(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 August 2010 (26.08.2010)

PCT

(10) International Publication Number
WO 2010/094626 A1

(51) International Patent Classification:
G06Q 10/00 (2006.01) *H04L 12/58* (2006.01)

(21) International Application Number:
PCT/EP2010/051766

(22) International Filing Date:
12 February 2010 (12.02.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09153230.9 19 February 2009 (19.02.2009) EP

(71) Applicant *(for all designated States except US)*: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, New York 10504 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PHILLIPS, Christopher** [GB/GB]; IBM United Kingdom Limited, Hursley Park, Hursley, Winchester Hampshire SO21 2JN (GB). **WINCHESTER, Joseph, Robert** [GB/GB]; IBM United Kingdom Limited, MP 189, Hursley Park, Hursley, Winchester Hampshire SO21 2JN (GB).

(74) Agent: **STRETTON, Peter, John**; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Hursley, Winchester Hampshire SO21 2JN (GB).

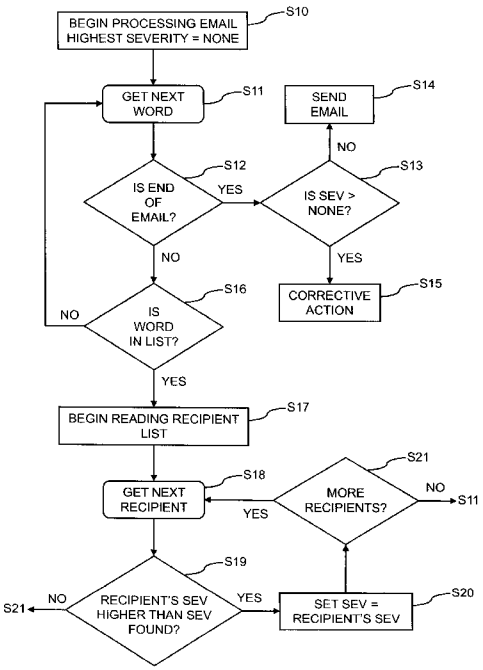
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: MESSAGE HANDLING

Fig. 6



(57) Abstract: A method of handling a message comprises receiving a message comprising content and one or more intended recipients, selecting one or more rules according to the or each intended recipient, checking the content of the message according to each selected rule to identify inappropriate content, and performing a predetermined corrective action, if inappropriate content is identified. In a preferred embodiment, the step of selecting one or more rules according to each intended recipient comprises identifying a group to which an intended recipient belongs, and selecting each rule according to the identified group.

WO 2010/094626 A1

Published:

— *with international search report (Art. 21(3))*

MESSAGE HANDLING

This invention relates to a method of, and system for, handling a message. In one embodiment, the invention can provide a method and process for checking that an email does not contain any information inappropriate for the recipient.

A user of a messaging system such as email will typically interact with many other users. An example of this is a user within an organisation such as a corporation or academic institution where some emails are received from and sent to colleagues in the same organisation, while other email correspondence may be personal, may be to customers, or may be to different organisations of which the same email user is a part, and so forth. Email, by its nature is informal and messages are often written in haste and without undue checking.

A known problem is where an email thread that begins within one group of recipients becomes forwarded or sent to a recipient outside the original group. A sender of an email in the original thread may have included information that was appropriate, in terms of content, confidentiality, and/or privacy, to the original recipient list yet is no longer appropriate to recipients in the new group. The person who sends an email containing the thread history may not be aware of whether the content is or isn't appropriate to each audience and may not read through the entire history to screen the content each time a recipient is added. This causes problems where information that was included originally is now sent inadvertently to a recipient where it is inappropriate. Examples of this includes information about a customer that is originally sent internally and now becomes sent to another customer, information concerning unannounced product material that is sent to external email recipients without an appropriate legal non-disclosure agreement being in place, profanity or humour in an internal email that now becomes external, or any information of a personal nature specific to a particular employee that now becomes external or is sent to an audience outside their management chain or human resource or any other party where such knowledge is required.

An existing solution to this problem is for each email user who is adding a new recipient to read the entire content of the thread and all previous emails included their own and identify all appropriate information and delete or screen such information. This requires manual work

for the user where mistakes can be made and incurs a cost as there is time involved, as well as the requirement for knowledge about the role of each recipient on the email thread.

Other known improvements to email systems include the type of system disclosed in United States of America Patent US 6460074. The discloses an electronic mail system which includes an electronic mail utility with a message creation interface responsive to user input to create an electronic mail message. A reconsideration prompting module is operative to extract one or more intended information elements from the message created using the electronic mail utility and to present them to the user in a display area. The reconsideration prompting module includes a reconsideration prompting control responsive to user input to confirm reconsideration of the meaning of intended information elements from the created message before sending the message. A network interface is operatively connected to a network and responsive to messages approved by the reconsideration prompting module.

The disadvantage of the system described in this prior art Patent, is that it is not sufficiently flexible to be useful. Content in email messages is checked to see if spelling and grammar are correct, and also to see if profanity is present in the user's email message. However, there is no distinction made between the fact that content that can be considered acceptable for one user may not be acceptable for another user. In the prior art system content is either acceptable, or it is not.

It is therefore an object of the invention to improve upon the known art.

According to a first aspect of the present invention, there is provided a method of handling a message comprising receiving a message comprising content and one or more intended recipients, selecting one or more rules according to the or each intended recipient, checking the content of the message according to the or each selected rule to identify inappropriate content, and performing a predetermined corrective action, if inappropriate content is identified.

