



(51) International Patent Classification:

H04L 12/58 (2006.01) *G06F 21/16* (2013.01)
H04L 12/859 (2013.01)

(21) International Application Number:

PCT/US2020/047731

(22) International Filing Date:

25 August 2020 (25.08.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 10300 Energy Drive, Spring, Texas 77389 (US).

(72) Inventor: **LEE, Atkinson**; 10F-2, No. 66, Jingmao 2nd Rd, NanGang, District, Taipei, 11568 (TW).

(74) Agent: **SU, Benjamin** et al.; HP Inc., Intellectual Property, 3390 E. Harmony Road, Mail Stop 35, Fort Collins, Colorado 80528 (US).

(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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) Title: EMAIL RECIPIENTS DETERMINATIONS

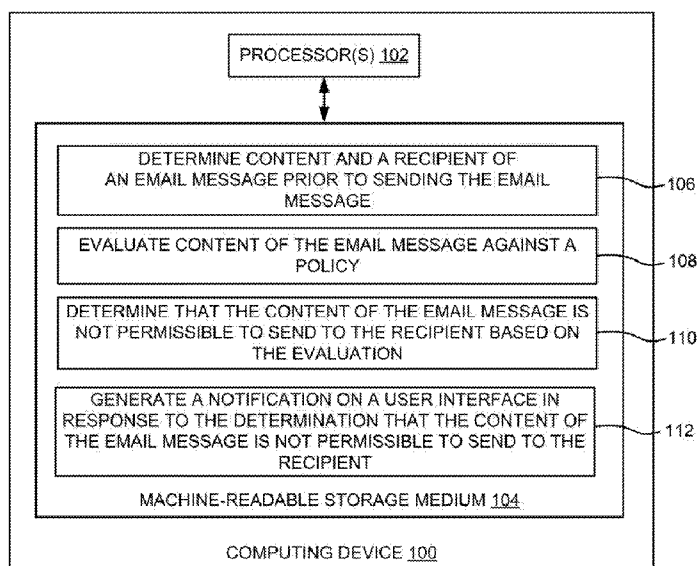


FIG. 1

(57) Abstract: In an example, a non-transitory computer-readable storage medium encoded with instructions that, when executed by a processor of a computing device, may cause the processor to determine content and a recipient of an email message prior to sending the email message, evaluate content of the email message against a policy, determine that the content of the email message is not permissible to send to the recipient based on the evaluation, and generate a notification on a user interface in response to the determination that the content of the email message is not permissible to send to the recipient.

Declarations under Rule 4.17:

- *as to the identity of the inventor (Rule 4.17(i))*
- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

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

EMAIL RECIPIENTS DETERMINATIONS

BACKGROUND

[0001] Computer generated communications, such as email applications, may be a regular form of communication for users in work and social interactions. Email applications may allow a user to send an email message to a single recipient or multiple recipients. Further, email addresses may be used to identify the recipients of the email messages. The email addresses may be stored in an electronic database (e.g., an email address book). Further, when a sender composes a new email, the sender may select the recipients for the email using the electronic database.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] Examples are described in the following detailed description and in reference to the drawings, in which:

[0003] FIG. 1 is a block diagram of an example computing device including a non-transitory machine-readable storage medium, storing instructions to determine whether an email message can be permissible to send to a recipient based on a policy;

[0004] FIG. 2A is an example graphical user interface, depicting an email message and a notification including a recommendation to add another recipient to the email message based on a content type;

[0005] FIG. 2B is an example graphical user interface, depicting another email message and a notification indicating that the email message is not permissible to send to a recipient;

[0006] FIG. 3 is a block diagram of an example computing device including a non-transitory machine-readable storage medium, storing instructions to detect an unintended recipient of an email message based on a whitelisting policy;

[0007] FIG. 4 is an example graphical user interface, depicting an email message and a prompt indicating an unintended recipient of the email message based on a whitelisting policy;

[0008] FIG. 5 is a block diagram of an example computing device including a non-transitory machine-readable storage medium, storing instructions to detect an unintended recipient of an email message based on domain addresses of recipient email addresses;

[0009] FIG. 6 is an example graphical user interface, depicting an email message and a notification indicating an unintended recipient of the email message based on domain addresses of recipients; and

[0010] FIG. 7 is a block diagram of an example email system, including an email client application to determine whether an email message can be sent to a recipient entered in a recipient field.

DETAILED DESCRIPTION

[0011] Emails may be used to convey messages, documents, pictures, and the like from a sender to a single recipient or multiple recipients. The recipients that the sender frequently corresponds with may be stored in an electronic database (e.g., an email address book), and when the sender composes a new email, the sender can select the recipients for the new email using the electronic database. In some examples, to select the recipients, the sender can either scroll through the electronic database to identify the desired email addresses and/or can utilize a predictive input text feature or an autocomplete feature of an email application.

