

NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

GOOGLE LLC,
Plaintiff-Appellant

v.

SONOS, INC.,
Defendant-Appellee

2025-1346

Appeal from the United States District Court for the
Northern District of California in No. 3:20-cv-03845-EMC,
Judge Edward M. Chen.

Decided: October 30, 2026

NATHAN KELLEY, Ashurst Perkins Coie US LLP, Wash-
ington, DC, argued for plaintiff-appellant. Also repre-
sented by JONATHAN IRVIN TIETZ; DAN L. BAGATELL,
Hanover, NH; PATRICK DANIEL CURRAN, Quinn Emanuel
Urquhart & Sullivan, LLP, Boston, MA; JEFFREY S.
GERCHICK, PATRICK STAFFORD, Washington, DC; DAVID A.
NELSON, Chicago, IL

ELIZABETH MOULTON, Orrick, Herrington & Sutcliffe
LLP, San Francisco, CA, argued for defendant-appellee.

Also represented by WILL MELEHANI; ALYSSA MARGARET CARIDIS, Los Angeles, CA; HARMANN SINGH, New York, NY; LAUREN WEBER, Seattle, WA.

Before STOLL and STARK, *Circuit Judges*, and BARKER,
District Judge.¹

BARKER, *District Judge*.

Google sued Sonos for patent infringement in the Northern District of California. Google had two theories of infringement for trial: (1) the Strong-Encryption Theory and (2) the Authentication Theory. At summary judgment, the district court construed two terms that, respectively, disposed of each of Google's theories of infringement: (1) "utilized" and (2) "private key." Having found no remaining genuine issue of material fact, the district court granted to Sonos summary judgment of non-infringement. Google now appeals. We have jurisdiction under 28 U.S.C. § 1295(a)(1) and affirm.

BACKGROUND

U.S. Patent No. 7,899,187, titled "Domain-Based Digital-Rights Management System with Easy and Secure Device Enrollment," discloses a system and method for preventing unlicensed parties from accessing proprietary digital content, such as music streamed over the internet from a licensed distributor to a licensed consumer. '187 Patent Title, 1:13–24. The invention does this by managing a domain of devices, associated with a particular account, which may share the protected content within the domain. *Id.* at 1:25–47. Devices outside the domain are unable to access an unencrypted version of the proprietary content.

¹ Honorable J. Campbell Barker, District Judge, United States District Court for the Eastern District of Texas, sitting by designation.

Id. at 2:45–49, 4:42–56. Devices within the domain use a private cryptographic key to decrypt the proprietary content. *Id.*

Google asserted independent claims 1 and 10 under its two infringement theories and raised no infringement issues unique to any dependent claims. Those two independent claims read as follows:

1. A method for registering a new device as part of a domain of devices, which share rights associated with a common account, for use in accessing protected digital content within a digital-rights management system, the method comprising the steps of:

receiving domain information corresponding to the domain of devices from a device existing within the domain of devices;

providing the domain information to a key issuer, which is separate from the domain of devices, causing the key issuer to issue a *private key* to the new device, wherein the *private key* is based on the domain information and is *utilized* by all devices within the domain of devices; and

receiving the *private key* from the key issuer for use in accessing the protected digital content within the digital-rights management system.

'187 Patent at 7:60–8:8 (emphasis added to terms at issue on appeal).

10. An apparatus comprising:

communication circuitry receiving domain information from a device existing within a domain of devices, which share rights associated with a common account, for use in accessing

protected digital content within a digital-rights management system;

storage for storing the domain information; and

logic circuitry for providing the domain information to a key issuer, which is separate from the domain of devices, causing the key issuer to issue a *private key* for use in accessing protected digital content to the apparatus, wherein the *private key* is based on the domain information and is *utilized* by all devices within the domain of devices.

Id. at 8:64–9:10 (emphasis added to terms at issue on appeal).

Sonos manufactures smart speakers that allow customers to play music. The speakers stream music from Sonos’s music service or from third-party services like Pandora or Spotify. Sonos’s products allow customers, via the Sonos application (“Controller”) installed on a user’s mobile device, to group multiple Sonos speakers into a “household” to play music in sync throughout their homes.

Once Sonos players are grouped into a set to play music throughout a user’s home, only one of the players receives an encrypted music stream. That one player uses a unique private key to decrypt digital content before sending the decrypted content to all group members for playback.

