United States Court of Appeals for the Federal Circuit

IN RE ENHANCED SECURITY RESEARCH, LLC

2013-1114

Appeal from the United States Patent and Trademark Office, Patent Trial and Appeal Board, in Reexamination No. 90/010,849.

Decided: January 13, 2014

MARTIN M. ZOLTICK and R. DANNY HUNTINGTOWN, Rothwell, Figg, Ernst & Manbeck, P.C., of Washington, DC, argued for appellant. With them on the brief were NANCY J. LINCK, DEREK F. DAHLGREN and MICHAEL V. BATTAGLIA.

MEREDITH H. SCHOENFELD, Associate Solicitor, Office of the Solicitor, United States Patent and Trademark Office, of Alexandria, Virginia, argued for appellee. With her on the brief were NATHAN K. KELLEY, Deputy Solicitor, and FARHEENA Y. RASHEED, Associate Solicitor.

Before DYK, O'MALLEY, and TARANTO, *Circuit Judges.*

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

Dissenting opinion filed by *Circuit Judge* O'MALLEY.

DYK, *Circuit Judge.*

Enhanced Security Research, LLC ("ESR") appeals from the decision of the Board of Patent Appeals and Interferences ("Board"), now the Patent Trial and Appeal Board, in an *ex parte* reexamination of U.S. Patent No. 6,119,236 ("the '236 patent"). The Board affirmed the Patent and Trademark Office ("PTO") examiner's rejection of claims 1-5 and 7-19 as obvious. We affirm.

BACKGROUND

The '236 patent, as amended, claims a computer security device and method for preventing unauthorized individuals from gaining access to a local computer network. The patent specification describes an "intelligent network security device" ("INSD") that is capable of balancing the desire for network security against the need for network accessibility. '236 patent col. 3 l. 47. The INSD protects a local network by: (1) monitoring the data packets flowing into and out of the network in order to detect suspicious patterns of communications; (2) assigning weighted values to any threatening activity it detects; and (3) blocking communications based on their assigned weight using a firewall.

Claim 1 of the amended '236 patent reads:

> In a computer system connected to an external communications medium, a security device comprising:
>
> > a programmable firewall device interposed between the computer system and the external communications medium;
> >
> > a controller device configured within the computer system such that said controller device can access all communications into and out of the computer system; and

> a communications device for communicating instructions from said controller device to said firewall device for controlling said firewall device; wherein
>
> said controller device is configured to operate generally continuously and repeatedly to:
>
> (i) examine, in essentially real time, communications incoming to the computer system;
>
> (ii) analyze, in essentially real time, communications to detect if the communications contain patterns of activity indicative of an attempted security breach;
>
> (iii) assign a weight to the attempted security breach if an attempted security breach is detected; and
>
> (iv) continuously control the firewall during the operation of the computer system to block communications between the computer system and the external communications medium, based on the weight assigned to the attempted security breach, when an attempted security breach is detected.

JA 9622-23. Thus, claim 1 pertains to a security device that provides protection to a local area network ("LAN") by monitoring communications, analyzing whether they represent attempted security breaches, assigning weights to any detected breach attempts, and, finally, commanding the firewall to block attempted breaches based on their assigned weight.

Claims 2-5 and 7-11 are dependent on claim 1.[1] Amended claims 8 and 9 relate to the blocking process. Claim 8 states:

> the controller controls the firewall to block the communication between the computer system and the external communication medium *for a predetermined period* according to the weight assigned to the attempted security breach.

Id. claim 8 (emphasis added). Claim 9 presents a slight variation on claim 8: after the controller assigns a weight to the attempted breach, "the controller controls the firewall to block communications between *a selected portion of the computer system and the external communications medium* according to the weight assigned to the perceived attempted security breach." *Id.* claim 9 (emphasis added). Thus, under these dependent claims, the INSD has limited blocking capabilities: the INSD can only command the firewall to undertake a certain, predetermined response.

Next, independent claim 12 covers the method portion of the '236 patent. According to amended claim 12, this method comprises

[1] In claim 2, the computer system is a LAN. In claim 3, the external communications medium is the Internet. In claim 4, the LAN is operating as an Ethernet network. In claim 5, the controller device examines communications entering the computer system for "code known to be associated with attempted security breaches." In claim 7, the communications device is a serial data communications link. In claim 10, "the controller is a general purpose computer," and in claim 11, the controller and the firewall are "physically distinct computerized units."

> monitoring, in essentially real time, communications between the local area network and the wide area network;
>
> determining, over time, if the communications between the local area network and the wide area network contain patterns of activity indicative of an attempted security breach;
>
> classifying by assigning a weight to the attempted security breach if an attempted security breach is detected; and
>
> generally simultaneously controlling a firewall to selectively block communications between the local area network and the wide area network depending upon the weighted classification assigned to the attempted security breach.

Id. claim 12. Under some of the dependent claims, the method entails classifying and assigning a weight to an attempted security breach depending on: (1) "the *importance of a portion of the local area network* which the attempted security breach attempts to access," *id.* claim 15 (emphasis added); (2) "the *number of attempts* made in the course of the attempted security breach," *id.* claim 16 (emphasis added); or (3) "*the relative sophistication* of the attempted security breach," *id.* claim 17 (emphasis added).

A third party requested reexamination of the original patent, and, among other documents, two potential pieces of prior art were before the PTO: the manual of a software product called NetStalker ("NetStalker" or the "Manual") and a scholarly article authored by G.E. Liepins and H.S. Vaccaro ("Liepins"). Similar to the '236 patent, the NetStalker software protects a LAN from attempted security breaches. The Manual describes how the product functions and teaches the user how to install the software and tailor it to his needs. Through these descriptions, the

Manual discloses a dynamic security device that provides protection to a LAN by monitoring the incoming and outgoing communications, identifying attempted security breaches, and then automatically blocking any unauthorized access attempts. As discussed below, ESR contends that the Manual is not prior art.

Liepins is a scholarly article that describes a computer system, called Wisdom and Sense ("W&S"), that is capable of detecting anomalous network activity. Liepins first recognizes that the identification of activity patterns not previously known to be associated with misuse is intrinsically difficult to systematize. Liepins also notes that "just checking" historical data regarding misuse patterns is not sufficient. To solve this problem, Liepins teaches a framework that can detect newly identified anomalous activity by automatically generating, weighing, and applying a "forest" of decision rules. Using stored data to identify patterns associated with unauthorized access, W&S generates rules that are capable of parsing new anomalous activity from acceptable activity.[2]

[2] Liepins explains that

> [f]or any test field (subject to the pruning conditions and sufficient number of observations) rules are generated with all possible combinations of the other fields in the conditional side. Thus, rules will be formed that predict port on the basis of any combination of user, time-of-day, and day-of-week (individually or in combination); time-of-day on the basis of the other fields; and so forth. In this way, W&S can be thought to extrapolate the available information of what value combinations can be expected to be common and which are unusual: For each field individually, the corresponding tree of the W&S rule forest effectively partitions the space of possible transactions into

Through this mechanism, the W&S system protects a LAN without shutting down all network activity. ESR does not dispute the prior art status of Liepins.

