IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

DIGITAL REG OF TEXAS, LLC,

Plaintiff,

v.

ADOBE SYSTEMS INCORPORATED, et al.,

Defendants.

/

No. C 12-1971 CW

ORDER REGARDING CLAIM CONSTRUCTION AND MOTIONS FOR SUMMARY JUDGMENT

(Docket Nos. 487, 556)

In this patent infringement case, Plaintiff Digital Reg of Texas, LLC has sued Defendants Adobe Systems, Inc., Symantec Corporation, and Ubisoft Entertainment, Inc. The parties originally identified about twenty-nine terms for construction, but eventually narrowed the dispute to nine terms. The three Defendants jointly brought a motion for summary judgment of non-infringement. On May 15, 2014, the parties appeared for a hearing. Having considered the papers and arguments of counsel, the Court construes the disputed terms as follows and GRANTS Defendants' summary judgment motion in part.

BACKGROUND

Digital rights management (DRM) is a generic term in the art which describes the control technologies that allow copyright holders, publishers, and hardware manufacturers to restrict access to digital content.

Digital Reg asserts six patents covering different aspects of DRM, which are organized into four families: "regulating" - U.S. Patent No. 6,389,541 (the '541 patent); "tracking" - U.S. Patent No. 6,751,670 (the '670 patent) and U.S. Patent No. 7,673,059 (the '059 patent); "delivering"[1] - U.S. Patent No. 7,272,655 (the '655 patent) and U.S Patent No. 7,562,150 (the '150 patent); and "securing" - U.S. Patent No. 7,421,741 (the '741 patent).

The "regulating" patent describes a computer-implemented method of regulating access to digital content stored on a personal home computer. '541 patent, Abstract. When the user attempts to access protected content, the user must first satisfy an authorization process by entering account or use data at the client computer. Id. The account or use data is transmitted to the server computer, which either approves or rejects the data and transmits a token indicating the result to the client computer. Id. If the token indicates approval, the client computer initiates installation of the digital content, which is locked to that particular client computer. Id. If the object is transmitted or copied to a different computer, the user must again enter the required payment or use information to access the content. Id.

[1] Plaintiffs originally asserted U.S. Patent No. 7,127,515 (the '515 patent), which is the parent patent in the "delivering" family of patents. However, the '515 patent is no longer in the case because it is not asserted against any Defendant. See Defendants' Motion for Summary Judgment at vii (chart of asserted claims).

The "tracking" patents aim to maintain contact with digital content after it is distributed. Content owners may package computer code with the protected content, which collects notification information from each user or recipient of the content, then communicates the information back to the content owner when triggered by an event. '670 patent, Abstract. The content owner can therefore restrict access to the content regardless of how each user acquires the copy of the content. See '059 patent, Abstract.

The "delivering" patents are directed at managing delivery of digital content. Users request content from a web page. '655 patent, 3:16-33. The claimed method provides instructions that cause the user's computer to collect identifying information from the user, such as an email address, IP address, or other identifier, and provide it to a second (remote) computer. Id., Abstract. The second (remote) computer processes the transmitted identifying information and selects appropriate electronic content to send to the first computer. Id.

The "securing" patent involves encrypting digital content and locking it to a particular user or device. The patented method secures the digital content with a symmetric-key technique. '741 patent, Abstract. Symmetric key encryption uses "a secret or hidden key that is shared by both the sender and recipient of the encrypted data." Id., 1:62-64. While symmetric key encryption is relatively simple and less costly than alternative methods, one

disadvantage is that the secret key may be discovered or intercepted and the encrypted data can be easily stolen. Id., 1:65-2:1. An alternative method is asymmetric key encryption, which uses both a public key and a private key for more security, but is more costly and burdensome to implement. Id., 1:41-61.

The claimed invention of the "securing" patent uses the symmetric key encryption to secure content, but protects the symmetric decryption keys by inserting them into a header associated with the digital content container and encrypting the header using an asymmetric encryption technique. Id., 2:10-18. When the user wishes to access the content, the header is re-encrypted using data from the user's device, thus locking the contents of the container to the user or device. Id., 2:18-22.

DISCUSSION

I. Claim Construction

A. Legal Standard

"To construe a claim term, the trial court must determine the meaning of any disputed words from the perspective of one of ordinary skill in the pertinent art at the time of filing." Chamberlain Group, Inc. v. Lear Corp., 516 F.3d 1331, 1335 (Fed. Cir. 2008). This requires a careful review of the intrinsic record, which includes the claim terms, written description, and prosecution history of the patent. Id.; Phillips v. AWH Corp., 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) (internal citations omitted). While claim terms "are generally given their ordinary

and customary meaning," the rest of the claim language and the context in which the terms appear "provide substantial guidance as to the meaning of particular claim terms." Phillips, 415 F.3d at 1312-15. Claims "must be read in view of the specification, of which they are a part." Markman v. Westview Instruments, Inc., 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc), aff'd, 517 U.S. 370 (1996). Although the patent's prosecution history "lacks the clarity of the specification and thus is less useful for claim construction purposes," it "can often inform the meaning of the claim language by demonstrating how the inventor understood the invention and whether the inventor limited the invention in the course of prosecution, making the claim scope narrower than it would otherwise be." Phillips, 415 F.3d at 1317 (internal quotation marks omitted). The court may also consider extrinsic evidence, including dictionaries, scientific treatises, and testimony from experts and inventors. Such evidence, however, is "less significant than the intrinsic record in determining the legally operative meaning of claim language." Id. (internal quotation marks omitted).

B. Discussion

1. "Token"

This term appears in several claims of the '541 patent. For example, claim 1 reads:

> 1. A computer implemented method of regulating access to digital content, the method comprising:
> [. . .]

> receiving from an external source a **token**;
> based on the received **token**, executing an installation process that generates at the client a permission that is locked uniquely to the client and that may be found by a later execution of the access checking process.

Defendants point to the specification, which explicitly defines "token": "The token is a file indicating whether the transaction has been approved; i.e. whether the object should be installed and access granted." '541 patent, 5:1-3. Defendants urge the Court to adopt the first part of this passage as the definition of "token," or "a file indicating whether the transaction has been approved. Viewing the same passage, Plaintiff contends that the Court should instead define the function of a "token" according to the second part of the passage, or "a file indicating whether the access to the content should be granted." Both parties adopt one half of the passage while ignoring the other half. At the hearing, the parties consented to the Court's suggested construction integrating both proposals: "a file indicating whether the transaction has been approved and access should be granted."

