEMBLING A DIARY PAGE IN ACCORDANCE WITH THAT INFORMATION.

15. The crux of Dr. Jones's argument appears to be that neither Salas nor Parker discloses the step of sending "privacy level information" to the user system, and therefore, they fail to teach assembling the diary page "in accordance with" the privacy level information as required by claim 1. I respectfully disagree with Dr. Jones's opinion on this point.

A. The Server in Salas Sends File Metadata to the User System

16. Dr. Jones's declaration contains a lengthy explanation of various aspects of Jones, but his explanations do not answer to the question raised by his argument – does the server in Salas send the file metadata (the "privacy level information") to the user system? (Jones Decl. ¶¶ 24-62.) Dr. Jones spends an inordinate amount of time attempting to show that the server in Salas is involved in controlling access to eRooms and their contents. I agree that the eRoom server

in Salas is certainly involved in these processes, but this does not mean the file metadata is not also sent to the user system.

17. Salas discloses "configuration information" and "privacy level information" in the form of file metadata, described in Salas as follows:

> 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.

('600, 13:52-57.)

18. As I explained in my first declaration, the disclosures of Salas make clear that the server sends this file metadata to the user system. (First Tittel Decl., Ex. 1002, ¶¶ 76-78, 81-82.) As the Board recognized in its decision, the eRoom page displayed on the user system (shown in Figure 4 within box **408**) expressly displays file metadata, "such as filename, creation date, modified date, and which application should be used to open and edit the file." (07/07/2014 Decision at 16-17.) I concur with the Board's analysis. The user system simply could not show an eRoom page with file names, dates, and other information if the eRoom server (**12**) did not send file metadata to the user system before the eRoom page was displayed.

19. Dr. Jones does not appear to dispute that the eRoom server (**12**) sends at least some of the file metadata listed in Column 16, lines 52-57 of Salas that I quoted above. Dr. Jones instead appears to suggest that Salas sends only a portion of the file metadata to the user system, which does not include the access information. (Jones Decl. ¶ 56.) I respectfully submit that this argument is based on speculation contradicted by the explicit teachings of Salas.

20. As I explained in my previous declaration, Salas discloses a "local database metadata" synchronization process that results in the eRoom server sending metadata to the user system for local storage. (First Tittel Decl., Ex. 1002, ¶ 78.) There is nothing in Salas supporting Dr. Jones's suggestion that the synchronized "**local database metadata**" in Columns 11 and 12 of Salas does not include the "**file metadata**" listed in Column 16, lines 52-57. (Jones Decl. ¶¶ 35-39.) Dr. Jones emphasizes that Salas's discussion of metadata synchronization in Columns 11 and 12 does not expressly mention updating "access control" metadata, but I do not perceive any relevance to this argument. (*Id.*) Salas similarly does not state that the file name and file creation and modification dates are synchronized – but this information is obviously provided to the client as shown in Figure 4 and observed by the Board. (07/07/2014 Decision at 16-17.)

There is nothing in Salas suggesting that the local database of file metadata specifically excludes the "access information" portion of that metadata.

21. Dr. Jones's assertion that "the file metadata is created and stored on at the server and not on the client" (Jones Decl. ¶ 52) is incorrect for another reason. As noted above, the file metadata in Salas includes "access information such as which users may open, view, and edit the file . . . ." (Salas, 13:54-55 (underlining added)). This access information is specifically checked by the system when a user attempts to access a file:

> If no edit lock has been set for a requested file, the access rights of the requesting user are checked. 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. In the case of a user that indicated editing will occur, an edit lock is set before the file is downloaded.

(Salas, 12:34-39 (underlining added).)

22. This passage makes clear that when a file is downloaded to the user system, there may be restrictions on how it will be used after it is downloaded. If the user's access privileges include "**can view**" but do not include "**can edit**," for example, the file will be downloaded and viewable by the user, but the user will not be allowed to modify the contents of the files. (*Id.*) In other words, the

downloaded file's access privileges indicate "read only," so the user can view the file but cannot delete, modify or add content to it.