During reexamination, the examiner rejected claims 1-19 as obvious in light of various prior art references. The examiner also rejected ESR's arguments that the Manual did not qualify as publically-available prior art. The applicant then amended the '236 patent claims and appealed to the Board.[3] The Board affirmed the rejection of amended claims 1-5 and 7-19.

ESR timely appealed to this court, and we have jurisdiction pursuant to 28 U.S.C. § 1295(a)(4)(A). We review the Board's legal determinations de novo, and its factual

> complementary "rectangular" regions (of arbitrary dimension) that suggest evidence for or against the transaction being an anomaly (conditioned on the available information in the other fields).

JA 400. Thus, W&S will detect unwanted communications or activity through this forest of rules that parse the anomalous activity from that which is authorized.

[3] The applicant amended the '236 patent claims in response to the PTO's Final Office Action. The examiner allowed the applicant to appeal the amended claims, rather than the claims she had actually rejected, reasoning that

> [the] proposed amendments to claims 1, 8, 9, and 12 would place the application in better form for appeal by materially reducing and simplifying the issues for appeal by limiting all the claims to ones requiring (1) assigning a weight or classifying by assigning a weight to an attempted security breach; and (2) blocking based on the assigned weight or weighted classification.

JA 9401.

findings for substantial evidence. *In re Baxter Int'l, Inc.*, 678 F.3d 1357, 1361 (Fed. Cir. 2012).

DISCUSSION

I. Obviousness

A determination of obviousness under 35 U.S.C. § 103 is a question of law based on underlying findings of fact. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966); *In re Baxter*, 678 F.3d at 1361. The differences between the claimed invention and the prior art as well as what a reference actually teaches are questions of fact. *In re Baxter*, 678 F.3d at 1361; *Rapoport v. Dement*, 254 F.3d 1053, 1060-61 (Fed. Cir. 2001).

With respect to obviousness, the critical issue is whether the Manual in combination with Liepins teaches a person of ordinary skill in the art how to assess the severity of an attempted security breach and then block that attempted breach *based on* its severity. (For the purposes of this discussion, we assume that the Manual constitutes valid prior art. This assumption is discussed in Section II.)

As previously described, the amended '236 patent claims a device that examines the data entering and exiting a LAN, assigns weights to any attempted security breaches, and initiates predetermined responses depending on the assigned weights of the attempted breaches. ESR argues that a combination of NetStalker and Liepins does not disclose: (1) assigning a weight to an attempted security breach; or (2) blocking incoming communications based on that assigned weight. The Board found that, in combination, these two pieces of prior art disclosed all of the elements of the '236 patent. Substantial evidence supports this conclusion.

NetStalker teaches: (1) assigning severity levels to network transactions or events based on the number of attempted intrusions;[4] (2) automatically blocking the source of communications when those transactions meet user-defined criteria; and (3) varying response type based on the number of breach attempts. More specifically, the software employs a system of filters to detect attempted security breaches, referred to in the Manual as "misuse." The NetStalker filters correspond to various activities that are associated with security breaches. The software then uses a program known as the "Misuse Detector" to "combine[] series of filters to 'sieve' the [network] data." JA 312. "Each filter reduces the total number of events sent to the next filter," and "[t]he result is a set of all events that match the specified filters." JA 312. If the number of events meets a specified threshold, the NetStalker software triggers an alarm. After a user has defined the filters and configured the Misuse Detector, he can "select one or more alarms and [] assign the parameters for triggering the alarm." JA 325. One of the alarm options available to the user is "Shun," which automatically blocks the unwanted communication.

Although the NetStalker software was sold with a default set of filters, the product permits users to create custom filters according to their specific security needs. The filters can monitor a variety of parameters and can be turned on or off at the discretion of the user. The NetStalker software also enables its users to configure the Misuse Detector, "to create custom detection configura-

[4] The parties agree on this disclosure of the Manual. *See* Reply Br. at 12 (the Manual "discloses that an alarm is triggered when a count of the number of events meets a threshold"); Resp. Br. at 8 ("The suspicious events are tallied [by the NetStalker software], and when they reach a threshold number an alarm is triggered.").

tions." JA 312. In other words, the software allows users to define what types of events (for example, an attempted login for a particular source) will count for the purposes of triggering an alarm.[5] The user can program the software such that it recognizes the number of intrusions of a particular type as more "severe" than others. Therefore, the NetStalker software teaches responding to attempted breaches *based on* user-defined criteria, *i.e.*, creating a causal connection between the user-defined parameters and the subsequent alarm response, including the "Shun" response.[6]

What the Manual does not disclose is the automatic assignment of different weights to different types of attempted security breaches. Liepins fills this gap with its

[5] The NetStalker software allows the user to set an alarm that is triggered by the user-defined "severity" of a particular event. This alarm parameter allows a user to define the severity of particular event from 1 to 10.

[6] The appellant's brief inaccurately states that "there is simply no disclosure [in the NetStalker Manual] that [the] severity rating is used to trigger an alarm, must less cause the software to block communications." The plain language of the Manual contradicts this statement.

The dissent also makes the puzzling suggestion that the Board found that "NetStalker and Liepins *do not* 'specifically teach[] using the assigned strength or severity level as a basis for blocking communications.'" Dissent at 14 (quoting Appellee's Br. at 1) (emphasis added). In fact, the Board specifically found that

> NetStalker discloses not only a user defined severity level of a security breach but also triggering an alarm when a certain number of (security) events are recognized and blocking communications when the alarm is triggered.

JA 15.

systematic rule-based framework that is capable of automatically identifying exceptional network activity. As previously discussed, the W&S system automatically generates rules wherein activity that is indicative of an attempted breach is more likely to fail a particular rule. Each rule is assigned a weight such that "the strengths . . . reflect the confidence that the rules flag transactions that should be flagged, and don't flag those that shouldn't." JA 402. If a transaction fails a particular rule, that failure will be assessed in combination with the strength of the particular rule it failed. Thus, whether the W&S system will flag a transaction as anomalous depends on whether that transaction passed or failed a rule as well as the weight of the rule itself.

The patent claims here assign weights to attempted security breaches based on factors such as: (1) "the *importance of a portion of the local area network* which the attempted security breach attempts to access," Amended '236 patent claim 15 (emphasis added); (2) "the *number of attempts* made in the course of the attempted security breach," *id.* claim 16 (emphasis added); and (3) "*the relative sophistication* of the attempted security breach." *Id.* claim 17 (emphasis added). Liepins similarly discloses a system of assessing how threatening a particular network event is based on a system of weighted rules. Nothing in the amended '236 patent claims suggests that ESR's method of assigning weights is any more sophisticated than that of Liepins. The broad language of claim 12 and its dependent claims fails to specify any teachings that would be nonobvious in light of the combination of the Manual and Liepins.