According to a second aspect of the present invention, there is provided a system for handling a message comprising a receiver arranged to receive a message comprising content

and one or more intended recipients, a storage device arranged to store rules, and a processor arranged to select one or more rules according to the or each intended recipient, to check the content of the message according to the or each selected rule to identify inappropriate content, and to perform a predetermined corrective action, if inappropriate content is identified.

According to a third aspect of the present invention, there is provided a computer program product on a computer readable medium for handling a message, the product comprising instructions for receiving a message comprising content and one or more intended recipients, selecting one or more rules according to the or each intended recipient, checking the content of the message according to the or each selected rule to identify inappropriate content, and performing a predetermined corrective action, if inappropriate content is identified.

Owing to the invention, it is possible to provide a system in which breaches of information content to inappropriate recipients is brought to the attention of the sender of the message so that they can take appropriate action, for example either not to send the email or to vet the content and deem it appropriate. This system provides a mechanism whereby the message software can determine if the email contains inappropriate content for any of the intended recipients.

Preferably, the step of selecting one or more rules according to the or each intended recipient comprises identifying a group to which an intended recipient belongs, and selecting the or each rule according to the identified group. The step of identifying a group to which an intended recipient belongs may also preferably comprise identifying whether the intended recipient is internal or external to an organisation. Recipients are placed into groups, a simple categorization being "internal" and "external", where "internal" may be recipients with a particular corporate domain and "external" as otherwise. When a message is sent externally, all the content is scanned for sensitive information such as any known trademarks or copyrights which aren't attributed correctly, any profanity phrases or words that might embarrass or compromise the sender's organization, any extension phone numbers in email footers or mobile phone numbers that might be appropriate for internal content but not appropriate or even valid for an external recipient.

Advantageously, the identified group comprises an external organisation, and the method further comprises accessing a confidentiality database and creating a rule according to the presence of the external organisation in the database. In this more advanced implementation, the list of external domains could be cross-referenced against those that have signed specific non-disclosure agreements concerning various products and discussions about non-public products or otherwise sensitive information could be approved for sending to domains from companies that had the appropriate legal agreement in place, and flagged to the sender's attention as a possible breach of sensitive material to external domains where no such agreement existed. The scanning in this case would be for keywords representing internal product names and other information bringing the email content to the sender's attention. In an additional implementation, certain patterns of keywords can be identified that represent information that is automatically deemed confidential, an example being internal numbers given to confidential information such as numbers given to patent proposals according to a known rubric. Any email containing such information would not be intended to be sent to someone outside the realm of being confidential.

A further example could be a rule designed to scan email for salary information or home addresses for employees; information that is appropriate for managers, their administrative assistants, human resources departments and so forth. Matching recipients against their role in an organization can be done by using corporate and organizational databases. If an email message containing salary content is inadvertently sent to a recipient not authorized to receive the message the email system would notify the user.

Ideally, the step of checking the content of the message according to the or each selected rule to identify inappropriate content comprises identifying potentially inappropriate material in the content, and comparing the identified potentially inappropriate material to the or each rule. The processing of the message by the system can be enhanced by using a set of keywords to first identify potential candidates within a message and then compare these candidates against the rules for the specific recipients. This supports and efficient processing of the messages.

Embodiments of the present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:-

Figure 1 is a schematic diagram of a computer running a messaging client,

Figure 2 is a schematic diagram of a display device,

Figure 3 is a schematic diagram showing processing of a message,

Figure 4 is a further schematic diagram of the display device,

Figure 5 is flowchart of a method of handling a message, and

Figure 6 is flowchart of a second embodiment of the method of handling a message.

A conventional desktop computer is shown in Figure 1a. The computer comprises a processor 10, a display device 12 and a user interface device 14, being a keyboard 14. Other interface devices 14 such as a mouse (not shown) can also be used. The processor 10 comprises a number of different components including a CPU, a display driver, a memory device, and input/output connections and so on. The processor 10 connects to an external network such as the Internet, through a suitable I/O interface, for communicating with other remote devices. The processor 10 is running a messaging client, which has a graphical user interface (GUI) 16 displayed on the display device 12. Figure 1b shows some of the internal components of the computer 2, with a receiver 4 for connecting to the input devices such as the keyboard 14 and a storage device 6. The processor 10 is running a client program 8.

The user of the computer 2 can perform actions with respect to the messaging client 8 via the user interface device 14. For example, the user can compose messages and via a "send/receive" function, can receive any messages that have been sent to them. The messaging client 8, which can be an email client 8 commonly used on desktop computing systems, allows the user of the computer to participate in communications with any other user who has an email address. A user of a messaging system can specify multiple recipients

for a message and all of the multiple recipients will receive the message. Likewise, a received message may specify other recipients, all of whom will see the content of the received message.

It is common for email clients to be configured so that when a message is composed, as a reply to an earlier message, the text of the earlier message is included in the reply. The net result of this "reply to" function is that as further messages are created as replies to earlier replies, a very long message is created as the default, often running to many pages in length. This means that when a user replies to such a long message, they may not be aware, or may have forgotten about, the contents of earlier messages in the thread. This can lead to inappropriate content being sent to the wrong recipients.

