APPENDICES

APPENDIX A

NOTE: This order is nonprecedential.

UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

2017-2223

SRI INTERNATIONAL, INC.,
Plaintiff-Appellee,

v.

CISCO SYSTEMS, INC.,
Defendant-Appellant.

Appeal from the United States District Court for the District of Delaware in No. 1:13-cv-01534-SLR-SRF, Judge Sue L. Robinson.

ON PETITION FOR PANEL REHEARING

Before LOURIE, O'MALLEY, and STOLL, *Circuit Judges.*

PER CURIAM.

O R D E R

Appellant Cisco Systems, Inc., filed a combined petition for panel rehearing and rehearing en banc on May 10, 2019. A response to the petition was invited by the court and filed by Appellee SRI International, Inc.

Upon consideration thereof,

IT IS ORDERED THAT:

1) The petition for panel rehearing is granted in part and denied in part.

2) The previous precedential opinion in this appeal, issued March 20, 2019, is withdrawn and replaced with the modified precedential opinion accompanying this order. The modifications appear in section V of the opinion, along with corresponding changes to the introduction and conclusion.

FOR THE COURT

July 12, 2019
Date

/s/ Peter R. Marksteiner
Peter R. Marksteiner
Clerk of Court

APPENDIX B

NOTE: This order is nonprecedential.

UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

2017-2223

SRI INTERNATIONAL, INC.,
Plaintiff-Appellee,
v.

CISCO SYSTEMS, INC.,
Defendant-Appellant.

Appeal from the United States District Court for the District of Delaware in No. 1:13-cv-01534-SLR-SRF, Judge Sue L. Robinson.

ON PETITION FOR PANEL REHEARING AND REHEARING EN BANC

Before PROST, *Chief Judge*, NEWMAN, LOURIE, DYK, MOORE, O'MALLEY, REYNA, WALLACH, TARANTO, CHEN, HUGHES, and STOLL, *Circuit Judges.*

PER CURIAM.

O R D E R

Appellant Cisco Systems, Inc., filed a combined petition for panel rehearing and rehearing en banc on May 10, 2019. A response to the petition was invited by the court and filed by Appellee SRI International, Inc. The petition was referred to the panel that heard the appeal

and was thereafter referred to the circuit judges who are in regular active service.

Upon consideration thereof,

IT IS ORDERED THAT:

1) The petition for panel rehearing is granted in part and denied in part. See accompanying order.

2) The petition for rehearing en banc is denied.

3) The mandate of this court will issue on August 19, 2019.

FOR THE COURT

July 12, 2019
Date

/s/ Peter R. Marksteiner
Peter R. Marksteiner
Clerk of Court

APPENDIX C

UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

2017-2223

SRI INTERNATIONAL, INC.,
Plaintiff-Appellee,
v.

CISCO SYSTEMS, INC.,
Defendant-Appellant.

Appeal from the United States District Court for the District of Delaware in No. 1:13-cv-01534-SLR-SRF, Judge Sue L. Robinson.

OPINION ISSUED: March 20, 2019
OPINION MODIFIED: July 12, 2019*

Before LOURIE, O'MALLEY, and STOLL, *Circuit Judges*.

Opinion for the court filed by *Circuit Judge* STOLL.

Dissenting opinion filed by *Circuit Judge* LOURIE.

STOLL, *Circuit Judge*.

This is an appeal from a final judgment in a patent case. Cisco Systems, Inc. ("Cisco") appeals the district court's (1) denial of Cisco's motion for summary judgment of patent ineligibility under § 101, (2) construction of the claim term "network traffic data," (3) grant of

* This opinion has been modified and reissued following a petition for rehearing filed by Defendant-Appellant.

summary judgment of no anticipation, and (4) denial of judgment as a matter of law of no willful infringement. Cisco also appeals the district court's grant of enhanced damages, attorneys' fees, and ongoing royalties.

We affirm the district court's denial of summary judgment of ineligibility, adopt its construction of "network traffic data," and affirm its summary judgment of no anticipation. We vacate and remand the district court's denial of judgment as a matter of law of no willful infringement, and therefore vacate and remand the district court's enhancement of damages and award of attorneys' fees. Finally, we affirm the district court's award of ongoing royalties on post-verdict sales of products that were actually found to infringe or are not colorably different. Accordingly, we affirm-in-part, vacate-in-part, and remand for further proceedings consistent with this opinion.

BACKGROUND

I.

While the interconnectivity of computer networks facilitates access for authorized users, it also increases a network's susceptibility to attacks from hackers, malware, and other security threats. Some of these security threats can only be detected with information from multiple sources. For instance, a hacker may try logging in to several computers or monitors in a network. The number of login attempts for each computer may be below the threshold to trigger an alert, making it difficult to detect such an attack by looking at only a single monitor location in the network. In an attempt to solve this problem, SRI developed the inventions claimed in U.S. Patent Nos. 6,484,203 and 6,711,615. The '615 patent (titled "Network Surveillance") is a

continuation of the '203 patent (titled "Hierarchical Event Monitoring and Analysis").

II.

SRI had performed considerable research and development on network intrusion detection prior to filing the patents-in-suit. In fact, SRI's Event Monitoring Enabling Responses to Anomalous Live Disturbances ("EMERALD") project had attracted considerable attention in this field. The Department of Defense's Defense Advanced Research Projects Agency, which helped fund EMERALD, called it a "gem in the world of cyber defense" and "a quantum leap improvement over" previous technology. J.A. 1272–73 at 272:16–17, 273:7–9. In October 1997, SRI presented a paper entitled "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances" ("EMERALD 1997") at the 20th National Information Systems Security Conference.

EMERALD 1997 is a conceptual overview of the EMERALD system. It describes in detail SRI's early research in intrusion detection technology and outlines the development of next generation technology for detecting network anomalies. *SRI Int'l Inc. v. Internet Sec. Sys., Inc.*, 647 F. Supp. 2d 323, 334 (D. Del. 2009). The parties do not dispute that EMERALD 1997 constitutes prior art under 35 U.S.C. § 102(b). EMERALD 1997 is listed as a reference on the face of the '615 patent.

III.

The patents share a nearly identical specification and a priority date of November 9, 1998. At the summary judgment stage, SRI asserted claims 1–4, 14–16, and 18 of the '615 patent and claims 1–4, 12–15, and 17

of the '203 patent. By the time of trial, SRI had narrowed the asserted claims to claims 1, 2, 12, and 13 of the '203 patent and claims 1, 2, 13, and 14 of the '615 patent. The jury considered only this narrower set of claims.

The parties identify different representative claims. Cisco proposes claim 1 of the '203 patent, while SRI proposes claim 1 of the '615 patent. The claims are substantially similar, as the minor differences between them are not material to any issue on appeal. As such, we adopt SRI's proposal and use '615 patent claim 1 as the representative claim.[1] It reads:

> 1. A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:
>
> > deploying a plurality of network monitors in the enterprise network;
> >
> > detecting, by the network monitors, suspicious network activity based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and

[1] The minor differences between the two claims are in the *detecting* clause—claim 1 of the '615 patent allows for network traffic data selected from "*one or more of*" the enumerated categories, and includes two extra categories in its list: "network connection acknowledgements" and "network packets indicative of well-known network-service protocols." *Compare* '203 patent col. 14 ll. 19–35 (claim 1), *with* '615 patent col. 15 ll. 2–21 (claim 1).

> network packets indicative of well-known network-service protocols};
>
> generating, by the monitors, reports of said suspicious activity; and
>
> automatically receiving and integrating the re-ports of suspicious activity, by one or more hierarchical monitors.

'615 patent col. 15 ll. 2–21.

After SRI sued Cisco for infringement of the '615 patent and the '203 patent, Cisco unsuccessfully moved for summary judgment on several issues, including that the claims are ineligible and that the EMERALD 1997 reference anticipates the claims.[2] *SRI Int'l, Inc. v. Cisco Sys., Inc.*, 179 F. Supp. 3d 339 (D. Del. Apr. 11, 2016) ("*Summary Judgment Op.*"). The district court denied Cisco's motions and instead sua sponte granted summary judgment of no anticipation in SRI's favor.[3] *Id.* at 369.

---

[2] The patents previously survived multiple anticipation challenges based on the EMERALD 1997 reference. The Patent Office considered EMERALD 1997 during the original prosecution and issued the patents over it. J.A. 32734 ¶ 47; J.A. 32814–15 ¶ 207. In addition, during the two reexaminations, the Patent Office again considered the validity of the asserted claims over EMERALD 1997 and again found the claims valid. J.A. 32734 ¶ 47. Additionally, in *SRI International Inc. v. Internet Security Systems, Inc.*, a jury found the patents not anticipated by EMERALD 1997. 647 F. Supp. 2d at 350. The district court denied JMOL, concluding that the verdict was supported by expert testimony that EMERALD 1997 failed to disclose the claim limitation at issue. *Id.* We affirmed without opinion. *SRI Int'l Inc. v. Internet Sec. Sys., Inc.*, 401 F. App'x 530 (Fed. Cir. 2010).

[3] The parties disputed only whether EMERALD 1997 discloses detection of any of the network traffic data categories listed

The court then held a jury trial on infringement, validity, and willful infringement of claims 1, 2, 13, and 14 of the '615 patent and claims 1, 2, 12, and 13 of the '203 patent, as well as damages. The jury found that Cisco intrusion protection system ("IPS") products, Cisco remote management services, Cisco IPS services, Sourcefire[4] IPS products, and Sourcefire professional services directly and indirectly infringed the asserted claims. The jury awarded SRI a 3.5% reasonable royalty for a total of $23,660,000 in compensatory damages. The jury also found by clear and convincing evidence that Cisco's infringement was willful.

After post-trial briefing, the district court denied Cisco's renewed motion for JMOL of no willfulness. *SRI Int'l, Inc. v. Cisco Sys., Inc.*, 254 F. Supp. 3d 680, 717 (D. Del. 2017) ("*Post-Trial Motions Op.*"). Based on the willfulness verdict, the district court determined that "some enhancement is appropriate given Cisco's litigation conduct," the "fact that Cisco lost on all issues during summary judgment," and "its apparent disdain for SRI and its business model." *Id.* at 723. The court then doubled the damages award. It also granted SRI's motion for attorneys' fees, compulsory license, and prejudgment interest.

---

in claim 1 of the '203 and '615 patents and whether EMERALD 1997 is enabled. One of the claimed categories of network traffic is "network connection requests," which Cisco asserts is disclosed by EMERALD 1997.

[4] "Sourcefire" is a network security company that Cisco acquired in 2013. J.A. 2467–68. Cisco now markets network security products and services under the Sourcefire name.

Cisco appeals the district court's claim construction and denial of summary judgment of ineligibility[5], as well as its grant of summary judgment of no anticipation, enhanced damages, attorneys' fees, and ongoing royalties. We have jurisdiction under 28 U.S.C. § 1295(a)(1).

DISCUSSION

I.

We review de novo whether a claim is drawn to patent-eligible subject matter. *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1365 (Fed. Cir. 2018) (citing *Intellectual Ventures I LLC v. Capital One Fin. Corp.*, 850 F.3d 1332, 1338 (Fed. Cir. 2017)). Section 101 defines patent-eligible subject matter as "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." 35 U.S.C. § 101. Laws of nature, natural phenomena, and abstract ideas, however, are not patentable. *See Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 70–71 (2012) (citing *Diamond v. Diehr*, 450 U.S. 175, 185 (1981)).

To determine whether a patent claims ineligible subject matter, the Supreme Court has established a

---

[5] We may review this denial of summary judgment because "a denial of a motion for summary judgment may be appealed, even after a final judgment at trial, if the motion involved a purely legal question and the factual disputes resolved at trial do not affect the resolution of that legal question." *United Techs. Corp. v. Chromalloy Gas Turbine Corp.*, 189 F.3d 1338, 1344 (Fed. Cir. 1999) (citing *Wolfgang v. Mid-Am. Motorsports, Inc.*, 111 F.3d 1515, 1521 (10th Cir. 1997); *Rekhi v. Wildwood Indus., Inc.*, 61 F.3d 1313, 1318 (7th Cir. 1995)). Neither party contends that fact issues arise in the patent-eligibility analysis in this case. Therefore, we may review the purely legal question of patent eligibility.

two-step framework. First, we must determine whether the claims at issue are directed to a patent-ineligible concept such as an abstract idea. *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 217 (2014). Second, if the claims are directed to an abstract idea, we must "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*, 566 U.S. at 79). To transform an abstract idea into a patent-eligible application, the claims must do "more than simply stat[e] the abstract idea while adding the words 'apply it.'" *Id.* at 221 (quoting *Mayo*, 566 U.S. at 72 (internal alterations omitted)).

We resolve the eligibility issue at *Alice* step one and conclude that claim 1 is not directed to an abstract idea. *See Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1337 (Fed. Cir. 2016). The district court concluded that the claims are more complex than merely reciting the performance of a known business practice on the Internet and are better understood as being necessarily rooted in computer technology in order to solve a specific problem in the realm of computer networks. *Summary Judgment Op.*, 179 F. Supp. 3d at 353–54 (citing '203 patent col. 1 ll. 37–40; *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1257 (Fed. Cir. 2014)). We agree. The claims are directed to using a specific technique—using a plurality of network monitors that each analyze specific types of data on the network and integrating reports from the monitors—to solve a technological problem arising in computer networks: identifying hackers or potential intruders into the network.

Contrary to Cisco's assertion, the claims are not directed to just analyzing data from multiple sources to

detect suspicious activity. Instead, the claims are directed to an improvement in computer network technology. Indeed, representative claim 1 recites using network monitors to detect suspicious network activity based on analysis of network traffic data, generating reports of that suspicious activity, and integrating those reports using hierarchical monitors. '615 patent col. 15 ll. 2–21. The "focus of the claims is on the specific asserted improvement in computer capabilities"—that is, providing a network defense system that monitors network traffic in real-time to automatically detect large-scale attacks. *Enfish*, 822 F.3d at 1335–36.

The specification bolsters our conclusion that the claims are directed to a technological solution to a technological problem. The specification explains that, while computer networks "offer users ease and efficiency in exchanging information," '615 patent col. 1 ll. 28–29, "the very interoperability and sophisticated integration of technology that make networks such valuable assets also make them vulnerable to attack, and make dependence on networks a potential liability." *Id.* at col. 1 ll. 36–39. The specification further teaches that, in conventional networks, seemingly localized triggering events can have glob-ally disastrous effects on widely distributed systems—like the 1980 ARPAnet collapse and the 1990 AT&T collapse. *See id.* at col. 1 ll. 43–47. The specification explains that the claimed invention is directed to solving these weaknesses in conventional networks and provides "a framework for the recognition of more global threats to interdomain connectivity, including coordinated attempts to infiltrate or destroy connectivity across an entire net-work enterprise." *Id.* at col. 3 ll. 44–48.