Finally, ESR argues that the Board "failed to address the limitations contained in dependent claims 9, 15, and 17." Appellant's Br. at 47. As the PTO points out on appeal, ESR waived this argument when it failed to separately argue these claims. As this court explained in *In re Lovin*, 652 F.3d 1349 (Fed. Cir. 2011), the Board may reasonably interpret 37 C.F.R § 41.37, the rule governing the briefing requirements in *ex parte* appeals, "to require applicants to articulate more substantive arguments if they wish for individual claims to be treated separately." *Id.* at 1356. ESR asserts that it separately argued claims 9, 15, and 17 when it quoted the claims in its appeal brief and stated that these limitations did not appear in the prior art. *Lovin* specifically held that this type of argument was insufficient, stating that "a mere recitation of the claim elements and a naked assertion that the corresponding elements were not found in the prior art" is insufficient under Rule 41.37. *Id.* at 1357.

Here, ESR did not argue the dependent claims under separate subheadings as Rule 41.37 (2012)[7] required. Instead, ESR grouped the dependent claims with their independent claims. ESR only referenced dependent claims 9, 15, and 17 as examples of "additional limitations which are neither taught nor suggested by [the prior art]." JA 9615; *see also* JA 9616. The Board found that ESR did not provide sufficient additional arguments in support of the dependent claims. Under *Lovin*, we conclude that the Board has not erred in using its discretion to interpret Rule 41.37 to require ESR to provide distinct substantive grounds if it wished to obtain separate consideration of claims 9, 15, and 17 by the Board. Thus, we hold that ESR has waived its arguments with respect to these claims.

In short, the features of the amended '236 patent claims were disclosed by the combination of the Manual and Liepins. ESR does not contest that a person of ordinary skill in the art would have been motivated to combine Liepins and NetStalker. *Graham* also instructs courts to consider the secondary indicia of non-obviousness, such as "commercial success, long felt but

[7] These provisions have since been amended. *See* 37 C.F.R § 41.37 (2013).

unsolved needs, failure of others, etc." *Graham*, 383 U.S. at 17. However, ESR does not reference any secondary considerations. We therefore conclude that the Board did not err in finding the claims obvious.

II. The NetStalker Manual as Prior Art

We have so far proceeded on the assumption that NetStalker constitutes a valid prior art reference. However, ESR contends that the Board erred in treating the Manual as prior art. Whether a document qualifies as a "printed publication" that is "available to the public" for the purposes of 35 U.S.C. § 102(a)(1) is a question of law based on underlying findings of fact. *See In re Hall*, 781 F.2d 897, 899 (Fed. Cir. 1986). Under 35 U.S.C. § 102(a)(1), prior art encompasses any matter that "was patented, described in a printed publication, or in public use, on sale, or otherwise available to the public before the effective filing date of the claimed invention." This court has interpreted § 102 broadly, explaining that even relatively obscure documents qualify as prior art so long as the public has a means of accessing them. *See, e.g.*, *Hall*, 781 F.2d at 899.

Our leading case on public accessibility is *In re Hall*, 781 F.2d 897 (Fed. Cir. 1986). In *Hall* we concluded that "a single cataloged thesis in one university library" constitutes "sufficient accessibility to those interested in the art exercising reasonable diligence." *Id.* at 900. Thereafter, in *Constant v. Advanced Micro-Devices, Inc.*, we explained that "[a]ccessibility goes to the issue of whether interested members of the relevant public could obtain the information if they wanted to." 848 F.2d 1560, 1569 (Fed. Cir. 1988). Therefore, "[i]f accessibility is proved, there is no requirement to show that particular members of the public actually received the information." *Id.*

In this case, the title page of the Manual contains an inscription dating it to May 1996. ESR, however, challenges the Manual's claimed date of priority, arguing that the version of the Manual that the examiner relied on may not have been available in May 1996 and that there are indications that this version was a draft rather than a final document available to the public. However, Stephen Smaha, the Chief Executive Officer of the company that produces the NetStalker software, filed a declaration ("Smaha Declaration") with the PTO averring that the version of the Manual before the examiner was available in May 1996. Smaha explained that "[m]embers of the public showing an interest in buying or licensing the NetStalker product could have obtained a copy of the manual by contacting Haystack or Network Systems Corporation and requesting one," and, indeed, "[t]he NetStalker product was sold to or installed for approximately a dozen customers." JA 9705 (footnote omitted). In view of the Manual's inscription date, the Smaha Declaration, and evidence of NetStalker advertisements published in 1995, we conclude that substantial evidence supports the Board's finding that the Manual constituted publically-available prior art under § 102(a)(1).

ESR also argues that the Manual should not be considered in the circumstances of this case because it was missing pages. To support this proposition, ESR relies on *Panduit Corp. v. Dennison Manufacturing Co.*, wherein this court explained that prior art "must be considered in its entirety, *i.e.*, as a whole, including portions that would lead away from the invention in suit." 810 F.2d 1561, 1568 (Fed. Cir. 1987). ESR contends that because the Manual was missing pages, it "cannot be considered as a whole" and therefore "should not be considered at all." Appellant's Br. at 26.

Panduit did not involve a situation similar to the missing pages at issue here. In *Panduit*, we reversed a district court's determination that a patent was obvious in light of the prior art. *Panduit*, 810 F.2d at 1565. We explained that this reversal was necessary because the district court "treated no claim, nor the entire prior art, nor any prior patent 'as a whole,' but [instead] selected bits and pieces from prior patents that might be modified to fit its legally incorrect interpretation of each claim as consisting of one word." *Panduit*, 810 F.2d at 1587. Thus, *Panduit* explains that § 103 does not permit a court to stitch together an obviousness finding from discrete portions of prior art references without considering the references as a whole. That is not what occurred here.

In addition to *Panduit*, ESR urges that the Manual of Patent Examining Procedures ("MPEP") supports its argument. To the contrary, the MPEP contemplates partial submissions of prior art documents. The primary regulation governing reexamination, 37 C.F.R. § 1.510, permits parties to submit partial prior art references: under § 1.510(b)(3), a requester is only required to submit the "pertinent parts" of any non-English translation. Commenting on § 1.510(b)(3), § 2214 of the MPEP explains that § 1.510(b)(3) requires the requester to submit "a translation of each non-English document (or a translation of at least the portion(s) relied upon)." Similarly, § 2218 of the MPEP, the very section of the MPEP that ESR argues supports its argument, only requires the submission of the "pertinent parts" of a non-English translation.