Figure 2 shows more detail of the user interface 16 to the messaging client 8, being shown by the display device 12. The email client interface 16 has five virtual "buttons" that the user can "press" with the cursor 20, under the control of the computer's mouse, in the conventional fashion. The five buttons provide various functions of the email client. The "new" button allows the user to compose a new email message; the "reply" button allows the user to compose an email message as a reply to a specific selected message, with the reply going only to the originator of the earlier message; the "reply all" button allows the user to compose an email message as a reply to a specific selected message, with the reply going to all of the original recipients of the earlier message; the "forward" button allows the user to forward a specific selected message to one or more new recipients; and the "send" button allows the user to send the current drafted email and also to receive any new emails.

In the example shown in Figure 2, the user has two email messages in their inbox, one from John and one from Mike. In reality, most email inboxes have hundreds of email messages arranged normally in date order, with the most recently received message at the top. The user can select any of the emails in their inbox in order to either view the email, for example in a preview pane, or to carry out one or more actions in respect of that email message. In this case, the user has selected the email message from John, and clicked the "reply all" button with the cursor 20. This action opens a new window 22 in the user interface 16. A new message 24 is created with content 26 and intended recipients 28. The new window 22

allows the user to enter text as content 26 for the reply to the original earlier email message. The recipients of the earlier message will all be recipients of the new message, as will be sender of the earlier message. The user can also add new recipients to the current list of recipients. In this case recipients A to D were the original recipients and the sender, and new recipient E has been added.

The email client of the present system is modified to provide protection against sending inappropriate material to one or more recipients. As discussed above, this commonly happens when the "reply" or "reply all" function is used in relation to an email thread that is already comprised of many previous messages, and new recipients are added to the thread. This creates the possibility that one or more of the new recipients will see material in the thread that is inappropriate for them. For example confidential or embarrassing material may be included within the email message, and this can be inadvertently maintained within the message thread, by virtue of the "reply" and "reply all" functions including all earlier content.

Figure 3 illustrates schematically the concept of an email message 24 being processed by the modified email client. The message 24 comprises content 26 and intended recipients 28. The content 26 will be the text message part of the overall message 24, but can also include attachments that may have been added to the message 24 by the new sender, or may already be attached to the message 24 and maintained by the email client. The recipients are represented by the letters A to E, normally within an email client such recipients 28 are listed by their respective email address, or a short title that links to their email address.

The recipients 28 are placed into groups 30 by the engine within the email client that is handling the issue of the inappropriate content. This is not an essential step within the process, the recipients 28 could each be handled individually, but it is more efficient to group the recipients 28 together. The group 30 that contains the recipients 28 A to C could be a group 30 of internal employees within an organisation, for whom it can be assumed that almost all material content 26 within the message 24 is acceptable. The group 30 containing recipients D could be a first customer of the organisation, and group 30 containing recipients

E could be a second customer of the organisation. For each group 30 there are respective rules 32, which are stored in a local storage device.

Figure 4 shows the message 24 after the user has added some text and clicked on the "send" button 18 with the cursor 20. The addition of the intended recipient E has caused a warning 34 to be produced in response to the send action of the user. The message 24 has not been sent, but has however resulted in the warning 34 being shown to the user. The implication of the warning is that there is material within the email message 24 somewhere, which is inappropriate for the intended recipient E. The user can click on this warning 34 to obtain more detail about the detected breach of the rules 32 relating to the user E.

In one embodiment, the email software will use the concept of blacklisted terms. This can be configured so that each term will have a group and a severity assigned to it. The following list describes the scenarios where document numbers and product keyword names are to be restricted. The words "Tie-line", "Skittles" and "Fudgemaker" are hypothetical names of unannounced products. The * mask is used to represent wild card characters. The use of the 07** *** *** mask is to look for internal phone numbers.

Keywords	Group	Severity
GB8-****-****	All External	High
GB8-****-****	Internal	Medium
GB8-****-****	Law	Low
07** *** ***	All External	High
07** *** ***	Internal	Medium
07** *** ***	Friends	Low
Tie-line	All External	Low
Skittles	All External	High
Skittles	External on an NDA list	Low
Skittles	Internal	Low
FudgeMaker	All External	High

Special cases would exist for profanity by searching for known words.

Profanity	All External	High
Profanity	Internal	Low

The severity dictates the users warning level. For example, if a blacklisted term being sent to a group produces a high severity the email would not be allowed to go through without being signed off. Medium severity would flag up a warning on the user's computer saying are you sure you want to send this email. In another implementation corrective action could be defined so profanity words and mobile phone numbers could have an auto-correction suggestion. In another implementation custom rules could be provided for what corrective action to take, including having the email client learn these from previous corrective actions based on the combinations of recipients and keywords. In all of these situations, the basic principle of the system remains the same, which is that the sender of the email is informed of any information in the entire email thread that might be inappropriate for the audience of the email's recipients.

The method of handling the message 24 is summarised in Figure 5. The method comprises the steps of, firstly step S1, receiving the message 24 comprising the content 26 and the one or more intended recipients 28. At step S2 there is carried out the selecting of the one or more rules 32 according to each intended recipient 28. Once the rules have been selected, at Step S3 there is performed the checking of the content 26 of the message 24 according to each selected rule 32 to identify any inappropriate content, and finally, there is the step S4 of performing a predetermined corrective action, if inappropriate content is identified.

The step S2 of selecting the rules 32 according to each intended recipient 28 can comprise the intermediate step of identifying a group 30 to which an intended recipient 28 belongs, and selecting each rule 32 according to the identified group 30. The process of aggregating the recipients 28 into the groups 30 streamlines the operation of the email client, in respect of the selection of which rules 32 to apply to the content 26 of the message 24. Since the number of potential recipients 28 can be enormous, by having a finite list of groups 30, which could contain only two groups 30, leads to a much faster selection of the appropriate rules 32 to apply to the content 26.

