NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

ZAPMEDIA SERVICES, INC.,
Plaintiff-Appellant,

v.

APPLE, INC.,
Defendant-Appellee.

2011-1546

Appeal from the United States District Court for the Eastern District of Texas in Case No. 08-CV-0104, Chief Judge David J. Folsom.

Decided: April 25, 2012

STEVEN G. HILL, Hill Kertscher & Wharton LLP, of Atlanta, Georgia, argued for plaintiff-appellant. With him on the brief were BLAKE H. FRYE and MARTHA L. DECKER.

WILLIAM C. ROOKLIDGE, Jones Day, of Irvine, California, argued for defendant-appellee. With him on the brief were ALYSON G. BARKER; and GEORGE A. CASTANIAS, of Washington, DC. Of counsel on the brief were LOUIS

BRUCCULERI, Wong, Cabello, Lutsch, Rutherford & Brucculeri, of Houston, Texas, and DANNY L. WILLIAMS, Williams Morgan & Amerson, P.C., of Houston, Texas.

Before LOURIE, LINN, and PROST, *Circuit Judges*.

LOURIE, *Circuit Judge*.

ZapMedia Services, Inc. ("ZapMedia") appeals from the final judgment of the United States District Court for the Eastern District of Texas, which granted summary judgment of noninfringement of claims 1, 4, 7, 8, 10, and 14 of U.S. Patent 7,343,414 (the "'414 patent") by Apple, Inc.'s ("Apple") iTunes product. *ZapMedia Servs., Inc. v. Apple, Inc.*, No. 2:08-CV-104-DF-CE (E.D. Tex. Jul. 20, 2011) (the "*Summary Judgment Op.*"). ZapMedia also challenges the underlying claim construction relied on by the district court. *ZapMedia Servs., Inc. v. Apple, Inc.*, No. 2:08-CV-104-DF-CE (E.D. Tex. Aug. 19, 2010) (the "*Claim Construction Op.*"). Because the court did not err in granting summary judgment of non-infringement or in its underlying claim construction, we *affirm*.

BACKGROUND

The '414 patent, owned by ZapMedia, discloses and claims a system and method for distributing media assets to user devices and managing user rights of the media assets. In the preferred embodiment, a user obtains an account on a server, is issued a password, and a virtual private media asset database is created:

> [A] user becomes a member or subscriber to a portal 300, . . . and he/she is issued a user-specific password. Once a membership exists, a virtual private media asset database is created and asso-

> ciated with the user's login account and password in the portal.

'414 patent col.10 ll.26–31. That account keeps track of the licensed media assets (*e.g.*, songs and video) and the various media player devices registered by the user. *Id.* col.9 ll.60–62, col.10 ll.31–34, col.10 ll.61–64. Claim 1 is representative:

> 1. A method of managing access to a plurality of media assets comprising the steps of:
>
> providing a user with a user account;
>
> storing references to a plurality of media assets which the user has a license to use; and
>
> authorizing over a network a plurality of media player devices with the user account,
>
> wherein the plurality of referenced media assets can be accessed by any one of the authorized plurality of media player devices.

Id. col.13 ll.13–22.

During the prosecution of the '414 patent and its parent, U.S. Patent 7,020,704 (the "'704 patent"), ZapMedia made several arguments to overcome a rejection based on U.S. Patent 6,345,256 ("Milsted"). Milsted describes a single-download, digital rights management ("DRM") protected digital media delivery system that allows any media player with the necessary software to copy and use the media asset. In amending its claims, ZapMedia explained that unlike application claim 84 (later issued as '414 patent claim 1), Milsted "does not describe, suggest or teach the provision of a user account to a user as recited in claim 84." J.A. 708. Pointing to the pending claims that required "associat[ing] a plurality of media player devices with the user account," ZapMedia noted

that claim 84 "recites that a user can enable a plurality of media player devices, on a user account basis, to access assets licensed to the user." J.A. 708. ZapMedia then distinguished Milsted, by noting that "Milsted does not disclose this element of claim 84" and that Milsted functions "without regard to the device being associated with the user account." J.A. 708–09. ZapMedia concluded that Milsted's media assets "can be copied and used by ANY player device, not a subset of player devices that are associated with a user account." J.A. 710 (emphasis in original). ZapMedia added a caveat: "Although the embodiments that are covered by claim 84 do not preclude technology such as described in Milsted, the applicants point out that the Milsted reference does not disclose . . . a plurality of media assets that may be accessed by any one of the media player devices that are associated with the user account." J.A. 711.