Cisco argues that the claims are directed to an abstract idea for three primary reasons. First, Cisco ar-

gues that the claims are analogous to those in *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350 (Fed. Cir. 2016), and are simply directed to generic steps required to collect and analyze data. We disagree. The *Electric Power* claims were drawn to using computers as tools to solve a power grid problem, rather than improving the functionality of computers and computer networks themselves. *Id.* at 1354. We conclude that the claims are more like the patent-eligible claims in *DDR Holdings*. In *DDR*, we emphasized that the claims were directed to more than an abstract idea that merely required a "computer network operating in its normal, expected manner." 773 F.3d at 1258. Here, the claims actually prevent the normal, expected operation of a conventional computer network. Like the claims in *DDR*, the claimed technology "overrides the routine and conventional sequence of events" by detecting suspicious network activity, generating reports of suspicious activity, and receiving and integrating the reports using one or more hierarchical monitors. *Id.*

Second, Cisco argues that the invention does not involve "an improvement to computer functionality itself." *Enfish*, 822 F.3d at 1336. In *Alice*, the Supreme Court advised that claims directed to independently abstract ideas that use computers as tools are still abstract. 573 U.S. at 222–23. However, the claims here are not directed to using a computer as a tool—that is, automating a conventional idea on a computer. Rather, the representative claim improves the technical functioning of the computer and computer networks by reciting a specific technique for improving computer network security.

Cisco also submits that the asserted claims are so general that they encompass steps that people can "go through in their minds," allegedly confirming that they

are directed to an abstract concept. Appellant Br. 27–28 (citing *Capital One*, 850 F.3d at 1340; I*ntellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1318 (Fed. Cir. 2016); *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1371 (Fed. Cir. 2011)). We disagree. This is not the type of human activity that § 101 is meant to exclude. Indeed, we tend to agree with SRI that the human mind is not equipped to detect suspicious activity by using network monitors and analyzing network packets as recited by the claims.

Because we conclude that the claims are not directed to an abstract idea under step one of the *Alice* analysis, we need not reach step two. *See Enfish*, 822 F.3d at 1339. Accordingly, we affirm the district court's summary judgment that the claims are patent-eligible.

II.

A district court's claim construction based solely on intrinsic evidence is a legal question that we review de novo. *See Teva Pharm. USA, Inc. v. Sandoz, Inc.*, 135 S. Ct. 831, 841 (2015). Claim construction seeks to ascribe the "ordinary and customary meaning" to claim terms as a person of ordinary skill in the art would have understood them at the time of invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005) (en banc) (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)). "[T]he claims themselves provide substantial guidance as to the meaning of particular claim terms." *Id.* at 1314. In addition, "the person of ordinary skill in the art is deemed to read 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.

The district court construed "[n]etwork traffic data" to mean "data obtained from direct examination of network packets." *SRI Int'l, Inc. v. Dell Inc.*, No. CV13-1534-SLR, 2015 WL 2265756, at *1–2 (D. Del. May 14, 2015). After reviewing the parties' pleadings on summary judgment, the district court determined that its construction would benefit from clarification. The district court explained that "[t]o say that the data 'is obtained from direct examination of network packets' means to differentiate the original source of the data, not how or where the data is analyzed. ... The fact that the data may be stored before analysis is performed on the data does not detract from its lineage." *Summary Judgment Op.*, 179 F. Supp. 3d at 363. The district court explicitly rejected the opinion of Cisco's expert, Dr. Clark, that the court's claim construction should require that the analysis of data obtained from network packets take place without any further manipulation whatsoever. *Id.*

On appeal, Cisco offers a more nuanced construction, asserting that term should instead be construed as "detecting suspicious network activity based on 'direct examination of network packets,' where such 'direct examination' does not include merely examining data that has been obtained, generated, or gleaned from network packets." Appellant Br. 42. According to Cisco, based on SRI's express prosecution disclaimer during reexamination, the claims require detecting suspicious activity based on "direct examination" of network packets, not data "generated" or "gleaned" from packets. Cisco would thus construe the term to exclude a process that decodes the network packet.

We conclude that Cisco's proposed construction goes too far in limiting the amount of preprocessing encompassed by the claim. The specification shows that

preprocessing is a contemplated and expected part of the claimed invention. Indeed, the specification specifically mentions different forms of preprocessing network packets prior to examination, including decryption ('615 patent col. 3 ll. 61–63), parsing (*id.* at col. 8 ll. 10–12), and decoding (*id.* at col. 8 ll. 7–9).

Cisco's argument that SRI disclaimed preprocessing during reexamination of its patents is also not persuasive. To invoke argument-based estoppel, "the prosecution history must evince a 'clear and unmistakable surrender'" of this kind of preprocessing. *Deering Precision Instruments v. Vector Distrib. Sys.*, 347 F.3d 1314, 1326 (Fed. Cir. 2003) (quoting *Eagle Comtronics, Inc. v. Arrow Commc'n Labs., Inc.*, 305 F.3d 1303, 1316 (Fed. Cir. 2002)); *see also Krippelz v. Ford Motor Co.*, 667 F.3d 1261, 1267 (Fed. Cir. 2012) (applying prosecution history disclaimer from reexamination proceedings). Here, SRI's statements during reexamination reflect that SRI drew the line between what does and does not comprise "direct examination" by excluding information derived from network packet data (for example, network traffic measures and network traffic statistics). At the same time, SRI explained that "direct examination" includes the data from which the network traffic measures and network traffic statistics are derived (that is, the data in the network packets). For example, SRI explained that the specification:

> [D]emonstrates that the term "network traffic data" requires information obtained by direct packet examination by using the distinctly different terms "network traffic measures" and "network traffic statistics" when discussing information *derived* from network traffic observation, as compared to the data from which the measures and statistics are derived.

Brief for the Patentee on Appeal at 7, *In re Porras*, Reexam No. 90/008,125 (B.P.A.I. Jan. 14, 2010) (citing '203 patent col. 4 ll. 55–60 (discussing "network traffic statistics") and col. 5 ll. 28–30 (discussing "network traffic measures")).

We read SRI's statements during reexamination as simply explaining that "network traffic statistics," such as number of packets and number of kilobytes transferred, are statistics *derived* from the network packet data—not the underlying data itself. SRI did not argue that the actual data underlying the measures and statistics—the data in the network packets—could not be subject to direct examination. Nor did SRI take the position that "direct examination" must take place before any or all processing. SRI did not mention processing at all during reexamination. Moreover, as the specification makes clear, the system may need to decrypt, parse, or decode the data packets—all forms of preprocessing—in order to directly examine the network packet data underlying the network traffic statistics.

We hold that SRI's statements in the prosecution history do not invoke a clear and unmistakable surrender of all preprocessing, including decryption, decoding, and parsing. Accordingly, we agree with the district court's construction of "network traffic data" to mean "data obtained from direct examination of network packets."

III.

We also hold that the district court did not err in granting summary judgment that the asserted claims are not anticipated by SRI's own EMERALD 1997 reference. We review the district court's summary judg-

ment of no anticipation under regional circuit law. *See MAG Aerospace Indus., Inc. v. B/E Aerospace, Inc.*, 816 F.3d 1374, 1376 (Fed. Cir. 2016). The Third Circuit reviews a grant of summary judgment de novo, applying the same standard as the district court. *See Gonzalez v. Sec'y of Dep't of Homeland Sec.*, 678 F.3d 254, 257 (3d Cir. 2012). Summary judgment is appropriate when, drawing all justifiable inferences in the nonmovant's favor, there exists no genuine issue of material fact and the movant is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a); *see also Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 255 (1986). Anticipation requires that a single prior art reference disclose each and every limitation of the claimed invention, either expressly or inherently. *See Verdegaal Bros. v. Union Oil Co. of Cal.*, 814 F.2d 628, 631 (Fed. Cir. 1987).

EMERALD 1997 discloses a tool for tracking malicious activity across large networks. The question before us is whether the district court erred in concluding on summary judgment that EMERALD 1997 does not disclose detection of any of the network traffic data categories listed in claim 1 of the '203 and '615 patents. The Patent Office considered EMERALD 1997 during the original examination of the '615 patent, and the patentability of the claims over the reference was confirmed in multiple reexamination and litigation proceedings. Indeed, during reexamination, the Patent Office accepted SRI's argument that the claim limitation requires detecting suspicious activity based on "direct examination" of network packets to distinguish EMERALD 1997. J.A. 26402 ("[T]he closest prior art of record, Emerald 1997, fails to teach direct examination of packet data."); J.A. 27101 (same).

EMERALD 1997 describes detecting a DNS/NFS attack in "real-time." J.A. 5004. To achieve this, EMERALD 1997 explains:

> The subscription list field is an important facility for gaining visibility into malicious or anomalous activity outside the immediate environment of an EMERALD monitor. The most obvious examples where relationships are important involve interdependencies among network services that make local policy decisions. Consider, for example, the interdependencies between access checks per-formed during network file system ["NFS"] mounting and the IP mapping of the DNS service. An unexpected mount monitored by the network file system service may be responded to differently if the DNS monitor informs the network file system monitor of suspicious updates to the mount requester's DNS mapping.

J.A. 5008. EMERALD 1997 further explains that:

> Above the service layer, signature engines scan the aggregate of intrusion reports from service monitors in an attempt to detect more global coordinated attack scenarios or scenarios that exploit interdependencies among network services. The DNS/NFS attack discussed [above] is one such example of an aggregate attack scenario.

J.A. 5010.

Cisco's expert submitted a report concluding that a person of ordinary skill in the art would understand from this disclosure that "monitoring specific network services, such as HTTP, FTP, network file systems,

finger, Kerberos, and SNMP would *require* detecting and analyzing packets indicative of those well-known network service protocols, one of the enumerated categories in claim 1 of the '615 patent." J.A. 30347 (emphasis added). During deposition, however, Cisco's expert retreated from this position, admitting that a person of ordinary skill reading EMERALD 1997 would have understood that it was not necessary to directly examine the packets, although that would be "one very good way" to prevent attacks. J.A. 50040 at 159:12–21.

On this record, we conclude that summary judgment was appropriate. EMERALD 1997 does not expressly disclose directly examining network packets as required by the claims—especially not to obtain data about network connection requests. Nor does Cisco's expert testimony create a genuine issue of fact on this issue. Rather, we agree with the district court that Cisco's expert's testimony is both inconsistent and "based on [] multiple layers of supposition." *Summary Judgment Op.*, 179 F. Supp. 3d at 358. Because the evidence does not support express or inherent disclosure of direct examination of packet data, we conclude that the district court did not err in holding that there was no genuine issue of fact regarding whether EMERALD 1997 disclosed analyzing the specific enumerated types of network traffic data recited in the claims.

Cisco next argues that the district court erred by granting summary judgment for SRI sua sponte despite SRI's failure to move for such relief. We disagree. Under Third Circuit law, a district court may properly enter summary judgment sua sponte "so long as the losing party was on notice that she had to come forward with all of her evidence." *Gibson v. Mayor & Council of City of Wilmington*, 355 F.3d 215, 222 (3d Cir. 2004) (quoting *Celotex Corp. v. Catrett*, 477 U.S.

317, 326 (1986)). By filing its own motion for summary judgment, Cisco was on notice that anticipation was before the court, and Cisco had the opportunity to put forth its best evidence. Additionally, SRI did argue, in opposition to Cisco's summary judgment motion, that the district court should outright reject Cisco's assertion of invalidity. J.A. 31650 ("Cisco's assertion of invalidity should be rejected ... ."). Indeed, SRI expressly took the position that EMERALD 1997 "does not anticipate any claim of the '203 or '615 patents." J.A. 31678. Thus, any notice requirement was satisfied because Cisco itself indicated that the issue was ripe for summary adjudication and SRI took the position that the claims were not anticipated. Accordingly, we see no error in the sua sponte nature of the district court's order and we affirm the summary judgment of no anticipation.

IV.

Cisco also appeals the district court's denial of JMOL that it did not willfully infringe the asserted patents because the jury's willfulness finding is not supported by substantial evidence. We agree that the jury's finding that Cisco willfully infringed the patents-in-suit prior to receiving notice thereof is not supported by substantial evidence and therefore vacate and remand.

We review decisions on motions for JMOL under the law of the regional circuit. *Energy Transp. Grp. Inc. v. William Demant Holding A/S*, 697 F.3d 1342, 1350 (Fed. Cir. 2012). The Third Circuit reviews district court decisions on such motions de novo. *Acumed LLC v. Adv. Surgical Servs., Inc.*, 561 F.3d 199, 211 (3d Cir. 2009) (citing *Monteiro v. City of Elizabeth*, 436 F.3d 397, 404 (3d Cir. 2006)). In the Third Circuit, a

"court may grant a judgment as a matter of law contrary to the verdict only if 'the record is critically deficient of the minimum quantum of evidence' to sustain the verdict." *Id.* (citing *Gomez v. Allegheny Health Servs., Inc.*, 71 F.3d 1079, 1083 (3d Cir. 1995)). The court should grant JMOL "sparingly" and "only if, viewing the evidence in the light most favorable to the nonmovant and giving it the advantage of every fair and reasonable inference, there is insufficient evidence from which a jury reasonably could find liability." *Marra v. Phila. Hous. Auth.*, 497 F.3d 286, 300 (3d Cir. 2007) (quoting *Moyer v. United Dominion Indus., Inc.*, 473 F.3d 532, 545 n.8 (3d Cir. 2007)).

As the Supreme Court stated in *Halo*, "[t]he sort of conduct warranting enhanced damages has been variously described in our cases as willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or—indeed—characteristic of a pirate." *Halo Elecs., Inc. v. Pulse Elecs., Inc.*, 136 S. Ct. 1923, 1932 (2016). While district courts have discretion in deciding whether or not behavior rises to that standard, such findings "are generally reserved for egregious cases of culpable behavior." *Id.* Indeed, as Justice Breyer emphasized in his concurrence, it is the *circumstances* that transform simple "intentional or knowing" infringement into egregious, sanctionable behavior, and that makes all the difference. *Id.* at 1936 (Breyer, J., concurring). A patentee need only show by a preponderance of the evidence the facts that support a finding of willful infringement. *Id.* at 1934.