The step of identifying a group 30 to which an intended recipient 28 belongs can comprise identifying whether the intended recipient 28 is internal or external to an organisation. Where the identified group 30 to which the recipient 28 belongs is an external organisation, the email client can be arranged to access a confidentiality database and creating a rule 32 according to the presence of the external organisation in the database. If a message 24 is going to an external organisation, then the presence or absence of this organisation in a confidentiality database can be used to drive a rule about the content 26. For example, a customer may be clear to receive information on one project but not on another, as defined by the details in the database. Rules 32 can be created to encode this information.

A flowchart of a second embodiment of the process is shown in Figure 6, which describes an example implementation. The logic for this implementation could occur in the email client based on personal rules, an email server based on corporate rules, and/or both. This implementation is based upon a word by word examination of the content 26 of the message 24. The rules 32 for each recipient 28 are based on the recipients 28 being placed into groups 30, and severity scores are present for specific words in the respective rules 32, as described above. For example, a specific rule 32 may be for a group 30 of recipients 28 who are defined as an external customer, with the word "Skittles" having a severity score of "high". Such scores could also be numerical.

At step S10, the message 24 is received and processing is begun with a severity variable set to "none". At step S11 the processing moves to the next word in the content 26. At step S12, a test is made to see if the end of the email message 24 has been reached. If yes, then the process moves to step S13, where a test is made to see is the severity score is greater than "none". If not, then at step S14 the message 24 is sent. If yes, then the process moves to step S15, where the appropriate corrective action is taken, such as displaying the warning 34.

If the end of the email has not been reached, then at step S16 a test is made to see if the word is present in a list of potentially inappropriate material. If not, then the process returns to step S11 and continues. If yes, then the process moves to step S17 where the recipient list for the message 24 is accessed. At step S18 the next recipient 28 is obtained, and at step S19 a check is made to see if the recipient's group 30 has a keyword severity which is higher than

the current maximum severity found do far in the checking process. If yes, then the severity score is set to that recipient's severity level for the specific keyword at step S20. If no, then the process returns to step S21. At this step S21 (also reached after step S20) a check is made to see if there are further recipients to consider. If there are, then the process moves to step S18. If not, then the process moves to step S11.

CLAIMS

1. A method of handling a message comprising:
- receiving a message comprising content and one or more intended recipients,
- selecting one or more rules according to the or each intended recipient,
- checking the content of the message according to the or each selected rule to identify inappropriate content, and
- performing a predetermined corrective action, if inappropriate content is identified.

2. A method according to claim 1, wherein the step of checking the content of the message according to the or each selected rule to identify inappropriate content comprises identifying potentially inappropriate material in the content, and comparing the identified potentially inappropriate material to the or each rule.

3. A method according to claim 1 or 2, wherein the step of selecting one or more rules according to the or each intended recipient comprises identifying a group to which an intended recipient belongs, and selecting the or each rule according to the identified group.

4. A method according to claim 3, wherein the step of identifying a group to which an intended recipient belongs comprises identifying whether the intended recipient is internal or external to an organisation.

5. A method according to claim 3 or 4, wherein the identified group comprises an external organisation, and the method further comprises accessing a confidentiality database and creating a rule according to the presence of the external organisation in the database.

6. A system for handling a message comprising:
- a receiver arranged to receive a message comprising content and one or more intended recipients,
- a storage device arranged to store rules, and
- a processor arranged to select one or more rules according to the or each intended recipient, to check the content of the message according to the or each selected rule to

identify inappropriate content, and to perform a predetermined corrective action, if inappropriate content is identified.

7. A system according to claim 6, wherein the processor is arranged, when checking the content of the message according to the or each selected rule to identify inappropriate content, to identify potentially inappropriate material in the content, and to compare the identified potentially inappropriate material to the or each rule.

8. A system according to claim 6 or 7, wherein the processor is arranged, when selecting one or more rules according to the or each intended recipient, to identify a group to which an intended recipient belongs, and to select the or each rule according to the identified group.

9. A system according to claim 8, wherein the processor is arranged, when identifying a group to which an intended recipient belongs, to identify whether the intended recipient is internal or external to an organisation.

10. A system according to claim 8 or 9, wherein the identified group comprises an external organisation, and the processor is further arranged to access a confidentiality database and to create a rule according to the presence of the external organisation in the database.

11. A computer program product on a computer readable medium for handling a message, the product comprising instructions for:

- receiving a message comprising content and one or more intended recipients,
- selecting one or more rules according to the or each intended recipient,
- checking the content of the message according to the or each selected rule to identify inappropriate content, and
- performing a predetermined corrective action, if inappropriate content is identified.

12. A computer program product according to claim 11, wherein the instructions for checking the content of the message according to the or each selected rule to identify

inappropriate content comprise instructions for identifying potentially inappropriate material in the content, and for comparing the identified potentially inappropriate material to the or each rule.

13. A computer program product according to claim 11 or 12, wherein the instructions for selecting one or more rules according to the or each intended recipient comprise instructions for identifying a group to which an intended recipient belongs, and for selecting the or each rule according to the identified group.

14. A computer program product according to claim 13, wherein the instructions for identifying a group to which an intended recipient belongs comprise instructions for identifying whether the intended recipient is internal or external to an organisation.