Additionally, to connect a household to a streaming service, the Controller sends a request for an authorization token to the streaming service. The streaming service returns an authorization token to the Controller, which shares the authorization token with all existing players in the household. When a new player joins the household later, it obtains the authorization token from one of the existing players and authenticates itself by presenting the token to the streaming service. It is undisputed that no Sonos

player ever uses the authorization token as a cryptographic key input to a cryptographic algorithm.

Google identified two theories of infringement for trial: the Strong-Encryption Theory and the Authentication Theory. Under the Strong-Encryption Theory, Google asserted that when *a single device* in the Sonos household uses a private key to decrypt encrypted content before distributing the content to the other devices, *all* the devices in the household have “utilized” the private key to access the content. See ’187 Patent at cl. 1 & cl. 10 (“wherein the private key is . . . *utilized* by *all* devices within the domain of devices” (emphasis added)). Under the Authentication Theory, Google contended that the authorization token satisfied the “private key” limitation because the token is an input to a cryptographic algorithm.

The district court granted to Sonos summary judgment of non-infringement on both of Google’s theories. On the Strong-Encryption Theory, the district court determined that a device does not “utilize” a private key merely by obtaining decrypted content from another device that ran a cryptographic algorithm with the private key as an input to decrypt the encrypted content. It held that because only one device in the household runs the cryptographic algorithm with the private key as an input, the private key is not “utilized by *all* devices within the domain of devices.” ’187 Patent at cl. 1 & cl. 10 (emphasis added). On the Authentication Theory, the district court construed “private key” as a “non-public cryptographic key that is used as the key input (rather than solely as the data input) to a cryptographic algorithm.” J.A. 56. The court held that, because the Sonos devices never use the authorization token as a key input to a cryptographic algorithm, the token cannot satisfy the “private key” limitation.

At summary judgment, the district court considered two other issues. First, under the Strong-Encryption Theory, the district court considered whether Google’s expert

conceded that the Controller app is a device within the domain of devices that does not “utilize” the private key, as required by both independent claims. Second, under the Authentication Theory, the district court considered but declined to address whether the authorization token constituted a private key that is “based on” the domain information, as required by both independent claims. Google raises these arguments as issues in this appeal, in addition to arguing that its expert’s concession, if any, only partially defeated the Strong-Encryption Theory. But because we agree with the district court’s constructions of “utilize” and “private key” and find them to be dispositive, we do not address the issues related to the expert’s concession or the term “based on.”

DISCUSSION

Our standard of review for a grant or denial of summary judgment is provided by the law of the applicable regional circuit. *Lexion Med., LLC v. Northgate Techs., Inc.*, 641 F.3d 1352, 1358 (Fed. Cir. 2011). So the grant of summary judgment here is reviewed de novo. *See Humane Soc’y of the U.S. v. Locke*, 626 F.3d 1040, 1047 (9th Cir. 2010). Substantively, 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” after drawing all justifiable inferences in the nonmovant’s favor. Fed. R. Civ. P. 56(a); *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 255 (1986).

An infringement analysis has two steps: first, the claim is construed to “determine its scope and meaning”; second, the properly construed claim “must be compared to the accused device or process.” *Carroll Touch, Inc. v. Electro Mech. Sys., Inc.*, 15 F.3d 1573, 1576 (Fed. Cir. 1993). The absence of a single claim element precludes a finding of infringement, and we may affirm a grant of summary judgment of non-infringement on that basis alone. *Bayer AG v. Elan Pharm. Rsch. Corp.*, 212 F.3d 1241, 1247 (Fed. Cir.

2000) (“If any claim limitation is absent from the accused device, there is no literal infringement as a matter of law.”).

