BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

Internal distribution code:
(A) [ ] Publication in OJ
(B) [ ] To Chairmen and Members
(C) [ ] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 5 December 2008

Case Number: T 1028/06 - 3.5.01

Application Number: 03006814.2

Publication Number: 1376427

IPC: G06F 17/60

Language of the proceedings: EN

Title of invention:
SPAM detector with challenges

Applicant:
MICROSOFT CORPORATION

Opponent:
-

Headword:
Spam detector/MICROSOFT

Relevant legal provisions:
-

Relevant legal provisions (EPC 1973):
EPC Art. 54(1)(2), 56

Keyword:
"Novelty - main request (no)"
"Inventive step - auxiliary requests (no)"
"Automation - obvious desideratum (yes)"
"Trade-off - derivable (yes)"
"Trade-off point - obvious (yes)"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1028/06 - 3.5.01

D E C I S I O N
of the Technical Board of Appeal 3.5.01
of 5 December 2008

Appellant: MICROSOFT CORPORATION
One Microsoft Way
Redmond, Washington 98052-6399 (US)

Representative: Grünecker, Kinkeldey,
Stockmair & Schwanhäusser
Anwaltssozietät
Leopoldstrasse 4
80802 München (DE)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 11 January 2006 refusing European application No. 03006814.2 pursuant to Article 97(1) EPC 1973.**

Composition of the Board:

Chairman: S. Steinbrener
Members: W. Chandler
P. Schmitz

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division to refuse the European patent application on the grounds that the subject-matter of independent claims 1, 23, 27 and 28 of the main request did not involve an inventive step (Article 56 EPC 1973), the same claims of the first auxiliary request did not disclose the invention sufficiently for it to be carried out (Article 83 EPC 1973) and claims 1 and 2 of the second auxiliary request did not involve an inventive step (Article 56 EPC 1973). The following documents were mentioned inter alia in the decision:

D1: US-A-6 161 130
D2: WO-A-99/10 817
D3: US-A-6 112 227

II. In the statement setting out the grounds of appeal the appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the main or first or second auxiliary request on file. The appellant also made an auxiliary request for oral proceedings.

III. In the communication accompanying the summons to oral proceedings, the Board summarised the issues to be discussed.

IV. At the oral proceedings before the Board, the appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the main request filed during the oral proceedings before the Board, or on auxiliary request 1 or 2 on which the

decision of the examining division was based. At the end of the oral proceedings, the Chairman announced the decision.

V. Claim 1 of the main request reads as follows:

"A computer system facilitating detection of unsolicited e-mail comprising:
an e-mail component that receives or stores messages and computes associated probabilities that the e-mail messages are spam; and,
a challenge component that sends a challenge to an originator of an e-mail message having an associated probability greater than a first threshold."

Claim 1 of the first auxiliary request essentially adds to the end of claim 1 of the main request that the "originator's computer automatically responds to the challenge".

Claim 1 of the second auxiliary request reads as follows:

"A method for detecting unsolicited e-mail, said method comprising the steps of:
receiving an e-mail message (804);
detecting (811) if the sender of the e-mail message is listed in a legitimate e-mail sender store and, if the sender of the e-mail is in the legitimate e-mail sender store, identifying the e-mail as not being a spam e-mail;
in case that the sender of the e-mail message is not in the legitimate e-mail sender store, determining (820) whether the sender of the e-mail message is in a spam

sender store and if so, identifying (816) the e-mail message as spam;
in case that the sender of the e-mail message is not in the spam sender store, determining (808,828) the probability that the e-mail message is spam;
comparing (828) the calculated probability with a first threshold and identifying the e-mail message as not being spam in case that the probability is smaller than that first threshold;
in case that the calculated probability is greater than the first threshold but smaller than a second threshold, sending (832) a challenge to the sender of the e-mail message and identifying the e-mail message as spam in case the calculated probability is greater than said second threshold value;
in case that a challenge has been sent to the sender, waiting (836) for a response from the sender to the challenge and when said response is received, determining whether the challenge has been correctly answered;
in case that the challenge has been correctly answered identifying the e-mail message as not being spam and adding (844) the sender to the legitimate e-mail sender store and in case the response has not been correctly answered, identifying (824) the e-mail message as spam and adding (848) the sender to the spam sender store."

VI. The appellant argued essentially as follows:

Dl did not suggest that the approach taken there had any deficiencies and in particular that the threshold suggested by Dl could no longer be used as a reference to distinguish between solicited e-mails and

unsolicited e-mails but as a trigger to send a challenge to the originator of the respective e-mail.