In denying Cisco's motion for JMOL on willfulness, the district court concluded that the jury's willfulness determination was supported by two evidentiary bases. First, the court identified evidence that "key Cisco employees did not read the patents-in-suit until their dep-

ositions." *Post-Trial Motions Op.*, 254 F. Supp. 3d at 717. Second, the court identified evidence that Cisco designed the products and services in an infringing manner and that Cisco instructed its customers to use the products and services in an infringing manner. Based on these two facts, the district court denied Cisco's renewed motion for JMOL on willfulness, stating that "[v]iewing the record in the light most favorable to SRI, substantial evidence supports the jury's subjective willfulness verdict." *Id.*

On appeal, SRI identifies additional evidence that purportedly supports the jury's willfulness verdict. Specifically, SRI presented evidence that Cisco expressed interest in the patented technology and met with SRI's inventor in 2000 before developing its infringing products. J.A. 1484–86; J.A. 5027. Additionally, SRI submitted evidence that Cisco received a notice letter from SRI's licensing consultant on May 8, 2012, informing Cisco of the asserted patents (a year before SRI filed the complaint). Finally, like the district court, SRI makes much of the fact that "key engineers" did not look at SRI's patents until SRI took their depositions during this litigation. In particular, Cisco engineers Martin Roesch and James Kasper did not look at the patent until their depositions in 2015.

Even accepting this evidence as true and weighing all inferences in SRI's favor, we conclude that the record is insufficient to establish that Cisco's conduct rose to the level of wanton, malicious, and bad-faith behavior required for willful infringement. First, it is undisputed that the Cisco employees who did not read the patents-in-suit until their depositions were engineers without legal training. Given Cisco's size and resources, it was unremarkable that the engineers—as opposed to Cisco's in-house or outside counsel—did not

analyze the patents-in-suit themselves. The other rationale offered by the district court—that Cisco designed the products and services in an infringing manner and that Cisco instructed its customers to use the products and services in an infringing manner—is nothing more than proof that Cisco directly infringed and induced others to infringe the patents-in-suit.

It is undisputed that Cisco did not know of SRI's patent until May 8, 2012, when SRI sent its notice letter to Cisco. Oral Arg. at 23:46, *available at* http://oralarguments.cafc.uscourts.gov/default.aspx?fl=2017-2223.mp3. It is also undisputed that this notice letter was sent years after Cisco independently developed the accused systems and first sold them in 2005 (Cisco) and 2007 (Sourcefire). As SRI admits, the patents had not issued when the parties met in May 2000. Indeed, the patent application for the parent '203 patent was not even filed until several months after the parties met. Thus, Cisco could not have been aware of the patent application.

While the jury heard evidence that Cisco was aware of the patents in May 2012, before filing of the lawsuit, we do not see how the record supports a willfulness finding going back to 2000. As the Supreme Court recently observed, "culpability is generally measured against the knowledge of the actor at the time of the challenged conduct." *Halo*, 136 S. Ct. at 1933. Similarly, Cisco's allegedly aggressive litigation tactics cannot support a finding of willful infringement going back to 2000, especially when the litigation did not start until 2012. Finally, Cisco's decision not to seek an advice-of-counsel defense is legally irrelevant under 35 U.S.C. § 298.

Viewing the record in the light most favorable to SRI, the jury's verdict of willful infringement before May 8, 2012 is not supported by substantial evidence. Given the general verdict form, we presume the jury also found that Cisco willfully infringed after May 8, 2012. When reviewing a denial of JMOL, "where there is a black box jury verdict, as is the case here, we presume the jury resolved underlying factual disputes in favor of the verdict winner and leave those presumed findings undisturbed if supported by substantial evidence." *Arctic Cat Inc. v. Bombardier Recreational Prods. Inc.*, 876 F.3d 1350, 1358 (Fed. Cir. 2017), (citing *WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1326 (Fed. Cir. 2016)), *cert. denied*, 139 S. Ct. 143(2018). We leave it to the district court to decide in the first instance whether the jury's presumed finding of willful infringement after May 8, 2012 is supported by substantial evidence.[6] In so doing, the court should bear in mind the standard for willful infringement, as well as the above analysis regarding SRI's evidence of willfulness. Accordingly, we vacate and remand the district court's denial of Cisco's renewed motion for JMOL of no willful infringement.

Cisco also argues that the district court abused its discretion by doubling damages. Enhanced damages under § 284 are predicated on a finding of willful in-

[6] We recognize that, ideally, it should not fall to the district court to determine when, if ever, willful infringement began through the mechanism of JMOL. Rather, the question of when willful infringement began is a fact issue that would have been best presented to the jury in a special verdict form with appropriate jury instructions. Better yet, perhaps SRI could have recognized the shortcomings in its case and presented a more limited case of willful infringement from 2012 onwards. Or perhaps Cisco could have filed a motion for summary judgment of no willful infringement prior to May 8, 2012.

fringement. Because we conclude that the jury's finding of willfulness before 2012 was not supported by substantial evidence, we do not reach the propriety of the district court's award of enhanced damages. Instead, we vacate the award of enhanced damages and remand for further consideration along with willfulness.

V.

We next turn to the district court's award of attorneys' fees under § 285, which we vacate and remand for further consideration. Under § 285, a "court in exceptional cases may award reasonable attorney fees to the prevailing party." An "exceptional" case under § 285 is "one that stands out from others with respect to the substantive strength of a party's litigating position (considering both the governing law and the facts of the case) or the unreasonable manner in which the case was litigated." *Octane Fitness, LLC v. ICON Health & Fitness, Inc.*, 572 U.S. 545, 554 (2014). The party seeking fees must prove that the case is exceptional by a preponderance of the evidence, and the district court makes the exceptional case determination on a case-by-case basis considering the totality of the circumstances. *See id.* at 554, 557.

We review a district court's grant or denial of attorneys' fees for an abuse of discretion, which is a highly deferential standard of review. *Highmark Inc. v. Allcare Health Mgmt. Sys., Inc.*, 572 U.S. 559, 564 (2014); *Bayer CropScience AG v. Dow AgroSciences LLC*, 851 F.3d 1302, 1306 (Fed. Cir. 2017) (citing *Mentor Graphics Corp. v. Quickturn Design Sys., Inc.*, 150 F.3d 1374, 1377 (Fed. Cir. 1998)). To meet the abuse-of-discretion standard, the appellant must show that the district court made "a clear error of judgment in weighing relevant factors or in basing its decision on an error

of law or on clearly erroneous factual findings." *Bayer*, 851 F.3d at 1306 (quoting *Mentor Graphics*, 150 F.3d at 1377); *see also Highmark*, 572 U.S. at 563 n.2.

We see no such error in the district court's determination that this was an exceptional case. The district court found:

> There can be no doubt from even a cursory review of the record that Cisco pursued litigation about as aggressively as the court has seen in its judicial experience. While defending a client aggressively is understandable, if not laudable, in the case at bar, Cisco crossed the line in several regards.

Post-Trial Motions Op., 254 F. Supp. 3d at 722.

The district court further explained that "Cisco's litigation strategies in the case at bar created a substantial amount of work for both SRI and the court, much of which work was needlessly repetitive or irrelevant or frivolous." *Id.* at 723 (footnotes omitted). Indeed, the district court inventoried Cisco's aggressive tactics, including maintaining nineteen invalidity theories until the eve of trial but only presenting two at trial and pursuing defenses at trial that were contrary to the court's rulings or Cisco's internal documents. *Id.* at 722. Nevertheless, the district court relied in part on the fact that the jury found that Cisco's infringement was willful in its determination to exercise its discretion pursuant to § 285 to award SRI its attorneys' fees and costs. *Id.* at 723. Accordingly, we vacate the district court's award of attorneys' fees and remand for further consideration along with willfulness.

We take no issue with the district court's award of attorneys' fees at the attorneys' billing rates without

adjusting them to Delaware rates. At the same time, however, the district court erred in granting all of SRI's fees. Section 285 permits a prevailing party to recover reasonable attorneys' fees, but not fees for hours expended by counsel that were "excessive, redundant, or otherwise unnecessary." *Hensley v. Eckerhart*, 461 U.S. 424, 434 (1983). We accordingly conclude that the district court should have reduced SRI's total hours to eliminate clear mistakes. For example, one billing entry reads "DON'T RELEASE, CLIENT MATTER NEEDS TO BE CHANGED." J.A. 32384. Accordingly, should the district court award attorneys' fees on remand, it must remove attorney hours clearly included by mistake in its calculation of reasonable attorneys' fees.

VI.

We review for abuse of discretion a district court's grant of an ongoing royalty. *Whitserve, LLC v. Comput. Packages, Inc.*, 694 F.3d 10, 35 (Fed. Cir. 2012). Here, the district court did not abuse its discretion in awarding "a 3.5% compulsory license for all post-verdict sales." *Post-Trial Motions Op.*, 254 F. Supp. 3d at 724. The district court's ongoing royalty rate equals the rate found by the jury and the base is limited to the "accused products and services." J.A. 182.

On appeal, Cisco argues that the district court abused its discretion in awarding the 3.5% ongoing royalty on "all post-verdict sales" without considering Cisco's design-arounds. According to Cisco, the court was obligated to assess whether Cisco's redesigned products and services were more than colorably different from those products and services adjudicated at trial, and if not, whether those redesigned products and services infringe. To this end, Cisco moved to supplement

its post-trial briefing with declarations describing its redesign efforts. Cisco argues that the district court abused its discretion by denying its motion to supplement.[7] We disagree. The district court properly exercised its discretion in denying Cisco's motion to supplement the record regarding alleged post-verdict design-around activity. Cisco did not redesign its products until after trial, and Cisco did not file its motion to supplement until after completion of post-trial briefing. Given the stage of the proceedings and SRI's opposition, the trial court acted within its discretion when denying Cisco's motion to supplement.

To the extent the district court's order is unclear—and we think it is not—we reconfirm that the ongoing royalty on post-verdict sales is limited to products that were actually found to infringe and products that are not colorably different. We discern no error in the district court's determination that Cisco's submissions were untimely. Nevertheless, we acknowledge that the district court has not yet determined whether products and services that were not accused (that is, changed after the jury verdict) are colorably different for purposes of ongoing royalty calculations. Such an issue could be resolved in a future proceeding.

---

[7] Finally, Cisco argues that, in the same order in which the court stated that "[t]here are no post-verdict royalties," the court awarded a post-verdict royalty—an internal inconsistency. J.A. 175. We do not ascribe weight to the apparent clerical error creating the inconsistency. The district court's final judgment order is clear that "Cisco shall pay a 3.5% compulsory license on all post-verdict sales of the accused products and services." J.A. 182. To the extent that clear statement conflicts with the single sentence in the memorandum opinion, we think the court made its intentions clear in its final judgment and we see no error by the district court.

CONCLUSION

For the reasons above, we affirm the district court's denial of summary judgment that the asserted claims are patent-ineligible. We also agree with the district court's construction of "network traffic data" and affirm the district court's grant of summary judgment of no anticipation. We vacate and remand the district court's denial of Cisco's renewed motion for judgment as a matter of law that Cisco did not willfully infringe the asserted claims. Accordingly, we vacate and remand the district court's awards of enhanced damages and attorneys' fees. Finally, we affirm the district court's orders granting enhanced damages and ongoing royalties.

AFFIRMED-IN-PART, VACATED-IN-PART, AND REMANDED

COSTS

No costs.

UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

2017-2223

SRI INTERNATIONAL, INC.,
Plaintiff-Appellee

v.

CISCO SYSTEMS, INC.,
Defendant-Appellant.

Appeal from the United States District Court for the District of Delaware in No. 1:13-cv-01534-SLR-SRF, Judge Sue L. Robinson.

LOURIE, *Circuit Judge*, dissenting.

I respectfully dissent from the majority's decision upholding the eligibility of the claims. In my view, they are clearly abstract. In fact, they differ very little from the claims in *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1355 (Fed. Cir. 2016), where we found the claims to be abstract.

The majority opinion focuses on claim 1 of U.S. Patent 6,711,615 ("the '615 patent"), which recites:

> 1. A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:
>
> deploying a plurality of network monitors in the enterprise network;
>
> detecting, by the network monitors, suspicious network activity based on analysis of

> network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols};
>
> generating, by the monitors, reports of said suspicious activity; and
>
> automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.

Similarly, the claim we reviewed in *Electric Power Group* recited "[a] method of detecting events on an interconnected electric power grid in real time over a wide area and automatically analyzing the events on the interconnected electric power grid," with the method comprising eight steps, including "receiving data," "detecting and analyzing events in real time," "displaying the event analysis results and diagnoses of events," "accumulating and updating measurements," and "deriving a composite indicator of reliability." 830 F.3d at 1351–52.

While that claim was lengthy, with eight steps, it merely described selecting information by content or source for collection, analysis, and display. *Id.* at 1351. In finding the claim directed to an abstract idea, we reasoned that "collecting information, including when limited to particular content (which does not change its character as information)" was an abstract idea. *Id.* at 1353. Limiting the claim to a particular technological

environment—power-grid monitoring—was insufficient to transform it into a patent-eligible application of the abstract idea at its core. *Id.* at 1354. The claim was rooted in computer technology only to the extent that the broadly-recited steps required a computer. At step two, we noted that the claim did not require an "inventive set of components or methods ... that would generate new data," and did not "invoke any assertedly inventive programming." *Id.* at 1355.

This case is hardly distinguishable from *Electric Power Group*. The claims in that case are said in the majority opinion to only be drawn to using computers as tools to solve a problem, rather than improving the functionality of computers and computer networks.

The claims here recite nothing more than deploying network monitors, detecting suspicious network activity, and generating and handling reports. The detecting of the suspicious activity is based on "analysis" of traffic data, but the claims add nothing concerning specific means for doing so. The claims only recite the moving of information. The computer is used as a tool, and no improvement in computer technology is shown or claimed. There is no specific technique described for improving computer network security.

I would find the claims directed to the abstract idea of monitoring network security and proceed to step two of *Alice*. As in *Electric Power Group*, however, "[n]othing in the claims, understood in light of the specification, requires anything other than off-the-shelf, conventional computer, network, and display technology ... ." 830 F.3d at 1355. The claims recite "types of information and information sources," *id.*, but such selection of information by content or source does not provide an inventive concept. *Id.* The specification fur-

ther makes clear that the claims only rely on generic computer components, including a computer, memory, processor, and mass storage device. *See* '615 patent, col. 14 ll. 50–57. Indeed, the specification even deems the relevant memory bus and peripheral bus "customary components." *Id.* col. 14 l. 55.