Section 1.105 of the PTO regulations permits an examiner to request more information from a patentee[8] in

[8] 37 C.F.R. § 1.105 permits the examiner to request such information from:

> (1) Each inventor named in the application; (2) Each attorney or agent who prepares or prosecutes the application; and (3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, the applicant, an assign-

the course of reexamination if such information is necessary "to properly examine or treat the matter." 37 C.F.R. § 1.105. With respect to such requests, the MPEP explains that "where the document is a bound text or a single article over 50 pages, the requirement may be met by providing copies of those pages that provide the particular subject matter indicated in the requirement, or where such subject matter is not indicated, the subject matter found in applicant's disclosure." MPEP § 704.14(a) ¶ 7.122. The version of the Manual that the Board relied on is over sixty pages long and appears to fall within this provision. We conclude that the PTO's own rules permit the consideration of selected portions of prior art references so long as the missing portions are not necessary to fully understand the submitted portions. ESR cites no authority for the proposition that the PTO is categorically precluded from considering a reference if it is incomplete. Indeed, ESR agrees that partial documents can be considered "[if] there is clear evidence the missing pages would not impact those that are available." Appellant's Br. at 26.

We agree that missing pages may sometimes be necessary for understanding a prior art reference. But nothing in the Manual here suggests that the missing pages were necessary to an understanding of the pertinent parts of the reference. The Manual's table of contents as well as its page numbering suggest that it was missing three additional pages in chapter five and seven pages in chapter seven. Titled "Running NetStalker," chapter five describes "the steps required to use the pre-defined configurations that are shipped with *NetStalker* and to start the *NetStalker* processes." JA 307. The available pages teach how to determine the type of alarm the NetStalker

ee, or anyone to whom there is an obligation to assign the application.

37 C.F.R. § 1.56(c).

security system triggers and the alarm parameters. One of the alarm type is "Shun," which automatically block unwanted communications. The table of contents and the list of figures indicate that the missing pages contained an explanation of what a user should do before running the NetStalker software, how to select a "scenario,"[9] how to configure alarm overrides, and how to run the software.[10] Nothing in the table of contents or the available chapter five pages suggests that the missing content contradicts the available portions of chapter five on which the PTO relied or other parts of the Manual.

Chapter seven describes "how to manage and analyze historical router event data," JA 329, the log of communications that have entered and exited the local network.[11] This chapter details the NetStalker software's ability to

[9] Chapter one of the NetStalker manual describes a number of possible scenarios involving attempted security breaches. These scenarios include breach attempts from bad hosts, IP spoofing, and false logins, among others. Therefore, the missing page on how to "select a scenario" most likely explains how to configure the software to detect different types of breach attempts.

[10] The table of contents states that the missing pages are titled: "Running NetStalker," "Before you run NetStalker," "To Select a Scenario," "To Configure Alarm Handler Overrides," and "To Run NetStalker." JA 271. The missing figure in chapter five is titled: "Configure Misuse Detector Window." JA 273.

[11] The missing pages in chapter seven are titled: "Schedule Log Manager," "Log Events Record Format & Sample Data," and "Analyzing Log Files." JA 272. The five missing figures are: "Schedule Log Manager Window," "Schedule Crontab Entries window," Event Data Available Window," Interactive Alarm Window," and "*NetStalker* window." JA 273-74.

save all router events and establish a "hierarchy of locations" for storing them. JA 330. Although ESR's security device must also manage historical data, the limitations of the amended '236 patent claims do not address the management of historical data.[12] Therefore, this chapter does not appear to be significant to the amended '236 patent claims.[13]

ESR claims that the missing sections were necessary because they could: "(1) clarify the often cryptic disclosure in the NetStalker Manual and thus alter its meaning; or (2) disparage or teach away from application of the relied upon teachings to the '236 invention." Appellant's Br. at 29. However, ESR fails to point to anything in the Manual that might support this conclusion. When the panel pressed ESR at oral argument to explain how the missing

[12] Instead, claim 5 simply states that "the controller device examines communications incoming to the computer system for code known to be associated with attempted security breaches." Amended '236 patent claim 5. The specification explains that "in order for the 'look for known patterns' operation to be successful, the INSD might require some knowledge of the configuration of the LAN . . . . This data can be stored in the memory of the INSD." '236 patent col. 6 ll. 57-61.

[13] The examiner did cite chapter seven for the proposition that "[a] threshold (factor . . . number of attempts) may be applied to a misuse signature, as a second form of analysis that also requires examination of a series of more than one packet." JA 9896. After stating this proposition, the examiner wrote "See Chapter 7 which describes how to manage and analyze historical (over time) router event data." JA 9896. This complete quotation reveals that the examiner merely cited chapter seven to show that NetStalker is capable of examining more than one packet. The Board did not rely on chapter seven at all.

pages might plausibly teach away from the '236 invention, ESR postulated that the missing pages "could have disparaged the use of a user-defined security level to trigger an alarm." *See* Oral Argument at 6:36, *available at* http://www.cafc.uscourts.gov/oral-argument-recordings/13-1114/all. This scenario is both speculative and highly implausible: a manual would not tell users how they can utilize the product in a particular way, only to then tell them not to do so. As the examiner explained, "[w]hen the source is reviewed as a whole, there is no evidence whatsoever that the missing pages detract in any way from the NetStalker manual's disclosures and teachings." JA 9157.[14] The Board reached a similar conclusion, and we agree.

[14] Had the missing pages been necessary to a full understanding of the software, the examiner, of course, could not have relied on the Manual without securing the missing pages. In *Star Fruits S.N.C. v. United States*, 393 F.3d 1277 (Fed. Cir. 2005), we held that the examiner could request further information from the applicant, and 37 C.F.R. § 1.156, *see supra* note 8, permits requests to others associated with the applicant. However, the relevant regulations do not provide a mechanism through which the PTO may request further information from a third party. This is clear from the history of the America Invents Act's new Third Party Preissuance Submission procedure, codified at 35 U.S.C. § 122(e). The final report of comments from the public notice period for the regulations reveals that commenters were concerned by the inability of examiners to request further information from third party submitters. In response to this concern, the PTO simply stated that

> [a]n examiner cannot . . . request additional information from a party who makes a third-party submission. The Office does not believe there is a

III. Diligence

Finally, ESR argues that even if the ’236 patent would have been obvious in light of NetStalker and Liepins, NetStalker should not be considered invalidating prior art because ESR conceived of the invention before the publication of the NetStalker Manual, and was diligent in reducing it to practice. The Manual contains an inscription that dates it to May 1996, and the ’236 patent is a continuation in part of an application filed on October 7, 1996. Even if ESR had established a conception date before May 1996 (earlier than the publication date of the Manual), we find no error in the Board’s decision that there was no showing of diligence in reducing the invention to practice.

Under 37 C.F.R. § 1.131, a party may file an oath or declaration establishing that the invention described in his rejected claims predates the reference on which the rejection was based. Under § 1.131, the party may remove

> need for a similar mechanism to require further information from third-party submitters as the third parties will be motivated to provide complete submissions that would not likely require further information.