[0012] The autocomplete feature may be a tool to predict a list of potential recipients, however, such predictions may lead to inadvertent copies to recipients. The autocomplete feature may work by matching the characters typed by a sender to a list of previous email addresses the sender has experienced. For example, when the sender begins to input first few characters of the recipient's name and/or email address in a recipient field (e.g., a "To" field, "CC" field, "BCC" field, or the like), a list of potential recipients matching the inputted characters may be

determined and presented to the sender for selection. The potential recipients that make up the list may be determined based upon a correspondence between a potential recipient's name or email address and the inputted first few characters.

[0013] Thus, the autocomplete feature may facilitate to complete the email address by matching against recently used email addresses, email addresses in the electronic address book, list of contacts, or the like. Even though autocompleting the email addresses may be helpful, the autocomplete feature may not be able to provide accurate potential recipients, for instance, when the intended recipient is not in contact with the sender for a significant time, when the email message is to be sent to a particular recipient for the first time, or the like.

[0014] Therefore, autocompleting the email addresses can present a risk of sending the email to an incorrect or unintended recipient, which may lead to undesirable consequences. When the sender's input is incorrect or when multiple possible email addresses match the partial input, the sender may inadvertently select an incorrect email address from the list. For example, consider that a priority of the potential recipients in the list may be assigned based on recently used email addresses. In this case, the first complete match in the list may be an incorrect or unintended recipient of the email message and the sender may inadvertently send a copy of the email message to the unintended recipient.

[0015] Thus, email messages with confidential information can be accidentally sent to the unintended recipient, such as a recipient outside the sender's domain, organizational network, or the like. Hence, privacy may be compromised by the wrong recipient receiving confidential information contained in an erroneously sent email message. Also, receiving such irrelevant email messages can be annoying to the recipients and may also consume a significant amount of time to ascertain that the email message is erroneously received.

[0016] Examples described herein may determine that a recipient entered in a recipient field of an email message is an unintended recipient prior to sending the email message. In an example, content and a recipient of an email message may be determined prior to sending the email message. Further, the content of the email

message may be evaluated against a policy. The policy may include rules to determine what action to be taken with respect to the email message based on a type of the content. For example, the policy may flag sensitive content in the email message may not be appropriate for sending to email addresses outside the sender's domain, may insist to include another recipient to the email message, or the like.

[0017] Furthermore, the content of the email message may be determined as being not permissible to send to the recipient based on the evaluation. Further, a notification may be generated on a user interface in response to the determination that the content of the email message is not permissible to send to the recipient. Thus, examples described herein may prevent sending inadvertent copies to unintended recipients, without compromising on benefits of the autocomplete feature in the email applications or calendar invitation programs.

[0018] In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present techniques. It will be apparent, however, to one skilled in the art that the present apparatus, devices, and systems may be practiced without these specific details. Reference in the specification to "an example" or similar language means that a particular feature, structure, or characteristic described is included in at least that one example, but not necessarily in other examples.

[0019] Turning now to the figures, FIG. 1 is a block diagram of an example computing device 100 including a non-transitory machine-readable storage medium 104, storing instructions to determine whether an email message can be permissible to send to a recipient based on a policy. Computing device 100 may include a processor 102 and machine-readable storage medium 104 communicatively coupled through a system bus. Processor 102 may be any type of central processing unit (CPU), microprocessor, or processing logic that interprets and executes machine-readable instructions stored in machine-readable storage medium 104. Machine-readable storage medium 104 may be a random-access memory (RAM) or another type of dynamic storage device that may store information and machine-readable instructions that may be executed by processor

102. For example, machine-readable storage medium 104 may be synchronous DRAM (SDRAM), double data rate (DDR), rambus DRAM (RDRAM), rambus RAM, etc., or storage memory media such as a floppy disk, a hard disk, a CD-ROM, a DVD, a pen drive, and the like. In an example, machine-readable storage medium 104 may be a non-transitory machine-readable medium. In an example, machine-readable storage medium 104 may be remote but accessible to computing device 100.

[0020] As shown in FIG. 1, machine-readable storage medium 104 may store instructions 106-112. In an example, instructions 106-112 may be executed by processor 102 to generate a notification in response to a determination that content of an email message is not permissible to send to the recipient.

[0021] Instructions 106 may be executed by processor 102 to determine content and a recipient of an email message prior to sending the email message. In an example, a sender may add or edit a participant or a list of recipients for the email message, for instance, in a recipient field (e.g., a "To" field, "CC" field, or the like).

[0022] The content may refer to text data, image data, or a combination thereof included in a body of the email message. Example image data may include security marks such as a topographical watermark, a logo, a symbol, a hologram, a bar code, a photograph, an emblem, or the like. For example, the content may include confidential information (e.g., project related information, intellectual property (IP) related information, and the like), sensitive information (e.g., privileged information, customer data, supplier data, program codes, information indicating a promise/commitment, and the like), financial information (e.g., price estimates, transactional information, and the like), or the like.

