United States Court of Appeals for the Federal Circuit

FINJAN, INC.,
Plaintiff-Appellee

v.

BLUE COAT SYSTEMS, INC.,
Defendant-Appellant

2016-2520

Appeal from the United States District Court for the Northern District of California in No. 5:13-cv-03999-BLF, Judge Beth Labson Freeman.

Decided: January 10, 2018

PAUL J. ANDRE, Kramer Levin Naftalis & Frankel LLP, Menlo Park, CA, argued for plaintiff-appellee. Also represented by JAMES R. HANNAH, LISA KOBIALKA.

MARK A. LEMLEY, Durie Tangri LLP, San Francisco, CA, argued for defendant-appellant. Also represented by SONALI DEEKSHA MAITRA, SONAL NARESH MEHTA, CLEMENT ROBERTS; OLIVIA M. KIM, EDWARD POPLAWSKI, Wilson, Sonsini, Goodrich & Rosati, P.C., Los Angeles, CA.

Before DYK, LINN, and HUGHES, *Circuit Judges.*

DYK, *Circuit Judge.*

A jury found Blue Coat Systems, Inc. ("Blue Coat") liable for infringement of four patents owned by Finjan, Inc. ("Finjan") and awarded approximately $39.5 million in reasonable royalty damages. After trial, the district court concluded that the '844 patent was patent-eligible under 35 U.S.C. § 101 and denied Blue Coat's post-trial motions for judgment as a matter of law ("JMOL") and a new trial. Blue Coat appeals.

We find no error in the district court's subject matter eligibility determination as to the '844 patent and agree that substantial evidence supports the jury's finding of infringement of the '844 and '731 patents. However, we conclude that Blue Coat was entitled to JMOL of non-infringement for the '968 patent because the accused products do not perform the claimed "policy index" limitation. On appeal, Blue Coat does not challenge the verdict of infringement for the '633 patent.

With respect to damages, we affirm the award with respect to the '731 and '633 patents. We vacate the damages award for the '968 patent, as there was no infringement. With respect to the '844 patent, we agree with Blue Coat that Finjan failed to apportion damages to the infringing functionality and that the $8-per-user royalty rate was unsupported by substantial evidence.

We therefore affirm-in-part, reverse-in-part, and remand to the district court for further consideration of the damages issue as to the '844 patent.

BACKGROUND

On August 28, 2013, Finjan brought suit against Blue Coat in the Northern District of California for infringement of patents owned by Finjan and directed to identifying and protecting against malware. Four of those patents

are at issue on appeal. Claims 1, 7, 11, 14, and 41 of U.S. Patent No. 6,154,844 ("the '844 patent") recite a system and method for providing computer security by attaching a security profile to a downloadable. Claims 1 and 17 of U.S. Patent No. 7,418,731 ("the '731 patent") recite a system and method for providing computer security at a network gateway by comparing security profiles associated with requested files to the security policies of requesting users. Claim 1 of U.S. Patent No. 6,965,968 ("the '968 patent") recites a "policy-based cache manager" that indicates the allowability of cached files under a plurality of user security policies. Claim 14 of U.S Patent No. 7,647,633 ("the '633 patent") relates to a system and method for using "mobile code runtime monitoring" to protect against malicious downloadables.

After a trial, the jury found that Blue Coat infringed these four patents and awarded Finjan approximately $39.5 million for Blue Coat's infringement: $24 million for the '844 patent, $6 million for the '731 patent, $7.75 million for the '968 patent, and $1,666,700 for the '633 patent. After a bench trial, the district court concluded that the '844 patent is directed to patent-eligible subject matter under 35 U.S.C. § 101.

Thereafter, the district court denied Blue Coat's motions for judgment as a matter of law and a new trial, concluding that Finjan had provided substantial evidence to support each finding of infringement and the damages award. Blue Coat appeals the district court's rulings on subject matter eligibility of the '844 patent; infringement of the '844, '731, and '968 patents; and damages for the '844, '731, '968, and '633 patents. We have jurisdiction pursuant to 28 U.S.C. § 1295(a)(1).

DISCUSSION

I. Subject Matter Eligibility of the '844 Patent

We first address subject matter eligibility with respect to the '844 patent. We review the district court's decision de novo. *McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1311 (Fed. Cir. 2016).