Changes To Implement the Preissuance Submissions by Third Parties Provision of the Leahy-Smith America Invents Act, 77 Fed. Reg. 42,150, 42,161 (July 17, 2012) (to be codified at 37 C.F.R. pt. 1 and 41). Thus, in this case, the examiner could not have requested the missing pages from the third party submitter. This result seems incongruous. While this case does not present an instance in which the missing pages were necessary for examination, in the event that such an instance arises, it would be useful for the PTO to provide a procedure through which an examiner could request further information from the third party requester.

his invention from the purview of the prior art reference by providing facts "in character and weight" that demonstrate "conception of the invention prior to the effective date of the reference coupled with due diligence." 37 C.F.R. § 1.131(b) (2012).[15] A party may prove due diligence by showing his attorney's efforts to achieve a constructive reduction to practice. *Bey v. Kollonitsch*, 806 F.2d 1024, 1026 (Fed. Cir. 1986).

In order to establish attorney diligence, ESR submitted declarations from Peter M. Shipley, the inventor of the '236 patent ("Shipley Declaration"), and F. Eric Saunders, the attorney who filed the '236 patent application ("Saunders Declaration"). In their declarations, Saunders and Shipley described meetings and telephone calls that took place from February 28, 1996 (when Shipley and Saunders first met in person) to October 7, 1996 (when the patent application of which the '236 patent is a continuation was filed). ESR argues that these declarations demonstrate the requisite attorney diligence during the critical period.

The Board disagreed and found that ESR failed to show that Saunders "'worked diligently and continuously' over the four month period preceding the filing date of October 7, 1996." JA 14. In making that determination, the Board relied on *Bey*, where this court examined the standard for attorney diligence in a patent interference case. In *Bey*, we explained that "reasonable diligence can be shown if it is established that the attorney worked reasonably hard on the particular application in question during the continuous critical period." 806 F.2d at 1027. We emphasized that the attorney's records should "show

[15] These provisions have since been amended. *See* 37 C.F.R. § 1.131 (2013).

the exact days when activity specific to [the patentee's] application occurred." *Id.* at 1028.[16]

In this case, the critical period in which ESR must demonstrate diligence spans from May 1996, when the relevant version of the Manual became available, to October 7, 1996, when Saunders filed Shipley's patent application. The record reveals that over the course of five months, Saunders had a few conversations with Shipley, conducted a prior art search, billed for under 30 hours of work, and drafted the patent application. Citing *Bey*'s emphasis on the importance of supplying specific dates of activity when attempting to establish diligence, the Board found that, apart from records showing work on "May 4, 6, and 20, and activity in July," JA 13, ESR failed to provide "records or other evidence showing the exact days when activity specific to this application occurred." JA 13. Although § 1.131 did not require Saunders to work on Shipley's patent application without pause, we hold that

[16] ESR not only argues that the Shipley and Saunders Declarations demonstrate the requisite attorney diligence, but also that the Board applied the wrong standard when assessing the sufficiency of these declarations. ESR contends that the Board applied a "clear and convincing evidence" standard from certain interference cases. *See In re Eickmeyer*, 602 F.2d 974 (C.C.P.A. 1979); *Wetmore v. Quick*, 536 F.2d 937 (C.C.P.A. 1976); *In re Moore*, 444 F.2d 572 (CCPA 1971). But the Board did not do so. It never articulated such a standard, and the sole interference case it cited was *Bey*, which involved a preponderance of the evidence standard because the interference in *Bey* was between two applications. *Bey*, 806 F.2d at 1025-26. The Board did not cite interference cases articulating a higher standard of proof for a junior party seeking to antedate—and thus invalidate—a senior party's issued patent.

substantial evidence supports the Board's finding that ESR failed to demonstrate the requisite attorney diligence.

CONCLUSION

In sum, we hold that the examiner and Board properly treated the NetStalker Manual as publically-available prior art and, having done so, correctly concluded that the teachings of the Manual and Liepins render the amended '236 patent claims at issue obvious under 35 U.S.C. § 103. We further hold that ESR has failed to demonstrate the requisite attorney diligence under Rule 131, and, therefore, the '236 patent does not predate the publication date of the Manual.

AFFIRMED

United States Court of Appeals for the Federal Circuit

IN RE ENHANCED SECURITY RESEARCH, LLC

2013-1114

Appeal from the United States Patent and Trademark Office, Patent Trial and Appeal Board in Reexamination No. 90/010,849.

O'MALLEY, *Circuit Judge*, dissenting.

Because the Board of Patent Appeals and Interferences ("Board"), now the Patent Trial and Appeal Board, erred in relying on a facially incomplete reference and was not supported by substantial evidence in finding that the same reference was publicly available as of the critical date, I would reverse its decision. I cannot endorse allowing the Board to strip Enhanced Security Research, LLC ("ESR") of its right to a validly issued patent on such a suspect record. I, thus, respectfully dissent.

The Board relied on an incomplete reference—Haystack Labs, Inc., NetStalker™, Installation and User's Guide, Version 1.0.2 (1996) ("NetStalker")—a reference which was missing all the even pages in one of the two chapters to which the Board cited to support its finding of obviousness, was missing entire sections of other chapters, and bore indicia of being a draft document. The reference was obtained from an interested party—a paid expert for a party opposing ESR in litigation, the same party who initiated the reexam of United States Patent No. 6,119,236 ("'236 Patent"). That paid expert, Stephen Smaha, was the only person who apparently had access to the reference, could explain whether a complete reference existed, could explain why, if so, the reference was submitted in incomplete form, and could explain what was in the missing portions of the reference. While Smaha submitted a declaration in support of the reference, he neither claimed that a more complete reference existed—at any time—explained why the reference was submitted in its incomplete state, or explained what the missing portions discussed. The government asserts no positive theory allowing it to rely on such a reference, arguing simply that it was ESR's burden to prove a negative—i.e., that the pages of the manual to which it has been denied access teach away from or undercut the teachings in the pages Smaha and the requestor selectively chose to provide to the Patent and Trademark Office ("PTO"). The government is mistaken, as is the majority. The PTO should have refused to rely on the NetStalker manual as a reference, and should have refused to instigate or maintain a reexamination on such grounds.

The Board compounded its error by finding that the NetStalker Manual was publicly accessible by the critical date, despite the omission of important details in the supporting declaration. The Smaha declaration was telling more for what it failed to state than for what little it actually did say with regard to accessibility. Given his undisputed bias, the Board and majority should demand precision with respect to such important facts, and not rely on what appeared to be half-truths. If the manual really was publicly accessible as of the critical date, it would not have been difficult for Smaha to actually say so, and to support his statements with verifiable facts.

