

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES

---

*Ex parte* HUNGCHOU TSAI

---

Appeal 2007-2300  
Application 09/972,596  
Technology Center 2100

---

Decided: December 18, 2007

---

Before LANCE LEONARD BARRY, HOWARD B. BLANKENSHIP, and  
JEAN R. HOMERE, *Administrative Patent Judges*.

BARRY, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF THE CASE

A Patent Examiner rejected claims 1-20. The Appellant appeals therefrom under 35 U.S.C. § 134(a). We have jurisdiction under 35 U.S.C. § 6(b).

A. INVENTION

The invention at issue on appeal protects a computer against a virus. With the widespread use of computers, computer networks such as the

Internet, and electronic mail ("e-mail"), computer viruses have become problematic to computers and their users. (Spec. 1.) In particular, the global nature of the Internet enables a virus-infected e-mail to spawn a large amount of network traffic that can jam servers and the Internet. Such a virus can be destructive and can cause lost business due to computer downtime. (*Id.* 6.)

For its part, the Appellant's invention does not detect or repair specific viruses, but alerts users to the fact that they are opening e-mails that could contain viruses and allows them to delete questionable e-mails. (*Id.* 10.) To wit, the invention downloads e-mail without executing it. The invention then determines whether the downloaded e-mail includes any infected e-mail. If so, it disposes of the infected e-mail. (*Id.* 25.)

#### B. ILLUSTRATIVE CLAIMS

Claims 1 and 11, which further illustrate the invention, follow.

1. A method for avoiding electronic mail (email) attacks on a computer, comprising:

downloading one or more emails in virtual-copy format to prevent the one or more emails from executing;

determining whether an infected email is in-the downloaded one or more emails; and

disposing of the infected email.

11. A system for avoiding electronic mail (email) attacks on a computer, comprising:

means for downloading one or more emails in virtual-copy format to prevent the one or more emails from executing;

means for determining whether an infected email is in the downloaded one or more emails; and

means for disposing of the infected email.

### C. REJECTIONS

Claims 1-3, 5-13, and 15-20 stand rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,785,732 ("Bates"). Claims 4 and 14 stand rejected under 35 U.S.C. § 103(a) as obvious over Bates and U.S. Patent No. 6,763,462 ("Marsh").

### II. CLAIM GROUPING

"When multiple claims subject to the same ground of rejection are argued as a group by appellant, the Board may select a single claim from the group of claims that are argued together to decide the appeal with respect to the group of claims as to the ground of rejection on the basis of the selected claim alone. Notwithstanding any other provision of this paragraph, the failure of appellant to separately argue claims which appellant has grouped together shall constitute a waiver of any argument that the Board must consider the patentability of any grouped claim separately." 37 C.F.R. § 41.37(c)(1)(vii) (2006).<sup>1</sup> When the patentability of dependent claims in

---

<sup>1</sup> We cite to the version of the Code of Federal Regulations in effect at the time of the Appeal Brief. The current version includes the same rules.

particular is not argued separately, the claims stand or fall with the claims from which they depend. *In re King*, 801 F.2d 1324, 1325 (Fed. Cir. 1986); *In re Sernaker*, 702 F.2d 989, 991 (Fed. Cir. 1983).

Here, claims 1-3, 5-13, and 15-20 are subject to the same ground of rejection. The Appellants argue claims 1-3 and 5-10 as a first group and claim 11-12 and 14-20 as a second group. (App. Br. 3-6). Therefore, we select independent claims 1 and 11 as the sole claims on which to decide the appeal of the respective groups. "With this representation in mind, rather than reiterate the positions of the parties *in toto*, we focus on the issues therebetween." *Ex Parte Zettel*, No. 2007-1361, 2007 WL 3114962, at \*2 (BPAI 2007).

### III. AVOIDING ATTACKS ON A COMPUTER

The Examiner finds, "As per claims 1 and 11, Bates teaches a method and system for avoiding electronic mail (email) attacks on a computer . . ." (Ans. 4.) The Appellants argues, "In contrast, in the present invention, the virus checking is done on the client machine, not on the mail server." (Reply Br. 3.) Therefore, the issue is whether Bates avoids e-mail attacks on a computer.

"Both anticipation under § 102 and obviousness under § 103 are two-step inquiries. The first step in both analyses is a proper construction of the claims . . . The second step in the analyses requires a comparison of the

properly construed claim to the prior art." *Medichem, S.A. v. Rolabo, S.L.*, 353 F.3d 928, 933 (Fed. Cir. 2003) (internal citations omitted).

#### A. CLAIM CONSTRUCTION

"[A] claim construction analysis must begin and remain centered on the claim language itself . . ." *Innova/Pure Water, Inc. v. Safari Water Filtration Systems, Inc.*, 381 F.3d 1111, 1116 (Fed. Cir. 2004). Here, contrary to the Appellant's argument, neither claim 1 nor claim 11 requires virus checking to be done on a client machine. Instead, the representative claims merely recite in pertinent part the following limitations: "avoiding electronic mail (email) attacks on a computer . . ."