15. A computer program product according to claim 13 or 14, wherein the identified group comprises an external organisation, and the product further comprises instructions for accessing a confidentiality database and for creating a rule according to the presence of the external organisation in the database.

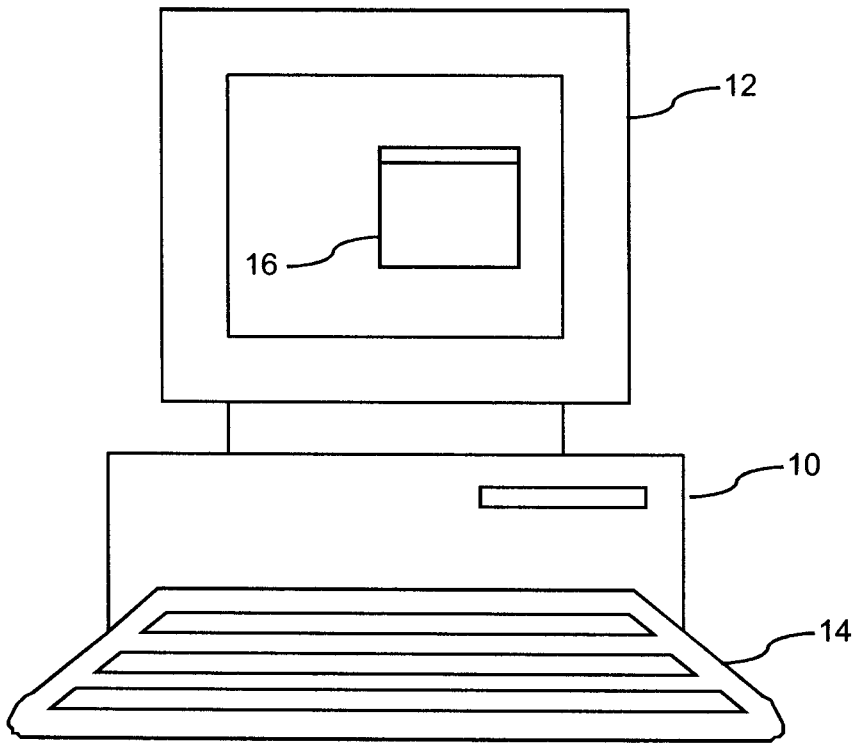


Fig. 1a

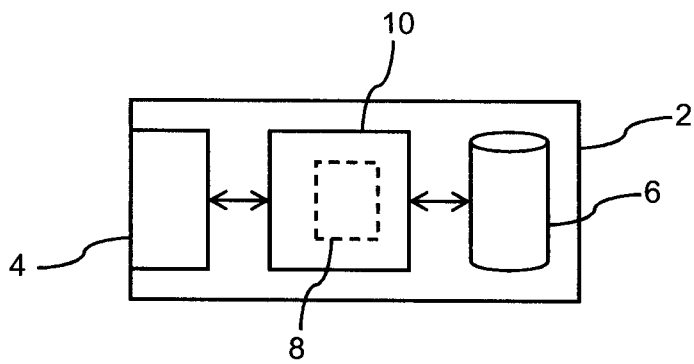


Fig. 1b

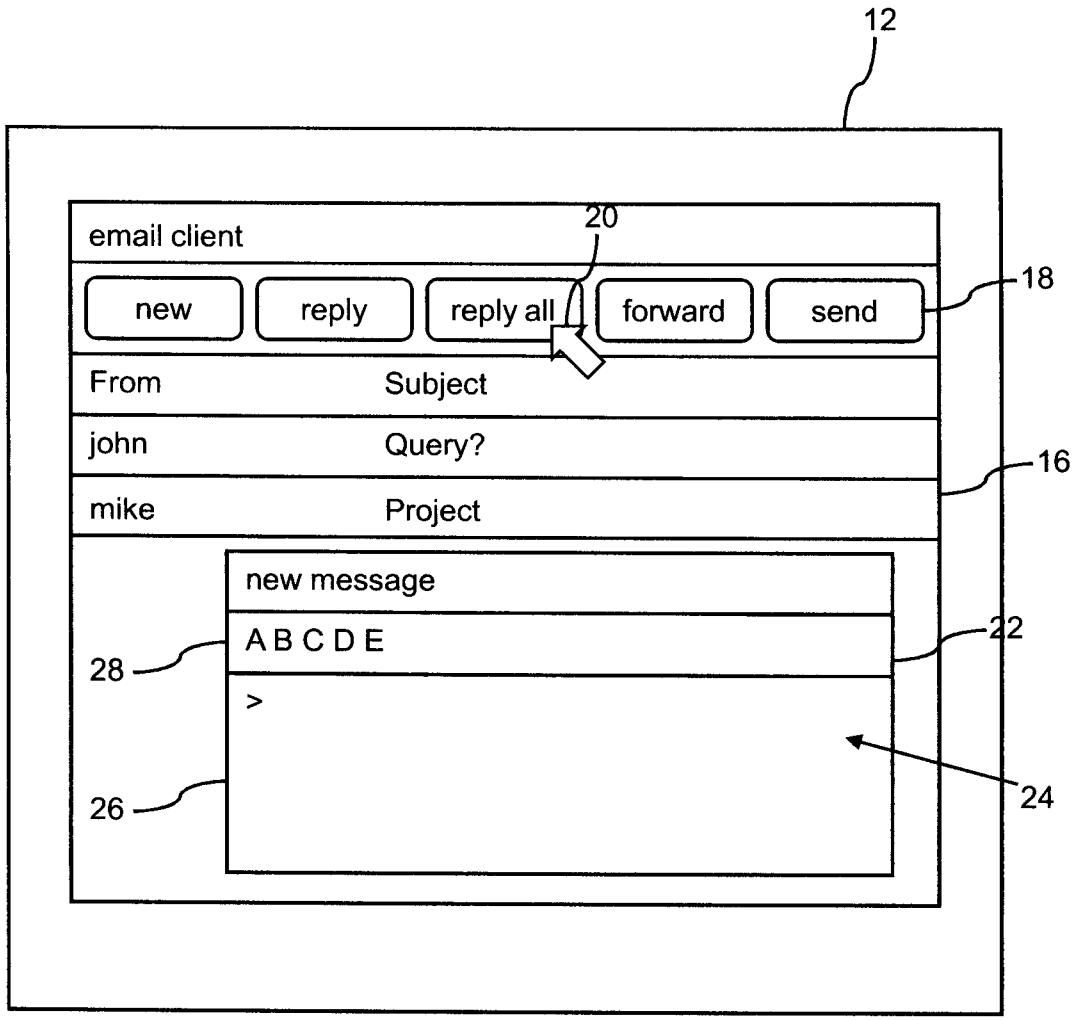

12
email client
20
new
reply
reply all
forward
send
18
From
Subject
john
Query?
16
mike
Project
new message
A B C D E
22
28
>
26
24