I. INCOMPLETENESS

The Board and the examiner relied on the facially incomplete NetStalker reference to find the claims of the ’236 Patent obvious. Specifically, the Board relied on pages from chapters 5 and 6 of NetStalker. Chapter 6, entitled “Configuring Misuse Detector,” appears to be complete. But chapter 5, entitled “Running *NetStalker*,” is woefully incomplete. The only pages present are 5-1, 5-3, 5-5, and 5-7. The Board relies specifically on page 5-5, despite the fact that the preceding and following pages are both missing. The very instructions on which the Board relied in chapter 5 are incomplete. While not cited by the Board, chapter 7, entitled “Managing and Analyzing Log Files,” contains only the first three pages of the chapter; despite that fact, the examiner found it meaningful to his analysis. The Board concluded that the portions of NetStalker that are present “serve to disclose that portion of NetStalker that *presumably* is relevant to the patentability of the ’236 patent” and that ESR did “not indicate[] that the portions of NetStalker provided are in any way irrelevant to the patentability of the ’975 [sic] patent.” *Ex Parte Enhanced Sec. Research, L.L.C.*, No. 2012-008692, Reexamination No. 90/010,849, 2012 WL 3801778, at *3 (B.P.A.I. Aug. 30, 2012) (“*Enhanced Sec.*”) (emphasis added).

Though the Board did not find or even consider whether the missing pages were unlikely to teach away from or further clarify the provided pages, the majority proceeds to make factual findings on those issues. The majority finds it implausible that the missing pages of NetStalker would contain evidence contrary to an obviousness finding and says it sees nothing in the submitted portions to clearly indicate that the missing pages would have been meaningful to the Board’s analysis. This is speculation on the part of the majority, however. Speculation cannot substitute for actual evidence that the missing pages are meaningless. Without those pages, neither this court nor the Board can determine whether the missing pages of NetStalker teach away from the claimed invention. Nor can we clarify whether the missing pages would reveal that NetStalker is actually less similar to the claimed invention than it might appear. And, we are unable to determine whether the NetStalker Manual was only an incomplete draft and, thus, not likely to be publicly accessible. Where a reference is proffered by an interested party with control over all information relating to that reference, it is not too much to ask that the proffer be complete in all material respects.

Though the majority disagrees, I believe the Board's analysis was legally insufficient because it was based only on a consideration of the evidence supporting a finding of obviousness, and did not consider the possibility of evidence contrary to such a finding. In an obviousness analysis, a reference must be considered "in its entirety, i.e., as a *whole*, including portions that would lead away from the invention in suit." *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561, 1568 (Fed. Cir. 1987). While the majority distinguishes *Panduit* on the ground that the contrary evidence ignored was clearly in the record in *Panduit*, I think that is a distinction without a meaningful difference. There is no doubt that what was missing from the reference here related to the operation of the NetStalker product—or at least that version of it—and related specifically to the disclosures in chapter 5 which the Board found central to its obviousness analysis. Whether the Board discounts evidence before it (what the majority says are the *Panduit* circumstances) or turns a blind eye to the existence of such evidence should not make a difference; in either instance, the Board's analysis is flawed.

This does not mean that the PTO can never rely on a reference that is incomplete. Considering an incomplete reference may be consistent with the obligation to consider a reference "as a whole" when only an incomplete reference is currently available and reliable evidence about what is missing from the reference is provided. The incomplete reference, in those circumstances, may be deemed the entire existing or relevant reference. This case does not fall into that category; the supporting declaration provides *no explanation* for NetStalker's incompleteness, and never even addresses that incompleteness. In fact, the Smaha declaration indicates that the version of NetStalker provided "is a true and correct copy," (J.A. 9705), which raises a question as to whether the manual ever existed in final form. Similarly, considering an incomplete reference may be consistent with the requirement to consider a reference "as a whole" when omitted portions of a voluminous reference clearly are not relevant because they are not directed to the field of the invention. In such a case, the reference is "whole" at least in *relevant* part. Again, this case is not that one; NetStalker's missing pages are in the very sections relevant to the field of the claimed invention. Thus, NetStalker cannot be considered by the Board "as a *whole*," *Panduit*, 810 F.2d at 1568, because it is facially incomplete in the relevant portions and there is no explanation for that incompleteness.

The government cites *In re NTP, Inc.*, 654 F.3d 1279, 1296 (Fed. Cir. 2011) for the proposition that a patentee "ha[s] the burden to prove that [a] document [i]s not authentic." Even assuming that a patentee by analogy has the burden to show the relevance of *missing* portions of a reference, *NTP* does not address relevance, and even if it did, ESR met that burden because the missing pages are from a chapter relevant to the field of the invention and contain portions of the very instructions on which the Board relied. Again, the pages *on either side* of the main page cited by the Board are not there. When a patentee does not have access to the missing pages, it can show little else, and this showing should be sufficient to render those pages relevant to the content of the prior art and to evidence potentially contrary to a conclusion of obviousness.

While I agree that section 2218 of the Manual of Patent Examining Procedure (8th ed. Rev. 9, Aug. 2012) is not dispositive, I believe it is consistent with a prohibition against the Board and the examiner relying on a reference that is incomplete in relevant part with no explanation of why that is so. Section 2218 requires that "a copy of each patent or printed publication relied on or referred to in the request, be filed with the request." *Id.* It does not indicate that *a portion* of a reference can be filed with a request. Section 2218 also provides that "[i]f any of the documents are not in the English language, an English language translation of all necessary and pertinent parts is also required." *Id.* Thus, the *entire* non-English document must be provided, which means that a patentee can gain access to the entire document by having it translated, and even the required *partial* translation must be sufficiently complete to include the relevant parts. No language in section 2218 suggests that a reference that is incomplete in relevant part can be submitted.

Given the potential impact of a Board decision on reexamination, due process concerns arise when, as here, a complete version of a reference is unavailable to a patentee, but the PTO relies on it with no explanation from the provider as to why it is incomplete. "[A] patent is a property right protected by the Due Process Clause . . . ." *Abbott Labs. v. Cordis Corp.*, 710 F.3d 1318, 1327 (Fed. Cir. 2013). While due process considerations frequently focus on notice and hearing, *cf. id.* at 1328, this court has acknowledged that additional procedures may be mandated by due process when the PTO acts. *See id.* at 1327. Beyond notice and an opportunity to be heard, "what additional procedures are guaranteed by due process requires balancing the various interests at stake." *Id.* at 1328 (citing *Mathews v. Eldridge*, 424 U.S. 319, 334-35 (1976)). While "excluding compulsory production of testimony in inter partes reexamination proceedings [did not] raise[] a serious constitutional problem" on the facts of *Abbott*, *id.* (internal quotation marks omitted), the same cannot be said in this case.

In determining what due process requires, the court is to consider three factors: "[f]irst, the private interest that will be affected by the official action; second, the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards; and finally, the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail." *Mathews*, 424 U.S. at 335. The second factor examines "the fairness and reliability of the existing . . . procedures." *Id.* at 343.