The Court's construction makes clear that a token does not indicate simply that access should be granted, but also contains a yes/no indication. The specification states, "If the token indicates approval, the token causes the client computer to execute the install process . . . If the token indicates rejection, the install process will not be initiated and access is denied." Id., 4:65-5:15. The specification explains in further

detail the make-up of the "token": "In FIG. 7B, the acceptance message is a 128-bit message wherein the first bit signifies acceptance and the following 127 bits are 'dummy' bits utilized for conveying information only when a rejection has occurred." Id., 10:26-47. These passages demonstrate that the token indicates either approval or rejection, not always that access should be granted.

In its brief, Plaintiff argues that Defendants' proposed construction is inaccurate because it uses the term "transaction." A financial transaction is not necessary to initiate a token; the '541 patent makes clear that either payment or use authorization can result in access. The '541 patent Abstract states, "The content is inaccessible to a user until a payment or use authorization occurs." See also '541 patent, 3:16-18 ("access is regulated through payment transactions or other authorization information"). Plaintiff points to the differences between claim 13, which recites a possibility where "the token received is based on a result of the authorization procedure," and claim 18, which recites an outcome where the authorization procedure is a payment transaction. But as Defendants argue, a "transaction" need not be so narrow as to include only a financial transaction. It can be any interaction between parties. Interpreted in this way, the construction is consistent with tokens arising from either payment or use authorization.

2. "An authorization procedure"

This term appears in claim 13 of the '541 patent:

> 13. The method of claim 1, wherein requesting the permission from the external source initiates an **authorization procedure**, and the token received is based on a result of the authorization procedure.

The parties' dispute over construction of this term mirrors that of the previous term. Plaintiff contends that an authorization procedure is a "process which determines whether access should be granted," while Defendants counter that it should "approve or reject a payment transaction or use information."

The Abstract describes the authorization procedure: "The payment authorization center approves or rejects the payment transaction, and bills the corresponding account. The authorization center then transmits an authorization signal to the payment server computer indicating whether the transaction was approved, and if not, which information was deficient." '541 patent, Abstract.

Defendants argue that as with the term "token," the specification establishes that the authorization procedure is based upon either approval or rejection of the payment or use information received. '541 patent, 4:30-31. In the case of a payment transaction, if it is approved, an authorization code is sent indicating acceptance and authorization. Id., 10:9-26. If the transaction is rejected, an authorization code indicating rejection is transmitted. Id.

Plaintiff again takes issue with Defendants' construction as improperly limited to a "transaction," which is necessarily a payment transaction. Plaintiff cites the same parts of the specification indicating that both payment information and other use information can be used to authorize access to the content. Authorization is not limited to a financial transaction. But Defendants explicitly recognize this point in their definition, which notes that the authorization procedure "approves or rejects a payment transaction or use information."

However, as pointed out by Plaintiff, Defendants' definition is a verb rather than a noun like the term to be construed. The Court therefore adopts the following construction for "an authorization procedure": "a process which approves or rejects a payment transaction or use information to determine whether access should be granted." This definition recognizes that the authorization procedure can result in either approval or rejection. It also notes that the underlying object of the authorization procedure is to determine whether access to the content should be granted.

3. "Based on a result of the attempted transmission"/"Based on the results of the attempt to transmit"

These substantially similar terms appear in claim 32 of the '670 patent (a "tracking" patent) and several claims of the '515, '655, and '150 patents (the "delivering" patents). Claim 32 of the '670 patent states:

> selectively granting access to the electronic content **based on a result of the attempted transmission** of the notification information,

Claim 33 of the '515 patent, claim 1 of the '655 patent, and claim 1 of the '150 patent are similar:

> wherein the executable instructions collect the notification information and selectively grants or denies access to the electronic content **based on the results of the attempt to transmit.** '515 patent, claim 33.
>
> . . . and the instructions are configured to grant or deny access to the requested data **based on the results of the attempt to transmit**. '655 patent, claim 1.
>
> wherein the instructions include executable instructions configured to: a) attempt to transmit the notification information based upon the attempt to access the requested data, and b) grant or deny access to the requested data **based on the results of the attempt to transmit.** '150 patent, claim 1.

Plaintiff states that no construction is necessary because these terms can be understood according to their plain and ordinary meanings. Defendants disagree, proposing that the terms should be defined as "based on whether or not notification information is sent."

Plaintiff contends that Defendants' construction ignores the "result" aspect of the phrase. It argues that the claim language plainly indicates that the result of the attempt to transmit matters, i.e., that notification information must be sent and received, not merely sent. Plaintiff argues that the specification supports this point. The '670 patent specification explains that an attempt to transmit the notification information may result in either a return acknowledgment (success) or a

timeout error code (failure). '670 patent, 8:9-15. Thus, notification information must be both sent and received.

Defendants contend that Plaintiff's construction requiring successful transmission is contrary to both the specification and prosecution history. Scrutinizing the same passage of the specification indicating that the attempt to transmit can be either successful or unsuccessful, Defendants argue that the grant or denial of access does not depend on successful receipt of the transmission, but only attempted transmission. The prosecution history too indicates that the attempt to transmit can be either successful or not -- the patentee referred to the attempt to transmit as "the act of trying." Lang Decl., Ex. 14 at 20-21 (12/14/2003 Response to Office Action for '670 patent). Defendants argue that "trying" to transmit the notification information is enough to trigger the selective grant or denial of access to the content. Although the claim language indicates "result" of the attempted transmission, a result does not necessarily indicate a response from the recipient.

Defendants further contend that the patentee disavowed claim scope during prosecution of the '515 patent. In distinguishing the Venkatraman reference, the patentee noted in an examiner interview that "the invention as claimed grants access immediately upon attempted transmission of the notification, without waiting for a response from the server to grant access. In other words, the transmission of the notification is the triggering event for

granting access, not an authorization from the server." Lang Decl., Ex. 15 (03/05/05 examiner interview summary from '515 patent). The patentee further noted, "One of ordinary skill in the art would recognize that in the instance of an 'attempt' to transmit a message in a network (for example), the transmission may, in situations, not succeed." Id. The patentee therefore distinguished Venkatraman, where the "server grants access if the contents of the notification is deemed appropriate by the server," on the basis that the claimed invention "grants access immediately upon transmission of the notification, without waiting for a response from the server to grant access." Id.

After the interview, the patentee amended the term "transmit" in the claims to read "attempting to transmit," and further added that the function of selective granting or denying of access was "based on results of the attempt to transmit." Plaintiff argues that this amendment occurred after the examiner interview put forth by Defendants, and therefore the statements made in the examiner interview have no bearing on the interpretation of claim language inserted later. However, it appears that the patentee amended the claim language in response to statements made at the examiner interview. The patentee stated that its reasons for amendment were to "more clearly distinguish these claimed inventions which now recite with variations in part that the executable instructions selectively grants or denies access to the electronic content based on results of an attempt to transmit."