Finally, the majority opinion quotes from and paraphrases language from the specification that only recites results, not means for accomplishing them. *See, e.g.*, *Majority Op.* at 9. The claims as written, however, do not recite a *specific way* of enabling a computer to monitor network activity. As we noted in *Electric Power Group*, result-focused, functional claims that effectively cover any solution to an identified problem, like those at issue here, frequently run afoul of *Alice*. 830 F.3d at 1356.

Thus, I would find the claims to be directed to an abstract idea at *Alice* step one, without an inventive concept at step two, and reverse the district court's finding of eligibility. Because I would find the claims at issue to be ineligible, I would not reach the remaining issues in the case.

APPENDIX D

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

Civ. No. 13-1534-SLR

SRI INTERNATIONAL, INC.,
Plaintiff,

v.

CISCO SYSTEMS, INC.
Defendant.

Filed: April 11, 2016
District Judge Robinson

MEMORANDUM OPINION

I. INTRODUCTION

Plaintiff SRI International, Inc. ("SRI") filed suit against defendant Cisco Systems Inc. ("Cisco"), alleging infringement of U.S. Patent No. 6,711,615 ("the '615 patent") and 6,484,203 ("the '203 patent") (collectively, "the patents") on September 4, 2013. (D.I. 1) On December 18, 2013, Cisco answered the complaint and counterclaimed for noninfringement and invalidity. (D.I. 9) SRI answered the counterclaims on January 13, 2014. (D.I. 11) The court issued a claim construction order on May 14, 2015. (D.I. 138) Trial is scheduled to commence on May 2, 2016. (D.I. 40)

Presently before the court are Cisco's motion for summary judgment of invalidity under 35 U.S.C. § 101

(D.I. 158); Cisco's motion for summary judgment of invalidity under 35 U.S.C. § 102(b) and § 103 (D.I. 182);[8] Cisco's motion barring SRI from recovery of pre-suit damages based on the equitable doctrine of laches (D.I. 182); Cisco's motion for summary judgment for non-infringement (D.I. 182); Cisco's motion to exclude certain opinions of Dr. Prowse regarding SRI's lump settlement agreements (D.I. 213); Cisco's motion to exclude the testimony of Dr. Lee regarding apportionment (D.I. 216); and SRI's motion for summary judgment that Netranger and Hunteman are not prior art (D.I. 219). The court has jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

II. BACKGROUND

A. The Parties

SRI is an independent, not-for-profit research institute incorporated under the laws of the State of California, with its principal place of business in Menlo Park, California. (D.I. 1 at ¶ 1) SRI conducts client-supported research and development for government agencies, commercial businesses, foundations, and other organizations. (*Id.* at ¶ 6) Among its many areas of research, SRI has engaged in research related to computer security and, more specifically, to large computer network intrusion detection systems and methods. (*Id.*)

Cisco is a corporation organized and existing under the laws of the State of California, with its principal place of business in San Jose, California. (*Id.* at ¶ 2) Cisco provides various intrusion prevention and intrusion detection products and services. (*Id.* at ¶ 14)

---

[8] Three motions were filed under D.I. 182.

B. Patents

The '615 patent (titled "Network Surveillance") is a continuation of the '203 patent (titled "Hierarchical Event Monitoring and Analysis"), and the patents share a common specification and priority date of November 9, 1998.[9] (D.I. 179 at 1) SRI has asserted infringement of claims 1-4, 14-16, and 18 of the '615 patent and claims 1-4, 12-15, and 17 of the '203 patent.[10] (Id. at 3) The patents relate to the monitoring and surveillance of computer networks for intrusion detection. In particular, the patents teach a computer-automated method of hierarchical event monitoring and analysis within an enterprise network that allows for real-time detection of intruders. Upon detecting any suspicious activity, the network monitors generate reports of such activity. The claims of the '203 and '615 patents focus on methods and systems for deploying a hierarchy of network monitors that can generate and receive reports of suspicious network activity. Independent claims 1 and 13 of the '615 patent read as follows:

---

[9] Unless otherwise indicated, citations are to the '615 patent.

[10] SRI previously asserted the '203 and '615 patents before this court in *SRI Int'l, Inc. v. Internet Security Sys., Inc.*, 647 F. Supp. 2d 323 (D. Del. 2009) (opinion after jury trial), 401 Fed App'x 530 (Fed. Cir. 2010) (SRI and Symantec then settled the litigation on confidential terms, Civ. No. 04-1199-SLR, 0.1. 722). The patents have also each undergone two reexaminations before the PTO, which reached the same result as the jury and confirmed the patentability of all claims. The patents were also the subject of two cases before Judge White in the Northern District of California: *Fortinet, Inc. v. SRI Int'l, Inc.*, Civ. No. 12-3231 JSW (N.D. Cal.), and *Checkpoint Software Technologies, Inc. v. SRI International, Inc.*, Civ. No. 12-3231-JSW (N.D. Cal.). (0.1. 220 at 7-8)

1. A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:

deploying a plurality of network monitors in the enterprise network;

detecting, by the network monitors, suspicious network activity based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols};

generating, by the monitors, reports of said suspicious activity; and

automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.

(15:1-21)

13. An enterprise network monitoring system comprising:

a plurality of network monitors deployed within an enterprise network, said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network

> connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols};
>
> said network monitors generating reports of said suspicious activity; and one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.

(15:56-16:6)

III. STANDARD OF REVIEW

"The court shall grant summary judgment if the movant shows that 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). The moving party bears the burden of demonstrating the absence of a genuine issue of material fact. *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 415 U.S. 475, 586 n. 10 (1986). A party asserting that a fact cannot be-or, alternatively, is-genuinely disputed must be supported either by citing to "particular parts of materials in the record, including depositions, documents, electronically stored information, affidavits or declarations, stipulations (including those made for the purposes of the motions only), admissions, interrogatory answers, or other materials," or by "showing that the materials cited do not establish the absence or presence of a genuine dispute, or that an adverse party cannot produce admissible evidence to support the fact." Fed. R. Civ. P. 56(c)(1)(A) & (B). If the moving party has carried its burden, the nonmovant must then "come forward

with specific facts showing that there is a genuine issue for trial." *Matsushita*, 415 U.S. at 587 (internal quotation marks omitted). The Court will "draw all reasonable inferences in favor of the nonmoving party, and it may not make credibility determinations or weigh the evidence." *Reeves v. Sanderson Plumbing Prods., Inc.*, 530 U.S. 133, 150 (2000).

To defeat a motion for summary judgment, the nonmoving party must "do more than simply show that there is some metaphysical doubt as to the material facts." *Matsushita*, 475 U.S. at 586-87; *see also Podohnik v. U.S. Postal Service*, 409 F.3d 584, 594 (3d Cir. 2005) (stating party opposing summary judgment "must present more than just bare assertions, conclusory allegations or suspicions to show the existence of a genuine issue") (internal quotation marks omitted). Although the "mere existence of some alleged factual dispute between the parties will not defeat an otherwise properly supported motion for summary judgment," a factual dispute is genuine where "the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 247-48 (1986). "If the evidence is merely colorable, or is not significantly probative, summary judgment may be granted." *Id.* at 249-50 (internal citations omitted); see also *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986) (stating entry of summary judgment is mandated "against a party who fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial").

IV. INVALIDITY

A. 35 U.5.C. § 101

1. Standard

Section 101 provides that patentable subject matter extends to four broad categories, including: "new and useful process[es], machine[s], manufacture, or composition[s] of matter." 35 U.S.C. § 101; *see also Bilski v. Kappas*, 561 U.S. 593, 601 (2010) ("*Bilski II*"); *Diamond v. Chakrabarty*, 447 U.S. 303, 308 (1980). A "process" is statutorily defined as a "process, art or method, and includes a new use of a known process, machine manufacture, composition of matter, or material." 35 U.S.C. § 100(b).

The Supreme Court has explained:

> A process is a mode of treatment of certain materials to produce a given result. It is an act, or a series of acts, performed upon the subject-matter to be transformed and reduced to a different state or thing. If new and useful, it is just as patentable as is a piece of machinery. In the language of the patent law, it is an art. The machinery pointed out as suitable to perform the process may or may not be new or patentable; whilst the process itself may be altogether new, and produce an entirely new result. The process requires that certain things should be done with certain substances, and in a certain order; but the tools to be used in doing this may be of secondary consequence.

Diamond v. Diehr, 450 U.S. 175, 182-83 (1981) (internal quotations omitted).

The Supreme Court recognizes three "fundamental principle" exceptions to the Patent Act's subject matter

eligibility requirements: "laws of nature, physical phenomena, and abstract ideas." *Bilski II*, 561 U.S. at 601. In this regard, the Court has held that "[t]he concepts covered by these exceptions are 'part of the storehouse of knowledge of all men ... free to all men and reserved exclusively to none.'" *Bilski II*, 561 U.S. at 602 (quoting *Funk Bros. Seed Co. v. Kato lnoculant Co.*, 333 U.S. 127, 130 (1948)). "[T]he concern that drives this exclusionary principle is one of pre-emption," that is, "'that patent law not inhibit further discovery by improperly tying up the future use of' these building blocks of human ingenuity." *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*,—U.S.—, 134 S.Ct. 2347, 2354 (2014) (citing *Bilski II*, 561 U.S. at 611-12 and *Mayo Collaborative Servs.v. Prometheus Labs., Inc.*, 566 U.S.—, 132 S.Ct. 1289, 1301 (2012)).

Although a fundamental principle cannot be patented, the Supreme Court has held that "an application of a law of nature or mathematical formula to a known structure or process may well be deserving of patent protection," so long as that application would not preempt substantially all uses of the fundamental principle. *Bilski II*, 561 U.S. at 611 (quoting *Diehr*, 450 U.S. at 187) (internal quotations omitted); *In re Bilski*, 545 F.3d 943, 954 (Fed. Cir. 2008) ("*Bilski I*"). The Court has described the

> framework for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts. First, we determine whether the claims at issue are directed to one of those patent-ineligible concepts. If so, we then ask, "[w]hat else is there in the claims before us?" To answer that question, we 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. We have described step two of this analysis as a search for an "'inventive concept'"-i.e., an element or combination of elements that is "sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself."

Alice, 134 S.Ct. at 2355 (citing *Mayo*, 132 S.Ct. at 1294, 1296-98).[11]

"[T]o transform an unpatentable law of nature into a patent-eligible application of such a law, one must do more than simply state the law of nature while adding the words 'apply it.'" *Mayo*, 132 S.Ct. at 1294 (citing *Gottschalk v. Benson*, 409 U.S. 63, 71-72 (1972)) (emphasis omitted). It is insufficient to add steps which "consist of well-understood, routine, conventional activity," if such steps, "when viewed as a whole, add nothing significant beyond the sum of their parts taken separately." *Mayo*, 132 S. Ct. at 1298. "Purely 'conventional or obvious' '[pre]-solution activity' is normally not sufficient to transform an unpatentable law of nature into a patent-eligible application of such a law." *Id.* (citations omitted). Also, the "prohibition against

---

[11] The machine-or-transformation test still may provide a "useful clue" in the second step of the *Alice* framework. *Ultramercial, Inc. v. Hutu, LLC*, 772 F.3d 709, 716 (Fed. Cir. 2014) (citing *Bilski II*, 561 U.S. at 604 and *Bancorp Servs., L.L.C. v. Sun Life Assurance Co. of Can.*, 687 F.3d 1266, 1278 (Fed. Cir. 2012)). A claimed process can be patent-eligible under § 101 if: "(1) it is tied to a particular machine or apparatus, or (2) it transforms a particular article into a different state or thing." *Bilski I*, 545 F.3d at 954, aff'd on other grounds, *Bilski II*, 561 U.S. 593.

patenting abstract ideas 'cannot be circumvented by attempting to limit the use of the formula to a particular technological environment' or adding 'insignificant post-solution activity.'" *Bilski II*, 561 U.S. at 610-11 (citation omitted). For instance, the "mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention." *Alice*, 134 S.Ct. at 2358. "Given the ubiquity of computers, wholly generic computer implementation is not generally the sort of 'additional featur[e]' that provides any 'practical assurance that the process is more than a drafting effort designed to monopolize the [abstract idea] itself.'" *Id.* (citations omitted).

Because computer software comprises a set of instructions,[12] the first step of *Alice* is, for the most part, a given; i.e., computer-implemented patents generally involve abstract ideas. The more difficult part of the analysis is subsumed in the second step of the *Alice* analysis, that is, determining whether the claims "merely recite the performance of some business practice known from the pre-Internet world along with the requirement to perform it on the Internet," or whether the claims are directed to "a problem specifically arising in the realm of computer technology" and the claimed solution specifies how computer technology should be manipulated to overcome the problem. *DDR Holdings, LLC v. Hotels.Com, L.P.*, 773 F.3d 1245, 1257 (Fed. Cir. 2014).

---

[12] Or, to put it another way, software generally comprises a method "of organizing human activity." *Intellectual Ventures I LLC v. Capital One Bank (USA)*, 792 F.3d 1363, 1367-68 (Fed. Cir. 2015) (citing *Alice*, 134 S.Ct. 2351-52, and *Bilski II*, 561 U.S. at 599).

Since providing that explanation, the Federal Circuit has not preserved the validity of any other computer-implemented invention under § 101.[13] Indeed, in reviewing post-*Alice* cases such as *DDR* and *Intellectual Ventures*, the court is struck by the evolution of the § 101 jurisprudence, from the complete rejection of patentability for computer programs[14] to the almost complete acceptance of such,[15] to the current (apparent) requirements that the patent claims in suit (1) disclose a problem "necessarily rooted in computer technology," and (2) claim a solution that (a) not only departs from the "routine and conventional" use of the technology, but (b) is sufficiently specific so as to negate the risk of pre-emption. *See DDR*, 773 F.3d at 1257; *Intellectual Ventures*, 792 F.3d at 1371. In other words, even though most of the patent claims now being challenged under § 101 would have survived such challenges if

[13] *See, e.g.*, *In re Smith*, Civ. No. 2015-1664, 2016 WL 909410 (Fed. Cir. Mar. 10, 2016); *Mortgage Grader, Inc. v. First Choice Loan Servs. Inc.*, 811 F.3d 1314 (Fed. Cir. 2016); *Vehicle Intelligence and Safety LLC v. Mercedes-Benz USA, LLC*, Civ. No. 2015-1411, 2015 WL 9461707 (Fed. Cir. Dec. 28, 2015); *Versata Dev. Grp., Inc. v. SAP America, Inc.*, 793 F.3d 1306 (Fed. Cir. 2015); *Intellectual Ventures*, 792 F.3d 1363; *Internet Patents Corp. v. Active Network, Inc.*, 790 F.3d 1343 (Fed. Cir. 2015); *O/P Techs., Inc. v. Amazon.com, Inc.*, 788 F.3d 1359 (Fed. Cir. 2015); All*voice Devs. US, LLC v. Microsoft Corp.*, 612 Fed. Appx. 1009 (Fed. Cir. 2015); *Content Extraction and Transmission LLC v. Wells Fargo Bank, Nat'l Ass'n*, 776 F.3d 1343 (Fed. Cir. 2014).