First, the patentee has a significant interest in the retention of its rights in a validly issued patent. This is unlike the situation in *Paltex Corp. v. Mossinghoff*, 771 F.2d 480 (Fed. Cir. 1985), in which this court concluded that a regulation barring a patentee "from communicating with the PTO during the three-month statutory period during which the PTO is required to decide whether any substantial new question of patentability is raised by a reexamination request" was not inconsistent with due process. *Id.* at 483, 486. In that case, the property interest was only "the temporary deprivation of full enjoyment of patent rights, for the period needed to correct an erroneous determination to reexamine [the] patents." *Id.* at 485. Here, the patentee is permanently, not temporarily, deprived of its enjoyment of patent rights.

Second, there is risk of an erroneous deprivation of those rights when the provider of an incomplete document is the one asking that a reexamination be instituted and is involved in active litigation with the patent holder. This is especially so where the only one with access to both the reference and information about the reference is a paid representative of that party. In such circumstances, minimal additional safeguards clearly are warranted. Allowing the PTO to rely on a reference that is unavailable and incomplete *without explanation* threatens the reliability and fairness of the proceedings.

The facts of this case illustrate the risk. Smaha, whose declaration purports to support NetStalker's use as a reference, was the Chief Executive Officer and chairman of the board of NetStalker's authoring organization. Smaha stated that he was "engaged as an expert by Juniper Networks, Inc. . . . in connection with the litigation against [ESR]," although he further stated that he had "no interest, personal or otherwise, in the outcome of Juniper's disputes with ESR." J.A. 9704. A paid expert for a party adverse to the patentee is not unqualifiedly disinterested; saying he lacks an interest does not change that fact. The provider of the NetStalker manual was in the best position to provide it in its entirety or explain the absence of the missing parts. ESR, on the other hand, had no formal procedural mechanisms to obtain the document or any further explanation from Smaha, and ESR's efforts to obtain that information informally were rebuffed. When PTO procedures do not require the provider of a reference to provide a complete reference or at least provide—under penalty for falsification—a statement that the document is complete in all relevant parts, that there is an explanation for any missing portions of the document, or that a document is otherwise available to the patentee, the incentive to mislead with partial submissions is great. Basic fairness to patentees should demand more.

Again, this case is different from *Paltex* in which the "risk of examiner error due to lack of information" is related "only to the question 'whether a substantial new question of patentability . . . is raised', 35 U.S.C. § 303, not the answer to the question." 771 F.2d at 485. Here, the risk of error does relate to the "answer to the question" of patent validity. While in *Paltex* the PTO's "expertise [wa]s a factor to be given weight in considering the risk of error *at this stage*," *id.* (emphasis added), the PTO's expertise can only be applied to the information provided to the examiner. When that information is fundamentally incomplete at the *resolution* of the validity inquiry, the benefit afforded by a "disinterested expert[]" cannot cure the problem.

Third, the PTO need not adopt any new, complex evidentiary procedures to cure this problem. The most straightforward corrective action is for the examiner or the Board to refuse to rely on a reference like the one proffered here. There may be some inconvenience and additional cost to the requester who would need to resubmit the reexamination request, but there would be none to the PTO. Requiring a complete document, an explanation for incompleteness, or an indication of public accessibility will strongly incentivize providers of references to meet at least one of these requirements in the first instance. The government's burden from this additional procedure would be minimal.

The relative dearth of other protective procedures in a reexamination reinforces the need to allow the patentee to challenge the examiner's and the Board's reliance on a reference that is unavailable and incomplete without explanation. A patentee may not seek discovery or resort to subpoenas to seek information in a reexamination. *See Abbott*, 710 F.3d at 1328. The absence of vehicles for discovery makes the ability of the patentee to challenge a reference on completeness grounds all the more critical;

otherwise the patentee would be defenseless against one who chooses to provide only those portions of a reference which undercut the validity of a patent. An interested provider of a reference should not be able to use a reference as a sword, while failing to provide the portions of it that may shield the patentee.

The due process balance also requires inquiry into the extent to which "judicial-type procedures must be imposed upon administrative action to assure fairness." *Mathews*, 424 U.S. at 348. Prohibiting the PTO from relying on non-probative evidence is hardly an elaborate judicial procedure and is certainly one that is necessary to assure the fairness of the proceedings. The Supreme Court has explained that "procedural due process rules are shaped by the risk of error inherent in the truthfinding process as applied to the generality of cases, not the rare exceptions." *Mathews*, 424 U.S. at 344. This does not bar finding a due process violation in an individual case, however, because "[a] fundamentally fair adjudication . . . is constitutionally required in all cases, and not just in the large majority." *Cushman v. Shinseki*, 576 F.3d 1290, 1299-1300 (Fed. Cir. 2009).

Due process requires "a fair hearing on the merits" of a claim. *Cushman*, 576 F.3d at 1299. In *Cushman*, the initial determination of the veteran's claim "was tainted by the presence of an improperly altered document," and "[t]he source of the fundamental unfairness that tainted the initial evaluation of Mr. Cushman's claim was never removed from any prior proceedings." *Id.* "The presentation of improperly altered material evidence has been found to constitute a due process violation in analogous cases." *Id.* at 1300. When the procedures applied by the PTO do not provide either this court or the patentee some means to determine whether, or some assurance that, the evidence on which the PTO relied was not improperly altered, those procedures cannot be consistent with due process.

The majority and the government cite nothing that *allows* the Board or the examiner to rely on an incomplete reference. I believe the majority errs in concluding that nothing *prohibits* the Board from relying on an incomplete reference; due process and concepts of fundamental fairness do. Accordingly, I would reverse the Board's obviousness finding because it is based on an unreliable reference.[1]

II. Public Accessibility

The majority also errs in concluding that Smaha's declaration was sufficient to establish that the NetStalker manual was accessible to the public before the critical date.

> Whether a reference is publicly accessible is a question of fact that we review for substantial evidence. A reference is publicly available if it was 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.

NTP, 654 F.3d at 1296 (citation omitted) (internal quotation marks omitted). "The proponent of the publication bar must show that prior to the critical date the reference was sufficiently accessible, at least to the public interest-

[1] While the majority emphasizes the Board's reliance on the Liepins article, the parties agree that Liepins provides only limited support for the Board's obviousness determination. Without the NetStalker Manual, there would have been no obviousness finding.

ed in the art . . . ." *In re Hall*, 781 F.2d 897, 899 (Fed. Cir. 1986).