Claim construction is an issue of law that we review de novo. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc), *aff’d*, 517 U.S. 370 (1996). The words of a claim “are generally given their ordinary and customary meaning,” which is “the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (citations omitted). A person of ordinary skill reads the claim term “not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification.” *Id.* at 1313. Courts first look to intrinsic evidence because “the claims themselves provide substantial guidance as to the meaning of particular claim terms.” *Id.* at 1314 (citations omitted). “[T]he context in which a term is used in the asserted claim can be highly instructive,” as can “[o]ther claims of the patent in question, both asserted and unasserted.” *Id.* (citation omitted). “Differences among claims can also be a useful guide in understanding the meaning of particular claim terms.” *Id.* (citation omitted). But claims must also “be read in view of the specification,” which “is always highly relevant to the claim construction analysis” and is often “dispositive.” *Id.* at 1315 (citations omitted). Finally, courts may consider extrinsic evidence, which “consists of all evidence external to the patent and prosecution history, including expert and inventor testimony, dictionaries, and learned treatises.” *Id.* at 1317 (citation omitted). However, extrinsic evidence is “less significant than the intrinsic record in determining the legally operative meaning of [the] claim language.” *Id.* (citation modified).

A. Strong-Encryption Theory and the term “utilized”

The parties agree on how Sonos players operate. A single player decrypts protected content by running a cryptographic algorithm. It then forwards the protected content to the rest of the players. All of the grouped players can then play the protected content. Google’s Strong-Encryption Theory thus turns on construction of the term “utilized.” As Google correctly puts it, “[t]he issue is whether the . . . players must *directly* use the private key for local encryption or whether they may *indirectly* use the private key by having [one] player perform the decryption for them and forward the resulting unencrypted data.” Reply Br. 13–14. Google contends that “[i]nfringement requires nothing more” than the latter. Opening Br. 32. Sonos argues for the former construction. We agree with Sonos.

Looking first at the claim language itself, Google relies heavily on the language requiring that the private key be “for use in accessing the protected digital content.” Opening Br. 32–33 (citing ’187 Patent at 8:3–8). That limitation speaks to the purpose of the private key generally but we cannot stop there as the claim contains additional relevant limitations. The context of the claim is “[a] method for registering a new device as part of a domain of devices,” and the method includes steps taken to register that new device, including that the “key issuer . . . issue a private key to the new device.” See ’187 Patent at 7:60–8:8. Moreover, the claim expressly requires that the private key be “*utilized* by *all* devices within the domain of devices.” *Id.* at 8:5 (emphasis added). Thus, the plain claim language requires that the new device receive a private key and that all devices utilize the private key.

We turn next to evidence from the specification to determine what it suggests it means for the private key to be “utilized” by a device. According to the specification, to “utilize” a private key is to input the private key into a cryptographic algorithm to decrypt data. The specification states

that when a new device receives the private key, it utilizes the key “to obtain *and render* digital content.” ’187 Patent Abstract (emphasis added); *id.* at 2:10–13. The specification also discloses that a device “must access DRM private key . . . and uses [sic] it *to decrypt* the content encryption key.” *Id.* at 6:57–60 (emphasis added). A “content encryption key is encrypted with the DRM public key so it can be decrypted only *using* the DRM private key.” *Id.* at 4:54–56 (emphasis added).

We find no persuasive argument arising from the intrinsic evidence that supports Google’s broader construction. Instead, we find only evidence that supports the idea that a person of ordinary skill in the art would understand that to “utilize” a private key is to decrypt with it. Google raises an argument based on claim differentiation that “claim 6 adds to claim 1 the step of ‘utilizing the private key to decrypt a second encryption key, the second encryption key utilized to decrypt digital content’” and that, therefore, claim 1 “necessarily covers other manners of utilization.” Opening Br. 36 (citing ’187 Patent at 8:31–32). But both claims still require the private key to be “*utilized* by *all* devices within the domain of devices.” ’187 Patent at 8:5 (emphasis added). The only potentially relevant difference in scope under Sonos’s construction is that if all devices use a private key to decrypt something other than a second encryption key, then the accused product may infringe claim 1 but not claim 6. That is consistent with the principle of claim differentiation.

Google contends that indirect use of the private key suffices for infringement. Sonos raises several analogies to challenge Google’s construction, asking whether the passengers on a bus are “utilizing” the bus driver’s key or whether a homeowner “utilizes” the turbines at a hydroelectric plant by turning on the lights at home. Google argues that the power-plant analogy is even more “far-fetched” than the bus analogy and that without Sonos’s analogies identifying a particular use, “that ambiguity lets

Sonos make its point without confronting Google's." Reply Br. 14–15.