Beebe Decl., Ex. 29. By amending the claims to avoid prior art that disclosed a server granting access only if the contents of the notification information were deemed appropriate, the patentee disavowed that claim scope. The patentee is limited to an invention that grants access immediately upon the attempt to transmit the notification, without waiting for a response from the server. Lang Decl., Ex. 15.

The next question is whether this disavowal regarding the subject matter of the '515 patent should be imputed to the '655, '150, and '670 patents. The '655 and '150 patents are continuations of the '515 patent, but the application of a disavowal in the parent patent to child patents is not automatic. Cf. Omega Eng'g, Inc. v. Raytek Corp., 334 F.3d 1314, 1333 (Fed. Cir. 2003) (disavowal of claim scope during prosecution of parent application applied where patents used same claim term involving same limitation) and Ventana Med. Sys., Inc. v. Biogenex Labs., Inc., 473 F.3d 1173, 1182 (Fed. Cir. 2006) (prosecution history disclaimer did not apply to descendant patent because it used different claim language). At the hearing, the parties agreed that, because all of the patents use substantially the same term in substantially the same way, the term should be construed consistently. Accordingly, "based on a result of the attempted transmission" and "based on the results of the attempt to transmit" is construed as "based on whether or not notification

information was sent" as to all asserted patents containing the term.

4. "Selectively grants/denies access to the electronic content"

This term appears in claim 32 of the '670 patent:

> **selectively granting access** to the electronic content based on a result of the attempted transmission of the notification information,
> wherein executable instructions collect the notification information and **selectively deny access** to the electronic content until the notification information is transmitted.

Plaintiff contends this term is readily understandable. Further, Defendants' proposal deletes "selectively" from the term and adds in "parts," which appears nowhere in the plain claim language.

Defendants explain the reasoning behind their proposed construction. The patentee described this function in detail in addressing a patentability rejection under 35 U.S.C. § 101. Beebe Decl., Ex. 29 at 11-12. The patentee stated that, before notification information is transmitted successfully, the invention may deny access to "at least certain operations such as, for example, viewing, listing, saving, printing, or the like," or alternatively, access may be denied to certain parts of the data. Id. Defendants' definition therefore makes clear that "selectively" granting or denying access does not mean doing so with regard to the entire body of content, but rather means allowing or restricting access to certain parts of the content,

such as select portions of the content, or operations such as "saving, printing, or the like."

The Court adopts Defendants' definition with the slight alteration that includes the second part of the prosecution history excerpt, which explains that "selectively" may also include restricting certain operations of accessing the content. The term is construed as "granting or denying access to the select parts or operations of the electronic content."

5. "Recipient"

This term appears in claim 32 of the '670 patent:

> collecting notification information from a recipient and successive recipients of the electronic content in response to an attempt to access the electronic content;

Plaintiff argues that no construction is necessary, as follows. The context of claim 32 already states that the recipient receives the electronic content, so Defendants' definition of "user that receives the electronic content" would be redundant. Further, the claim language says nothing about a "user" or "use of the electronic content." The recipient's role is about access, not use.

But even if the claim language itself does not contain the term "user," the specification and prosecution history are replete with the term. The claims must be read in light of the specification, of which they are a part. Markman, 52 F.3d at 979. Here, the specification makes clear that the recipient of the electronic content is a "user" of that data. The specification

states: "Electronic mail (e-mail) enables computer users to conveniently share information . . . recipients sometimes delete or otherwise fail to read received email. Thus, a user sending e-mail often cannot be sure the intended recipient ever read or received the email." '670 patent, 1:15-17. See also id., 1:31-33 ("user receiving an e-mail attachment to easily forward attachments to other recipients."). The prosecution history also discusses "users" and "recipients" of the electronic content interchangeably. Smith Decl., Ex. 5 at 9-10 ("the executable instructions allows for the collection of notification information . . . for the successive recipients (i.e., users)."). See also id. at 10 (noting that the prior art "indicates a pre-determined addressing scheme wherein the recipients are pre-targeted . . . It is clearly not the dynamic successive user identification of the present invention.").

As Defendants note, if "recipient" is construed too broadly to include any entity that can receive electronic content, it could encompass a server computer, which would be contrary to the apparent intent of the patentee. Because the specification and prosecution history make clear that the recipient of electronic content is an end-user, the Court adopts Defendants' definition and construes "recipient" as "a user that receives the electronic content."

6. "Successive recipient"

This term appears in claims 32 and 45 of the '670 patent. For example, in claim 32:

> collecting notification information from a recipient and **successive recipients** of the electronic content in response to an attempt to access the electronic content;

The parties' dispute over this limitation centers on whether it requires serial succession (Defendants) or succession only in time (Plaintiff).

Plaintiff argues that nothing in the plain and ordinary reading of the term precludes a "successive recipient" from receiving the content from the same server as the first recipient, but later in time than the first recipient. For example, claim 74 states that an envelope from one computer can be sent from the server to "one or more successive recipients." This allows for server A to send content to recipient B, then server A to send content to "successive recipient" C. Plaintiff's expert, Dr. Wicker, agrees that the patent does not preclude such a possibility.

On the other hand, Defendants advocate that "successive recipient" is limited to a recipient who receives the content from a previous recipient, not directly from the server. Fig. 2B in the specification shows a second recipient receiving content from the first recipient. See '670 patent, 5:14-21. Moreover, during the prosecution history, the patentee amended the independent claims of the patent to include the phrase: "transmitting,

notification information to successive recipients to an address other than that of the immediate sender of the electronic content." Smith Decl., Ex. 6 at 4. The patentee therefore limited the term "successive recipients" to "those who receive the electronic content from an intended recipient (i.e., when an e-mail is forwarded to other recipients)." Id. Even if this statement alone is not enough to evidence a clear disclaimer of claim scope, the patentee's statements later in the prosecution history are unmistakable. After the patentee's amendment, the PTO again rejected the patent as obvious based on the Venkatraman prior art reference. The patentee again confirmed the claimed meaning of the term "successive recipient" as follows: "The present invention is directed, in general, to a method of tracking electronic content through successive recipients"; "The envelope may be re-transmitted by an initial recipient to successive recipients." Smith Decl., Ex. 5 at 6-7. The patentee stated that the prior art reference Venkatraman, by contrast, does not teach "that the initial recipient is capable or even permitted to re-transmit the initial e-mail onward to other (successive) recipients." Id. at 10.

Plaintiff may not now recapture exactly what was disclaimed to distinguish Venkatraman. Omega Eng'g, Inc., 334 F.3d at 1324. Accordingly, a "successive recipient" must be a "user that receives electronic content from a previous recipient."

7. "Successive computer"

This term appears in all asserted claims (16, 17, 19) of the '059 patent. The parties agree that it is substantially similar to the term "successive recipient" discussed previously. As with the previous term, the disagreement is over whether the term requires serial succession.