Smaha said, "This version of the NetStalker manual was available in May 1996. Members of the public showing an interest in buying or licensing the NetStalker product could have obtained a copy of the manual by contacting Haystack . . . and requesting one." J.A. 9705. Smaha also said, "NetStalker was advertised no later than 1995." *Id.* The Board and the majority both conclude that members of the public would have known of NetStalker based on the advertisements as early as 1995 and would have received the manual upon request in May 1996. The first weakness in that conclusion is the supposed connection between the product advertised in 1995 and the May 1996 Manual. Smaha says "[t]his version," of the manual was "available" in May 1996. The front page of the manual indicates that it is "version 1.0.2." Nowhere does Smaha say that the 1.0.2 version of NetStalker is what was advertised in 1995. Nor does Smaha ever say that the version described in the manual was *ever* advertised to the public. Pointedly, while Smaha says members of the public interested in the NetStalker *product* could have gotten the relevant manual upon request, there is no indication that the public had any information available to it which would have prompted anyone to make such a request for that particular manual. And, there is no evidence that version 1.0.2 of NetStalker was ever manufactured or offered for sale.

Thus, not only is there no evidence that the version of NetStalker discussed in the manual was ever advertised, but there is no evidence—from the Smaha declaration or otherwise—that *any* sales ever occurred prior to the critical date, that the sales that did occur were of the version of the product described in the reference, or that any of those sales were accompanied by the relevant manual. Smaha's declaration was submitted by counsel.

Had the gaps in his testimony been fillable—rather than conveniently omitted—it is likely those gaps would have been filled. The majority reads facts into the declaration that are simply not there; the absence of those facts is not harmless as the majority seems to believe, they are telling.

Perhaps most troubling is Smaha's statement that the reference submitted is a "true and correct copy" of the manual which he said would have been made available to members of the public in May 1996, if requested. It is undisputed, however, that the submitted manual was incomplete. And it is undisputed that the submitted manual bore several indicia of a draft document: a cryptic date legend on its cover, question marks in the index, and the absence of the last ten pages of the final chapter. If an incomplete and unfinished manual is the "true and correct" version of the reference in existence in May 1996, any claim that the public would have been given access to it, or even would have known to request it, is even more suspect.

It is worth noting, moreover, that Smaha filed his own patent application—after the critical date of the '236 patent—to similar technology, but did not list his own manual as prior art. If we assume Smaha was not purposely misleading the PTO with that filing, the failure to cite the manual indicates that it was either an unfinished draft document or never available to the public.

For all these reasons, I believe the Board's finding that the reference was publicly accessible before the critical date is not supported by substantial evidence. Smaha's statements are sufficiently ambiguous to encompass both scenarios in which the NetStalker manual would have been publicly accessible and those in which it would not have been so. The Board cannot conclude that a reference was publicly accessible when no evidence provides sufficient specificity to support that conclusion. The majority should not endorse its having done so.

III. Obviousness

Because I believe the Board should never have reached the question of obviousness on this record, I do not analyze the majority's obviousness analysis in detail. I take issue, however, with the fact that the majority bases its judgment on grounds that differ from those upon which the Board relied. This Court may not stray from the Board's reasoning for purposes of supporting its judgment. *See SEC v. Chenery Corp.*, 332 U.S. 194, 196 (1947) ("[A] reviewing court, in dealing with a determination or judgment which an administrative agency alone is authorized to make, must judge the propriety of such action solely by the grounds invoked by the agency.");*see also, In re Applied Materials, Inc.,* 692 F.3d 1289, 1294 (Fed. Cir. 2012) ("The Board's judgment must be reviewed on the grounds upon which the Board actually relied."). Notably, the Board did not, as the majority states, find that, "in combination, these two pieces of prior art [NetStalker Manual and Liepins] disclosed all of the elements of the '236 patent." Maj. at 8.

Instead, the Board found, and the government admits that, NetStalker and Liepins do not "specifically teach[] using the assigned strength or severity level as a basis for blocking communications." Appellee's Br. 1. The Board filled this gap by relying on what it characterized as "ordinary creativity":

> NetStalker discloses not only a user defined severity level of a security breach but also triggering an alarm when a certain number of (security) events are recognized and blocking communications when the alarm is triggered. Based on the NetStalker reference, one of ordinary skill in the

> art would have known to characterize a security breach based on level of severity (i.e., user defined severity) and block communications based on when a condition has been achieved (for example, when a threshold number of security events have been encountered).
>
> Given NetStalker's disclosure of blocking communications when a threshold criteria is met indicating a security breach and given that one of ordinary skill in the art is a person of ordinary creativity, not an automaton, one of skill in the art would have understood the practice of blocking communications when a security breach is detected, the security breach being of sufficient severity as to exceed a threshold. NetStalker further discloses that a severity level is assigned to security breach events thus further indicating that blocking communications when a severity level of security breach is identified would have been obvious (as assigning severity levels to security breaches were known to those of ordinary skill in the art), or at least obvious to try, as a matter of ordinary creativity and common sense.

Enhanced Sec., at *8 (citations omitted) (internal quotation marks omitted).

As ESR argues, however, obviousness is not shown by the mere fact that each of the elements "was, independently, known in the prior art." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007). "Although common sense directs one to look with care at a patent application that claims as innovation the combination of two known devices according to their established functions, it can be important to identify *a reason* that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does." *Id.* (emphasis added). The Board identified no such reason. Specifically, the Board identifies no "design need or market pressure to solve a problem," *id.* at 421, such that the new combination using severity as the basis for blocking communication would have been "obvious to try," *id.* And, the Board identifies no "problem" that one of ordinary skill was trying to solve at the time of the invention.

Apparently recognizing these gaps in the Board's analysis, the majority accepts the government's suggestion that it fill them with an alternative analysis. The government argues that the undisclosed use of severity assessments for blocking purposes is actually disclosed in the NetStalker reference because "NetStalker itself includes the idea of tailoring the response to the severity of a threat, *i.e.*, by only initiating action after a threshold number of events has occurred." Appellee's Br. 20. The Board expressly found this teaching missing in NetStalker, however. I agree.

While the majority relies on the statement in NetStalker that "you may want *NetStalker* to take an automatic action (a 'response')," a "[r]esponse" is simply another type of alarm that is listed in a "description of supplied alarms." NetStalker at 4-2, 4-4. It is described as "[p]rovid[ing] a general purpose response to activities taking place on the network [reserved for future use]." *Id.* at 4-4 (final brackets in original). The pages referenced by the Board also indicate that "[r]esponse" is "Reserved for future use." *Id.* at 5-5, 6-16. While the "User Defined" alarms are also referred to as "responses," the response "can be as simple as sending a beep to the system console or more complex such as logging the event in syslog." *Id.* at 4-5, 5-5, 6-16. None of this suggests that the response is necessarily related to a shun alarm or that the response would be triggered by the severity.

Thus, not only does the majority violate the principles described in *Chenery* governing review of administrative agency determinations, but its independent obviousness analysis seems inconsistent with the very reference upon which the majority's alternative analysis relies.

IV. Conclusion

For these reasons, I cannot join the majority in its conclusions on the reliability of the NetStalker reference, on public accessibility, or on the obviousness of the relevant claims of the '236 patent. I cannot join in depriving a patentee of its patent rights on these grounds. I respectfully dissent.