Fig. 2

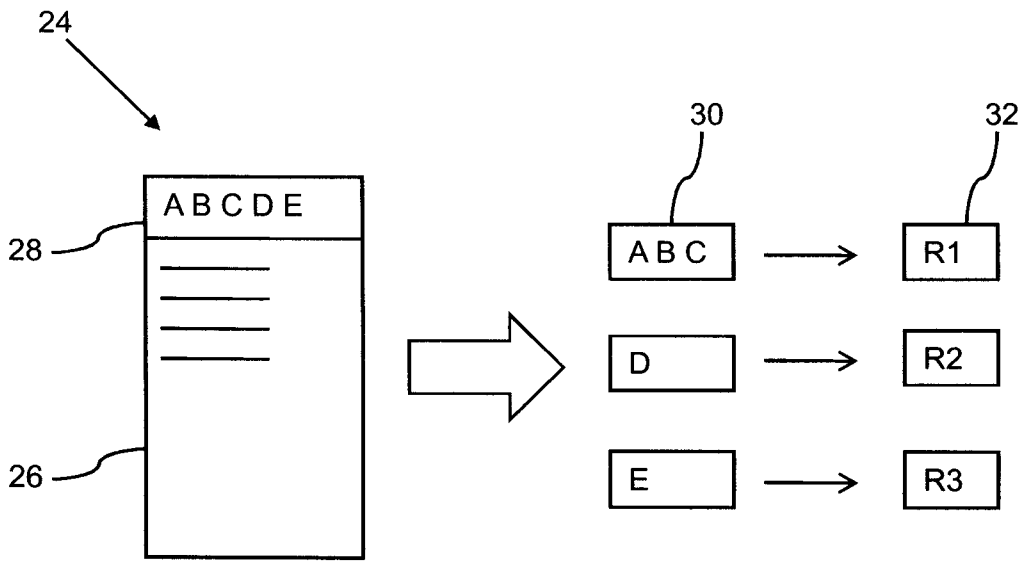


Fig. 3

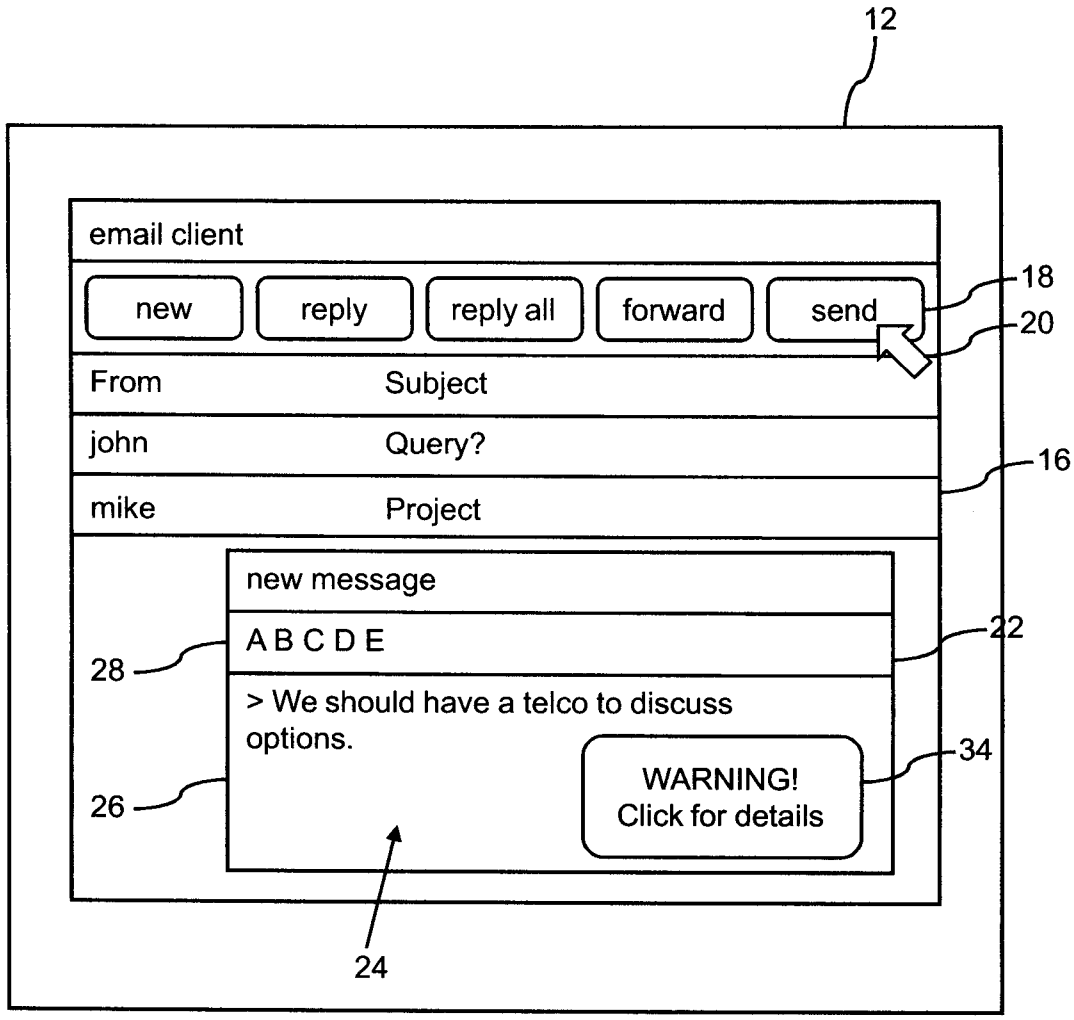

12
email client
new
reply
reply all
forward
send
18
20
From
Subject
john
Query?
16
mike
Project
new message
A B C D E
22
28
> We should have a telco to discuss options.