The prosecution history of the '059 patent suggests that the same disclaimer of scope applies here. In a June 2005 Response to Office Action, the patentee again argued that "the term 'successive' has a specific meaning which includes 'consecutive,' for example." Smith Decl., Ex. 7 at 10. This indicates that "successive" means one who receives the content, not from the server, but from a previous similar entity. In this context, "successive computer" means "user's computer that receives electronic content from a previous user's computer."

8. "Header"

The parties dispute the meaning of the term "encrypting a header," which is in claim 1 of the '741 patent. Both parties' definitions begin with no change to the term "encrypting," which means that what they are trying to define is actually "header." This definition of header shall apply to all disputed terms containing "header."

Plaintiff proposes "control information including at least a key associated with a data block." Plaintiff cites the specification, which demonstrates that the header does indeed

include a key for encryption. '741 patent, 3:27-35, 3:15-18. ("The computer program product . . . using a symmetric encryption technique and to encrypt a header associated with a first data block of the electronic content using an asymmetric encryption technique, the header including a symmetric decryption key."). However, Plaintiff cites no evidence, either intrinsic or extrinsic, to support the contention that a header is "control information." When asked at the hearing, Plaintiff could provide no persuasive reasoning for construing a "header" as "control information."

Defendants suggest that a "header" is well-known as "the beginning of a block of data." For example, a header of a document implies the beginning of the document. This interpretation is supported by the '741 patent specification. See Fig. 2 (depicting secure digital container (SDC) 120, with the header of the SDC at the beginning of the first data block); Fig. 6 (header 605 is at the head of the permission token structure). Plaintiff responds that Defendants are importing limitations from the specification, and that the header need only be "associated" with the first data block, and not necessarily physically connected.

Defendants also contend that, during prosecution, the patentee expressly disclaimed systems sending a key separately from the content. The patentee distinguished the Downs reference because the symmetric key and electronic content "are never

together in the same container," while in the claimed invention, "the electronic content and symmetric decryption key are associated with the same container." Beebe Decl., Ex. 20 at 9. The patentee derided the method disclosed by the Downs reference, stating that the claimed method had a "significant advantage [because] multiple containers are not necessary as is the case in Downs." Id.

Because the ordinary meaning of header is information at the beginning of the data, and all of the intrinsic evidence supports Defendants' proposal, the Court construes "header" as "the beginning of a block of data."

9. "Re-keying the header"

As with the last term, this term appears in claim 1 of the '741 patent. The Court's construction of "header" applies here. The parties further dispute the meaning of "re-keying the header."

Both parties appear to agree that re-keying the header has to do with re-encrypting the key in the header. The specification explains repeatedly that re-keying the header is "re-encrypting." '741 patent, 4:46-55, 14:12-21 (if access is not permitted, then "it may be assumed that the digital container is now present on another or different device from the original device from which the client footprint was originally created and for which a re-keying (i.e., re-encrypting) . . . may occur for establishing the new device or user"). See also id. at 3:17-21 ("the header including a symmetric decryption key, and re-keying the header

using data associated with a user or a user's device to lock at least a portion of the electronic content to the user or the user's device . . .''). The specification demonstrates that the key inside the header is replaced.

Where the parties disagree is over how to express that concept. Plaintiff merely suggests "re-encrypting the key." Defendants counter that this rewrites the claim language so that the key, rather than the header, is being re-encrypted. The Court agrees. The more thorough construction here is "re-encrypting the header using a different encryption key."

10. "Header associated with a first data block of the electronic content"

Regarding this term, which appears in claims 1 and 7 of the '741 patent, Plaintiff claims that no construction is necessary. Defendants offer that the term should be construed as "data at the beginning of the first block of the electronic content," reasserting many of the same arguments as for the term "encrypting a header." The Court has already construed "header" to mean "the beginning of a block of data;" there is no need to construe the rest of this term, which can be understood according to its plain and ordinary meaning.

II. Summary Judgment

A. Legal standard

Summary judgment is appropriate only where the moving party demonstrates there is no genuine dispute as to any material fact

such that judgment as a matter of law is warranted. Fed. R. Civ. P. 56(a); Celotex Corp. v. Catrett, 477 U.S. 317, 323 (1986). Material facts are those that might affect the outcome of the case, as defined by the framework of the underlying substantive law. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248 (1986). A dispute is genuine if the evidence is such that a reasonable jury could return a verdict for either party. Id.

The moving party bears the initial burden of informing the district court of the basis for its motion and identifying those portions of the pleadings, discovery, and affidavits that demonstrate the absence of a disputed issue of material fact. Celotex, 477 U.S. at 323. In opposing the motion, the non-moving party may not rely merely on allegations or denials of its pleadings, but must set forth "specific facts showing that there is a genuine issue for trial." Anderson, 477 U.S. at 248 (citing Fed. R. Civ. P. 56(e)). The court must construe the evidence in the light most favorable to the non-moving party, making all reasonable inferences that can be drawn. Matsushita Elec. Indus. Co., Ltd. v. Zenith Radio Corp., 475 U.S. 574, 587 (1986); Intel Corp. v. Hartford Accident & Indem. Co., 952 F.2d 1551, 1558 (9th Cir. 1991); Eisenberg v. Ins. Co. of N. Am., 815 F.2d 1285, 1289 (9th Cir. 1987).

To infringe a claim, each claim limitation must be present in the accused product, literally or equivalently. Dawn Equip. Co. v. Kentucky Farms, Inc., 140 F.3d 1009, 1014 (Fed. Cir. 1998). A

product may also infringe under the doctrine of equivalents, which must be evaluated on a limitation-by-limitation basis. Freedman Seating Co. v. American Seating Co., 420 F.3d 1350, 1356-57 (Fed. Cir. 2005). The standard test for equivalence is whether the accused product performs substantially the same function, in substantially the same way, to obtain substantially the same result for every asserted claim. Id. at 1358.[2]

B. Factual background of accused products

The Adobe accused products are: Adobe Flash Platform; Adobe LiveCycle; Adobe Software Delivery, Licensing, and Activation; and Adobe Digital Publishing Tools. The Adobe accused products allow content providers to deliver digital content (such as PDFs, Flash, eBooks, and other documents) to end-users.