[0023] Instructions 108 may be executed by processor 102 to evaluate the content of the email message against a policy. In one example, instructions to evaluate the content of the email message against the policy may include instructions to determine a content type of the email message and evaluate the content type against the policy to determine whether the email message is

permissible to send to the recipient. In an example, the content type may be determined based on confidential information, sensitive information, financial information, or a combination thereof in the content of the email message. For example, the content type may be determined based on words/phrases in the content such as secret, dollars, quote, new project, sensitive, privileged, or the like.

[0024] In one example, the policy may flag that the sensitive information in the email message may not be appropriate for sending to an email address outside the sender's domain (e.g., @xyz.com). In this example, the policy may indicate that sending the content including confidential information, sensitive information, or financial information to an email address outside the company's domain or sender's domain may be contrary to company's policy. In another example, the policy may indicate that the email message copied to an attorney may have to be copied to another attorney or a director to comply with the company's policy. In this example, the content may include terms such as "privileged", "Attorney", or the like, which may indicate that the email message is copied to the attorney (i.e., the recipient).

[0025] In some examples, the content of the email message may be evaluated against the policy by applying a machine learning model, a rule-based grouping algorithm, or the like. Instructions 110 may be executed by processor 102 to determine that the content of the email message is not permissible to send to the recipient based on the evaluation. Instructions 112 may be executed by processor 102 to generate a notification on a user interface in response to the determination that the content of the email message is not permissible to send to the recipient.

[0026] In an example, the notification may indicate a refusal to send the email message to the recipient based on a type of the content (i.e., the content type). In this example, the notification may indicate a refusal to send the email message to the recipient when the type of the content indicates the confidential information such as a trade secret, sensitive information, and the like.

[0027] In another example, the notification may provide a recommendation to include another recipient to the email message based on a type of the content. In

this example, the notification may provide a recommendation to include another recipient to the email message when the type of the content includes the privileged information (i.e., legal information). In yet another example, the notification may indicate a replacement or removal of the recipient from the email message based on a type of the content. In this example, the notification may indicate the replacement or removal of the recipient when the recipient's domain is outside the sender's domain and the type of the content includes the confidential information such as the project related information.

[0028] Thus, examples described herein may determine the type of content of the email message (e.g., based on confidential/sensitive words in the content) and generate the notification indicating a remediation action to send the email message based on the type of the content. An example user interface depicting an email message and a notification is explained in FIG. 2A.

[0029] FIG. 2A is an example graphical user interface 200A, depicting an email message 202 and a notification 208 including a recommendation to add another recipient to email message 202 based on a content type. As shown in the FIG. 2A, content 206 in an email body and recipient 204 in a recipient field may be determined prior to sending email message 202 (e.g., when a sender selects a send option in email message 202).

[0030] In the example shown in FIG. 2A, content 206 may include confidential/sensitive words such as 'attorney privilege' 206A. In this example, content 206 can be determined as a confidential type. Further, content 206 including the confidential /sensitive words 206A may be evaluated against a policy. In this example, the policy may indicate that email message 202 may have to be copied to another attorney or a director to comply with company's policy based on the type of content 206.

[0031] Furthermore, content 206 of email message 202 may be determined as being not permissible to send to recipient 204 based on the evaluation. Further, notification 208 may be generated on graphical user interface 200A (e.g., on a display of a computing device). Notification 208 may indicate that content 206

includes confidential information and provide a recommendation to copy email message 202 to the company's attorney (e.g., harris@xyz.com as shown in notification 208) in order to send email message 202 to recipient 204. Thus, when content of an email message includes confidential/sensitive words such as 'attorney privilege', examples described herein may indicate refusal to send the email message and/or provide a recommendation to copy the email message to another recipient so as to send the email message to an intended recipient.

[0032] FIG. 2B is an example graphical user interface 200B, depicting another example email message 252 and a notification 260 indicating that email message 252 is not permissible to send to a recipient 254. As shown in the FIG. 2B, content 256 in an email body and recipient 254 in a recipient field may be determined prior to sending email message 252 (e.g., when a sender selects a send option in email message 252).

[0033] In the example shown in FIG. 2B, content 256 includes confidential/sensitive words such as "project details" 256A and "intellectual property" 256B. In this example, content 256 can be determined as a confidential type. Further, content 256 including the confidential/sensitive words 256A and 256B may be evaluated against a policy. In this example, the policy may indicate that the confidential/sensitive information in the email message may not be appropriate for sending to an email address outside the sender's domain.

[0034] Furthermore, content 256 of email message 252 may be determined as being not permissible to send to recipient 254 based on the evaluation. As shown in FIG. 2B, sender 258 may have an email address "mike.rrr@xyz.com" and a domain address "@xyz.com" and recipient 254 may have an email address "joy.kr@abf.com" and a domain address "@abf.com". Therefore, the recipient's domain address is different from the sender's domain address. For example, users from the same company or office may have the same domain address.