Section 101 provides that a patent may be obtained for "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." 35 U.S.C. § 101. The Supreme Court has long recognized, however, that § 101 implicitly excludes "laws of nature, natural phenomena, and abstract ideas" from the realm of patent-eligible subject matter, as monopolization of these "basic tools of scientific and technological work" would stifle the very innovation that the patent system aims to promote. *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2354 (2014) (quoting *Ass'n for Molecular Pathology v. Myriad Genetics, Inc.*, 133 S. Ct. 2107, 2116 (2013)); *see also Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 132 S. Ct. 1289, 1294-97 (2012); *Diamond v. Diehr*, 450 U.S. 175, 185 (1981).

The Supreme Court has instructed us to use a two-step framework to "distinguish[] patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts." *Alice*, 134 S. Ct. at 2355. At the first step, we determine whether the claims at issue are "directed to" a patent-ineligible concept. *Id.* If they are, we then "consider the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." *Id.* (quoting *Mayo*, 132 S. Ct. at 1298). This is the search for an "inventive concept"—something sufficient to ensure that the claim amounts to "significantly more" than the abstract idea itself. *Id.* (quoting *Mayo*, 132 S.Ct. at 1294).

Starting at step one, we must first examine the '844 patent's "claimed advance" to determine whether the claims are directed to an abstract idea. *Affinity Labs of Tex., LLC v. DIRECTV, LLC*, 838 F.3d 1253, 1257 (Fed. Cir. 2016). In cases involving software innovations, this inquiry often turns on whether the claims focus on "the specific asserted improvement in computer capabilities . . . or, instead, on a process that qualifies as an 'abstract idea' for which computers are invoked merely as a tool." *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335–36 (Fed. Cir. 2016).

The '844 patent is directed to a method of providing computer security by scanning a downloadable and attaching the results of that scan to the downloadable itself in the form of a "security profile." Claim 1 of the '844 patent, which the district court found representative for § 101 purposes, reads:

> 1. A method comprising:
>
> receiving by an inspector a Downloadable;
>
> generating by the inspector a first Downloadable security profile that identifies suspicious code in the received Downloadable; and
>
> linking by the inspector the first Downloadable security profile to the Downloadable before a web server makes the Downloadable available to web clients.

'844 patent, col. 11 ll. 11–21. At claim construction, the parties agreed that "Downloadable" should be construed to mean "an executable application program, which is downloaded from a source computer and run on the destination computer." Additionally, the district court construed "Downloadable security profile that identifies suspicious code in the received Downloadable" to mean "a profile that identifies code in the received Downloadable that performs hostile or potentially hostile operations."

We determined in *Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1319 (Fed. Cir. 2016), that "[b]y itself, virus screening is well-known and constitutes an abstract idea." We also found that performing the virus scan on an intermediary computer—so as to ensure that files are scanned before they can reach a user's computer—is a "perfectly conventional" approach and is also abstract. *Id.* at 1321. Here the claimed method does a good deal more.

Claim 1 of the '844 patent scans a downloadable and attaches the virus scan results to the downloadable in the form of a newly generated file: a "security profile that identifies suspicious code in the received Downloadable." The district court's claim construction decision emphasizes that this "identif[y] suspicious code" limitation can only be satisfied if the security profile includes "details about the suspicious code in the received downloadable, such as . . . 'all potentially hostile or suspicious code operations that may be attempted by the Downloadable.'" *Finjan, Inc. v. Blue Coat Sys., Inc.*, No. 13-CV-03999-BLF, 2014 WL 5361976, at *9 (N.D. Cal. Oct. 20, 2014). The security profile must include the information about *potentially* hostile operations produced by a "behavior-based" virus scan. This operation is distinguished from traditional, "code-matching" virus scans that are limited to recognizing the presence of previously-identified viruses, typically by comparing the code in a downloadable to a database of known suspicious code. The question, then, is whether this behavior-based virus scan in the '844 patent constitutes an improvement in computer functionality. We think it does.

The "behavior-based" approach to virus scanning was pioneered by Finjan and is disclosed in the '844 patent's specification. In contrast to traditional "code-matching" systems, which simply look for the presence of known viruses, "behavior-based" scans can analyze a downloadable's code and determine whether it performs poten-

tially dangerous or unwanted operations—such as renaming or deleting files. Because security profiles communicate the granular information about potentially suspicious code made available by behavior-based scans, they can be used to protect against previously unknown viruses as well as "obfuscated code"—known viruses that have been cosmetically modified to avoid detection by code-matching virus scans.

The security profile approach also enables more flexible and nuanced virus filtering. After an inspector generates a security profile for a downloadable, a user's computer can determine whether to access that downloadable by reviewing its security profile according to the rules in whatever "security *policy*" is associated with the user. Administrators can easily tailor access by applying different security policies to different users or types of users. And having the security profile include information about particular potential threats enables administrators to craft security policies with highly granular rules and to alter those security policies in response to evolving threats.