Regarding Symantec, Plaintiff accuses a number of features of the Norton Antivirus consumer software. An end-user may freely download, install, and use Norton software from third-party websites. Smith Decl., Ex. 3 at 25:21-26:4. During a trial

[2] To defeat a motion for summary judgment of non-infringement on doctrine of equivalents grounds, a patentee must provide "particularized testimony and linking argument," on a limitation-by-limitation basis, "that creates a genuine issue of material fact as to equivalents." AquaTex Indus., Inc. v. Techniche Solutions, 479 F.3d 1320, 1328 (Fed. Cir. 2007). "Generalized testimony as to the overall similarity between the claims and the accused infringer's product or process will not suffice." Id. Plaintiff failed to address any doctrine of equivalents theory, much less explain how each accused product practices every limitation by performing substantially the same function, in substantially the same way, to obtain substantially the same result. The Court therefore considers only Plaintiff's literal infringement theories.

period and a subsequent grace period, the Norton software repeatedly asks the end-user whether she wishes to purchase an annual subscription. Id. If the end-user buys an annual subscription, she can access the Norton software's full functionality for an additional year. Id. at 30:24-31:12. If, on the other hand, the end-user does not buy an annual subscription, then the Norton software disables certain of its security features. Id. at 31:21-32:11.

The Ubisoft accused product is the Uplay PC platform. It is a stand-alone PC desktop client that allows users to log into their Uplay account to gain access to their library of games through an Ubisoft authentication server. Uplay PC is free to download and is distributed separately from the Uplay video games.

Users can purchase games through the Uplay Express shop, a store embedded in the Uplay PC client, and Ubishop, which is a stand-alone game store website. Both stores are operated by third party Digital River. When a game is purchased, Digital River sends a CD key for a purchased game to Ubisoft servers, which are located outside of the United States. Lang Decl., Ex. 5 at 20:20-21:9, 68:4-11, 130:17-25. A different third party, Limelight Networks, distributes games purchased through Ubishop and Uplay Express shop. Id. at 150:18-151:14. Games can be purchased, downloaded, and launched through the Steam Platform (operated by Valve Corporation). Lang Decl., Ex. 6. Users may also purchase games through third parties such as Best Buy and EA.

C. Summary judgment arguments that apply to all parties

Because all the asserted claims are method claims, in order to prove infringement, Plaintiff must prove that each Defendant practices each step of the asserted claims. "It is well established that a patent for a method or process is not infringed unless all steps or stages of the claimed process are utilized" within the United States. NTP, Inc. v. Research In Motion, Ltd., 418 F.3d 1282, 1318 (Fed. Cir. 2005).

Defendants first contend that Plaintiff cannot prove direct infringement because Plaintiff has admitted that each claim requires multiple actors. In the context of direct infringement of a method claim, all of the claimed steps must be "attributable to the same defendant." Limelight Networks, Inc. v. Akamai Technologies, Inc., 2014 WL 2440535, at *4 (U.S. June 2, 2014). On the other hand, a defendant cannot avoid liability "for direct infringement by having someone else carry out one or more of the claimed steps on its behalf." Muniauction, Inc. v. Thomson Corp., 532 F.3d 1318, 1329 (Fed. Cir. 2008). When multiple actors are involved, the accused infringer nevertheless directly infringes if it "exercises 'control or direction' over the entire process such that every step is attributable to the controlling party." Limelight Networks, Inc., 2014 WL 2440535, at *3 (quoting Muniauction, Inc., 532 F.3d at 1329).

Plaintiff's expert conceded that multiple actors are necessary to practice each of the method claims:

> Q: You would agree for the '670 and '059 patents asserted against Symantec, that multiple actors are needed to practice each of the method claims?
> A: Yes, the content distribution network and Symantec and the client.

Smith Decl., Ex. 11 at 718:7-13. See also Beebe Decl., Ex. 13 at 665:3-7 (regarding Adobe, infringement requires a user at the client site as well as a content owner/distributor); Lang Decl., Ex. 7 at 408:18-409:8 (admitting that regarding Ubisoft's alleged infringement, steps of the '655 patent are performed by third parties). At the hearing, Plaintiff confirmed that its theory of direct infringement involved the participation of certain third parties, such as the customers of all three Defendants.

Defendants have not shown that there is no genuine dispute as to whether they direct or control third parties to perform some of the steps. The primary purpose of Defendants' software is to maintain control over the user's operation of and access to the provided content. Wicker Depo. at 120:2-5 (admitting that Adobe's licensing-related code is "intended to maintain some level of control over the user's operation and use of the software."). Defendants all have software licensing agreements which aim to prevent unauthorized use and reproduction of their software -- in other words, to direct or control users to use the software as Defendants intended. See, e.g., Docket No. 531, Ex. R.

Ubisoft makes a separate but related argument that, because its Uplay PC platform uploads video games to third party CDNs from a third party in Malmö, Sweden, and many of its servers and data

centers are abroad, it cannot perform every step of the method within the United States. NTP, Inc., 418 F.3d at 1318. The authentication procedures, for example, allegedly occur abroad. Lang Decl., Ex. 7 at 390:12-13; Ex. 12 at 53, 61-62, 71. However, scrutinizing the actual claim language of claim 32 of the '670 patent, for example, shows that all of the limitations occur on the client side. While the claim requires "attempted transmission" to a third party, the grant of access occurs at the user's computer. Because Uplay PC distributes games in the United States, some users will have computers located in the United States. Moreover, Plaintiff cites evidence showing that at least some CDNs are located in the United States.

Defendants next assert that Plaintiff cannot prove indirect infringement because there is no evidence of the underlying direct infringement, nor does it have evidence of each Defendant's specific intent to cause infringement. Plaintiff's indirect infringement theories include both contributory and induced infringement. For contributory infringement, Plaintiff must prove (1) direct infringement, (2) the alleged infringer knew that the accused products were especially made to practice the patented method, and (3) the accused products have no substantial non-infringing uses. Joy Technologies, Inc. v. Flakt, Inc., 6 F.3d 770, 774 (Fed. Cir. 1993). To establish induced infringement, Plaintiff must prove (1) direct infringement, (2) the alleged infringer intended to cause the acts constituting the direct

infringement, (3) the alleged infringer knowingly and actively aided and abetted the direct infringement, and (4) the alleged infringer had specific intent to encourage the direct infringement. DSU Med. Corp. v. JMS Co., Ltd., 471 F.3d 1293, 1305 (Fed. Cir. 2006).[3]

Defendants argue that Plaintiff has not pointed to specific instances of direct infringement by customers. "[A] patentee must either point to specific instances of direct infringement or show that the accused device necessarily infringes the patent in suit." ACCO Brands, Inc. v. ABA Locks Mfrs. Co., Ltd., 501 F.3d 1307, 1313 (Fed. Cir. 2007). Defendants contend there is no evidence that users have deployed the accused products in an infringing manner. But direct infringement can be proved by circumstantial evidence, which must show that "at least one person directly infringed an asserted claim during the relevant time period." Toshiba Corp. v. Imation Corp., 681 F.3d 1358, 1364 (Fed. Cir. 2012). Plaintiff argues that it has provided sufficient evidence to show that at least some customers allowed a license to expire. For example, Symantec has technical design documents devoted to