WARNING!
Click for details
34
26
24

Fig. 4

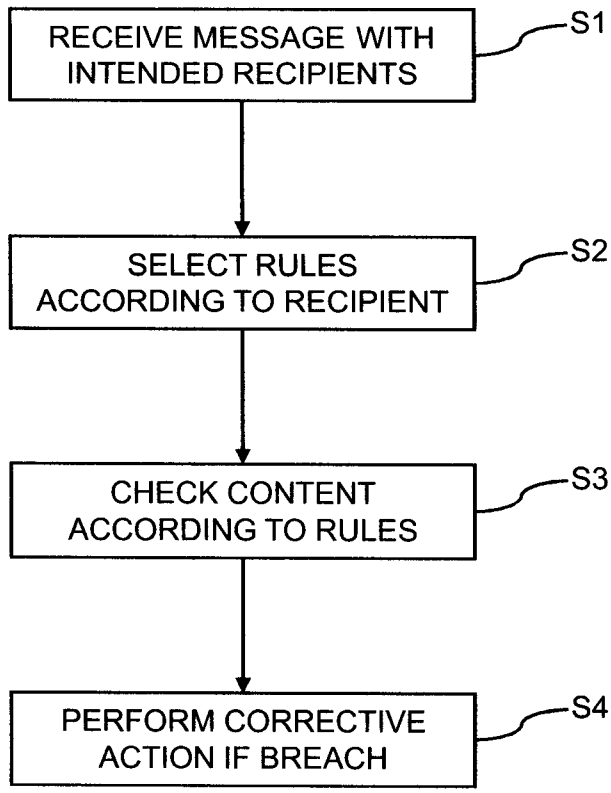

RECEIVE MESSAGE WITH INTENDED RECIPIENTS
S1
SELECT RULES ACCORDING TO RECIPIENT
S2
CHECK CONTENT ACCORDING TO RULES
S3
PERFORM CORRECTIVE ACTION IF BREACH
S4