Our cases confirm that software-based innovations can make "non-abstract improvements to computer technology" and be deemed patent-eligible subject matter at step 1. *Enfish*, 822 F.3d at 1335–36. In *Enfish*, for instance, the court determined that claims related to a database architecture that used a new, self-referential logical table were non-abstract because they focused on "an improvement to computer functionality itself, not on economic or other tasks for which a computer is used in its ordinary capacity." *Id.* at 1336. Indeed, the self-referential database found patent eligible in *Enfish* did more than allow computers to perform familiar tasks with greater speed and efficiency; it actually permitted users to launch and construct databases in a new way. While deployment of a traditional relational database involved "extensive modeling and configuration of the various

tables and relationships in advance of launching the database," *Enfish*'s self-referential database could be launched "with no or only minimal column definitions" and configured and adapted "on-the-fly." *Id.* at 1333.

Similarly, the method of claim 1 employs a new kind of file that enables a computer security system to do things it could not do before. The security profile approach allows access to be tailored for different users and ensures that threats are identified before a file reaches a user's computer. The fact that the security profile "identifies suspicious code" allows the system to accumulate and utilize newly available, behavior-based information about potential threats. The asserted claims are therefore directed to a non-abstract improvement in computer functionality, rather than the abstract idea of computer security writ large.

Even accepting that the claims are directed to a new idea, Blue Coat argues that they remain abstract because they do not sufficiently describe how to implement that idea. To support this argument, Blue Coat points to *Apple, Inc. v. Ameranth, Inc.*, where we invalidated claims related to a computer system that can generate a second menu from a first menu based on a selection of items on the first menu. 842 F.3d 1229, 1240–41 (Fed. Cir. 2016). In that case, we held that the patents were directed to an abstract idea because they "d[id] not claim a particular way of programming or designing the software . . . but instead merely claim the resulting systems." *Id.* at 1241. Blue Coat also relies on *Affinity Labs*, where we held that a claim related to wirelessly communicating regional broadcast content to an out-of-region recipient was abstract and patent ineligible because there was nothing in the claim "directed to *how* to implement [the idea]. Rather, the claim is drawn to the idea itself." 838 F.3d at 1258. And Blue Coat also notes that, in *Intellectual Ventures*, we found claims directed to email filtering to be abstract and patent ineligible when there is "no re-

striction on how the result is accomplished . . . [and] [t]he mechanism . . . is not described." 838 F.3d 1307, 1316 (Fed. Cir. 2016) (quoting *Internet Patents Corp. v. Active Network, Inc.*, 790 F.3d 1343, 1348 (Fed. Cir. 2015)).

Apple, *Affinity Labs*, and other similar cases hearken back to a foundational patent law principle: that a result, even an innovative result, is not itself patentable. *See Corning v. Burden*, 56 U.S. 252, 268 (1853) (explaining that patents are granted "for the discovery or invention of some practicable method or means of producing a beneficial result or effect . . . and not for the result or effect itself"); *O'Reilly v. Morse*, 56 U.S. 62, 112–113 (1853) (invalidating a claim that purported to cover all uses of electromagnetism for which "the result is the making or printing intelligible characters, signs, or letters at a distance" as "too broad, and not warranted by law").

Here, the claims recite more than a mere result. Instead, they recite specific steps—generating a security profile that identifies suspicious code and linking it to a downloadable—that accomplish the desired result. Moreover, there is no contention that the only thing disclosed is the result and not an inventive arrangement for accomplishing the result. There is no need to set forth a further inventive concept for implementing the invention. The idea is non-abstract and there is no need to proceed to step two of *Alice*.

II. Infringement

At trial, the jury found that Blue Coat's products infringed the '844, '731, and '968 patents. The district court denied Blue Coat's post-trial motions for judgment as a matter of law and a new trial, finding that Finjan had provided substantial evidence to support each finding of infringement and that the jury verdict was not against the weight of the evidence. We review denials of motions for JMOL de novo and motions for new trial for abuse of

discretion. *Revolution Eyewear, Inc. v. Aspex Eyewear, Inc.*, 563 F.3d 1358, 1370–71 (Fed. Cir. 2009).

A. '844 Patent

Blue Coat first argues that the district court should have granted JMOL of non-infringement as to the asserted claims in the '844 patent because substantial evidence did not support the jury verdict. Specifically, Blue Coat contends that the asserted claims, requiring linking a security profile to a downloadable "before a web server makes the Downloadable available to web clients," can only be infringed by a server-side product that evaluates content before it is published to the Internet in the first place. Blue Coat's product, WebPulse, is a cloud-based service that provides information about downloadables to a customer's network gateway in order to help the network gateway determine whether a particular downloadable can be accessed by a specific end user. Because WebPulse only evaluates downloadables that are already publicly available on the Internet, Blue Coat argues that it does not infringe.