ZapMedia filed a complaint against Apple alleging that Apple's iTunes system infringes the '414 patent. Based on the statements in the prosecution history and, in particular, the claim language regarding "authorized" media player devices with "access" to media assets, the court found that all the asserted claims require that access to the media assets be limited *only* to those media players specified in the user account. *See Claim Construction Op.*, at 14, 17–18; *Summary Judgment Op.*, at 9. In other words, if a system allowed access to media assets through the user account by an unauthorized device, it would not infringe. The court construed: (1) "user account" to mean "a record, including a login and password, indicating that the user has the right to access the media assets and indicating which media player devices may access referenced media assets"; (2) "authorizing . . . a plurality of media player devices with the user account" to mean "specifying two or more media players in the user

account, whereby referenced media assets can be copied (and/or used) through the user account only by those media players"; and (3) "a plurality of media player devices as being authorized with the user account" to mean "two or more media players specified in the user account, whereby referenced media assets can be copied (and/or used) through the user account only by those media players." *See Summary Judgment Op.*, at 22; *Claim Construction Op.*, at 22.

In its motion for summary judgment of noninfringement, Apple submitted evidence in the form of expert testimony that an unauthorized media player could download a media asset from iTunes. In this experiment, Apple's expert used an undisputedly unauthorized device to download a pre-purchased media asset after logging in to an iTunes store account. The experiment also showed that, to enable that download, iTunes provides a URL directing the user to a third party server to download the media asset.

Based on the claim construction and the download experiment, the court held that there was no genuine issue of material fact that iTunes could infringe because it allowed an unauthorized media player device to download and use files through an iTunes user account. *Summary Judgment Op.*, at 21. In other words, iTunes did not meet the authorization-related limitations. The court also held that a user account is not limited only to that part of the iTunes store account that contains the media asset and device data and rejected ZapMedia's argument that there was an issue of fact whether downloading from a third party server was "through the user account." *Id.* at 14–17. The court also held that the "user account" requires login and password information. *Id.* at 15–17. ZapMedia timely appealed. We have jurisdiction under 28 U.S.C. § 1295(a)(1).

DISCUSSION

I.

We review *de novo* the district court's grant of summary judgment, drawing all reasonable inferences in favor of the nonmovant. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 255 (1986); *Hologic, Inc. v. SenoRx, Inc.*, 639 F.3d 1329, 1334 (Fed. Cir. 2011). Summary judgment is appropriate when there is "no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." FED. R. CIV. P. 56(a). We address claim construction as a matter of law, which we review without formal deference on appeal, although we give respect to the judgments of the district courts. *See Cybor Corp. v. FAS Techs., Inc.*, 138 F.3d 1448, 1456 (Fed. Cir. 1998) (en banc).

ZapMedia argues that the court erroneously construed a negative "exclusivity" limitation requiring copying and usage of licensed media through the user account *only* by media players specified in the user account. ZapMedia contends that the use of the term "plurality" suggests a broader number of authorized and unauthorized devices. In addition, ZapMedia posits that the written description and statements in the prosecution history regarding Milsted cover "access" to media assets other than through the user account (*e.g.*, by using watermarking and encryption). ZapMedia argues that Milsted was distinguished, not based on access, but because it did not teach: (1) the association of media player devices with a user account; and (2) authorizing a plurality of media players.

In addition, ZapMedia argues that there is a genuine issue of material fact as to whether the downloading experiments Apple submitted actually illustrate copying or use of media assets "through the user account." Ac-

cording to ZapMedia, the copying on iTunes occurs after purchase, and the download does not occur through the Apple user account, but from a third party server, without traversing the account. Alternatively, ZapMedia also argues that a user account does not require a login/password, contrary to the court's construction, and that the district court conflated the iTunes store account with the claimed "user account," which is more narrowly limited to the list of media and devices.

Apple responds that the plain language of the claims requires "authorizing" the "plurality of media players devices with the user account," linking "authorization" with both the device and the user account. In other words, access through a user account for unauthorized media players is contrary to the claim language, and the use of the term "plurality" does not negate this requirement. Apple notes that the specification expressly states that each user account has a media player device associated with it and that only those devices can access the media assets associated with that account. The presence of DRM technology, according to Apple, does not change this requirement, since those devices must still be associated with an account. Apple also relies on the statements made by ZapMedia during the prosecution history distinguishing Milsted as supporting the construction that only authorized media player devices can access media through a user account.

Apple also argues that the grant of summary judgment was based entirely on a question of law (claim construction) with no factual disputes. According to Apple, the issue raised by ZapMedia—whether media assets are copied through a user account in iTunes—is a claim construction issue because the functionality of iTunes is not disputed. Apple notes that a user must still interact with the user account to retrieve the media from

the third party servers via logging in and receiving a URL from iTunes. Apple notes that ZapMedia's expert even admitted that the iTunes store account is a "user account" under the court's original construction. Finally, Apple contends that the court does not need to reach the question whether a "user account" requires a login/password, because the opinion below was based solely on the authorization-related limitations.