[0035] Further, notification 260 may be generated on graphical user interface 200B. Notification 260 may indicate that content 256 includes confidential information and a refusal to send email message 252 to recipient 254 as recipient's

domain address is different from the sender's domain address. In other examples, notification may also provide a recommendation to remove recipient 254 or replace recipient 254 with an email address within the sender's domain. Thus, when content of an email message includes confidential/sensitive words such as "project details", "quote", "price", or the like, examples described herein may indicate a refusal to send the email message or provide a recommendation to remove or replace a recipient.

[0036] FIG. 3 is a block diagram of an example computing device 300 including a non-transitory machine-readable storage medium 304, storing instructions to detect an unintended recipient of an email message based on a whitelisting policy. Computing device 300 may include a processor 302 and machine-readable storage medium 304 communicatively coupled through a system bus. Processor 302 may be any type of central processing unit (CPU), microprocessor, or processing logic that interprets and executes machine-readable instructions stored in machine-readable storage medium 304. Machine-readable storage medium 304 may be a random-access memory (RAM) or another type of dynamic storage device that may store information and machine-readable instructions that may be executed by processor 302. For example, machine-readable storage medium 304 may be synchronous DRAM (SDRAM), double data rate (DDR), rambus DRAM (RDRAM), rambus RAM, etc., or storage memory media such as a floppy disk, a hard disk, a CD-ROM, a DVD, a pen drive, and the like. In an example, machine-readable storage medium 304 may be a non-transitory machine-readable medium. In an example, machine-readable storage medium 304 may be remote but accessible to computing device 300.

[0037] As shown in FIG. 3, machine-readable storage medium 304 may store instructions 306-312. In an example, instructions 306-312 may be executed by processor 302 to detect an unintended recipient of an email message. Instructions 306 may be executed by processor 302 to determine a first recipient email address inputted in a recipient field of an email message prior to sending the email message.

[0038] Instructions 308 may be executed by processor 302 to compare the first recipient email address with a second email address associated with the email message or client data in a body of the email message. In an example, the second email address may include an email address of a sender, a second recipient in the recipient field, or a previous recipient associated with an email thread of the email message.

[0039] Instructions 310 may be executed by processor 302 to detect that a recipient associated with the first recipient email address is an unintended recipient of the email message by applying a whitelisting policy to the comparison. In an example, the whitelisting policy may indicate a permitted email address corresponding to the second email address or the client data.

[0040] In one example, instructions to compare the first recipient email address with the second email address may include instructions to compare a domain address of the first recipient email address to a domain address of the second email address to detect the unintended recipient. In this example, the whitelisting policy may include the domain address of the second email address mapped to a domain address that is permitted to send the email message.

[0041] For example, consider that the domain address of second email address "@xyz.com". In this example, the whitelisting policy may indicate that domain address "@xyz.com" is mapped to "@stu.com" and "@gyo.com". Therefore, recipients with domain addresses "@stu.com" and "@gyo.com" may be permitted to send the email message along with domain address "@xyz.com". Particularly, if the first recipient email address belongs to the domain address "@xyz.com", "@stu.com", or "@gyo.com", then the email message may be permitted to send to the first recipient email address. If the first recipient email address does not belong to the domain address "@xyz.com", "@stu.com", or "@gyo.com", then the recipient may be detected as the unintended recipient.

[0042] In another example, instructions to compare the first recipient email address with the client data in the body of the email message may include instructions to compare a domain address of the first recipient email address with

the client data provided in the body of the email message. Example client data may include a client name (e.g., a competitor name). In this example, the whitelisting policy may include the client data mapped to a domain address that is permitted to send the email message.

[0043] For example, consider that the content in the body of the email message may include a client/competitor name "xyz". In this example, the whitelisting policy may indicate that the client name "xyz" is mapped to "@stu.com" and "@gyo.com". Therefore, recipients with a domain address "@stu.com" or "@gyo.com" may be permitted to send the email message when client name "XYZ" is mentioned in the body of the email message. In the above example, if the first recipient email address belongs to the domain address "@stu.com" or "@gyo.com", then the email message may be permitted to send to the first recipient email address. If the first recipient email address does not belong to the domain address "@stu.com" or "@gyo.com", then the recipient may be detected as the unintended recipient.

[0044] Instructions 312 may be executed by processor 302 to generate a prompt to amend the first recipient email address in response to the detection. In an example, instructions to generate the prompt may include instructions to generate a recommendation to replace or remove the first recipient email address in response to an attempt to send the email message. An example user interface depicting an email message and a notification is explained in FIG. 4.

[0045] FIG. 4 is an example graphical user interface 400, depicting an email message 402 and a prompt 414 indicating an unintended recipient of email message 402 based on a whitelisting policy. As shown in FIG. 4, a recipient email address 404 "randy@mmm.com" inputted in a recipient field of email message 402 may be determined prior to sending email message 402. Recipient email address 404 may be a new recipient added by a sender 408 to a list of recipients (e.g., recipient email address 406) associated with an email thread of email message 402 or added to a new email message.