[14] *See, e.g.*, 33 Fed. Reg. 15581, 15609-10 (1968), and Justice Steven's dissent in *Diehr*, whose solution was to declare all computer-based programming unpatentable, 450 U.S. at 219.

[15] *State Street Bank & Trust Co. v. Signature Fin. Group, Inc.*, 149 F.3d 1368 (Fed. Cir. 1998), abrogated by *Bilski I*, in which "a computer-implemented invention was considered patent-eligible so long as it produced a 'useful, concrete and tangible result.'" *DDR*, 773 F.3d at 1255 (citing *State Street Bank*, 149 F.3d at 1373).

mounted at the time of issuance, these claims are now in jeopardy under the heightened specificity required by the Federal Circuit post-*Alice*. Moreover, it is less than clear how a § 101 inquiry that is focused through the lens of specificity can be harmonized with the roles given to other aspects of the patent law (such as enablement under § 112 and non-obviousness under § 103),[16] especially in light of the Federal Circuit's past characterization of § 101 eligibility as a "coarse" gauge of the suitability of broad subject matter categories for patent protection. *Research Corp. Techs., Inc. v. Microsoft Corp.*, 627 F.3d 859, 869 (Fed. Cir. 2010). Given the evolving state of the law, the § 101 analysis should be, and is, a difficult exercise.[17] At their broadest, the various decisions of the Federal Circuit[18] would likely

---

[16] Indeed, Judge Plager, in his dissent in *Dealertrack*, suggested that,

> as a matter of efficient judicial process I object to and dissent from that part of the opinion regarding the '427 patent and its validity under § 101, the section of the Patent Act that describes what is patentable subject matter. I believe that this court should exercise its inherent power to control the processes of litigation ... , and insist that litigants, and trial courts, initially address patent invalidity issues in infringement suits in terms of the defenses provided in the statute: "conditions of patentability," specifically §§ 102 and 103, and in addition §§ 112 and 251, and not foray into the jurisprudential morass of § 101 unless absolutely necessary.

Dealertrack, 674 F.3d at 1335. *But see CLS Bank Int'l v. Alice Corp. Pty.*, 717 F.3d 1269, 1277 (Fed. Cir. 2013), *aff'd*, 134 S. Ct. 2347 (2014).

[17] And, therefore, not an exercise that lends itself to, e.g., shifting fees pursuant to 35 U.S.C. § 285.

[18] *See, e.g.*, *Dealertrack*, where the claim was about as specific as that examined in DDR, yet the Federal Circuit found the patent

ring the death-knell for patent protection of computer-implemented inventions,[19] a result not clearly mandated (at least not yet). On the other hand, to recognize and articulate the requisite degree of specificity—either in the equipment used[20] or the steps claimed[21]—that transforms an abstract idea into patent-eligible subject matter is a challenging task. In trying to sort through the various iterations of the § 101 standard, the court looks to *DDR* as a benchmark; i.e., the claims (informed by the specification) must describe a problem and solution rooted in computer technology, and the solution must be (1) specific enough to preclude the risk of pre-emption, and (2) innovative enough to "override the routine and conventional" use of the computer. *DDR*, 773 F. 3d at 1258-59.

---

deficient because it did "not specify how the computer hardware and database [were] **specially programmed** to perform the steps claimed in the patent," 674 F.3d at 1333-34 (emphasis added). The disclosure of such programming details would likely nullify the ability of a patentee to enforce the patent, given the ease with which software can be tweaked and still perform the desired function.

[19] Ironically so, given the national concerns about piracy of American intellectual property.

[20] *See, e.g., SiRF Tech., Inc. v. Int'l Trade Comm'n*, 601 F.3d 1319 (Fed. Cir. 2010), a case where the Federal Circuit found that a GPS receiver was "integral" to the claims at issue. The Court emphasized that a machine will only "impose a meaningful limit on the scope of a claim [when it plays] a significant part in permitting the claimed method to be performed, rather than function solely as an obvious mechanism for permitting a solution to be achieved more quickly, i.e., through the utilization of a computer for performing calculations." *Id.* at 1333.

[21] *See, e.g., DDR*, 773 F.3d at 1257-58; *TQP Dev., LLC v. Intuit Inc.*, Civ. No. 12-180, 2014 WL 651935 (E.D. Tex. Feb. 19, 2014); *Paone v. Broadcom Corp.*, Civ. No. 15- 0596, 2015 WL 4988279 (E.D.N.Y. Aug. 19, 2015).

2. Analysis

Applying the analytical framework of *Alice*, the court first "determine[s] whether the claims at issue are directed to one of those patent-ineligible concepts," namely, laws of nature, natural phenomena, and abstract ideas. 134 S.Ct. at 2354-55. Cisco argues that the claims are directed to the abstract idea "of monitoring and analyzing data from multiple sources to detect broader patterns of suspicious activity," which is "a fundamental building block of intelligence gathering and network security." (D.I. 159 at 7) Cisco analogizes this idea to a number of spy and security gathering endeavors, including "networks [employed by] ancient Chinese military strategists and both sides during the Revolutionary War" and police departments using crime reports to detect "broader patterns of criminal activity." (*Id.* at 7-8) More specifically, Cisco argues that humans can perform each of the steps of the method (detecting suspicious network activity, generating reports of said activity, and receiving and integrating the reports), concluding that it is a process that may be performed in the human mind or using a pen and paper, thus, unpatentable. (*Id.* at 10-11) SRI disagrees, pointing out that a human would need to use hardware and software in order to examine network traffic. (D.I. 179 at 10-12)

That Cisco can simplify the invention enough to find a human counterpart (or argue that a human could somehow perform the steps of the method) does not suffice to make the concept abstract, as "[a]t some level, 'all inventions ... embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas.'" *Alice*, 134 S.Ct. at 2354 (quoting *Mayo*, 132 S.Ct. at 1293). The patents address the vulnerability of computer networks' "interoperability and sophisticated

integration of technology" to attack. (1:37-40) The claims at bar are, therefore, more complex than "merely recit[ing] the performance of some business practice known from the pre-Internet world along with the requirement to perform it on the Internet," and are better understood as being "necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks." *DDR*, 773 F.3d at 1257.

Turning to step two of the *Alice* framework, Cisco argues that the claims do not provide an inventive concept, describing the method as follows: A first step reciting conventional pre-solution activity (configuring and installing software); a generic and abstract second step (analyzing data from certain categories); a non-inventive third and fourth step (generating and receiving reports at a centralized computer); and, a fifth step (combining reports to create new information). (D.I. 159 at 12-14) According to Cisco, the patents recite generic computers, i.e., the network monitors, which the parties have agreed are "software and/or hardware that can collect, analyze and/or respond to data." (*Id.* at 16; D.I. 47 at 1) The patents explain that "[s]election of packets can be based on different criteria" (5: 12-38) and the claims at bar identify "particular categories of network traffic data ... well suited for analysis in determining whether network traffic was suspicious when used in a hierarchical system." (D.I. 179 at 12) As to the hierarchical analysis, the patents explain that the "tiered collection and correlation of analysis results allows monitors 16a-16f to represent and profile global malicious or anomalous activity that is not visible locally." (8:53-56) The claims as an ordered combination (in light of the specification) sufficiently delineate "how" the method is performed to "improve the functioning of

the computer itself," thereby providing an inventive concept. *Alice*, 134 S.Ct. at 2359. The same specificity suffices to negate the "risk [of] disproportionately tying up the use of the underlying ideas." *Alice*, 134 S.Ct. at 2354; *Mayo*, 132 S.Ct. at 1294. Cisco's motion for invalidity (D.I. 158) is denied.

B. Anticipation

1. Standard

Under 35 U.S.C. § 102(b), "[a] person shall be entitled to a patent unless the invention was patented or described in a printed publication in this or a foreign country ... more than one year prior to the date of the application for patent in the United States." The Federal Circuit has stated that "[t]here must be no difference between the claimed invention and the referenced disclosure, as viewed by a person of ordinary skill in the field of the invention." *Scripps Clinic & Research Found. v. Genentech, Inc.*, 927 F.2d 1565, 1576 (Fed. Cir. 1991). In determining whether a patented invention is explicitly anticipated, the claims are read in the context of the patent specification in which they arise and in which the invention is described. *Glaverbel Societe Anonyme v. Northlake Mktg. & Supply, Inc.*, 45 F.3d 1550, 1554 (Fed. Cir. 1995). The prosecution history and the prior art may be consulted if needed to impart clarity or to avoid ambiguity in ascertaining whether the invention is novel or was previously known in the art. *Id.* The prior art need not be ipsissimis verb is (i.e., use identical words as those recited in the claims) to be anticipating. *Structural Rubber Prods. Co. v. Park Rubber Co.*, 749 F.2d 707, 716 (Fed. Cir. 1984).

A prior art reference also may anticipate without explicitly disclosing a feature of the claimed invention if that missing characteristic is inherently present in the single anticipating reference. *Continental Can Co. v. Monsanto Co.*, 948 F.2d 1264, 1268 (Fed. Cir. 1991). The Federal Circuit has explained that an inherent limitation is one that is necessarily present and not one that may be established by probabilities or possibilities. *Id.* That is, "[t]he mere fact that a certain thing may result from a given set of circumstances is not sufficient." *Id.* The Federal Circuit also has observed that "[i]nherency operates to anticipate entire inventions as well as single limitations within an invention." *Schering Corp. v. Geneva Pharms. Inc.*, 339 F.3d 1373, 1380 (Fed. Cir. 2003). Moreover, recognition of an inherent limitation by a person of ordinary skill in the art before the critical date is not required to establish inherent anticipation. *Id.* at 1377.

An anticipation inquiry involves two steps. First, the court must construe the claims of the patent in suit as a matter of law. *Key Pharms. v. Hereon Labs Corp.*, 161 F.3d 709, 714 (Fed. Cir. 1998). Second, the finder of fact must compare the construed claims against the prior art. *Id.* A finding of anticipation will invalidate the patent. *Applied Med. Res. Corp. v. U.S. Surgical Corp.*, 147 F.3d 1374, 1378 (Fed. Cir. 1998).

2. Analysis

Cisco moves for summary judgment that EMERALD 1997[22] anticipates the patents. (D.I. 182 at 10;

[22] Philip Porras and Peter G. Neumann, *EMERALD: Event Monitoring Enabling Response to Anomalous Live Disturbances*, Proceedings of the 20th National Information Systems Security Conference (October 1997).

D.I. 186, ex. 3) EMERALD 1997 has been discussed in the court's prior opinions and by the Federal Circuit. *SRI*, 647 F. Supp. 2d at 333-34 (citing *SRI*, 456 F. Supp. 2d at 626); *SRI*, 511 F.3d at 1188-89. In short, EMERALD 1997 is a conceptual overview of the EMERALD system, the brainchild of SRI's EMERALD project on intrusion detection, published by Phillip Porras and Peter G. Neumann (both SRI employees) on behalf of SRI in October 1997. EMERALD 1997 contains a detailed description of SRI's early research in Intrusion Detection Expert System ("IDES") technology, and outlines the development of the Next Generation IDES ("NIDES") for detecting network anomalies. *Id.* at 334. The parties do not dispute that EMERALD 1997 is 35 U.S.C. § 102(b) prior art to the patents at issue. EMERALD 1997 is listed as a reference on the face of the '615 patent. The parties dispute only whether EMERALD 1997 discloses detection of any of the network traffic data categories listed in claim 1 of the '203 and '615 patents and whether EMERALD 1997 is enabled. One of the claimed categories of network traffic is "network connection requests."

EMERALD 1997 "introduces a hierarchically layered approach to network surveillance," pointing out that "[m]echanisms are needed to provide realtime detection of patterns in network operations that may indicate anomalous or malicious activity, and to respond to this activity through automated countermeasures." (D.I. 186, ex. 3 at 354-55) EMERALD 1997 describes in relevant part:

> The subscription list field is an important facility for gaining visibility into malicious or anomalous activity outside the immediate environment of an EMERALD monitor. The most obvious examples where relationships are im-

> portant involve interdependencies among network services that make local policy decisions. Consider, for example, the interdependencies between access checks performed during network file system ["NFS"] mounting and the IP mapping of the DNS service. An unexpected mount monitored by the network file system service may be responded to differently if the DNS monitor informs the network file system monitor of suspicious updates to the mount requester's DNS mapping.

(D.I. 186, ex. 3 at 358; D.I. 221, ex. A at~ 55) EMERALD 1997 further explains that "[a]bove the service layer, signature engines scan the aggregate of intrusion reports from service monitors in an attempt to detect more global coordinated attack scenarios or scenarios that exploit interdependencies among network services. The DNS/NFS attack discussed in Section III-B is one such example of an aggregate attack scenario." (D. I. 186, ex. 3 at 360)

Cisco's expert, Dr. Clark, explains that one of ordinary skill in the art would understand from the disclosures of EMERALD 1997 that "detecting the 'DNS/NFS attack discussed in Section III-B' of EMERALD 1997 would require analysis of network connection requests." He also opines that "[a]n NFS mount involves a network connection request and thus the network file system monitor disclosed in EMERALD 1997 would detect suspicious mounts by examining and analyzing network connection request packets." He concludes:

> A person of ordinary skill in the art would understand that monitoring specific network services ... would require detecting and analyzing

> packets indicative of those well-known network service protocols, one of the enumerated categories in claim 1 of the '615 patent. EMERALD 1997 additional[ly] discloses two protocol-specific monitors in the "DNS/NFS attack discussed in Section 111-B" of EMERALD 1997 (p. 360): the "DNS monitor" and "the network file system monitor." (p. 358). A monitor that observes only a specific network protocol, such as DNS or NFS, would monitor and analyze packets indicative of those well-known service protocols while ignoring other packets that are not indicative or DNS or NFS.