We do not address whether Sonos's hypotheticals are based on a completely accurate abstraction of Google's proposed construction. But, to the extent that Sonos's argument is against ambiguity itself, we find the argument persuasive. Google argues that indirect use is sufficient for infringement, but Google offers no persuasive limiting principle on when indirect use of a private key would be so "attenuated" as to be too "far-fetched" for infringement. *See* Oral Arg. at 8:55–9:18, https://www.cafc.uscourts.gov/oral-arguments/25-1346_09112026.mp3; *see also* Reply Br. 14. We adhere to the rule that constructions that are more likely to result in an indefinite claim should be avoided. *See Geneva Pharms., Inc. v. GlaxoSmithKline PLC*, 349 F.3d 1373, 1384 (Fed. Cir. 2003).

We therefore adopt Sonos's construction of "utilized." Because the parties agree that all but one player per household only "indirectly 'utilizes' [one] player's private key," Reply Br. 13, there is no genuine issue of material fact that precludes summary judgment against Google's Strong-Encryption Theory.

B. Authentication Theory and the term "private key"

Similarly, it is undisputed that no Sonos product uses the authorization token as a key input to a cryptographic algorithm. Google argues that the district court's original construction of the term was "both correct and sufficient." Opening Br. 38. The district court's original construction of the term was "[a] non-public key that is used as an input to a cryptographic algorithm designed such that, without the key, the output of the algorithm cannot be computed." J.A. 2216. Sonos points out that cryptographic algorithms generally require at least two inputs: a key input and a data input. A simple encryption algorithm, for example, renders ciphertext as a function of a key input and plaintext input.

Google’s proposed construction could create a fact issue because it would allow for the possibility of infringement so long as the “private key” is used as *any* input to a cryptographic algorithm. Sonos supports the construction of the term that the district court made at summary judgment: the “private key” must be used strictly as a *key* input to a cryptographic algorithm. Thus, the issue is whether a person of ordinary skill in the art would understand, within the context of the claim language and the specification, that (1) the claimed “private key” is *any* input to a cryptographic algorithm, or (2) the claimed “private key” is a *key* input to a cryptographic algorithm. We again agree with Sonos.

As is often the case, we are persuaded by the intrinsic record, which shows the “private key” is used only in accordance with its *telos*—its identity *as* a cryptographic key. The claim language requires the private key to be “utilized by all devices within the domain of devices.” ’187 Patent at 8:5, 9:9–10. And the court has already construed “utilized,” based on intrinsic evidence, to require actual decryption with the key. That carries with it a distinction between the private key and the data on which it acts. And the distinction is substantiated throughout the intrinsic record. The specification provides, in its explanation of public-key cryptography, that “[t]he private key is used for either decrypting data or generating digital signatures.” *Id.* at 2:45–49. The specification also teaches that the private key may be used to “[d]ecrypt the content encryption key.” *Id.* at 6:57–60. Accordingly, the specification treats the private key as the required key input to control the cryptographic algorithm rather than the data input that is the object of the algorithm.

Even where the specification describes a “content encryption key . . . encrypted with the DRM public key so it can be decrypted only using the DRM private key,” *id.* at 4:54–56, the “content encryption key” is the data input of the DRM algorithm but still functions as the key input

that controls decryption of other data in the context of the content encryption algorithm. Indeed, the specification explains that the “content encryption key” is “an encrypted encryption key . . . needed to render (execute) the digital content.” *Id.* at 4:52–56. Although this example shows that a key can take the form of data input in an algorithm, it also shows that in all three examples describing a “key,” the specification described the key as controlling an algorithmic function. This is also supported by claim 6, where the data input is an encrypted “second encryption key” and the “private key” of the claims is used as the key input that decrypts the second encryption key. *See id.* at 8:29–32.

Moreover, Sonos’s extrinsic evidence bears out the idea that, in the field of cryptography around the time of the invention, even where a cryptographic algorithm may act on virtually any type of data, a “key” is distinguished over all other types of data by its inherent nature as “the thing that acts upon data, information, or a message” to generate an encrypted output. Resp. Br. 53–57. Thus, when “private key” is grounded in the context of the claim language and the specification, we find that a person of ordinary skill would understand the “private key” to necessarily be a key input to a cryptographic algorithm.

CONCLUSION

We have considered Google’s remaining arguments, and we find them unpersuasive. For the foregoing reasons, we affirm.

AFFIRMED