Blue Coat made no request for a claim construction that would require linking the security profile to the downloadable before the downloadable is placed on the Internet. Blue Coat cannot raise the claim construction issue for the first time in post-trial motions: "it is too late at the JMOL stage to argue for or adopt a new and more detailed interpretation of the claim language and test the jury verdict by that new and more detailed interpretation." *Hewlett-Packard Co. v. Mustek Sys., Inc.*, 340 F.3d 1314, 1321 (Fed. Cir. 2003). Under such circumstances, "the question for the trial court is limited to whether substantial evidence supports the jury's verdict under the issued construction." *Wi-Lan, Inc. v. Apple, Inc.*, 811 F.3d 455, 465 (Fed. Cir. 2016). Here, the claim, as construed by the district court, requires "linking by the inspector the first Downloadable security profile to the Downloadable

before [a/the] non-network gateway web server make[s] the Downloadable available to web clients." '844 patent, col. 11 ll. 18-20; J.A. 25. The jury was instructed to apply this construction.

It was reasonable for the jury to interpret "web clients" in this context to refer to the specific web clients protected by the claimed system. Likewise, the limitation requiring that linking occur before a downloadable is "ma[de] . . . available to web clients" could reasonably be understood to require that linking occur at some point before users are *permitted to access* that downloadable—but not necessarily before the downloadable is made available on the Internet. Blue Coat concedes that, at the time a security profile is linked, the "particular web client cannot yet ***receive*** the downloadable—but the ***web server*** has made it available . . . ." Reply Br. 9. Given the undisputed evidence that WebPulse links security profiles to downloadables before downloadables can be received by users of the service, we find that the '844 infringement verdict was supported by substantial evidence.

B. '731 Patent

We next consider Blue Coat's claim that it was entitled to JMOL of non-infringement as to the asserted claims of the '731 patent. The '731 patent is directed to a computer gateway that protects a private intranet from malicious software embedded in webpages on the public Internet.[1] The claimed gateway operates by scanning

---

[1] Claim 1 of the '731 patent reads:

1. A computer gateway for an intranet of computers, comprising:

a scanner for scanning incoming files from the Internet and deriving security profiles for the incoming files, wherein each of the security

potentially malicious files and creating "security profiles" that each comprise "a list of computer commands that the file is programmed to perform." '731 patent, col. 4 ll. 47–48. Claim 17 further specifies that the security profile include "a list of at least one computer command that the retrieved file is programmed to perform." '731 patent, col. 13 ll. 7–8. Once these security profiles have been generated, they can be compared with the security policy associated with a given user in order to decide whether the file should be provided to that user.

Blue Coat argues that the '731 patent was not infringed as a matter of law because the "security profiles" created by the accused product do not contain the requi-

---

> profiles comprises a list of computer commands that a corresponding one of the incoming files is programmed to perform;
>
> a file cache for storing files that have been scanned by the scanner for future access, wherein each of the stored files is indexed by a file identifier; and
>
> a security profile cache for storing the security profiles derived by the scanner, wherein each of the security profiles is indexed in the security profile cache by a file identifier associated with a corresponding file stored in the file cache; and
>
> a security policy cache for storing security policies for intranet computers within the intranet, the security policies each including a list of restrictions for files that are transmitted to a corresponding subset of the intranet computers.

'731 patent, col. 11 ll. 35–55.

site "list of computer commands." Because Blue Coat did not request a construction of the "list of commands" term, we apply the ordinary meaning. We find that substantial evidence supports the jury's finding of infringement.

At trial, Finjan presented evidence demonstrating that the accused product creates a new file called "cookie2" each time it scans an incoming file for potential malware. Cookie2 comprises a set of fields, each field representing various characteristics about the downloadable file. Fields 78–80 of Cookie2 represent certain commands and show whether those commands—such as eval(), unescape(), and document.write()—appear in the incoming file. In fields 78–80, an integer represents the number of times each command appears. Finjan's expert, Dr. Mitzenmacher, testified that the data contained in fields 78–80 "is clearly a list of computer commands." J.A. 40383.