(D.I. 185, ex. A at ,m 104-05) SRI's expert, Dr. Lee, opines that "Dr. Clark makes several unsupportable leaps of inference" in his analysis. More specifically, although EMERALD 1997 describes "monitoring certain computer system activities," Dr. Lee does not agree that "such monitoring must be done using not only data obtained from the direct examination of network packets but also corresponding to one of the enumerated categories of such data." (D.I. 221, ex. A at~ 54) (emphasis omitted) Dr. Lee opines that,

> [w]hile it may be true that an "NFS mount involves a network connection request" it is clear that EMERALD 1997 makes no indication that directly monitoring network packets categorized as "network connection requests" is the way to detect suspicious NFS mounts. Indeed, EMERALD 1997 does not even suggest that directly monitoring network packets in general and analyzing the data obtained from them (as opposed to host audit logs or some other data source)—let alone any specific type of network traffic data—is the way to detect suspicious

> NFS mounts. As explained above, EMERALD 1997 merely identifies a range of possible sources of data for analysis and a few examples of suspicious behavior that the yet-to-be designed EMERALD system should be able to detect (such as the aforementioned NFS mounts and DNS table updates). However, none of the disclosure of EMERALD specifically teaches using the data obtained from packets transporting these requests ....

(*Id.* at ¶ 55) Dr. Lee concludes:

> Merely reciting monitoring network services does not disclose to or enable one of skill in the art to practice the claimed inventions of detecting suspicious network activity based on analysis of network traffic data (data obtained from the direct examination of network packets) selected from, inter alia, well known network service protocols.

(*Id.* at ¶ 56) (emphasis omitted)

Cisco cites to a single case, *Kennametal, Inc. v. Ingersoll Cutting Tool Co.*, 780 F.3d 1376 (Fed. Cir. 2015), in arguing that "a reference can anticipate a claim even if it 'd[oes] not expressly spell out' all the limitations arranged or combined as in the claim, if a person of skill in the art, reading the reference, would 'at once envisage' the claimed arrangement or combination." *Id.* at 1381 (citation omitted); (D.I. 184 at 10) The underlying facts in *Kennametal*, however, are distinguishable from those at bar. In *Kennametal*, it was not disputed that the reference ("Grab") expressly recited all the elements of the asserted claim; the only question was "whether the number of categories and components" disclosed in Grab was so large that the claimed

combination "would not be immediately apparent to one of ordinary skill in the art." *Id.* at 1382. The Federal Circuit declared that, "[a]t the very least, Grab's express 'contemplat[ion]'" of the claimed combination was "sufficient evidence that a reasonable mind could find that a person of skill in the art, reading Grab's claim 5, would **immediately envisage**" the asserted combination. *Id.* at 1383 (emphasis added). The Court concluded:

> Thus, substantial evidence supports the Board's conclusion that Grab effectively teaches 15 combinations, of which one anticipates pending claim 1.
>
> Though it is true that there is no evidence of "actual performance" of combining the ruthenium binder and PVD coatings, this is not required. … "Rather, anticipation only requires that those suggestions be enabled to one of skill in the art."

Id. (citations omitted).

Unlike the facts in *Kennametal*, EMERALD 1997 does not expressly recite all the limitations of the asserted claims, specifically, the analysis of network traffic data from at least one of the enumerated categories. Nor does Cisco argue that the missing limitation is inherently disclosed in the reference. Instead, the essence of what Cisco argues is that, because EMERALD 1997 discloses monitoring of network traffic data in general, it would be obvious to a person of ordinary skill in the art to detect "suspicious activity by analysis of particular network traffic data that falls within at least one of the enumerated categories in the claims." (D.I. 184 at 12) Cisco reasons in this regard that EMERALD 1997 identifies a type of attack as a target for

EMERALD 1997's signature engines, that such an attack involves a "network connection request" (one of the specifically enumerated categories of network traffic data in the asserted claims), and that "network packets indicating a network connection request would be the natural source to use" for the detection. (*Id.* at 12-13)

Based on the record presented, the court concludes that no reasonable jury could find that EMERALD 1997 discloses all the limitations arranged as in the asserted claims. As noted above, the court starts with the premise that the very case law cited by Cisco is distinguishable on its facts in a dramatic way. Without EMERALD 1997 expressly (or inherently) disclosing all of the limitations of the asserted claims,[23] the rest of *Kennametal*'s teaching must be tempered with the reality that anticipation cannot be based on the multiple layers of supposition created by Cisco to construct its theory of anticipation[24] and still meet the requirement that the claimed limitation be immediately apparent. Although Cisco has attempted to package its anticipation argument in slightly different language than liti-

[23] Which was also the starting point for the court's anticipation analysis in the prior case. In that case, SRI did not argue that EMERALD 1997 failed to disclose each of the limitations of the asserted claims of U.S. Patent 6,708,212 (the '212 patent"), instead, SRI contended that EMERALD 1997 was not an enabling disclosure with respect to the '212 patent. The court determined that EMERALD 1997 enabled statistical profiling of network traffic, therefore, anticipated the '212 patent, in part based on the similarities between the '212 specification and EMERALD 1997. *SRI*, 456 F. Supp. 2d at 632-35; *SRI*, 511 F.3d at 1192-94.

[24] Starting with the suggestion that EMERALD 1997 directs monitoring a target specific event stream and including the argument that network packets, rather than, e.g., host audit data, would be the natural source to use.

gants have in prior litigation,[25] the argument fails as a matter of law. The court denies Cisco's motion for summary judgment in this regard and grants, *sua sponte*, summary judgment of no anticipation by EMERALD 1997.[26] *See Anderson v. Wachovia Mortg. Corp.*, 621 F.3d 261, 280 (3d Cir. 2010) (quoting *Celotex Corp. v. Catrett*, 477 U.S. 317, 326 (19,86)) ("[D]istrict courts are widely acknowledged to possess the power to enter summary judgments sua sponte, so long as the losing party was on notice that [it] had to come forward with all of [its] evidence."); *see also Talecris Biotherapeutics, Inc. v. Baxter Int'l, Inc.*, 510 F. Supp. 2d 356, 362 (D. Del. 2007) (This court has held that when one party moves for summary judgment against an adversary, Fed.R.Civ.P. 54(c) and 56, when read together, give the court the power to render a summary judgment for the adversary if it is clear that the case warrants that result, even though the adversary has not filed a cross-motion for summary judgment.).

C. Prior Art

1. Standard

The "printed publication" bar of 35 U.S.C. § 102 states:

A person shall be entitled to a patent unless—

---

[25] A jury found that the '615 and '203 patents were not anticipated by EMERALD 1997 and such verdict was upheld by the court, which opinion was affirmed by the Federal Circuit. *SRI*, 647 F. Supp. 2d 323 (opinion after jury trial), 401 Fed App'x 530.

[26] The court does not address the issue of enablement, but notes that its prior finding—that EMERALD 1997 enabled statistical profiling of network traffic generally—does not necessarily mean that it is an enabling disclosure for the limitations at issue.

> ...
>
> (b) the invention was patented or described in a printed publication in this or a foreign country ... more than one year prior to the date of the application for patent in the United States ... .

"The bar is grounded on the principle that once an invention is in the public domain, it is no longer patentable by anyone." *In re Hall*, 781 F.2d 897, 898 (Fed. Cir. 1986) (citing *In re Bayer*, 568 F.2d 1357, 1361 (C.C.P.A. 1978)). The touchstone in determining whether a reference constitutes a "printed publication" under 35 U.S.C. § 102(b) is "public accessibility." *Id.* at 899 (citing *In re Bayer*, 568 F.2d at 1359; *In re Wyer*, 655 F.2d 221, 224 (C.C.P.A. 1981)).

> A given reference is "publicly accessible" upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it and recognize and comprehend therefrom the essentials of the claimed invention without need of further research or experimentation.

Bruckelmyer v. Ground Heaters, Inc., 445 F.3d 1374, 1378 (Fed. Cir. 2006) (citing *In re Wyer*, 655 F.2d at 226); *see also Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1568 (Fed. Cir. 1988) ("Accessibility goes to the issue of whether interested members of the public could obtain the information if they wanted to."). The determination of whether a reference is a "printed publication" under § 102(b) involves a case-by-case inquiry into the facts and circumstances surrounding the reference's disclosure to persons of skill in the art. *In re Cronyn*, 890 F.2d 1158, 1161 (Fed. Cir. 1989) (citing

In re Hall, 781 F.2d at 899; *In re Wyer*, 655 F.2d at 227).

"The law has long looked with disfavor upon invalidating patents on the basis of mere testimonial evidence absent other evidence that corroborates that testimony." *Finnigan Corp. v. Int'l Trade Comm'n*, 180 F.3d 1354, 1366 (Fed. Cir. 1999). Invalidating "activities are normally documented by tangible evidence such as devices, schematics, or other materials that typically accompany the inventive process." *Finnigan*, 180 F.3d at 1366 (citing *Woodland Trust v. Flowertree Nursery, Inc.*, 148 F.3d 1368, 1373 (Fed. Cir. 1998)). Corroboration applies to any subsections of § 102:

> [A] witness's uncorroborated testimony is equally suspect as clear and convincing evidence if he testifies concerning the use of the invention in public before invention by the patentee (§ 102(a)), use of the invention in public one year before the patentee filed his patent (§ 102(b)), or invention before the patentee (§ 102(g)).

Martek Biosciences Corp. v. Nutrinova, Inc., 579 F.3d 1363, 1375 n.4 (Fed. Cir. 2009). "When determining whether [a witness'] testimony is sufficiently corroborated, we apply a rule-of-reason analysis and consider all pertinent evidence" to determine whether the story is credible. *Martek*, 579 F.3d at 1374 (citing *Sandt Tech., Ltd. v. Resco Metal & Plastics Corp.*, 264 F.3d 1344, 1350 (Fed. Cir. 2001)).

2. NetRanger

To establish that the NetRanger Guide for Version 1.3.1[27] ("NetRanger 1.3.1 ") is prior art, Cisco offers the following evidence.[28] NetRanger 1.3.1 has a copyright date of 1997 and includes an example of an "interactive component of an event query" wherein the date provided for the event is May 1, 1997. (D.I. 186, ex. 4 at 1, 5-23) James Kasper ("Kasper"), a former employee of WheelGroup who joined the company in 1996 and who worked on the NetRanger technology (including versions 1.0, 1.1, 1.2, 1.3.1), testified that he was involved "with the tech writers for drafting, editing, and polishing the material related to the software components [he] worked on." (D.I. 186, ex. 12 at 25:20-26: 10, 28:3-20) Kasper testified that NetRanger 1.3.1 was prepared "as a reference for ... customers" and was provided to the customers in the "summer [of 19]97, but before the 2.0 release which was later, maybe fall [of 19]97." (*Id.* at 28:21-29:2, 70:8-10, 112:3-10) He stated that the soft-

---

[27] NetRanger is the user's guide covering installation, configuration, and operation of the NetRanger System.

[28] Daniel Teal ("Teal"), co-founder of WheelGroup, provided a declaration in the exparte reexamination stating that version 1.3.1 was released prior to version 2.0, which was released on August 25, 1997. Teal also stated that the user's guide "was provided along with each sale of the NetRanger product version 1.3.1" or if requested by a potential customer. (D.I. 238, ex. 47 at ¶¶ 14-15) He stated that a sales list from Wheel Group showed that there were numerous customers of WheelGroup that had "maintenance" contracts in place in the summer of 1997. (*Id.* at ¶ 15 and ex. C) Teal testified that the majority of customers had maintenance contracts, whereby they would receive the latest version and user guide automatically when released. (D.I. 238, ex. 48 at 201:21-202:2) SRI points out that Teal is not a witness in the current case and his "opinion is based on the same speculation and inference as found in the declaration of Mr. Kasper." (D.I. 251 at 8 n.4)

ware versions would be released consecutively and customers received the software version along with the corresponding user guide. Maintenance contract customers received the latest version of the software and the corresponding user guide automatically. (*Id.* at 23:25-24:22; D.I. 239 at ¶¶ 4-5) He further testified that the user guide was created in 1997 by employees of WheelGroup as part of its regular business. (D.I. 186, ex. 12 at 30:2-21) He testified that he was "not really sure," but thought the tech writers would send the user guides out to Kinkos to print. (*Id.* at 120: 13-122: 18) He testified (based on presentation slides[29] "probably [created by] a collaboration of marketing and tech writing with review by engineering") that version 2.0 was released on or about August 1, 1997. (*Id.* at 114:20-117:23) Kasper's declaration includes a WheelGroup price list dated September 11, 1997 listing a user guide for sale and stating that one guide is included with the product. (D.I. 239 at ¶ 15, ex. F) A report from the U.S. Air Force Information Warfare Center in February 1997 described its assessment of NetRanger version 1.1. (D.I. 186, ex. 23) A press release on August 25, 1997 issued by WheelGroup announced the release of version 2.0. (*Id.*, ex. 24) SRI questions the authenticity of the WheelGroup documents on which Kasper relies. Moreover, SRI points out that Kasper relies on documents which he himself seeks to authenticate.

The record at bar contains no direct evidence that a member of the public actually received NetRanger 1.3.1. Indeed, the sales list showing maintenance cus-

---

[29] A business plan presentation titled "1997 Business Plan Overview." Page 18 is titled "Development Schedule - 1997" and provides a list of dates including May 16, 1997, version 1.3, "Enhanced default signatures, NetView Support, digital licensing" and August 1, 1997, version 2.0. (D.I. 223, ex. F)

tomers does not indicate which versions of software and the corresponding user guide were actually distributed to such customers. The price list does not state a particular version of the user guide for sale. While the versions of NetRanger software (like any software) would typically be released in numerical order (and allegedly be accompanied by a user guide), the record at bar does not establish that version 1.3.1 was actually disseminated. On the record at bar, the court concludes that NetRanger 1.3.1 was not "publically accessible" and grants SRI's motion that NetRanger 1.3.1 is not prior art.[30]

3. Hunteman

Cisco contends that Hunteman[31] was presented at the Proceedings of the 20th National Information Systems Security Conference in October 1997. Hunteman is listed in the table of contents for the conference[32] at page 394 and Cisco has provided the paper incorporated into the conference materials with corresponding pagination. (D.I. 223, ex. J at 3; D.I. 238, ex. 51 at 394) SRI contends that Cisco has not provided evidence that William Hunteman "attended the conference, if he presented at the conference, what he presented at the conference, or when the papers were distributed following the conference." (D.I. 251 at 17)

"The publication requirement may ... be satisfied by distributing or making the paper available at a confer-

---

[30] As such, Cisco's motion that the combination of EMERALD 1997 and NetRanger renders the asserted claims obvious is denied.