D2 suggested that when an e-mail message was received from a sender who was not known by the system, a challenge was sent back to the sender to which he had to give a response. The response was checked and if it was valid, the message was accepted. The approach taken by D2 did not lead in the direction of the present invention because in D2 the challenge was sent to any originators of e-mails that were not already known to the receiving system. It appeared that the examining division had the same understanding of Dl and D2 as the appellant, but had constructed a combination of the two teachings based on hindsight.

The checks made in D2 before sending the challenge were hard yes/no decisions that were not equivalent to the soft probability checks of the invention.

Concerning the objection under Article 83 EPC to the first auxiliary request, the skilled person would know how to implement the additional feature of automatically responding to the challenge based on his relevant skills. It was not the implementation of this feature, but the idea itself that was not obvious. A straightforward implementation would be a computational challenge so that an automatic response caused considerable computational load for senders of mass e-mails.

Claim 1 of the second auxiliary request had a great number of details not known from either Dl nor D2 and therefore it was not understood why the examining

division came to the conclusion that the subject-matter was rendered obvious in the light of D1 and D2. Again, the argumentation provided by the examining division under item 5 of the decision was artificial and based on hindsight.

Reasons for the Decision

1. The appeal complies with the requirements referred to in Rule 65(1) EPC 1973 and is therefore admissible.

2. The application relates to filtering unsolicited e-mails or "spam". It is generally known to classify e-mails using a rule-based classifier, e.g. by looking for certain words in the subject line or the body of the text. However, this is not always accurate (see paragraphs [0007] to [0010] of the application).

3. The idea of the invention in the main and first auxiliary requests (embodiments of Figures 1 to 4) is that if an e-mail has a probability of being spam that is greater than a (first) threshold, a "challenge" is sent to the originator of the e-mail that must be answered ("automatically" in the first auxiliary request). In the second auxiliary request (embodiment of Figure 6), the challenge is only sent if the probability is in a "questionable" area between the first threshold and a second threshold. The response to the challenge is used to classify the e-mail as being or not being spam and for classifying the originator as being a spam sender or a legitimate sender, respectively.

Main request

4. The examining division considered that the subject-matter of claim 1 was not inventive over the combination of D1 and D2. The Board essentially agrees with the examining division's approach (see below in connection with the more limited second auxiliary request). However, the Board considers that because of the broad formulation of the claim, it is even not new over D2 alone.

5. D2 discloses a system that filters e-mails according to whether the originator is known to the recipient and according to various parts of the message (see Figure 7). It sends a challenge 450 if the validity of the originator cannot be determined. One of the tests for this is whether the originator is on the acceptance list of recipient (Figure 7: 425 and page 27, lines 1 to 10). In the Board's view this test can be considered to be a computation of the probability that the e-mail message is spam, in the sense of the first feature of the claim; if the sender is on the list, the probability is zero, otherwise it is non-zero. As a result, the challenge is sent to the sender of the e-mail if the probability is greater than a first threshold, in this case zero, according to the second feature of the claim.

6. The appellant argued that when D2 checks whether the originator is on the acceptance list, it does not compute a probability that the e-mail is spam in the sense of the claim, but simply makes a hard yes/no decision. However, the Board cannot agree with this distinction based on the wording of the claim because

in its broadest English meaning, "compute" covers any type of information processing producing the probability, which is what happens in D2, albeit that the probability is zero or non-zero.

7. Accordingly, under this interpretation, the subject-matter of claim 1 is not new (Article 54(1) and (2) EPC 1973).

First auxiliary request

8. Claim 1 of the first auxiliary request adds to that of the main request the feature that the originator's computer automatically responds to the challenge.

9. There was some discussion before the examining division and before the Board as what the effect of this feature was and how it was achieved. The predominant idea at the oral proceedings before the examining division was that the sender of the e-mail had some secret that was used to reply to the challenge (see minutes of the oral proceedings at page 4). At the oral proceedings before the Board, the representative argued that no secret was necessary, but the level of computational difficulty of the challenge must be manageable for the sender of a single e-mail, but too demanding for a spammer sending millions of e-mails. The representative found support for this interpretation in the application at column, 13, lines 25 to 28.

10. Under the latter interpretation, the intended effect of automatically responding to the challenge is to make the response easier for a legitimate sender, but difficult for a spammer. However, the actual means for

doing this are not claimed (and arguably not described). Even the appellant argues that it is not the implementation of this feature, but the idea itself that it not obvious. In the Board's view, the mere idea of automating a task to make it easier for the user is an obvious desideratum. If it turns out that this automatic response is a burden to a spammer, a bonus effect is achieved that cannot confer an inventive step to an otherwise obvious solution.