Blue Coat argues that this is not enough and that the "list of commands" limitation cannot be satisfied by "an ***identifier*** of a ***type*** of command the system should watch for." Appellant Br. 34. But the claim language simply requires that the security profile contain "a list of computer commands that a corresponding one of the incoming files is programmed to perform." It does not mandate any particular representation of that information—much less require that the commands be listed in the form of executable code. Dr. Mitzenmacher testified at trial that the integers in fields 78–80 are "clearly a list of computer commands" because "those numbers determine whether or not those commands are in the security profile." J.A. 40383–84. He also notes that "there are many ways of representing a list [of computer commands], including the way it is represented here." J.A. 40384. Substantial evidence supports the jury's implied finding that the "list of commands" limitation is satisfied by the integers in Fields 78–80 of Cookie2, and the patent is infringed.

C. '968 Patent

Blue Coat also argues that it was entitled to JMOL of non-infringement with respect to the '968 patent because Finjan failed to introduce substantial evidence that the accused products implement the claimed "policy index." We agree.

The '968 patent is directed to a "policy-based" cache manager that can efficiently manage cached content according to a plurality of security policies. The patentee agrees that a "policy" is a rule or set of rules that determines whether a piece of content can be accessed by a user. Different policies can apply to different users, and the decision of whether to let a user access content is made by comparing the content's security profile with the policy governing the user's access. Thus, the policy based cache manager in the '968 patent is a data structure that keeps track of whether content is permitted under various policies. Claim 1, the sole asserted claim, is reproduced below, with key language underlined:

1. A policy-based cache manager, comprising:

> a memory storing a cache of digital content, a plurality of policies, and a policy index to the cache contents, the policy index including entries that relate cache content and policies by indicating cache content that is known to be allowable relative to a given policy, for each of a plurality of policies;
>
> a content scanner, communicatively coupled with said memory, for scanning a digital content received, to derive a corresponding content profile; and
>
> a content evaluator, communicatively coupled with said memory, for determining whether a given digital content is allowa-

> ble relative to a given policy, based on the content profile, the results of which are saved as entries in the policy index.

'968 patent col. 9 ll. 47–62. At claim construction, the parties stipulated that "policy index" means "a data structure indicating allowability of cached content relative to a plurality of policies." The jury was instructed to apply this construction. Once again, we test the jury's infringement verdict based on this claim language and claim construction. *Hewlett-Packard Co.*, 340 F.3d at 1320–21.

Trial testimony demonstrated that the accused product, Proxy SG, is a gateway between an intranet of computers and the Internet at large. Every time a user requests a file, Proxy SG will analyze that file and determine whether access is permitted under the user's security policy. As Proxy SG evaluates a file, it can cache the results of individual rules *within* a policy and use that information to speed up the process of making an ultimate policy decision. Early in its analysis, for instance, Proxy SG can check the "category" of the file and then determine whether the user's policy has any rules related to the "category" field. Proxy SG can then store "the evaluations of the parts of the rules that deal with this category field . . . . So you don't have to reevaluate those conditions again." J.A. 40327–28. As Finjan's expert expressly acknowledged, however, Proxy SG does not save final decisions about whether content can be accessed by users subject to a given policy. It simply stores the evaluation of each individual rule that goes into making an ultimate policy decision. This is not what the claim language requires. The policy index claimed in the '968 patent must store the "results" of a content evaluator's determination of "whether a given digital content is allowable relative to a given policy."

At summary judgment, the district court agreed that this claim language requires the policy index to store final allowability determinations and noted that "Defendant's argument would likely prevail if all policies consist of multiple rules or conditions." *Finjan, Inc. v. Blue Coat Sys., Inc.*, No. 13-CV-03999-BLF, 2015 WL 3630000, at *9 (N.D. Cal. June 2, 2015). The court nevertheless declined to grant summary judgement because "the '968 patent specifically provides that a policy can be just one rule." *Id.* If Proxy SG saved the results of applying each rule that makes up a one-rule policy, it would be saving final allowability determinations for a plurality of policies and thus infringing. The district court therefore gave Finjan the opportunity to prove at trial that "the Proxy SG policy cache contains a number of condition evaluations, each of which is determinative of whether a file is allowable relative to one of a plurality of single condition policies." *Id.*

At trial, Finjan made no such showing. There was no evidence indicating that the condition determinations stored by Proxy SG are final allowability decisions for users governed by single-rule policies. Indeed, Finjan's expert acknowledged that Proxy SG never saves final allowability determinations and must instead re-evaluate the allowability of content each time it is requested. It is therefore clear that the jury's infringement verdict was not supported by substantial evidence.

Because Finjan failed to present evidence that the accused product ever stores final allowability determinations, Blue Coat was entitled to JMOL of non-infringement.