23. It is well-known to persons of ordinary skill in the art that the user's local computer must enforce "can view" and "can edit" access privileges for a downloaded file. This is a standard feature of any modern operating system, including the Windows operating system, and it requires that the server send the access privilege information to the user system. If the server did not send this information, the user system would not know what access the requesting user is allowed. Dr. Jones agreed with this point in his deposition:

> Q: And what's your understanding of what access privileges are?
>
> A: Typically describe whether -- the kinds of access that a user could have; for example, a read access, a write access, an execute access would be examples of the types of access that would be described.
>
> Q: Okay. So for example, for a particular user, a file can be read only, correct?
>
> A: Yes.
>
> Q: And what does it mean for a file to be read only?
>
> A: It means the user can only read the information in the file or a program acting on the user's behalf could only access that information and -- but it would not allow that user to modify the information in that file or including add new information to it.

Q: Okay. And it's also possible that for a particular -- for a particular user, a file can be rewrite [sic; read/write], correct?

A: Yes.

Q: And what's your understanding of what it means for a file to be rewrite?

A: Well, in order to be able to read information, the user can write information to the file which could be overwriting existing information or adding to the information in the file.

Q: Okay. And it's the operating system that enforces these access privileges, correct?

MR. GOETZ: Objection to form.

THE WITNESS: It's the file system that does that.

Q (BY MR. MACE) And so -- but it's the file system on the user's computer, correct?

A: It depends on where the files are.

Q: So if the files are on the user's computer, the file system on the user's computer enforces the access privileges?

A: Yes. The files are -- if the -- if the file service is -- for the files that the user is accessing is on the user's computer, then it will be enforcing those privileges.

(Jones Depo., Ex. 1016, at 12:24-14:18.) The term "file system" refers to the software on a user's computer (normally a portion of the operating system,

especially for client/end-user operating systems such as Windows, MacOS, Linux, and so forth) that manages access to the files stored on the computer.

24. In the case of Salas, the files being accessed are downloaded to the user's computer. (Salas, 12:23-28 ("Referring to FIG. 6, the first step taken by the background daemon is that the local file directory is checked to determine if the file is already present in local mass storage… If the file is not present or is stale, it must be downloaded from server **14**.") (emphasis added).) In order for the local computer's file system to enforce the access privileges specified for the file and the requesting user, the server must have sent them to the user system.

25. Accordingly, the fact that the eRoom server may check the access rights of the requesting user does not mean that the access information is not sent to and used by the user system. As I explained above, there is nothing in the "assembly" step of claim 1 under its broadest reasonable construction that requires the user system to filter out content the user is not permitted to see. One of ordinary skill in the art would interpret Salas as disclosing the sending of the access information metadata to the client workstation along with other file metadata, notwithstanding that that metadata is also used by the server.

B. The Server in Parker Also Sends "Privacy Level Information" to the User System and Assembles the Page for the User "in Accordance with" that Information

26. Even if there was some merit to Dr. Jones's position that Salas does not disclose transmission of "privacy level information" to the user system, this step is also disclosed by Parker. As I explained in my previous declaration, Parker describes a system that allows files, folders and other "sharepoints" to be displayed to a particular user in a way that visually indicates the privilege or access level granted to that user. This is shown in the user interface of Figure 7:

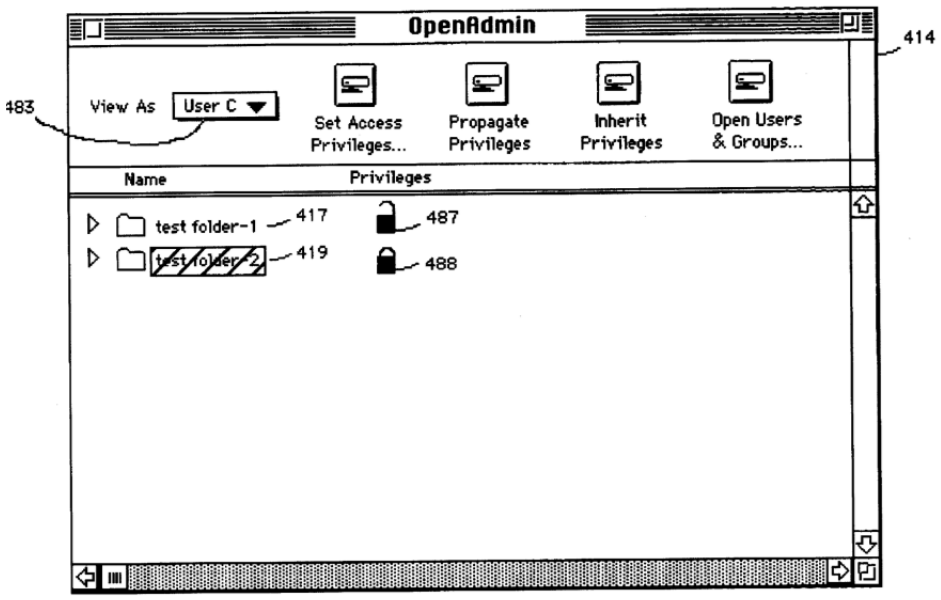


FIG. 7

(Parker, Fig. 7.)

27. Figure 7 shows exactly how "**User C**" would see the two folders (**417**, **419**) on its display screen. (Parker, 11:32-35.) The administrator granted "**User C**"

access to "test folder 1" (**417**), so that folder will appear to "**User C**" with unobstructed text and with a "lock open" icon (**487**). But for "test folder 2," the administrator did not grant "**User C**" rights to it, so that folder's name appears greyed out and is accompanied by a "lock closed" icon (**488**). (Parker, 11:40-47.)

28. Parker specifically states Figure 7 shows the view "from user C's perspective (i.e., in accordance with user C's access privileges as if the administrator was sitting at user C's client terminal)." (Parker, 11:32-35 (underlining added).) Parker further explains that other possible "access indicating icons" can be displayed to the user such "eye glasses" to indicate read privileges, a "writing instrument" indicating write privileges. (Parker, 11:50-64.)

29. One of ordinary skill in the art would have understood that Parker, like Salas, discloses the server sending the access privilege information to the user system. This is because in order to show "test folder 1" and "test folder 2" to "**User C**" in accordance with his or her access privileges, server must have sent those access privileges to the user's workstation. This point was directly confirmed by Dr. Jones in his deposition:

> Q (BY MR. MACE) Okay. So in order for the application to create the type of folder that's shown in figure 7, the user system needs to have the access privilege information that's being displayed, correct?

MR. GOETZ: Objection to form.

THE WITNESS: It has to ask the server about the access of User C.

Q (BY MR. MACE) And the server has to tell the user system what those access privileges are?

MR. GOETZ: Objection to form.

THE WITNESS: I don't know that it's -- necessarily a user system. It's just a system -- this is just the administrator's program running wherever it's running, but that program has to be told or has to ask the server, for example, does this user have read privilege, does this user have write privileges with respect to these folders.

Q (BY MR. MACE) So the application needs to have the access privilege information that's being displayed?

A: It at least has to -- after asking the server, it has to know whether or not, for example, to display the lock and unlock that the user has access privileges to test folder-1 and User C has no access privileges to test folder-2.

Q: So the application, in order to display the icons, needs to have the information sent from the server, correct?

MR. GOETZ: Objection to form.

THE WITNESS: It needs to have received the answers, for example, from the server of whether test -- whether the User C has access privileges to test folder-1, and in this case, that -- the user doesn't have access privileges to test folder-2; and then based on that, would determine whether to display the unlock or lock icon.

(Jones Depo., Ex. 1016, at 21:23-23:12 (underlining added).)

30. I agree with Dr. Jones on this point. The fact that Parker can display the files and folders "in accordance with user C's access privileges" (Parker, 11:32-35) indicates that those access privileges were sent from the server to the user system before the sharepoints were displayed.

31. Dr. Jones states that "Parker does not teach that decisions with respect to access control are made at the client." (Jones Decl. ¶ 66.) As I explained above, this does not mean that the access information is not sent to the client, and the claims under their broadest construction do not require this.