[0046] Further, recipient email address 404 may be compared with a second email address associated with email message 402 or client data 412 in a body of

email message 402. Example client data 412 may include a client name (e.g., "LMN company limited" as shown in FIG. 4). Example second email address may include an email address of sender 408 (e.g., mike.rrr@xyz.com), a second recipient 406 (e.g., john@abc.com) in the recipient field, or a previous recipient 410 (e.g., joy.kr@abf.com) associated with the email thread of email message 402.

[0047] Furthermore, a recipient associated with first recipient email address 404 may be detected as an unintended recipient of email message 402 by applying a whitelisting policy to the comparison. The whitelisting policy may indicate a permitted email address corresponding to the second email address or client data 412. For example, the whitelisting policy may indicate recipients with domain addresses "@abf.com" and "@xyz.com" may be permitted to send email message 402 for domain address "@abc.com" of second recipient 406. Similarly, the whitelisting policy may also indicate domain addresses that can be permitted to send email message 402 corresponding to a domain address of sender 408, a domain address of previous recipient 410, or client data in the body of email message 402.

[0048] In the example shown in FIG. 4, domain address "@mmm.com" of recipient email address 404 may not be matched with domain addresses "@abf.com" and "@xyz.com" that may be permitted to send email message 402 as per the whitelisting policy. Therefore, prompt 414 indicating that the whitelisting policy may not permit to send email message 402 to recipient 404 may be generated. Prompt 414 may also provide a recommendation to amend recipient email address 404. In other examples, prompt 414 may seek confirmation from sender 408 to send email message 402 to recipient email address 404. Thus, examples described herein may determine whether email message 402 may include domain addresses of known clients or competitors and generate notification 414 to avoid unintentional sharing of email message 402 between the clients or competitors. For example, simultaneous copy of competitors on email message 402, or sharing of a relationship with other customers can be avoided by detecting the domain addresses of recipients (e.g., including prior recipients of the email thread) or client data 412.

[0049] FIG. 5 is a block diagram of an example computing device 500 including a non-transitory machine-readable storage medium 504, storing instructions to detect an unintended recipient of an email message based on domain addresses of recipient email addresses. Computing device 500 may include a processor 502 and machine-readable storage medium 504 communicatively coupled through a system bus. Processor 502 may be any type of central processing unit (CPU), microprocessor, or processing logic that interprets and executes machine-readable instructions stored in machine-readable storage medium 504. Machine-readable storage medium 504 may be a random-access memory (RAM) or another type of dynamic storage device that may store information and machine-readable instructions that may be executed by processor 502. For example, machine-readable storage medium 504 may be synchronous DRAM (SDRAM), double data rate (DDR), rambus DRAM (RDRAM), rambus RAM, etc., or storage memory media such as a floppy disk, a hard disk, a CD-ROM, a DVD, a pen drive, and the like. In an example, machine-readable storage medium 504 may be a non-transitory machine-readable medium. In an example, machine-readable storage medium 504 may be remote but accessible to computing device 500.

[0050] As shown in FIG. 5, machine-readable storage medium 504 may store instructions 506-514. In an example, instructions 506-514 may be executed by processor 502 to detect the unintended recipient of the email message. Instructions 506 may be executed by processor 502 to enable to create an email message, for instance, via a user interface of computing device 500.

[0051] Instructions 508 may be executed by processor 502 to determine a first recipient email address, a second recipient email address, and a third recipient email address inputted into a recipient field of the email message, for instance, prior to sending the email message. Instructions 510 may be executed by processor 502 to analyze a first domain address, a second domain address, and a third domain address of the first recipient email address, the second recipient email address, and the third recipient email address, respectively.

[0052] Instructions 512 may be executed by processor 502 to detect that the first recipient email address is in a different domain compared to the second

recipient email address and the third recipient email address that are in a same domain based on the analysis. Instructions 514 may be executed by processor 502 to generate a notification indicating that the first recipient email address is an unintended recipient email address of the email message in response to the detection.

[0053] In an example, instructions to generate the notification that the first recipient email address is the unintended recipient email address may include instructions to:

- determine that a number of recipient email addresses in a domain of the first recipient email address is less than a threshold, and
- generate the notification indicating that the first recipient email address is the unintended recipient when the number of recipient email addresses in the domain of the first recipient email address is less than the threshold.

[0054] In one example, instructions to generate the notification may include instructions to provide a recommendation to replace or remove the first recipient email address. In another example, instructions to generate the notification may include instructions to provide an option to seek confirmation to send the email message to the first recipient email address.

[0055] FIG. 6 is an example graphical user interface 600, depicting email message 602 and a notification 620 indicating an unintended recipient of email message 602 based on domain addresses of recipients (e.g., recipients 604-618). In the example shown in FIG. 6, recipient email addresses 604-618 inputted in a recipient field of email message 602 may be determined in response to an attempt to send email message 602. In this example, recipient email addresses 608 and 616 may be in a first domain "@xyz.com" and recipient email addresses 604, 606, 610, 612, 614, and 618 are in a different domain "@abc.com".