11. Accordingly, the subject-matter of claim 1 of the first auxiliary request does not involve an inventive step (Article 56 EPC 1973).

Second auxiliary request

12. The Board agrees with the appellant that claim 1 of the second auxiliary request has "a great number of details", at least compared to claim 1 of the main request. However, the Board does not agree that they are not known from either D1 or D2 since these documents together disclose most of them. In fact, the examining division's analysis at point 5 of the reasons appears to be correct, namely that the only features not anticipated by the combination of these documents are the automatic update of the blocking list and not sending a challenge if the probability is greater than a second threshold.

13. In detail, it is common ground that D1 discloses a method for detecting unsolicited e-mail comprising the steps of:

determining the probability that the e-mail message is spam (column 4, lines 62 to 67);
comparing the calculated probability with a first threshold and identifying the e-mail message as not being spam in case that the probability is smaller than that first threshold (column 5, lines 4 to 7 and the "non-spam" category mentioned at line 21);
identifying the e-mail message as spam in case the calculated probability is greater than a second threshold value (implicit from the classification into the categories corresponding to "different degrees" of spam, namely "certain spam", "questionable spam" and non-spam" at column 5, lines 18 to 21).

14. Claim 1 therefore differs from D1 by:
a) identifying the e-mail as not being spam if the sender of the e-mail is in a legitimate e-mail sender store;
b) identifying the e-mail message as spam if the sender of the e-mail message is in a spam sender store;
c) in case that the calculated probability is greater than the first threshold but smaller than the second threshold, sending a challenge to the sender of the e-mail message;
d) determining whether the sent challenge has been correctly answered;
e) in case that the challenge has been correctly answered identifying the e-mail message as not being spam and adding the sender to the legitimate e-mail sender store and in case the response has not been correctly answered, identifying the e-mail message as spam and adding the sender to the spam sender store.

15. It is also agreed that these features solve the problem of increasing the reliability provided by the spam classification of the probabilistic classifier.

16. The appellant argues that Dl does not suggest that there is any problem with the approach used to detect spam. However, the Board considers that, firstly, such problems would come to light in the normal operation of probabilistic spam filters. In particular, the "certain spam" in D1 might turn out not to be so and the "questionable spam" must be checked manually. Secondly, the general problem of misclassifying e-mails by spam filters was well known in the art. D2 gives an account of such problems at page 4, line 15 to column 5, line 26. In particular, D2 mentions the problem of the risk of automatically discarding e-mails and the problem of having to scan manually suspected spam, which would be problems facing the user of D1.

17. As a result, the Board is of the view that the skilled person would consider improving the reliability of the spam filtering in D1 with the solutions proposed in D2. Firstly, the idea of using acceptance/blocking lists is described in D2 at page 5, lines 2 to 10 as conventional. D2 also discloses automatically accepting or rejecting e-mails from senders on these respective lists ("acceptance list" - Figure 7: 425 and "blocking list" - Figure 7: 415). The Board considers that it would be obvious to incorporate this idea into D1 according to distinguishing features a) and b), the order having no effect on the system.

18. Furthermore, the Board considers that it would be obvious to increase the reliability by incorporating a

challenge component (Figure 7: 450). The appellant argues that combining Dl and D2 would lead to a system where, irrespective of the probability, a challenge is sent to all originators of e-mails not known to the receiving system. However, the Board considers that the skilled person would consider only challenging some e-mails for various reasons. Firstly, challenging all e-mails would make the probabilistic classification redundant. Secondly, D2 does not challenge every e-mail anyway. Apart from distinguishing e-mails from senders on the acceptance and blocking lists, it also checks another situation, namely whether the originator's address is, or appears to be ("as best possible"), valid "before going through the trouble of composing and returning a Challenge" (Figure 7: 450 and page 27, line 26 to page 28, line 13). In the Board's view, the skilled person would derive from this the general idea that challenging a subset of e-mails is a trade-off between "trouble" or effort and additional certainty of classification. One obvious trade-off point would be to challenge the e-mails identified as "questionable spam" by the classifier of D1, i.e. where the calculated probability is greater than the first threshold but smaller than a second threshold, according to distinguishing feature c). After sending a challenge, it follows that the system must determine whether it has been correctly answered, according to feature d).

19. Finally, D2 discloses adding the sender to the legitimate e-mail sender store if the challenge is answered correctly (Figure 7: 470), according to part of feature e). The Board agrees with the examining division that it would be an obvious analogy to add the sender to the spam sender store if the response is not

answered correctly, according to the remaining part of the feature.

20. Accordingly, the subject-matter of claim 1 of the second auxiliary request does not involve an inventive step (Article 56 EPC 1973).

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

T. Buschek S. Steinbrener