[31] William Hunteman, *Automated Information System - (AIS) Alarm System*.

[32] As is EMERALD 1997.

ence where persons interested or skilled in the subject matter of the paper were told of the paper's existence and informed of its contents." *Friction Div. Products, Inc. v. E.I. DuPont de Nemours & Co.*, 658 F. Supp. 998, 1008 (D. Del. 1987) aff'd sub nom. *Friction Div. Products, Inc. v. E.I. du Pont de Nemours & Co.*, 883 F.2d 1027 (Fed. Cir. 1989) (citing *Massachusetts Institute of Technology v. AB Fortia*, 774 F.2d 1104, 1109 (Fed. Cir. 1985)); cf *Norian Corp. v. Stryker Corp.*, 363 F.3d 1321, 1330 (Fed. Cir. 2004) ("Although there was testimony that it was the general practice at IADR meetings for presenters to hand out abstracts to interested attendees, the lack of substantial evidence of actual availability of the Abstract adequately supports the court's conclusion that dissemination of the Abstract was not established."). The court concludes that the inclusion of Hunteman in the conference materials (independent from whether William Hunteman attended the conference) is sufficient to make it "publically accessible."

V. NON-INFRINGEMENT

A. Standard

When an accused infringer moves for summary judgment of non-infringement, such relief may be granted only if one or more limitations of the claim in question does not read on an element of the accused product, either literally or under the doctrine of equivalents. *See Chimie v. PPG Indus., Inc.*, 402 F.3d 1371, 1376 (Fed. Cir. 2005); *see also TechSearch, L.L.C. v. Intel Corp.*, 286 F.3d 1360, 1369 (Fed. Cir. 2002) ("Summary judgment of noninfringement is ... appropriate where the patent owner's proof is deficient in meeting an essential part of the legal standard for infringement, because such failure will render all other facts immate-

rial."). Thus, summary judgment of noninfringement can only be granted if, after viewing the facts in the light most favorable to the non-movant, there is no genuine issue as to whether the accused product is covered by the claims (as construed by the Court). *See Pitney Bowes, Inc. v. Hewlett-Packard Co.*, 182 F.3d 1298, 1304 (Fed. Cir. 1999).

B. Analysis

1. "Network traffic data" limitation

SRI accuses two of Cisco's product lines of infringing the asserted claims—stand-alone Cisco IPS Sensors ("IPS Sensors") and Sourcefire Sensors in combination with a Defense Center ("Sourcefire Sensors") (collectively, "the accused sensors"), as well as ancillary services for these products. The accused sensors' functionality is largely undisputed. The accused sensors obtain certain data from the network packet. The data is pre-processed. The pre-processed data is then put into a data structure and analysis is performed on the data structure. Specifically, the IPS Sensor captures network packets from a network interface and stores these in a packet buffer. The header portion of the stored packet is decoded, and relevant information is extracted, converted into host-byte order and stored in a new data structure called the "CIDS Header." The content portion of the stored packet is then subject to various pre-processing steps (reassembly, defragmentation, normalization and deobfuscation), and the resulting data derived from this pre-processing is stored in a separate data structure called the "CIDS Buffer." The CIDS Header and CIDS Buffer data structures are inspected and analyzed by a series of signature engines in order to detect undesirable network activity. Similarly, the Sourcefire Sensors capture network packets from a

network interface and store them in memory. The stored network packets then have their header decoded, and the packet content is subjected to similar pre-processing steps. The decoded header data and the pre-processed packet data are stored in a synthetic packet data structure. The Sourcefire Sensors then run signature engines applying "Snort" rules against the synthetic packet data structure in order to detect undesirable network activity. (D.I. 208 at 11-13; D.I. 240 at 8-12)

The parties dispute whether the accused sensors meet the limitation "detecting suspicious network activity based on analysis of network traffic data."[33] The court construed "network traffic data" as "data obtained from direct examination of network packets." In prosecution, the patentee argued that "direct examination of network packets" was required and distinguished such examination from examining "logs or other information generated ... or otherwise gleaned" from "analysis of the network packets" or from analysis of a proxy of the network packets. The court concluded that the "disclaimer of claim scope, therefore, is broader than excluding host-based monitoring of audit logs, and explicitly extends to proxy information or 'other information generated therefrom or otherwise gleaned.'" (D.I. 138 at 2-3; D.I. 96 at JA3489)

The parties' experts apply the claim construction differently. SRI's expert, Dr. Lee, opines that the accused sensors "analyze data obtained from direct examination of network packets," by "captur[ing] each pack-

---

[33] Found in claim 13 of the '615 patent and claim 12 of the '203 patent. Claim 1 of the '615 patent and claim 1 of the '203 patent similarly recite "detecting, by the network monitors, suspicious network activity based on analysis of network traffic data."

et and then perform[ing] 'deep packet inspection.'" The accused sensors "obtain data from the headers and payload of each packet by directly examining each packet and its contents. For each packet, this data may then be stored in data structures in memory but the analysis is still performed on data that has been obtained from directly examining the received packets themselves." (D.I. 243, ex. A at ¶¶ 160, 199) According to Dr. Lee, Cisco's argument that "the analysis must occur directly upon network packets themselves" is incorrect. Dr. Lee opines that applying the court's construction, "the limitation does not exclude analysis of network traffic data that has been obtained from direct examination of network packets and then stored in memory." (*Id.* at ¶¶ 167-68, 206) He explains that the patents at issue "embrace that a network monitor may normalize, reassemble, defragment, or deobfuscate packets because SRI's patents teach that the network monitor may be deployed at a gateway and may perform 'application-layer monitoring.'" (*Id.* at ¶¶ 169, 207-208)

Cisco's expert, Dr. Clark, disagrees with Dr. Lee's analysis and opines that the accused sensors "analyze information derived from network packets that has been translated, reassembled, defragmented, normalized, and de-obfuscated." (D.I. 211, ex. A at ¶¶ 88, 303) Dr. Clark explains that such steps are necessary to avoid "evasion techniques." Without these pre-processing steps, the IPS sensor would not act like the destination device and "malicious actors can easily evade what protections the sensor is intended to provide." He concludes that "the derived information that results from this IP and TCP defragmentation is not data obtained from direct examination of network packets." (*Id.* at ¶¶ 90-91, 305) He opines further that "in the 1997-1998 time period, one of skill in the art

would not have understood that normalization, deobfuscation, defragmentation, and reassembly were required to obtain meaningful data, because the commercial systems available at that time did not do so." (*Id.* at ¶¶ 95, 310) Moreover, according to Dr. Clark, the "examination of ... translated data [from the CIDS header] does not involve direct examination of data obtained from network packets;" such examination is "even further removed from direct examination than the type of analysis discussed" in the prosecution history." (*Id.* at ¶¶ 98-101, 312-13)

Having reviewed the summary judgment record, the court concludes that the construction of "network traffic data" will benefit from clarification. In essence, Dr. Clark has opined that the current construction—"data obtained from direct examination of network packets"—requires that the analysis of such data take place without any further manipulation. The court, in its construction, did not mean to so narrowly (and unrealistically) confine the scope of the limitation. It is the court's understanding that there are many sources of data (besides network packets) that could be analyzed, as noted in the prosecution history[34] and in the prior art.[35] To say that the data "is obtained from direct examination of network packets" means to differentiate the original source of the data, not how or

[34] "[T]he claim language requires the suspicious network activity to follow from analysis of the network packets, not logs or other information generated therefrom or otherwise gleaned." (D.I. 96 at JA3489)

[35] "[T]he event stream mentioned in EMERALD 1997 may originate 'from a variety of sources including audit data, network datagrams, SNMP traffic, application logs, and analysis results from other intrusion-detection instrumentation."' (D.I. 220 at 32, citing EMERALD 1997 at 356, D.I. 186, ex. 3)

where the data is analyzed. As explained by Dr. Lee, the accused sensors obtain the data from the headers and payload of each packet and may store such data in data structures in memory. The data may then be normalized, reassembled, defragmented, or deobfuscated for purposes of analysis to detect suspicious network activity. (D.I. 243, ex A at ¶¶ 160-69) In other words, although the data obtained from the network packets is manipulated, each packet is captured in the first instance before it is examined. The fact that the data may be stored before analysis is performed on the data does not detract from its lineage.

As noted, Dr. Clark has offered an opinion that is inconsistent with the court's clarified construction. If he did not specifically address Dr. Lee's opinion in the alternative, the court will have to address the issue at the pretrial conference. The court denies Cisco's motion in this regard.[36]

2. "Hierarchical monitor" limitation

The IPS Sensor uses software, including a SensorApp process, responsible for inspecting traffic flowing on a network and detecting undesirable network activity. The SensorApp process uses a variety of signature engines that match data from network packets to a set of predefined "signatures." If a signature engine detects a match, then the IPS Sensor will generate an event, drop the network traffic, modify the network traffic, or take no action at all, depending upon how the device is configured. The SensorApp process is a mul-

[36] Cisco's argument that the doctrine of equivalents is inapplicable based on prosecution history disclaimer is also informed by the court's analysis above and will be addressed, as needed, at the pre-trial conference if the parties cannot reach agreement.

tithreaded process with one or more "SensorApp processing threads." The Meta Event Generator (a particular signature engine) is contained within a "SensorApp processing thread" and inspects events generated by the other signature engines to determine if they match any Meta Signature. If there is a match, the Meta Event Generator creates a Meta Event that is then forwarded (along with the other events) from the IPS Sensor to management devices such as the Cisco Security Manager. (D.I. 208 at 5-6)

The parties agreed during claim construction that a "network monitor" is "software and/or hardware that can collect, analyze and/or respond to data" and a "hierarchical monitor" is "a network monitor that receives data from at least two network monitors that are at a lower level in the analysis hierarchy." (D.I. 47 at 1-2) Dr. Lee opines that the Meta Event Generator is a hierarchical monitor, which applies meta-signatures to each IPS event. The meta-signatures operate on IPS events rather than on network traffic data. He explains that "any and all of the 'monitors' may be either hardware or software based so long as the hardware or software modules exist in a hierarchy, as required by the claims. One of skill in the art would understand that multiple network monitors and a hierarchical monitor may all be software modules and may all be deployed within the same hardware box." (D.I. 243, ex. A at ¶¶ 311-313) Dr. Clark disagrees and opines that the SensorApp threads are not separate software programs and, therefore, the Meta Event Generator "cannot be a hierarchical monitor because it does not receive events from at least two network monitors that are at a lower level in the analysis hierarchy." (D.I. 211, ex. A at ¶¶ 78, 141) He further explains that "treating individual signature engines as network mon-

itors is inconsistent with the" patents at issue, because the specification "draws a distinction between network monitors and signature engines." Specifically, "[s]ignature engines exist within a network monitor; they are not network monitors themselves." (*Id.* at 11140)

According to Cisco, the Meta Event Generator is an integral part of the SensorApp processing thread and, therefore, is not at a higher level in the analysis hierarchy. (D.I. 208 at 16) In other words, Cisco argues that the SensorApp processing thread cannot simultaneously be both the alleged "network monitor" and "hierarchical monitor" under the claims, because they are not "separate and distinct structures." (D.I. 250 at 9-10) The claim language and the parties' constructions do not require that the "network monitor" and "hierarchical monitor" be separate structures. Indeed, as pointed out by Dr. Lee, all of the "monitors" in the claims could be software. The court concludes that the expert opinions present factual disputes on whether the Meta Event Generator meets the claim limitation. Such disagreements are issues of material fact and will be left to a jury. Cisco's motion is denied in this regard.[37]

3. Direct infringement by Cisco or its customers

The parties agree that not all uses of the accused sensors infringe. A patentee must "either point to spe-

[37] Cisco contends (in its reply brief) that SRI avoided accusing individual signature engines within a SensorApp processing thread of meeting the "network monitor" limitation and should be precluded from such argument. (D.I. 250 at 10) Such an evidentiary issue is better addressed at the pre-trial conference if the parties cannot reach agreement.

cific instances of direct infringement or show that the accused device necessarily infringes the patent in suit." *ACCO Brands v. ABA Locks Manufacturer Co., Ltd.*, 501 F.3d 1307, 1313 (Fed. Cir. 2007); *see also Dynacore Holdings Corp. v. U.S. Philips Corp.*, 363 F.3d 1263, 1275-76 (Fed. Cir. 2004). "Direct infringement can be proven by circumstantial evidence." *Vita-Mix Corp. v. Basic Holding, Inc.*, 581 F.3d 1317, 1326 (Fed. Cir. 2009) (citing *Moleculon Research Corp. v. CBS, Inc.*, 793 F.2d 1261, 1272 (Fed. Cir. 1986)). Such "[c]ircumstantial evidence 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) (citing *Lucent Techs., Inc. v. Gateway, Inc.*, 580 F.3d 1301, 1317 (Fed. Cir. 2009) ("[A] finding of infringement can rest on as little as one instance of the claimed method being performed during the pertinent time period.").

Cisco disputes whether SRI has provided sufficient evidence of direct infringement, arguing that SRI must show actual use of the accused sensors configured in an infringing manner. Dr. Lee opines that the IPS Sensors infringe in their default configuration and that Cisco instructs its customers not to disable the Meta Event Generator. (D.I. 243, ex. A at ¶ 86) The parties also dispute the meaning of a survey, wherein 60-64% of customers responded that they "currently use[d]" or "enabled" the Meta Event Generator.[38] That Cisco and

[38] Cisco points to the deposition testimony of the Home Depot corporate representative, agreeing that "Home Depot has not used any IDS functionality" in certain products as evidence that Home Depot "never enabled the IPS functionality of those products." (D.I. 250 at 11; D.I. 252, ex. 35 at 120:4-9) Such argument is unhelpful as it equates intrusion defense systems (IDS) and intrusion

its expert disagree with many of Dr. Lee's conclusions does not suffice to negate the evidence that SRI has put forward at the summary judgment stage.

As to the Sourcefire Sensors, the parties generally agree that the compliance engine (configured to provide the claimed integration/correlation functionality) is turned off by default, but some Cisco customers enable it. In order to infringe the claims, a customer must also write a particular compliance rule. (D.I. 240 at 30-32; D.I. 250 at 14-15) SRI provides the following circumstantial evidence of direct infringement: Customers enable the compliance engine; the Cisco user guide informs users how to "nest rules" after creating new rules; and, a certain customer, Trans Union, correlates multiple IPS events using the compliance engine. (D.I. 240 at 30-32) (citations omitted) Cisco and its expert disagree with the presentation, explanation, and conclusions drawn by SRI and its expert regarding whether such evidence demonstrates infringement. Such disagreements preclude summary judgment.