III. Damages

We now turn to Blue Coat's damages arguments with respect to the '844, '731, and '633 patents. The starting point is 35 U.S.C. § 284, which limits damages to those "adequate to compensate for the infringement." Two

categories of compensation for infringement are the patentee's lost profits and the "reasonable royalty he would have received through arms-length bargaining." *Lucent Techs., Inc. v. Gateway, Inc.*, 580 F.3d 1301, 1324 (Fed. Cir. 2009).

The only measure of damages at issue in this case is a reasonable royalty, which "seeks to compensate the patentee . . . for its lost opportunity to obtain a reasonable royalty that the infringer would have been willing to pay if it had been barred from infringing." *AstraZeneca AB v. Apotex Corp.*, 782 F.3d 1324, 1334 (Fed. Cir. 2015) (citing *Lucent Techs.*, 580 F.3d at 1325).

A. '844 Patent

Blue Coat first argues that, in calculating a royalty base, Finjan failed to apportion damages to the infringing functionality. We agree.

When the accused technology does not make up the whole of the accused product, apportionment is required. "[T]he ultimate combination of royalty base and royalty rate must reflect the value attributable to the infringing features of the product, and no more." *Ericsson, Inc. v. D–Link Sys., Inc.*, 773 F.3d 1201, 1226 (Fed. Cir. 2014); *see also Mentor Graphics v. EVE-USA*, 870 F.3d 1298, 1299 (Fed. Cir. 2017) (order denying rehearing en banc) ("[W]here an infringing product is a multi-component product with patented and unpatented components, apportionment is required."); *VirnetX, Inc. v. Cisco Sys., Inc.*, 767 F.3d 1308, 1326 (Fed. Cir. 2014) ("No matter what the form of the royalty, a patentee must take care to seek only those damages attributable to the infringing features."). In such cases, the patentee must "give evidence tending to separate or apportion the [infringer]'s profits and the patentee's damages between the patented feature and the unpatented features, and such evidence must be reliable and tangible, and not conjectural or speculative." *Garretson v. Clark*, 111 U.S. 120, 121 (1884).

Finjan, as the present patent holder, had the burden of proving damages by a preponderance of the evidence.

WebPulse, the infringing product, is a cloud-based system that associates URLs with over eighty different categories, including pornography, gambling, shopping, social networking, and "suspicious"—which is a category meant to identify potential malware. WebPulse is not sold by itself. Rather, other Blue Coat products, like Proxy SG, use WebPulse's category information to make allowability determinations about URLs that end users are trying to access.

DRTR, which stands for "dynamic real-time rating engine," is the part of WebPulse responsible for analyzing URLs that have not already been categorized. DRTR performs both infringing and non-infringing functions. When a user requests access to a URL that is not already in the WebPulse database—a brand new website, for instance—DRTR will analyze the content, assign a category or categories, and collect metadata about the site for further use. As part of that analysis, DRTR will examine the URL for malicious or suspicious code, create a kind of "security profile" highlighting that information, and then "attach" the security profile to the given URL. This infringes the '844 patent. But the DRTR analysis also evaluates whether the URL fits into categories ranging from pornography to news. These additional categories are unrelated to DRTR's malware identification function but are still valuable for companies trying to, say, prevent employees from using social media while on the job. DRTR also collects metadata about the URL for Blue Coat's later use. In other words, all of the infringing functionality occurs in DRTR, but some DRTR functions infringe and some do not.

At trial, Finjan attempted to tie the royalty base to the incremental value of the infringement by multiplying WebPulse's total number of users by the percentage of

web traffic that passes through DRTR, the WebPulse component that performs the infringing method. DRTR processes roughly 4% of WebPulse's total web requests, so Finjan established a royalty base by multiplying the 75 million worldwide WebPulse users by 4%. Although DRTR also performs the non-infringing functions described above, Finjan did not perform any further apportionment on the royalty base.

Finjan argues that apportionment to DRTR is adequate because DRTR is the "smallest, identifiable technical component" tied to the footprint of the invention. Appellee Br. 49–50. This argument, which draws from this court's precedent regarding apportionment to the "smallest salable patent-practicing unit" of an infringing product, does not help Finjan. The smallest salable unit principle directs that "in any case involving multi-component products, patentees may not calculate damages based on sales of the entire product, as opposed to the smallest salable patent-practicing unit, without showing that the demand for the entire product is attributable to the patented feature." *LaserDynamics, Inc. v. Quanta Comput., Inc.*, 694 F.3d 51, 67–68 (Fed. Cir. 2012). The entire market value rule is not at issue in this case, however, and the fact that Finjan has established a royalty base based on the "smallest, identifiable technical component" does not insulate them from the "essential requirement" that the "ultimate reasonable royalty award must be based on the incremental value that the patented invention adds to the end product." *Ericsson*, 773 F.3d at 1226. As we noted in *VirnetX*, if the smallest salable unit—or smallest identifiable technical component—contains non-infringing features, additional apportionment is still required. *VirnetX*, 767 F.3d at 1327 (rejecting a jury instruction that "mistakenly suggest[ed] that when the smallest salable unit is used as the royalty base, there is necessarily no further constraint on the selection of the base").