[3] Defendants correctly point out that, in order to prove that Defendants indirectly infringed, Plaintiff must prove that all of the steps constituting infringement are attributable to one direct infringer. Limelight Networks, Inc., 2014 WL 2440535, at *5 ("in this case, performance of all the claimed steps cannot be attributed to a single person, so direct infringement never occurred"). Defendants cannot be both the direct and the indirect infringer, and so Plaintiff's indirect infringement theory must identify a separate direct infringer. At this time, however, Plaintiff properly asserts theories in the alternative.

dealing with expired and revoked licenses. Docket No. 560, Ex. 48; see also id., Ex. 28 at 80:5-11. Adobe instructs its users in the operation of the accused products, and takes technical steps to maintain control over the user's operation and access to parts of the software. Id., Ex. 16 §§ 6.2, 6.5; Ex. 14 at 113:7-114:25, 114:17-25, 115:2-120:5, 120-2:5; Ex. 19. Ubisoft contractually and technically seeks to control end-users' operation of the product. Id., Exs. 42-44. This evidence indicates that it is likely that at least some users allowed their licenses to elapse, then subsequently had access restricted until they entered payment or use information. See Moleculon Research Corp. v. CBS Inc., 793 F.2d 1261 (Fed Cir. 1986) (finding that Moleculon had met its burden of showing direct infringement with circumstantial evidence of extensive puzzle sales, dissemination of an instruction sheet teaching the method of restoring the preselected pattern with each puzzle, and the availability of a solution booklet on how to solve the puzzle).

Defendants also challenge that Plaintiff cannot prove there are no substantial non-infringing uses. If a product has substantial non-infringing uses, it does not contributorily infringe. Fujitsu Ltd. v. Netgear Inc., 620 F.3d 1321, 1326 (Fed. Cir. 2010). To determine whether there are substantial non-infringing uses, "where the alleged method is embodied in a larger product, the Court must examine whether the particular components that allegedly practice the patented method have substantial non-

infringing uses, and not the entire product as a whole." Mformation Techs, Inc. v. Research in Motion Ltd., 830 F. Supp. 2d 815, 841-42 (N.D. Cal. 2011) (citing Fujitsu Ltd., 620 F.3d at 1330-31 (holding that to determine whether there were substantial non-infringing uses, the relevant component was the specific hardware and software that performed the infringing fragmentation)). Here, the methods claimed by the asserted patents involve DRM technology. Any substantial non-infringing uses must be considered with regards to the DRM features of the accused products, and not the products as a whole. See i4i Ltd. Partnership v. Microsoft Corp, 598 F.3d 831, 849 (Fed. Cir. 2010). Defendants' arguments that their products as a whole have other substantial non-infringing uses are therefore unavailing.

The same is true for Defendants' arguments that they did not have the requisite intent or specific intent to encourage the direct infringement. Defendants contend that they never intended users to allow their licenses to elapse. But there is at least a disputed issue that Defendants intended that the overarching process would occur -- if the user did not at first initiate payment or other authorization, the client computer would deny access to the digital content and prompt the user to submit authenticating information. As evidenced by Defendants' technical documentation and licensing agreements, the accused products were designed to anticipate and address the circumstance of the user trying to avoid digital content control.

D. Adobe

The Court turns next to the Adobe-specific summary judgment arguments. Adobe asserts that its accused products do not infringe based on either the agreed-upon constructions or its proposed constructions, if the Court chooses to adopt those constructions. Adobe also renews its previous summary judgment motion that Microsoft's license with Plaintiff regarding Windows shields Adobe from liability.

a) Microsoft's Windows license with Plaintiff

Adobe asserts that, because Microsoft holds a license at least regarding the '541 patent with Plaintiff and the accused products run at least sometimes in a Windows environment, in those instances the accused products are shielded from infringement. Adobe previously brought a summary judgment motion on this issue, which the Court denied because it found that "Defendants have not shown as a matter of law that the Microsoft License extends to any product when used in combination with a Microsoft product. The Microsoft License may only extend to Microsoft products that perform any claim of any Licensed Patent, whether used alone or in combination with other things." Docket No. 438 at 7. Adobe now reasserts its argument based on Plaintiff's expert's statement that at least three steps of the '541 patent must be performed on a computer. But these steps -- "requesting permission from an external source for the resource to access the digital content"; "receiving from an external source a token"; and "executing an

access checking process" -- are not executed by the Microsoft product, or the Windows operating system. The fact that the accused product allegedly executes the infringing code on the Windows operating system is not enough to say that the Windows operating system is performing these steps. Accordingly, Adobe's renewed motion for summary judgment on this point is denied.

b) The term "token"

The Court construed "token" to include Defendants' proposed definition: "a file indicating whether the transaction has been approved and access should be granted." This construction indicates that the token is capable of exhibiting either approval or rejection of the payment or use information. Adobe's expert opines that none of the accused products practice a "token" under this definition. Beebe Decl., Ex. 8 at ¶¶ 98-101. Plaintiff's expert, who reviewed the source code and technical literature related to the accused products, asserts the opposite, identifying a token for each product. Docket No. 560, Ex. 3. See also Plaintiff's Reply at 14 (identifying a "token" for each accused product). Plaintiff further asserts that its expert's identification of a token in each of Adobe's accused products is consistent with the Court's construction. Defendants have not explained why Plaintiff's expert's opinion is inconsistent with the Court's construction. Accordingly, there are disputed issues as to infringement of the "token" limitation.

c) The term "executing an installation process that generates at the client a permission that is locked uniquely to the client and that may be found by a later execution of the access checking process"

The parties agreed that this term should be construed as "running an installation program that creates a permission locally, which permission is (1) locked uniquely to the client and (2) capable of being found locally by a later execution of the access checking process." See Defendants' Motion at 10.

Adobe contends that Plaintiff has asserted irreconcilable positions on infringement and validity regarding this term. For infringement, Plaintiff states that the object accused as the permission is created remotely and then passed to the local machine. Beebe Decl., Ex. 13 at 619:4-8. For validity, Plaintiff has distinguished the '541 patent from the prior art on the basis that, for the '541 patent, the permission cannot be created at the remote server and passed to the local machine. Beebe Decl., Ex. 14. Adobe argues that the permission must be generated locally, as the agreed-upon construction requires.

Plaintiff responds that its expert, Dr. Devanbu, has opined that the input of the permission comes from the remote server. This is required by the claim in question, which states before the phrase identified by Adobe, "based on the received token . . ." '541 patent, claim 1. Claim 1 therefore allows for the input of the permission, generated locally, to be received from an external source. According to Dr. Devanbu, the permission itself however

is a decryption key that is produced at the client. See Plaintiff's Reply at 14 (explaining how, for each product, the permission is produced at the client device). Accordingly, summary judgment of non-infringement is not warranted on this point.