We agree with Apple and the district court that in light of the claim language, written description, and the prosecution history, the authorizing limitations limit "access" to media assets only to "authorized" media player devices by way of the user account. To ascertain the scope and meaning of the asserted claims, we look to the words of the claims themselves, the specification, the prosecution history, and, if necessary, any relevant extrinsic evidence. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1315–17 (Fed. Cir. 2005) (en banc). As the district court noted, the claim limitations focused on whether authorized media players can *access* media assets from the asset management system, not on whether unauthorized devices can *play* those assets. *Claim Construction Op.*, at 12–13. For example, claim 4 of the '414 patent requires "enabling the at least one authorized media player device to *access* one or more of the media assets associated with the user account." Claims 1 and 10 have similar language: "wherein the plurality of referenced media assets can be *accessed* by any one of the authorized plurality of media player devices" (claim 1) and "providing *access* to at least one of the plurality of licensed media assets by any one of the plurality of authorized media player devices" (claim 10). The relevant inquiry for infringement is therefore whether authorized devices are *accessing* media assets, not whether those devices can play them.

The claim language by itself suggests that access must be exclusively limited to authorized devices by way of the user account. Claim terms of course should not be interpreted "in a vacuum, devoid of the context of the claim as a whole." *Kyocera Wireless Corp. v. Int'l Trade Comm'n*, 545 F.3d 1340, 1347 (Fed. Cir. 2008). But the claims each require authorization prior to access, as the access is given to "authorized" devices, and each of the claims links both the media assets and the authorization "with the user account." For example, claim 1 requires that authorization of the media player devices be "with the user account . . . *wherein* the . . . media assets can be accessed." Claims 4 and 10 similarly require a previously authorized media player to access media assets that are associated with the user account. Taking the claim terms as a whole, as the authorization of the devices is with the user account and the media assets are associated with that user account, the access given to the authorized devices must therefore be by way of the user account. In addition, because the claims require access to media assets by an authorized media player device, logically an unauthorized media player device cannot access the media assets. The authorization would be superfluous if unauthorized devices had the same access functionality as authorized devices. And contrary to ZapMedia's argument, the claim's use of the term "plurality" does not negate this fact, instead only specifying that there can be a number of authorized media player devices.

Supporting this reading, the written description identifies a preferred embodiment limiting access to authorized media players:

> The system according to the present invention permits users to download their licensed digital media assets to secure client media player devices and to use their licensed digital media assets on

> those devices. As with the physical use of a CD in the bricks and mortar world, a user will have *access* to use his or her licensed assets on other infotainment devices that he or she owns or uses, *provided those other client media player devices are registered within the portal as being authorized to use the user's licensed assets*.

'414 patent col.10 l.61–col.11 l.2 (emphases added). The written description continues, describing the use of a previously purchased media asset on authorized devices. *Id.* col.11 ll.60–64 ("An asset stored locally on a media player . . . can be identified and uploaded to the portal for use on other authorized media player devices of that user."). The only other mention of authorized devices is in the negative, describing a security lockout feature to prevent unauthorized media players from using media assets after synchronizing with the server. *Id.* col.12 l.54–col.13 l.10 ("To protect the usage of a digital media asset and a media player device, the security lockout procedure is provided to lockout unauthorized media player devices."). These three references to authorized devices show one common thread: authorized devices have access; unauthorized devices do not.

If there were any lingering doubt, ZapMedia, during the prosecution of the '414 patent, made several statements distinguishing Milsted on that very basis. Again, Milsted describes a single-download, DRM-protected digital media delivery system that allows any media player (authorized or not) with the necessary software to copy and use the media asset. ZapMedia, in response to a rejection, noted that claim 1 "recites that a user can enable a plurality of media player devices, on a user account basis, to access assets licensed to the user" and that "Milsted does not disclose this element" because Milsted functions "without regard to the device being

associated with the user account." J.A. 708–09. ZapMedia concluded that Milsted's media assets "can be copied and used by ANY player device, not a subset of player devices that are associated with a user account." J.A. 710. These statements stand for the proposition in the '414 patent that only the "subset of player devices associated with the user account" can copy and use media assets. In other words, if an unauthorized media player (one not associated with the user account) can access a media asset that system cannot infringe.