Fig. 5

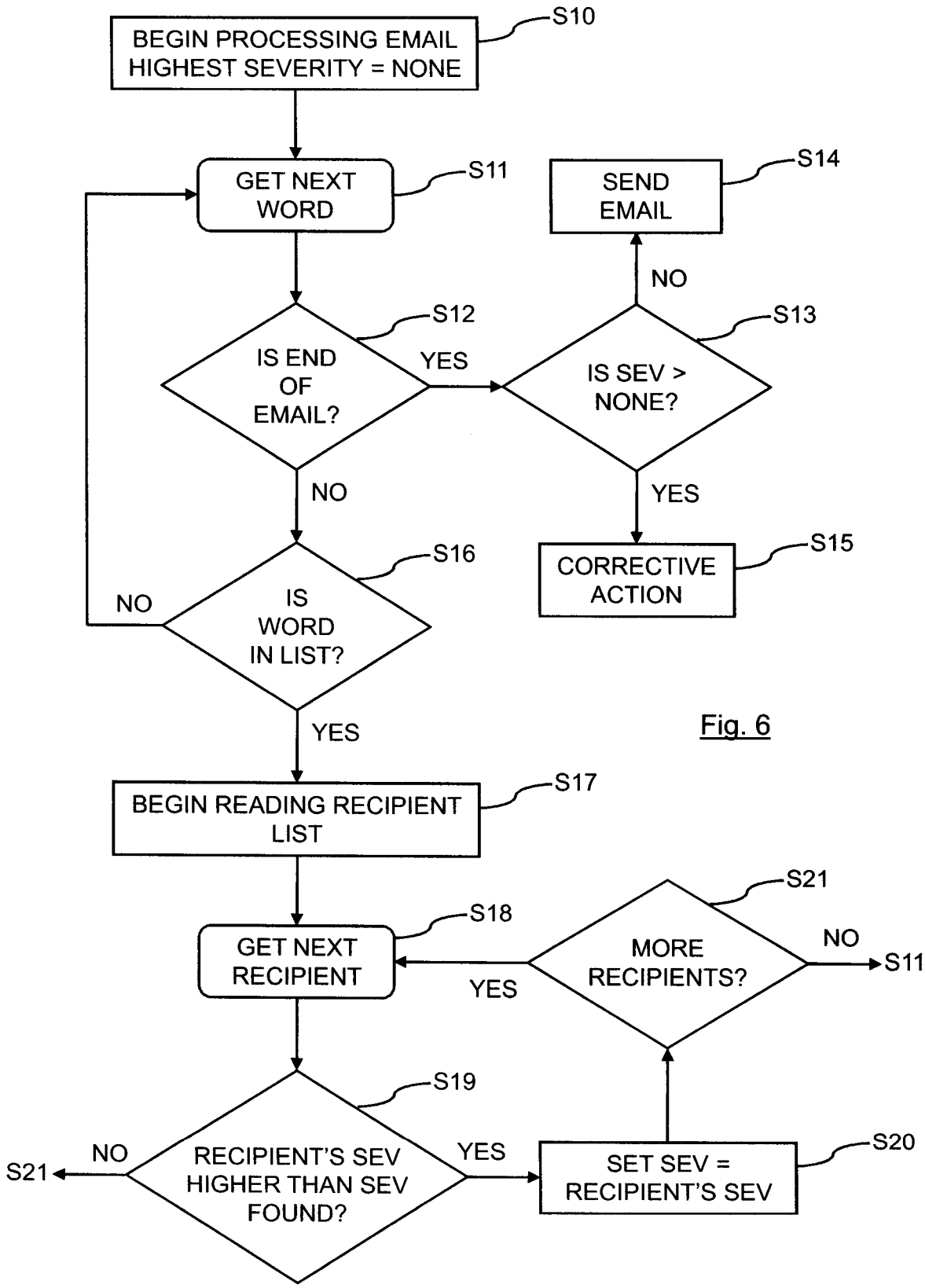

BEGIN PROCESSING EMAIL
HIGHEST SEVERITY = NONE
S10
GET NEXT WORD
S11
IS END OF EMAIL?
S12
YES
NO
IS SEV > NONE?
S13
NO
SEND EMAIL
S14
YES
CORRECTIVE ACTION
S15
IS WORD IN LIST?
S16
NO
YES
BEGIN READING RECIPIENT LIST
S17
GET NEXT RECIPIENT
S18
YES
MORE RECIPIENTS?
S21
NO
S11
RECIPIENT'S SEV HIGHER THAN SEV FOUND?
S19
NO
S21
YES
SET SEV = RECIPIENT'S SEV
S20

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/051766

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q10/00 H04L12/58
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2006/088915 A1 (INBOXER INC [US]; TRUE SEAN DANIEL [US]; MATUS ROGER L [US]; INGOLD CH) 24 August 2006 (2006-08-24) abstract paragraph [0005] - paragraph [0009] paragraph [0013] - paragraph [0017]	1-15
X	US 6 460 074 B1 (FISHKIN MARTIN E [US]) 1 October 2002 (2002-10-01) column 1, line 45 - line 50 column 14, line 23 - line 48	1-15
X	US 2005/198175 A1 (THOMAS ROWLAND H [US] ET AL THOMAS ROWLAND HAYES [US] ET AL) 8 September 2005 (2005-09-08) paragraph [0085]	1-15

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 April 2010	28/04/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Siebel, Christian

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/051766

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/150253 A1 (DOUGHERTY JESSE M [US] ET AL) 28 June 2007 (2007-06-28) paragraph [0001] - paragraph [0003] paragraph [0011]	1-15
X	US 2007/067436 A1 (VAUGHN HEATHER [US]) 22 March 2007 (2007-03-22) paragraphs [0003] - [0006]	1-15
X	US 2007/214353 A1 (DICKINSON ROBERT D III [US] ET AL DICKINSON III ROBERT D [US] ET AL) 13 September 2007 (2007-09-13) paragraph [0010] paragraph [0007]	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2010/051766

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2006088915 A1	24-08-2006	US 2008162652 A1	03-07-2008
US 6460074 B1	01-10-2002	NONE	
US 2005198175 A1	08-09-2005	US 2009210505 A1	20-08-2009
		WO 2005072153 A2	11-08-2005
US 2007150253 A1	28-06-2007	NONE	
US 2007067436 A1	22-03-2007	WO 2007037917 A1	05-04-2007
US 2007214353 A1	13-09-2007	AT 444614 T	15-10-2009
		AT 347200 T	15-12-2006
		AU 8759098 A	16-02-1999
		CA 2301147 A1	04-02-1999
		DE 69836545 T2	16-05-2007
		EP 1750384 A1	07-02-2007
		EP 1010283 A2	21-06-2000
		HK 1029013 A1	08-06-2007
		JP 3932319 B2	20-06-2007
		JP 2001518724 T	16-10-2001
		WO 9905814 A2	04-02-1999
		US 6609196 B1	19-08-2003
		US 2003196098 A1	16-10-2003
		US 2007005983 A1	04-01-2007
		US 2007245416 A1	18-10-2007