As for Adobe's validity argument, Adobe has not proven by clear and convincing evidence that the patent is obvious or anticipated. Microsoft Corp. v. i4i Ltd. Partnership, 131 S.Ct. 2238, 2242-43 (2011).

d) Plaintiff's purportedly irreconcilable definitions of "container identifier"

Adobe contends that Dr. Keller, Plaintiff's expert, distinguished Adobe's Digital Content system by adopting a different claim construction of the term "container identifier." Dr. Keller stated that a container identifier must be container specific, not content specific, such that each transmission of a container (such as a copy of a downloaded book) must use a unique identifier, instead of unique identifiers for the book itself. Beebe Decl., Ex. 15 at 193:15-20. Dr. Keller used this aspect to distinguish the '741 patent from the prior art. In analyzing infringement, however, Plaintiff asserted that Adobe's products use a content-specific identifier, not a container-specific identifier. Beebe Decl., Ex. 22 at 4. Because these definitions are "irreconcilable," Adobe argues that it is entitled to summary judgment, either of non-infringement or invalidity.

Adobe, however, must carry its burden of persuasion at the summary judgment stage. To prove invalidity, it must prove with clear and convincing evidence that the patent is obvious or anticipated. Microsoft Corp., 131 S.Ct. at 2242-43. It has not done so.

Nor has Adobe shown that Dr. Keller's container specific, not content specific, interpretation of "container identifier" is the correct one as supported by the intrinsic and extrinsic evidence. Accordingly, summary judgment is not warranted.

e) The terms "encrypting a header" and "re-keying the header"

Adobe argues regarding the "header" terms that if Defendants' proposed constructions are adopted, then Adobe is entitled to summary judgment of non-infringement of all terms of the '741 patent because Dr. Devanbu did not opine as to infringement under those constructions. Plaintiff produces no evidence in response and does not even attempt to explain why the accused products infringe these limitations. See Plaintiff's Reply at 17-19. Accordingly, summary judgment is warranted.[4]

[4] Where the moving party informs the Court of the basis of its motion, putting the non-moving party "on notice that she had to come forward with all of her evidence," but the non-moving party failed to do so, summary judgment is warranted. Celotex Corp., 477 U.S. at 326.

f) The term "based on the result of the attempted transmission"

The Court adopted Defendants' construction of this term: "based on whether or not notification information is sent."

Adobe asserts that, because Plaintiff's infringement analysis was based on an application-level response and its invalidity analysis was based on a network-level response, they are contradictory and summary judgment is warranted. But Adobe does not explain whether a network-level response or an application-level response would be inconsistent with the Court's constructions of this term. See Defendants' Motion at 19. Accordingly, Adobe has not satisfied its initial burden of informing the Court of the grounds of the summary judgment motion. Summary judgment is not warranted here.

g) Plaintiff's purportedly irreconcilable definitions of "notification information"

Neither side proposed this term for construction. Dr. Keller, Plaintiff's validity expert, discussed the term and referred to it as used in the '670 patent as "to identify and track the recipient." Beebe Decl., Ex. 14 ¶ 140. Adobe claims that Plaintiff has no support for this "construction," and, if adopted, Adobe is entitled to summary judgment with respect to Digital Publishing Tools, Flash, and its Software Delivery, Licensing, and Activation services because Plaintiff has no evidence that those products track or use content. But even assuming the "construction" in Plaintiff's expert report is a

binding limitation, it is not content that is being tracked, but the recipient. Adobe has not provided any legal basis for summary judgment on this contention.

E. Symantec

Symantec, whose products are charged with infringing various claims of the "tracking" patents, has moved for summary judgment based on Plaintiff's lack of evidence and the Court's constructions.

a) The '059 patent claims

The Court granted Symantec's motion to strike portions of Dr. Devanbu's expert report relating to claim 16 of the '059 patent as asserted against the Consumer Licensing Technologies (CLT) products because they were not properly disclosed in Plaintiff's infringement contentions. Docket No. 509 at 2:10-18. Claim 16 of the '059 patent is therefore not asserted against the CLT products. To the extent that other Norton features, such as SOS/SCSS or ACT-WEB, are properly disclosed in Plaintiff's infringement contentions, Plaintiff may continue to pursue infringement claims against Symantec. Symantec has not shown that Plaintiff's infringement theories asserting claim 16 of the '059 patent should be stricken as to any other Symantec feature or product.

b) The term "deny access to electronic content until notification information is transmitted"

Claim 32 of the '670 patent requires executable instructions that "selectively deny access to the electronic content until the notification is transmitted." Similarly, claim 45 of the '670 patent requires a "file that includes electronic content and causes access to the electronic content to be denied until notification information collected by executable instructions has been successfully transmitted." In other words, both claims of the '670 patent asserted against Symantec require access to electronic content to be denied, at least in part, until notification information is transmitted.

Symantec alleges that its products do not infringe because it is undisputed that they allow access to the content before the alleged notification information is transmitted. See Smith Decl., Ex. 8 at 77-11:15. Plaintiff concedes that the CLT products transmit notification information at the same time as software activation. Id. at 83:11-15. Plaintiff also admits that software activation does not occur until after "the end-user is provided with full access to all features within Symantec products." Id. at 204:22-205:12. Accordingly, Symantec argues that it should be entitled to summary judgment because access is not denied until notification information is transmitted.

Plaintiff responds that Symantec has only pointed to an instance where it does not infringe, but ignores instances of

where it does infringe. Plaintiff accuses the steps that occur once the CLT product expires. At that point, access to the electronic content is denied until notification information is sent. Plaintiff's seat transfer theory regarding the Norton products provides another possible example of infringement. A license allows for a limited number of "seats," or slots for installation. If a license only permits three seats, but the user attempts to install the product on a fourth computer, access to content is immediately denied. Docket No. 560, Ex. 25 at 29:22-30:5. A reasonable jury might find that either of these theories fulfills the requirement that access is denied until notification information is sent. Therefore, summary judgment on this point would be improper.

c) The terms "successive recipient" and "successive computer"

The Court adopted Defendants' proposed construction of "successive recipient" and "successive computer," which require a "user that receives electronic content from a previous recipient" and a "user's computer that receives electronic content from a previous user's computer," respectively. These terms appear in all of the asserted claims.

Plaintiff's theory as to Symantec's infringement under this construction is that the first recipient would be Symantec's server, whereas the second recipient is the end-user and the end-user's computer. However, this theory ignores the Court's claim

construction. Plaintiff's XLok theory is similar -- "Additionally, each Symantec product binary is 'wrapped' with an XLok wrapper before being transmitted to a distribution server. These binaries are then downloaded by Symantec customers, therefore the customers themselves are also successive recipients even upon their first installation of a Symantec product." Docket No. 560, Ex. 26 at 91. This theory is again contrary to the Court's construction requiring a user of the electronic content because a server cannot be such a user.