[0056] Further, the domains of recipient addressees 608-618 may be compared to identify a minority of inconsistent domains. In this example, recipient email addresses 608 and 616 are in a minority domain compared to other

recipient email addresses 604, 606, 610, 612, 614, and 618, i.e., the number of recipient email addresses 608 and 616 in the first domain may be less than the number of recipient email addresses 604, 606, 610, 612, 614, and 618 in the different domain.

[0057] In this case, the number of recipient email addresses 608 and 616 in the first domain may be determined as being less than a threshold. The threshold may be user defined. For example, the threshold may be 10%. In this case, consider that less than 10% of recipient email addresses or a single recipient may be in the first domain compared to other recipients who are in the different domain. Furthermore, a notification 620 indicating that the recipient email addresses 608 and 616 are unintended recipients may be generated when the number of recipient email addresses 608 and 610 in the first domain are less than the threshold. Further, notification 620 may seek confirmation from the sender to send email message 602 to recipient email addresses 608 and 610. Thus, examples described herein may detect an unusual balance of domain addresses in the recipient field of email message 602.

[0058] FIG. 7 is a block diagram of an example email system 700, including an email client application 706 to determine whether an email message can be sent to a recipient entered in a recipient field. Example email system 700 may include an email user/sender 702 who interacts with an email user interface 704 of email client application 706 running on a computing device 708. Example email client application 706 may be a stand-alone email application or part of a combined scheduling and calendar application.

[0059] Email client application 706 may communicate via a network 710 with other computing devices (e.g., computing device 712), each running an associated own email client application. A server 714 may provide an email server application 716 for email client application 706. Email client application 706 may include an email analyzer 720 to determine content in a body of the email message and/or a list of recipients in the email message created by email user 702 to check if the list of recipients is likely to include any incorrect recipients. In one example, email analyzer 720 may use a policy (e.g., a policy 722, a whitelisting policy 724, or the

like) stored in a repository 726 to detect the incorrect recipients. Repository 726 may be internal to computing device 708 or accessible to email client application 706 via network 710.

[0060] Example network 710 can be a local area network (LAN) or a wide area network (WAN). Network 710 can include any suitable technology, such as Public Switched Telephone Network (PSTN), Ethernet, Wi-Fi, or the like. For simplicity, example email system 700 depicts two computing devices 708 and 712 and server 714 connected to network 710. However, any number of computing devices and servers can be connected to network 710.

[0061] In an example, email analyzer 720 may evaluate the content and/or the list of recipients using an algorithm, a machine learning model, or the like. For example, machine learning may refer to an application of artificial intelligence (AI) that provides systems an ability to automatically learn and improve from experience without being explicitly programmed. In an example, the machine learning model may be trained on input words and/or strings of words using machine learning and natural language processing methods to implement the functionalities described with respect to FIGs. 1-6.

[0062] For example, the machine learning model may be trained to evaluate the content of the email message against a policy (e.g., as described in FIG. 1), compare a first recipient email address with a second email address associated with the email message or client data in the body of the email message (e.g., as described in FIG. 3), or analyze domain addresses of recipient email addresses (e.g., as described in FIG. 5). Further, the machine learning model may be trained to detect an unintended recipient/confidential data in the email message and generate a prompt 718 in response to the detection.

[0063] Example prompt 718 may be provided in the form of a dialogue box on the email user interface 704 when email analyzer 720 determines that the email message cannot be permissible to send to the recipient (e.g., an incorrect recipient). Prompt 718 on email user interface 704 may include appropriate recommendations, warnings, confirmations, and the like. Email user 702 can

select the relevant/irrelevant addressees, amend the email message appropriately, or may decide to disregard prompt 718.

[0064] Further, email analyzer 720 can be provided as part of the email client application 706. Alternatively, email analyzer 720 can be provided as a service provided over network 710 from server 714. In other examples, email analyzer 720 may also be implemented as part of a server within the user's organization. Email analyzer 720 can be selectively enabled (e.g., by email user 702 or an administrator) to provide the prompts tailored to user's requests or company's policies.

[0065] The above-described examples are for the purpose of illustration. Although the above examples have been described in conjunction with example implementations thereof, numerous modifications may be possible without materially departing from the teachings of the subject matter described herein. Other substitutions, modifications, and changes may be made without departing from the spirit of the subject matter. Also, the features disclosed in this specification (including any accompanying claims, abstract, and drawings), and/or any method or process so disclosed, may be combined in any combination, except combinations where some of such features are mutually exclusive.

[0066] The terms "include," "have," and variations thereof, as used herein, have the same meaning as the term "comprise" or appropriate variation thereof. Furthermore, the term "based on", as used herein, means "based at least in part on." Thus, a feature that is described as based on some stimulus can be based on the stimulus or a combination of stimuli including the stimulus. In addition, the terms "first" and "second" are used to identify individual elements and may not meant to designate an order or number of those elements.

[0067] The present description has been shown and described with reference to the foregoing examples. It is understood, however, that other forms, details, and examples can be made without departing from the spirit and scope of the present subject matter that is defined in the following claims.