#### B. ANTICIPATION ANALYSIS

"[A]nticipation is a question of fact." *In re Hyatt*, 211 F.3d 1367, 1371-72 (Fed. Cir. 2000) (citing *Bischoff v. Wethered*, 76 U.S. (9 Wall.) 812, 814-15, 19 L. Ed. 829 (1869); *In re Schreiber*, 128 F.3d 1473, 1477 (Fed. Cir. 1997)). "A reference anticipates a claim if it discloses the claimed invention 'such that a skilled artisan could take its teachings in combination with his own knowledge of the particular art and be in possession of the invention.'" *In re Graves*, 69 F.3d 1147, 1152 (Fed. Cir. 1995) (quoting *In re LeGrice*, 301 F.2d 929, 936 (CCPA 1962)).

Here, Bates describes "a web server computer system[, which] includes a virus checker and mechanisms for checking e-mails and their

attachments, downloaded files, and web sites for possible viruses." (Col. 2, ll. 11-14.) "When an e-mail message contains a detected virus, the message is discarded, and both the sender and recipient are informed via e-mail that the message contained a virus." (*Id.* at ll. 14-16.) "This configuration allows one virus checker on the web server to protect each web client [computer] connected to it from viruses . . ." (Col. 4, ll. 47-49.) "[T]he likelihood of a web server spreading viruses is greatly reduced when information received by the web server is checked for viruses before forwarding the information to a web client." (*Id.* at ll. 54-57.) Because the web server discards infected e-mail before such e-mail can reach the client computers connected thereto, we agree with the Examiner's finding that Bates avoids e-mail attacks on a computer.

#### IV. DOWNLOADING E-MAIL WITHOUT EXECUTING IT

The Examiner finds, "Bates discloses downloading e-mails to an intermediate location, such as a web server, preventing the emails to execute on the client . . . column 6, lines 31-37 . . ." (Ans. 4.) The Appellant argues that "there is no mention of downloading in a virtual copy format to prevent execution." (Reply Br. 2.) Therefore, the issue is whether Bates downloads e-mail without executing it.

##### A. CLAIM CONSTRUCTION

"Claims must be read in view of the specification, of which they are a part." *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc). Here, claims 1 and 11 recite in pertinent part the following

limitations: "downloading one or more emails in virtual-copy format to prevent the one or more emails from executing . . ." The Appellant identifies no definition of the term "virtual-copy format" in his Specification. For our part, we only find an explanation that "[t]he virtual-copy format allows the downloaded content to be safely analyzed in that virtual-copy format data cannot be executed." (Spec. 11.) Reading the representative claims in view of this explanation, therefore, the limitations merely require downloading e-mail without executing it.

#### B. ANTICIPATION ANALYSIS

Figure 1 of Bates shows "specific implementation of [its] web server computer system . . ." (Col. 4, ll. 58-59.) The web server hosts a number of software applications including an "e-mail server application 124; a virus checker application 125 with associated virus definitions 126; . . . a virus control mechanism 131 that includes a web page virus processing mechanism 132, an e-mail virus processing mechanism 134, and a file virus processing mechanism 136; and a virus information database 138." (Col. 5, ll. 5-12.)

The reference explains that the "[e]-mail virus processing mechanism 134 . . . processes e-mails received by e-mail server application 124 from other e-mail servers," (col. 6, ll. 21-25), "scan[ning] . . . incoming . . . e-mail messages for viruses." (*Id.* at ll. 26-27.) "If a virus is detected in the e-mail itself, the e-mail message is deleted, and an e-mail

message is sent to the sender and intended recipient notifying both that the e-mail contained a virus." (*Id.* at ll. 27-30.)

Based on this explanation, we find that the web server computer system receives and processes e-mail messages without executing the messages.<sup>2</sup> Because the web server computer system receives and processes e-mail messages without executing the messages, we agree with the Examiner's finding that Bates downloads e-mail without executing it. Therefore, we affirm the rejection of claim 1 and of claims 2, 3, and 5-10, which fall therewith.

Rather than arguing the rejection of claim 4 separately, the Appellant reiterates the aforementioned arguments. (App. Br. 6-9.) Unpersuaded by these arguments, we also affirm the rejection of this claim. We have one more issue, however, to address regarding claims 11-20.

## V. MEANS FOR DETECTING AND DISPOSING

The Examiner finds that "Bates teaches a . . . system for avoiding electronic mail (email) attacks on a computer" (Answer 4) and that the system comprises the following features:

determining whether an infected email is in the downloaded one or more emails (using the virus checking software to check for viruses in the message; column 2, lines 10-20; column 5, lines 44-57; column 6, lines 21-27; column 8, lines 1-44; column 9, lines 22-40);

---

<sup>2</sup> In fact, the web server is not described as hosting an application for executing e-mail.

and disposing of the infected email, wherein the infected email is determined based on one or more of the following: an email from field, an email to field, and an email subject field (deleting an infected email; column 2, lines 10-20; column 6, lines 27-30; column 6, lines 39-49; column 9, lines 28-30 and lines 36-40; column 11, lines 59-65).