Finjan further defends its apportionment methodology by asserting that it demonstrated that "many of these other categories were unimportant." Appellee Br. 51. But the claimed unimportance of particular categories (e.g. "Macy's and shopping") does not speak to the overall importance of identifying categories unrelated to malware. Malware detection is undoubtedly an important driver of DRTR's (and WebPulse's) value. At trial, for instance, Dr. Layne-Farrar pointed to an internal Blue Coat email stating that "[t]oday the main value of [WebFilter and WebPulse] centers around zero-day malware protection." J.A. 40571. She also referenced a 2012 public-facing document entitled "Five reasons to choose Blue Coat," which gave "negative-day defense: stop malware at the source" as reason number two. J.A. 40572–73. But it is evident that Blue Coat's customers also value WebPulse's ability to identify and filter other categories of content. A Blue Coat whitepaper discussed at trial prominently advertises the fact that WebPulse provides "the granular category control that businesses need to implement acceptable Internet use policies." J.A. 53136. And Finjan's expert used an example about a company that wanted to bar access to certain sites categorized as "gambling." "Whether 'viewed as valuable, important, or even essential,' the patented feature must be separated." *VirnetX,* 767 F.3d at 1329 (quoting *LaserDynamics,* 694 F.3d at 68).

Because DRTR is itself a multi-component software engine that includes non-infringing features, the percentage of web traffic handled by DRTR is not a proxy for the incremental value of the patented technology to WebPulse as a whole. Further apportionment was required to reflect the value of the patented technology compared to the value of the unpatented elements.

Blue Coat also identifies a second error in Finjan's reasonable royalty calculation. To arrive at a lump sum reasonable royalty payment for infringement of the '844

patent, Finjan simply multiplied the royalty base by an $8-per-user royalty rate. Blue Coat contends that there is no basis for the $8-per-user rate.

We agree with Blue Coat that the $8-per-user royalty rate employed in Finjan's analysis was unsupported by substantial evidence. There is no evidence that Finjan ever actually used or proposed an $8-per-user fee in any comparable license or negotiation. Rather, the $8-per-user fee is based on testimony from Finjan's Vice President of IP Licensing, Ivan Chaperot, that the current "starting point" in licensing negotiations is an "8 to 16 percent royalty rate or something that is consistent with that . . . like $8 per user fee." J.A. 40409. Mr. Chaperot further testified that the 8–16% figure was based on a 2008 verdict obtained by Finjan against Secure Computing. On this basis, Finjan's counsel urged the jury to use an $8-per-user royalty rate for the hypothetical negotiation because "that's what Finjan would have asked for at the time." J.A. 41654.

While any reasonable royalty analysis "necessarily involves an element of approximation and uncertainty, a trier of fact must have some factual basis for a determination of a reasonable royalty." *Unisplay, S.A. v. Am. Elec. Sign Co.*, 69 F.3d 512, 517 (Fed. Cir. 1995). Mr. Chaperot's testimony that an $8-per-user fee is "consistent with" the 8–16% royalty rate established in *Secure Computing* is insufficient. There is no evidence to support Mr. Chaperot's conclusory statement that an 8–16% royalty rate would correspond to an $8-per-user fee, and Finjan fails to adequately tie the facts of *Secure Computing* to the facts in this case. *See LaserDynamics*, 694 F.3d at 79 ("[A]lleging a loose or vague comparability between different technologies or licenses does not suffice.").

Secure Computing did not involve the '844 patent, and there is no evidence showing that the patents that were at issue are economically or technologically comparable.

Finjan's evidence on this point is limited to the fact that that the infringing products in *Secure Computing* were also in the computer security field and that Secure Computing was a competitor of Blue Coat in 2008. This surface similarity is far too general to be the basis for a reasonable royalty calculation. In any case, Mr. Chaperot's testimony that an 8–16% royalty rate would be the *current starting point* in licensing negotiations says little about what the parties would have proposed or agreed to in a hypothetical arm's length negotiation in 2008. And Finjan's evidence of a $14–34 *software* user fee is not indicative of how much the parties would have paid to license a patent. *See Uniloc USA, Inc. v. Microsoft Corp.*, 632 F.3d 1292, 1317 (Fed. Cir. 2011) ("[T]here must be a basis in fact to associate the royalty rates used in prior licenses to the particular hypothetical negotiation at issue in the case."). In short, the $8-per-user fee appears to have been plucked from thin air and, as such, cannot be the basis for a reasonable royalty calculation.