SRI contends that the IOC feature of the Sourcefire Managers performs the limitation "integrating the reports of suspicious activity, by one or more hierarchical monitors." (D.I. 243, ex. A at ¶¶ 343-344) While the Sourcefire Sensors are shipped with the feature disabled, customers are instructed that the feature may be enabled and used." (D.I. 241, ex. 9) Moreover, the evidence shows that customers have purchased the specific license required to use such feature. (D.I. 243, ex. A at ¶¶ 343-344) Cisco relies upon the declaration of a principle engineer to argue that the IOC feature does not perform the claim limitation. (D.I. 208 at 24-25; D.I.

---

prevention systems (IPS), which are not the same. (D.I. 252, ex. 35 at 78:6-9)

210) At the summary judgment stage, the court concludes that SRI's evidence suffices to create genuine issues of material fact. For each of the above arguments, SRI's evidence suffices to go beyond a showing that the accused sensors are "capable" of infringing and is sufficient to create a genuine issue of material fact. *Toshiba Corp. v. Imation Cor*p., 681 F.3d 1358, 1365 (Fed. Cir. 2012) (Evidence that an infringing mode "is not disabled by default" and that it is "recommended that customers use the infringing mode," is "evidence [that] goes beyond showing that the accused DVDs are 'capable of' infringing; the evidence is sufficient to create a genuine issue of material fact, thus precluding summary judgment.").

As to the Cisco and Sourcefire services, the parties appear to agree that the services are not "separate technology" from the accused sensors. The court understands that the accused services provide a customer with one of the accused sensors and then either provide management or updates to the accused sensor. Therefore, the infringement of the accused services rises and falls with the infringement of the sensors. (D.I. 240 at 35-40; D.I. 250 at 19) Having denied Cisco's motion for summary judgment of non-infringement of the accused sensors, the court denies the motion with regard to the services.

VI. PRE-SUIT DAMAGES - LACHES

A. Standard

Laches is defined as "the neglect or delay in bringing suit to remedy an alleged wrong, which taken together with lapse of time and other circumstances, causes prejudice to the adverse party and operates as an equitable bar." *A.C. Aukerman Co. v. R.L Chaides*

Const. Co., 960 F.2d 1020, 1028-29 (Fed. Cir. 1992) (*en banc*). For a defense of laches, defendant has the burden of proving that: (1) plaintiff delayed in filing suit for an unreasonable and inexcusable length of time after plaintiff knew or reasonably should have known of its claim against the defendant; and (2) defendant suffered material prejudice or injury as a result of plaintiff's delay. *Id.* at 1028.

With regard to the first prong of unreasonable delay, "[t]he length of time which may be deemed unreasonable has no fixed boundaries but rather depends on the circumstances." *Id.* at 1032. In determining whether plaintiff's delay in filing suit was unreasonable, the court must look to the period of time beginning when plaintiff knew or reasonably should have known of defendant's alleged infringing activity and ending when plaintiff filed suit. The period does not begin, however, until the patent issues. *Id.* In addition, the court must consider and weigh any excuses offered by plaintiff for its delay including, but not limited to: (1) other litigation; (2) negotiations with the accused; (3) possible poverty or illness under limited circumstances; (4) wartime conditions; (5) the extent of the alleged infringement; and (6) a dispute over the ownership of the asserted patent. *Id.* at 1033.

A presumption of laches arises if plaintiff delays filing suit for six years after actual or constructive knowledge of the defendant's acts of alleged infringement. *Id.* at 1037. "[T]he law is well settled that where the question of laches is in issue ... plaintiff is chargeable with such knowledge as he might have obtained upon inquiry, provided the facts already known by him were such as to put upon a man of ordinary intelligence the duty of inquiry." *Wanlass v. Gen. Elec. Co.*, 148 F.3d 1334, 1338 (Fed. Cir. 1998). The period of delay

continues if prior products are the same or similar to the alleged infringing products. *See Symantec Corp. v. Computer Assocs. Int'l, Inc.*, 522 F.3d 1279, 1295 (Fed. Cir. 2008). Once the presumption is met, the burden shifts to plaintiff to present evidence to create a genuine dispute with respect to the reasonableness of the delay.[39] *See Aukerman*, 960 F.2d at 1028. However, this presumption may be rebutted if plaintiff is able to show sufficient evidence to generate a genuine issue of fact as to the existence of either one of the factual elements associated with the laches defense.[40] *Id.* at 1038.

Turning to consider the second prong of material prejudice, defendant can establish either evidentiary prejudice or economic prejudice. *Id.* Evidentiary prejudice may arise where the delay has curtailed defendant's ability to present a full and fair defense on the merits due to the loss of evidence, the death of a witness, or the unreliability of memories. *Id.* Economic prejudice arises where a defendant suffers the loss of monetary investments or incurs damages which would have been prevented if plaintiff had filed suit earlier. *Id.* In this regard, courts must look for a change in the economic position of the alleged infringer during the period of delay; courts cannot simply infer economic prejudice from the possibility of damages pursuant to a finding of liability for infringement. *Id.*

---

[39] In *Aukerman*, the court made clear, however, that "at all times, ... defendant bears the ultimate burden of persuasion of the affirmative defense of laches; the burden of persuasion does not shift by reason of ... plaintiff's six-year delay. 960 F.2d at 1038.

[40] If the presumption of laches is rebutted, the defense of laches is not eliminated. Rather, defendant can still establish laches by establishing the elements for this defense based upon the totality of the evidence presented. *Aukerman*, 960 F.2d at 1038.

"The application of the defense of laches is committed to the sound discretion of the district court." *Id.* at 1032. Because it is equitable in nature, "mechanical rules" do not govern its application. *Id.* at 1032. Instead, the court must consider all of the facts and circumstances of the case and weigh the equities of the parties. "The issue of laches concerns delay by one party and harm to another. Neither of these factors implicates the type of special considerations which typically trigger imposition of the clear and convincing standard." Consequently, the defendant must establish the elements for the laches defense by the preponderance of the evidence, consistent with the burden of proof in equitable laches and estoppel cases. *Intuitive Surgical, Inc. v. Computer Motion, Inc.*, Civ. No. 01-203, 2002 WL 31833867, *5 n.4 (D. Del. 2002). When laches is applied, the plaintiff may not recover any damages for the period of time prior to filing suit. *Aukerman*, 960 F.2d at 1028.

B. Analysis

Cisco asserts that SRI knew about Cisco's alleged infringement of the patents by no later than 2003-2004, approximately ten years before SRI filed suit; therefore, the doctrine of laches is presumed to apply. (D.I. 183 at 6) SRI contends that: (1) genuine issues of material fact exist as to whether SRI can be charged with constructive knowledge of Cisco's infringement; and (2) genuine issues of fact exist as to whether Cisco was prejudiced either through loss of evidence or economically due to SRI's delay. (D. I. 197 at 1)

Cisco contends that, while SRI asserts that it did not have actual knowledge of infringement, this is insufficient to defeat summary judgment, for SRI had a duty to police its patent rights and the court should im-

pose constructive knowledge based on the required reasonable, diligent inquiry. (D.I. 183 at 5) The court agrees. SRI admits that it was aware of Cisco's product offerings such as "CiscoWorks," "Cisco Integrated Router 7301 ,"and "Cisco IDS" sensor products around 2004 and knew there was a possibility of infringement. (D.I. 197 at 2) Therefore, SRI reasonably should have known of its claims against Cisco. A presumption of laches applies.

Because the presumption is met, the two facts of unreasonable delay and prejudice **must** be inferred, absent rebuttal evidence. *Aukerman*, 960 F.2d at 1037. SRI bears the burden only of coming forward with sufficient evidence to raise a genuine factual issue respecting the reasonableness of its conduct, that defendant suffered no prejudice, or both. *Id.*; *see also TWM Mfg. Co. v. Dura Corp.*, 592 F.2d 346, 349 (6th Cir. 1979); *Maloney-Crawford Tank Corp. v. Rocky Mountain Natural Gas Co.*, 494 F.2d 401, 404 (10th Cir. 1974). The court finds that SRI has met this burden. SRI presents evidence that, during the delay, it was engaged in other litigation.[41] (D.I. 197 at 2) Courts have routinely held that this type of excuse may be considered and weighed as a justification for the delay, and rebuts the presumption of laches. *See, e.g.*, *Aukerman*, 960 F.2d at 1033, 1038; *Jamesbury Corp. v. Litton Indus. Prods.*, 839 F.2d 1544, 1552-53 (Fed. Cir.), *cert. denied*, 488 U.S. 828 (1988); *Hottel Corp. v. Seaman Corp.*, 833 F.2d 1570, 1572-73 (Fed. Cir. 1987); *American Home Prods. v. Lockwood Mfg. Co.*, 483 F.2d 1120, 1123 (6th Cir.

[41] SRI provides information that from 2004 until SRI provided notice to Cisco on May 8, 2012, SRI filed two infringement actions that involved two appeals to the Federal Circuit and a jury trial, and also prosecuted four ex parte reexaminations. (D.I. 197 at 12)

1973). Cisco's assertion that for other litigation to excuse a delay there must be adequate notice of the proceedings to defendant is incorrect. (D. I. 183 at 8) The court in *Aukerman* made clear that the district court's rejection of plaintiff's excuse of other litigation because they did not give notice to defendant was erroneous, "for there can be no rigid requirement in judging a laches defense that such notice **must** be given." 960 F.2d at 1039 (emphasis in original). The court concludes that SRI has raised genuine issue of fact regarding whether an unreasonable delay can be shown due to SRI's alleged excuses and, therefore, denies Cisco's motion for summary judgment of laches.[42]

VII. MOTIONS TO EXCLUDE

Rule 702 of the Federal Rules of Civil Procedure allows a qualified witness to testify in the form of an opinion if the witness' "scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue" and if his/her testimony is the product of reliable principles and methods which have been reliably applied to the facts of the case.

A. Dr. Prowse's Opinions

Cisco moves to exclude certain opinions of SRI's damages expert, Dr. Prowse, regarding royalty rates

---

[42] By raising a genuine issue respecting either factual element of a laches defense, the presumption of laches is overcome. *Aukerman*, 960 F.2d at 1038; *see also Watkins v. Northwestern Ohio Tractor Pullers*, 630 F.2d 1155, 1159 (6th Cir. 1980). Because the court finds that SRI has raised a genuine issue of fact regarding the reasonableness of the delay and, thus, defeated the presumption of laches, it declines to address SRI's argument that there exists a material issue of fact regarding prejudice.

as lacking the required "sufficient facts or data." *Whitserve LLC v. Computer Packages, Inc.*, 694 F.3d 10, 30 (Fed. Cir. 2012) ("[L]ump sum payments ... should not support running royalty rates without testimony explaining how they apply to the facts of the case."). Specifically, Cisco moves to exclude Dr. Prowse's opinions based on "seven non-comparable lump sum settlement agreements." (D.I. 263 at 3) Dr. Prowse has opined, based in part on a number of license agreements that SRI has entered into, that damages should be based on a reasonable royalty rate on the apportioned value of the accused products of at least 7.5%. (D.I. 215, ex. 2 at ¶ 152) Several of the licenses disclose such a rate. (D.I. 215, exs. 3, 4, 6, 10) Dr. Prowse also cites to deposition testimony and other documents. (D.I. 245, ex. 4 at ¶¶ 55, 57, 59-60, 63, 66 70-73, 75, 77) SRI points out that certain of the licenses did not arise in the context of litigation. (D.I. 244 at 7 n.5) Cisco argues that, because the court does not allow discovery or testimony into a negotiation process, the settlement agreements (a product of such negotiations) should be excluded. (D.I. 214 at 7-8)

The court, consistent with the policies of Rule 408 of the Federal Rules of Evidence and its practice, will exclude those settlement agreements (and the opinions based thereon) that are a product of litigation, as such settlements reflect the parties' consideration of multiple factors unrelated to valuation issues. *PharmaStem Therapeutics, Inc. v. Viacell Inc.*, Civ. No. 02-148 GMS, 2003 WL 22387038, at *2 (D. Del. Oct. 7, 2003) ("Specifically, a license agreement may be excluded from evidence under Rule 408 where it (1) was reached under a threat of litigation, (2) arose in a situation where litigation was threatened or probable, or (3) was negotiated against a backdrop of continuing litigation infringe-

ment."). The licenses entered into as a product of business negotiations outside the context of litigation are properly considered. To the extent the parties cannot reach agreement on the IBM and McAfee licenses,[43] the parties may present such issues at the pre-trial conference. The motion to exclude is granted in part and denied in part.

B. Dr. Lee's Testimony

Cisco moves to exclude the opinions of Dr. Lee regarding apportionment, arguing that he is unqualified to provide such economic expert opinion. SRI responds that Cisco's expert, Dr. Leonard, arrived at many of the same apportionment numbers. Moreover, Dr. Lee's opinions are technically based and should be allowed. (D.I. 246) Dr. Leonard's "methodology for determining the properly apportioned royalty base" relies either on Dr. Lee's apportionment figures or on figures derived from speaking with Dr. Clark (Cisco's technical expert). (D.I. 247, ex. 1 at ¶¶ 176-78 & n.382-83) Cisco is free to challenge the conclusions and analysis provided by Dr. Lee on cross-examination. The court denies the motion to exclude.

VIII. CONCLUSION

For the foregoing reasons, the court denies Cisco's motion for summary judgment of invalidity under 35 U.S.C. § 101 (D.I. 158); denies Cisco's motion for summary judgment of invalidity under 35 U.S.C. § 102(b) and § 103 (D.I. 182); denies Cisco's motion barring SRI from recovery of pre-suit damages based on the equitable doctrine of laches (D.I. 182); denies Cisco's motion

---

[43] SRI states that these two licenses are not the product of litigation. (D.I. 244 at 7 n.5) Cisco disagrees. (D.I. 263 at 4)

for summary judgment for noninfringement (D.I. 182); grants in part and denies in part Cisco's motion to exclude certain opinions of Dr. Stephen Prowse regarding SRI's lump settlement agreements (D.I. 213); denies Cisco's motion to exclude the testimony of Dr. Wenke Lee regarding apportionment (D.I. 216); and grants in part and denies in part SRI's motion for summary judgment that Netranger and Hunteman are not prior art (D.I. 219); and *sua sponte* grants summary judgment of no anticipation by EMERALD 1997. An appropriate order shall issue.