C. Salas and Parker Are Fully Combinable

32. Dr. Jones asserts that there would be no motivation to combine Salas with Parker. (Jones Decl. ¶¶ 75-83.) I respectfully disagree.

33. Dr. Jones points to the fact that members of an eRoom can be assigned different roles, each role specifying a different level of access to the content of an eRoom. (Jones Decl. ¶ 77.) Although this is not entirely clear, Dr. Jones appears to suggest that there would be no reason to combine Salas with Parker because a user's access rights are determined by the "group" to which the member was assigned (e.g. coordinator, reader and participant), and therefore,

there is no need to display to an eRoom member the access rights for files or folders on the page. (Jones Decl. ¶¶ 76-77.)

34. Dr. Jones's argument about eRoom roles and groups is based on a passage at Column 14, lines 42-50, that Dr. Jones reproduced in his declaration. (Jones Decl. ¶ 77.) But Dr. Jones failed to quote an earlier sentence of that same paragraph, which confirms that access levels can be assigned to each individual file in the database. (Salas, 14:37-39.) Salas makes clear that access rights for files may be separately assigned on a user-by-user basis, and that assignment of "access rights" based on roles is just an "alternative" embodiment:

> Access rights may be checked over the network in many ways. For example, each object may be provided with a field or fields which identify users that may open, view, and edit the object. ***Alternatively***, an object may assign a pre-defined value to a field which controls access to the object. For example, a "coordinator" role may be defined and an object may identify that any coordinator may edit, open or view it.

(Salas, 13:31-37 (emphasis added); *see also Salas*, 13:52-57 ("File metadata may include: . . . access information such as which users may open, view, and edit ***the file***…") (emphasis added).) As shown above, the assignment of access rights based on the "role" of the eRoom member is simply an "alternative" to assigning access

rights on a file-by-file basis. This alternative embodiment would not have discouraged a person of ordinary skill in the art from combining Salas with Parker.

35. Nor is there any basis for Dr. Jones's assertion that there is no reason to indicate "that a user can only read but not write certain content because the user's role in the room will determine this right for all content in the room." (Jones Decl. ¶ 82.) As shown in the preceding paragraph, Salas expressly permits user-by-user assignment for individual files. Moreover, as I explained previously, Salas also discloses that users may have access rights that allow them to view but not edit the files. (Salas, 12:34-39 (checking "can edit" and "can view" privileges for specific requested file).) The system of Salas would directly benefit from Parker's disclosure of visual indications of this distinction. As explained in Parker:

> In one embodiment, it is envisioned that a user accessing the network via its user privilege, will be able to distinguish whether the listed sharepoints are inaccessible, or accessible for read & write, read-only or write only via various access indicating icons. For illustration purposes, an open or closed lock icon will denote respectively user access privilege granted or no user access privilege. The open lock icon **487** is shown associated with sharepoint test folder-1 indicating access privilege for user C for this item. The closed lock icon **488** is shown associated with sharepoint test folder-2 indicating no access privileges. Alternative embodiments may

> include, but are not limited to, a set of "eye glasses" indicating read privileges, a "lock and key" indicating no access and a "writing instrument" indicating write privileges.

(Parker, 11:50-64 (underlining added).)

36. Finally, Dr. Jones does not address the fact that Parker provides an express encouragement to combine by explaining that a user accessing the network via its user privilege can visually ascertain their access for individual files, such as being able to determine if the file is "read only." (Parker, 11:50-54.) This would have been beneficial to Salas because it would have allowed the system of Salas to inform the viewing user of the actions it is allowed to take on a file.

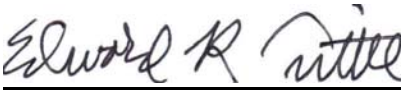
IV. CONCLUSION

37. In signing this Declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in this proceeding. If required, I will appear for cross-examination at the appropriate time. I reserve the right to offer opinions relevant to the invalidity of the '316 patent claims at issue and/or offer testimony in support of this Declaration.

38. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 28 U.S.C. § 1001.

Dated: January 20, 2015

Respectfully submitted,



Edward R. Tittel
Austin, Texas