Plaintiff lastly offers a seat transfer theory, where a license is transferred from one end user customer's computer to another end-user's computer. Docket No. 560, Ex. 27 at 36-37. This theory is the only one that conforms to the Court's construction and survives summary judgment.

F. Ubisoft

Ubisoft's UPlay platform is accused of infringing claims of the "tracking" and "delivering" patents. Ubisoft moves for summary judgment based on the application of the Valve license and on the Court's claim construction.

a) Valve license on the Steam platform

Valve, previously a Defendant in this action, entered into a Settlement Agreement with Plaintiff which included licensing the patents-in-suit. The language of the Agreement provides that any third party "use" of a Valve licensed product is also licensed, to the extent of such use. Lang Decl., Ex. 18 § 2.7. Covered third

parties include "users," "developers," and "partners" of Valve. Id. §§ 2.1, 2.4, 2.7. Products covered by the Agreement include Valve's Steam Platform, a digital distribution system for video games covered by the Agreement. Id. § 1. To the extent that Valve's Steam Platform acts as a third party that performs a required step, limitation, or element of an asserted claim against a Ubisoft game, that performance would constitute licensed "use" of a Valve product, which is immune from an infringement suit. Plaintiff is therefore precluded from asserting that Valve acts as a third party in performing any required step, limitation, or element of the asserted claims.

b) The terms "based on a result of the attempted transmission"/"based on the results of the attempt to transmit"

Ubisoft contends that Plaintiff has disclosed no expert opinion nor evidence that would support a finding of infringement under the Court's construction. The Court adopted Defendants' construction of this term, which requires that the grant or denial of access occur upon the attempted transmission of the notification information, not its authentication. Plaintiff's infringement expert testified that access to Ubisoft's products depends on the server authenticating the login information and "sending a message back." Lang Decl., Ex. 7 at 462:1-464:21. By the expert's own admission, access to Ubisoft's products depends on server authentication (i.e. successful transmission and

approval of notification information) rather than the act of transmitting the notification information itself.

In its response, Plaintiff fails to provide any evidence in support of an infringement theory utilizing the Court's construction, but instead confirms its infringement expert's view. Plaintiff explains that, regarding "Ubisoft's Uplay-enabled games, without a successful transmission of notification information, no access granting message would be received by the transmitting computer." Plaintiff's Reply at 20. In other words, access to the Uplay game content is predicated on the server receiving the successful transmission and sending an access granting message in return. Id. Because Ubisoft's products wait for the server to respond rather than granting access immediately upon transmission of the notification information, they do not infringe the limitation in question. According to Plaintiff itself, Ubisoft does not practice these limitations as construed by the Court and summary judgment is warranted on all claims of the '670, '655, and '150 patents.

c) The terms "successive recipient" and "successive computer"

Ubisoft contends that Plaintiff has no evidence supporting an infringement theory that conforms to the Court's construction of this term, which requires that both the first and the successive recipient/computer be that of an end-user, and that the successive recipient/computer receive the content from a previous end-user.

Plaintiff offers in response a couple of theories that do not meet this limitation: where a CDN server is the first recipient and sends it to an end-user; and where a CDN server sends one end-user a game, then sends the game to another end-user at a later time. Both of these theories were rejected by the Court's construction. Plaintiff then asserts, without citation to any evidence, that an end-user "receives a Uplay-enabled game from a CDN server and then sends that game on to another end user/end user computer ('successive recipient')." Plaintiff's Reply at 27. Plaintiff provides no expert opinion or other evidence showing that this scenario occurs with Ubisoft's products. Ubisoft confirms that this theory has never been espoused by Plaintiff before and that there is no expert testimony or other evidence to support this notion. Defendants' Reply at 14 (citing Lang Decl., Ex. 7 at 456:21-457:23). Summary judgment in favor of Ubisoft is therefore warranted on this point, which covers all asserted claims of the '670 and '059 patents.

d) The term requiring that access be granted "upon transmission" of an authorized user identifier

Ubisoft argues that summary judgment is warranted regarding a limitation which appears in independent claim 16 of the '059 patent:

> wherein the computer executable instructions are executed at the one or more successive computers and **upon transmission of an authorized user identifier** to a network address other than a network address of the sending computer, access is granted to at least a portion of the electronic data.

(emphasis added). Ubisoft interprets this claim to mean that access is granted once the authorized user identifier is transmitted, as opposed to being granted only after the server authenticates the authorized user data. Ubisoft alleges that Plaintiff's theory of infringement relies on granting access upon server authentication, not upon transmission. Plaintiff's theory is that, when the user logs in to the Ubisoft server and provides the authorized user identifier and "the authorized user identifier has been transmitted and processed successfully, a user is granted access to game content." Lang Decl., Ex. 9 at 34-35. Ubisoft argues that it is therefore undisputed that its accused products provide access only after both transmission of authorized user identifier and successful processing of that identifier, which is contrary to the limitation.

Plaintiff responds that nothing precludes the account credential and CD keys that enable a user to access the games to be the authorized user identifier. Docket No. 560, Ex. 2 at 2:41-47, 1:63-67. Even if Plaintiff is correct that the account credential and CD keys can act as the authorized user identifier, Plaintiff's response does not answer the issue raised by Ubisoft, which is that the claim requires access to be granted "upon transmission" of said authorized user identifier. A plain reading of the claim language reveals that access is granted "upon transmission" of the user information, which is distinct from

Plaintiff's infringement theory that Uplay grants access only upon successful processing of that information. Summary judgment for Ubisoft is appropriate on all asserted claims of the '059 patent.

CONCLUSION

Adobe is entitled to partial summary judgment of non-infringement of the '741 patent based on the header limitations. Claims of the '541 and '670 patents remain asserted against Adobe.

Symantec is entitled to partial summary judgment of non-infringement of all asserted claims of the '670 and '059 patents, on all theories except for the seat transfer theory, based on the limitations "successive recipient" and "successive computer."

Ubisoft is entitled to summary judgment of non-infringement on all the claims asserted against it for several reasons. First, Plaintiff is precluded from bringing any theories that require Valve's Steam Platform to perform any limitation or step. Second, all claims of the '670 and '059 patents are barred as to Ubisoft for failure to satisfy the limitations "successive recipients/computers." Third, because Ubisoft does not infringe the "based on a result of the attempted transmission"/"based on the results of the attempt to transmit" terms contained in the claims of the '655, '150, and '670 patents, the Court grants summary judgment on all asserted claims of those patents as well. Fourth, Ubisoft is entitled to summary judgment of non-infringement of the limitation requiring access to be granted

"upon transmission" of an authorized user identifier, which appears in claims of the '059 patent.

IT IS SO ORDERED.

Dated: 6/10/2014

CLAUDIA WILKEN
United States District Judge