Consistent with this understanding, ZapMedia also made similar statements in the prosecution and reexamination of the parent '704 patent. *See TIP Sys., LLC v. Phillips & Brooks/Gladwin, Inc.*, 529 F.3d 1364, 1371 (Fed. Cir. 2008) ("[P]rosecution history of a related patent application may inform construction of a claim term, when the two applications are directed to the same subject matter and a clear disavowal or disclaimer is made during prosecution of the related application."). In response to a rejection over Milsted, ZapMedia stated that the "user account" "manage[s] media assets across a plurality of media player devices" by specifying "the plurality of media player devices that may access the media assets." J.A. 808. ZapMedia also stated that that is a requirement for both the '414 and '704 patents. J.A. 765–66.

In response, ZapMedia relies on its own statement in the prosecution history that the '414 patent does not preclude using the technology of Milsted. J.A. 711 ("[T]he embodiments that are covered by claim 84 do not preclude technology such as described in Milsted . . . ."). In support of this position, ZapMedia cites the written description's discussion that watermarking and encryption techniques can be used with the '414 patent. '414 patent col.11 ll.12–56. However, the use of watermarking, encryption, and

other DRM technology as additional safeguards do not preclude practicing the '414 patent's limited access by only authorized devices. In other words, the fact that the '414 patent discloses using watermarking and DRM technologies does not mean that the claim term "access" covers that technology for unauthorized devices. In fact, ZapMedia during reexamination stated that such technologies were irrelevant to the authorization and access claim language:

> [R]egardless whether that particular media asset is or is not protected by some kind of encryption, the claims of the '414 patent are directed to methods and systems that can further manage access to media assets by requiring there to be a user account under which a plurality of media player devices are *authorized*.

J.A. 752–53 (emphases in original). In other words, the authorization and access claim language in the '414 patent has nothing to do with watermarking or DRM technology.

Neither party disputes that iTunes is capable of accessing a licensed media asset using an unauthorized device, as shown in the downloading experiments conducted by Apple. Instead, ZapMedia argues that because the actual file is downloaded from a third party server, the media asset is not copied "through the user account." Alternatively, ZapMedia argues that claimed "user account" is not coextensive with the iTunes store account, and is more narrowly limited only to the list of licensed media assets and authorized devices. The parties' dispute in this case thus comes down to the proper scope of the disputed claims.

The asserted claims each require access to the "media assets." The written description states that the user

account, which contains a list of these media assets, does not have to actually store the media assets:

> The master media library database 330 need not locally store all of the media assets; in some cases the master media library database 330 will maintain a *reference to the media asset* that is stored by a media source 100 and accessed by the portal 300 as needed to satisfy the needs of users.

'414 patent col.10 ll.35–40; *see also* col.5 ll.23–24 ("The portal may interface to third party databases for access to media assets."). Thus, because the "references to the media asset" are stored in the user account's media library, access must be through the user account to retrieve either the "media asset" itself or a "reference" to that media asset, which may or may not be stored elsewhere. The fact that iTunes provides a URL (a reference to the media asset), and the file is ultimately downloaded from a third party (a media source), meets this limitation.

But that is a distinction without a difference. Under the district court's construction, iTunes allows unauthorized devices to access the media assets through the user account and cannot infringe. Under ZapMedia's alternative proposal of a more narrow "user account," iTunes does not download through the user account at all, and thus cannot infringe. Either way, iTunes does not infringe.

ZapMedia's remaining arguments are not persuasive. The construction of "user account" to require a login/password is not necessary to decide on appeal because the failure to meet the authorizing limitations does not turn on the use of a login/password, but on the access of an unauthorized device. Even so, ZapMedia admitted that the iTunes store account is a "user account" and includes a username and password. J.A. 1776 (stating in

ZapMedia's claim chart the "[t]he iTunes store account is a user account."); J.A. 1545 ("The user account is, therefore, a 'record,' meaning a collection of user-related data, including user credit card information, address information, username and password."). In addition, there is ample support in the specification to require a user account to have such a password. *E.g.*, '414 patent col.10 ll.26–31("[A] user . . . is issued a user-specific password," and "a virtual private media asset database is created and associated with the user's login account and password."), col.3, ll.15–17 ("Each user within the user family would have his/her own identifier and password.").

Taken together, the court correctly construed "authorizing . . . a plurality of media player devices with the user account" to mean "specifying two or more media players in the user account, whereby referenced media assets can be copied (and/or used) through the user account only by those media players" and "a plurality of media player devices as being authorized with the user account" to mean "two or more media players specified in the user account, whereby referenced media assets can be copied (and/or used) through the user account only by those media players." While iTunes accesses media assets "through the user account," iTunes, by allowing unauthorized devices to do so cannot meet the exclusive authorizing limitations and thus does not infringe.

CONCLUSION

We have considered ZapMedia's remaining arguments and conclude that they are without merit. For the foregoing reasons, the judgment of the district court is

AFFIRMED