While it is clear that Finjan failed to present a damages case that can support the jury's verdict, reversal of JMOL could result in a situation in which Finjan receives no compensation for Blue Coat's infringement of the '844 patent. Ordinarily, "the district court must award damages in an amount no less than a reasonable royalty" when infringement is found, *Dow Chem. Co. v. Mee Indus., Inc.*, 341 F.3d 1370, 1381 (Fed. Cir. 2003); *see Riles v. Shell Expl. & Prod. Co.*, 298 F.3d 1302, 1313 (Fed. Cir. 2002), unless the patent holder has waived the right to damages based on alternate theories, *Promega Corp. v. Life Tech. Corp.*, No. 2013-1011, slip op. at 15 (Fed. Cir. 2017). We therefore remand to the district court to determine whether Finjan has waived the right to establish reasonable royalty damages under a new theory and whether to order a new trial on damages.

B. ’731 and ’633 Patents

For the ’731 and ’633 patents, Finjan’s expert did apportion the revenues comprising the royalty base between infringing and non-infringing functionality of Proxy SG. Blue Coat argues that the apportionment was insufficient. We disagree.

Finjan’s expert, Dr. Layne-Farrar, based her apportionment analysis for the ’731 and ’633 patents on an architectural diagram prepared by Blue Coat. The diagram is entitled “Secure Web Gateway: Functions” and shows twenty-four boxes representing different parts of the Secure Web Gateway system. Dr. Layne-Farrar assumed that each box represented one top level function and that each function was equally valuable. Thus, because one function infringed the ’633 patent, and three infringed the ’731 patent, she used a 1/24th apportionment for the ’633 patent and a 3/24th apportionment for the ’731 patent.

Blue Coat argues that there was no evidence to support Dr. Layne-Farrar’s assumption that each box represents a “function” and that each function should be treated as equally valuable. But at trial, Dr. Layne-Farrar testified that her assumption was based on Blue Coat’s own diagram, which is entitled “Secure Web Gateway: Functions”, as well as her discussions with Mr. Medovic, a Finjan technical expert who explained the use of architectural diagrams and identified certain components within the diagram that did and did not infringe. Dr. Layne-Farrar also testified that she relied on the deposition of a Blue Coat engineer, in which the engineer stated that the diagram in question represents the full scope of Secure Web Gateway functionality. Based on this evidence, Dr. Layne-Farrar based her analysis on the twenty-four “functions” identified in the Blue Coat diagram and considered each function equally valuable.

Blue Coat notes that Dr. Layne-Farrar's conclusions conflict with testimony from Mr. Shoenfeld, Blue Coat's Senior VP of Products, stating that each box in the diagram can "have many, many things behind [it] . . . so there's no equal weighing of these [boxes] . . . ." *See* J.A. 40756. But the existence of conflicting testimony does not mean the damages award is unsupported by substantial evidence. The jury was entitled to believe the patentee's expert. The jury's damages awards for infringement of the '731 and '633 patents were based on substantial evidence.[2]

CONCLUSION

For the foregoing reasons, we reverse the denial of JMOL of non-infringement with respect to the '968 patent and remand to the district court to determine the issue of damages with respect to the '844 patent. We affirm in all other respects.

---

[2] Blue Coat also argues that the damages award was flawed because the jury awarded damages in excess of the estimates offered by Finjan's damages expert. Indeed, Finjan's damages expert gave a range of $2,979,805 to $3,973,073 for infringement of the '731 patent and a range of $833,350 to $1,111,133 for infringement of the '633 patent, JA 40623, but the jury awarded $6,000,000 for the '731 patent and $1,666,700 for the '633 patent, J.A. 125. We agree with Blue Coat that the statute's direction to award damages "in no event less than a reasonable royalty" does not mean that the patentee need not support the award with reliable evidence. 35 U.S.C. § 284. A jury may not award more than is supported by the record, but here the record contains evidence that the expert's estimates were conservative and that the underlying evidence could support a higher award. J.A. 40619–20, 40656.

AFFIRMED-IN-PART, REVERSED-IN-PART, AND REMANDED.

COSTS

Each party shall bear its own costs.