WHAT IS CLAIMED IS:

1. A non-transitory computer-readable storage medium encoded with instructions that, when executed by a processor of a computing device, cause the processor to:
 - determine content and a recipient of an email message prior to sending the email message;
 - evaluate the content of the email message against a policy;
 - determine that the content of the email message is not permissible to send to the recipient based on the evaluation; and
 - generate a notification on a user interface in response to the determination that the content of the email message is not permissible to send to the recipient.
2. The non-transitory computer-readable storage medium of claim 1, wherein the notification may indicate a refusal to send the email message to the recipient based on a type of the content.
3. The non-transitory computer-readable storage medium of claim 1, wherein the notification is to provide a recommendation to include another recipient to the email message based on a type of the content.
4. The non-transitory computer-readable storage medium of claim 1, wherein the notification may indicate a replacement or removal of the recipient from the email message based on a type of the content.
5. The non-transitory computer-readable storage medium of claim 1, wherein instructions to evaluate the content of the email message against the policy comprise instructions to:
 - determine a content type of the email message, wherein the content type is determined based on confidential information, sensitive information, financial information, or a combination thereof in the content of the email message; and
 - evaluate the content type against the policy to determine whether the email message is permissible to send to the recipient.

6. The non-transitory computer-readable storage medium of claim 1, wherein instructions to evaluate the content of the email message against the policy comprise instructions to:

evaluate the content of the email message against the policy by applying a machine learning model.

7. A non-transitory computer-readable storage medium encoded with instructions that, when executed by a processor of a computing device, cause the processor to:

determine a first recipient email address inputted in a recipient field of an email message prior to sending the email message;

compare the first recipient email address with a second email address associated with the email message or client data in a body of the email message;

detect that a recipient associated with the first recipient email address is an unintended recipient of the email message by applying a whitelisting policy to the comparison, wherein the whitelisting policy is to indicate a permitted email address corresponding to the second email address or the client data; and

generate a prompt to amend the first recipient email address in response to the detection.

8. The non-transitory computer-readable storage medium of claim 7, wherein instructions to generate the prompt to amend the first recipient email address comprise instructions to:

generate a recommendation to replace or remove the first recipient email address in response to an attempt to transmit the email message.

9. The non-transitory computer-readable storage medium of claim 7, wherein instructions to compare the first recipient email address with the second email address comprise instructions to:

compare a domain address of the first recipient email address to a domain address of the second email address to detect the unintended recipient.

10. The non-transitory computer-readable storage medium of claim 7, wherein instructions to compare the first recipient email address with the client data in the body of the email message comprise instructions to:

compare a domain address of the first recipient email address with the client data provided in the body of the email message, the client data comprises a client name.

11. The non-transitory computer-readable storage medium of claim 7, wherein the whitelisting policy includes:

a domain address of the second email address mapped to a domain address that is permitted to send the email message; or

the client data mapped to a domain address that is permitted to send the email message.

12. The non-transitory computer-readable storage medium of claim 7, wherein the second email address comprises an email address of a sender, a second recipient in the recipient field, or a previous recipient associated with an email thread of the email message.

13. A non-transitory computer-readable storage medium encoded with instructions that, when executed by a processor of a computing device, cause the processor to:

enable to create an email message;

determine a first recipient email address, a second recipient email address, and a third recipient email address inputted into a recipient field of the email message;

analyze a first domain address, a second domain address, and a third domain address of the first recipient email address, the second recipient email address, and the third recipient email address, respectively;

detect that the first recipient email address is in a different domain compared to the second recipient email address and the third recipient email address that are in a same domain based on the analysis; and

generate a notification indicating that the first recipient email address is an unintended recipient email address of the email message in response to the detection.

14. The non-transitory computer-readable storage medium of claim 13, wherein instructions to generate the notification comprise instructions to:

provide a recommendation to replace or remove the first recipient email address; or

provide an option to seek confirmation to send the email message to the first recipient email address.

15. The non-transitory computer-readable storage medium of claim 13, wherein instructions to generate the notification that the first recipient email address is the unintended recipient email address comprise instructions to:

determine that a number of recipient email addresses in a domain of the first recipient email address is less than a threshold; and

generate the notification indicating that the first recipient email address is the unintended recipient when the number of recipient email addresses in the domain of the first recipient email address is less than the threshold.