(*Id.*) Noting that "claim 11 is expressed as a means claims pursuant to Section 112," (App. Br. 6), the Appellant makes the following allegations

The structure for the means for determining an infected email is the client computer that can download one or more emails and executes a browser or an email-like software (such as the embodiments shown in Figs. 4-5) to allow the user to safely view the content of the email before making a decision to delete or keep the email. The structure for the means for disposing the infected email in one embodiment is the client computer running a human user interface that allows the user to make the deletion decision.

(*Id.*) Based on these allegation, he argues, "Since Bates fail [sic] to show any corresponding structure, Bates cannot anticipate claim 1[1]." (*Id.*) Therefore, the issue is whether Bates discloses a software process for determining whether e-mail is infected with a virus and for disposing of infected e-mail.

#### A. CLAIM CONSTRUCTION

"[D]uring examination proceedings, claims are given their broadest reasonable interpretation consistent with the specification." *Hyatt*, 211 F.3d at 1372. In particular, "[a]n element in a claim for a combination . . . expressed as a means . . . for performing a specified function without the

recital of structure, material, or acts in support thereof . . . shall be construed to cover the corresponding structure . . . described in the specification and equivalents thereof." 35 U.S.C. §112, ¶ 6 (2007).

Here, claim 11 recites in pertinent part the following limitations: "means for determining whether an infected email is in the downloaded one or more emails; and means for disposing of the infected email." To the extent the Appellant is arguing that the "means for determining" should be construed to cover a human user making a deletion decision, we remind him that "a human being cannot constitute a 'means' . . ." *Default Proof Credit Card System, Inc. v. Home Depot U.S.A., Inc.*, 412 F.3d 1291, 1300 (Fed. Cir. 2005) (citing *In re Prater*, 415 F.2d 1393, 1398 (CCPA 1969)).

Turning to the Appellant's Specification, we note that it describes "an exemplary process 200 to detect and delete emails potentially infected with a virus or a worm." (Spec. 10.) More specifically, "the process 200 displays brief information for each email and highlights potential emails that contain worms or viruses (step 224)." (*Id.* 12.) "Based on [a] user's instructions, the process 200 accesses the user's mail server and removes the selected emails stored in the user's account at the mail server . . . (step 228)." (*Id.*) Construing the representative claim to cover the broadest, reasonable structure described in the Specification, the limitations require a software process for determining whether e-mail is infected with a virus and for disposing of infected e-mail.

## B. ANTICIPATION ANALYSIS

As mentioned regarding the prior issue, Bates' web server computer system hosts a number of software applications including an e-mail virus processing mechanism 134. More specifically, the reference's "FIG. 7 is a flow diagram of a method performed by the e-mail virus processing mechanism 134 . . ." (Col. 3, ll. 15-16.) When an e-mail message is received, "the e-mail virus processing mechanism reads the e-mail message (step 720), and checks the e-mail message body for viruses (step 722) using [a] selected virus checker application." (Col. 9, ll. 25-28.) "If a virus is found (step 724=YES), the e-mail message is deleted (step 730). . ." (*Id.* at ll. 34-35.)

Because the reference's e-mail virus processing mechanism checks e-mail messages for viruses and deletes infected messages, we agree with the Examiner's finding that Bates discloses a software process for determining whether e-mail is infected with a virus and for disposing of infected e-mail. Therefore, we affirm the rejection of claim 11 and of claims 12, 13, and 15-20, which fall therewith.

Rather than arguing the rejection of claim 14 separately, the Appellant reiterates the aforementioned arguments. (App. Br. 6-9.) Unpersuaded by these arguments, we also affirm the rejection of this claim.

## VI. ORDER

In summary, the rejection of claims 1-3, 5-13, and 15-20 under § 102(e) is affirmed. The rejection of claims 4 and 14 under § 103(a) is also affirmed.

"Any arguments or authorities not included in the brief or a reply brief filed pursuant to [37 C.F.R.] § 41.41 will be refused consideration by the Board, unless good cause is shown." 37 C.F.R. § 41.37(c)(1)(vii). Accordingly, our affirmance is based only on the arguments made in the briefs. Any arguments or authorities omitted therefrom are neither before us nor at issue but are considered waived. *Cf. In re Watts*, 354 F.3d 1362, 1367 (Fed. Cir. 2004) ("[I]t is important that the applicant challenging a decision not be permitted to raise arguments on appeal that were not presented to the Board.")

No time for taking any action connected with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

**AFFIRMED**

pgc

TRAN & ASSOCIATES  
6768 MEADOW VISTA CT.  
SAN JOSE CA 95135