1/8

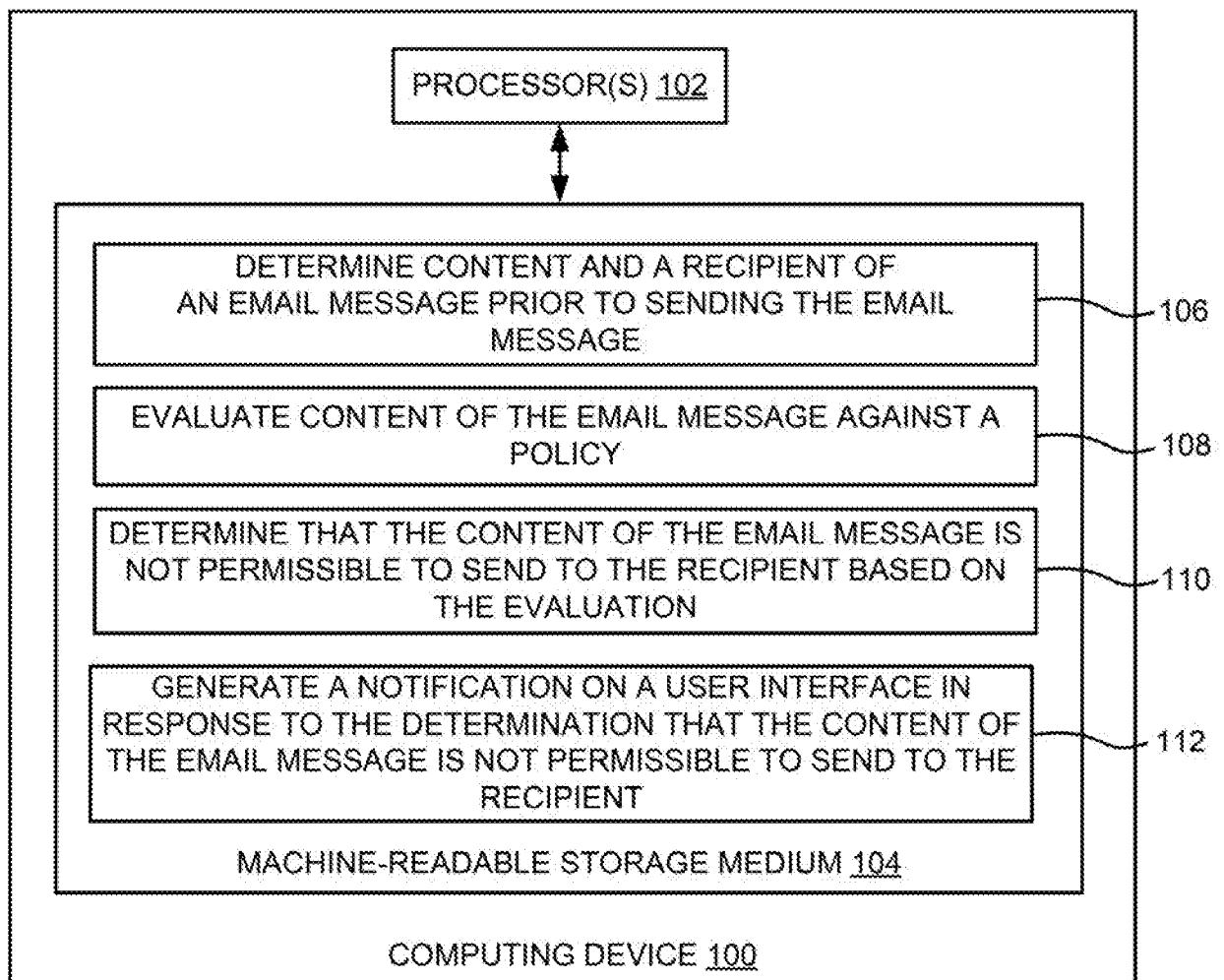


FIG. 1

FILE

MESSAGE

INSERT

FORMAT TEXT

HELP

UNTITLED - MESSAGE (HTML)

FROM

MIKE.RRR@XYZ.COM

TO

JOHN@LMN.COM

CC

SEND

SUBJECT REF. NO. 12345: FIRST DRAFT

ATTORNEY PRIVILEGE COMMUNICATION

HI JOHN,

PLEASE FIND THE ATTACHED DRAFT ASSIGNMENT BETWEEN "XYZ CORPORATION LTD" AND "LMN COMPANY LTD" FOR YOUR REVIEW.

KINDLY CONTACT US IF YOU HAVE ANY QUESTIONS

REGARDS,
MIKE
XYZ CORPORATION

ALERT

THIS EMAIL INCLUDES CONFIDENTIAL INFORMATION. PLEASE INCLUDE COMPANY'S ATTORNEY "HARRIS@XYZ.COM" TO THE EMAIL MESSAGE

CANCEL

FIG. 2A

FILEMESSAGEINSERTFORMAT TEXTHELP

UNTITLED – MESSAGE (HTML)

FROM

MIKE.RRR@XYZ.COM

258

TO

JOY.KR@ABF.COM

254

CC

SEND

SUBJECTREF. NO. 12345: FIRST DRAFT

HI JOY,

PLEASE FIND THE BELOW PROJECT DETAILS, WHICH WE

ARE PLANNING TO OBTAIN INTELLECTUAL PROPERTY

IN UNITED STATES.

{.....

.....

.....}

REGARDS,

MIKE

XYZ CORPORATION

256A

256B

252

ALERT

THIS EMAIL INCLUDES CONFIDENTIAL INFORMATION AND CANNOT BE SENT TO "JOY.KR@ABF.COM"

CANCEL

260

256

200B

FIG. 2B

4/8

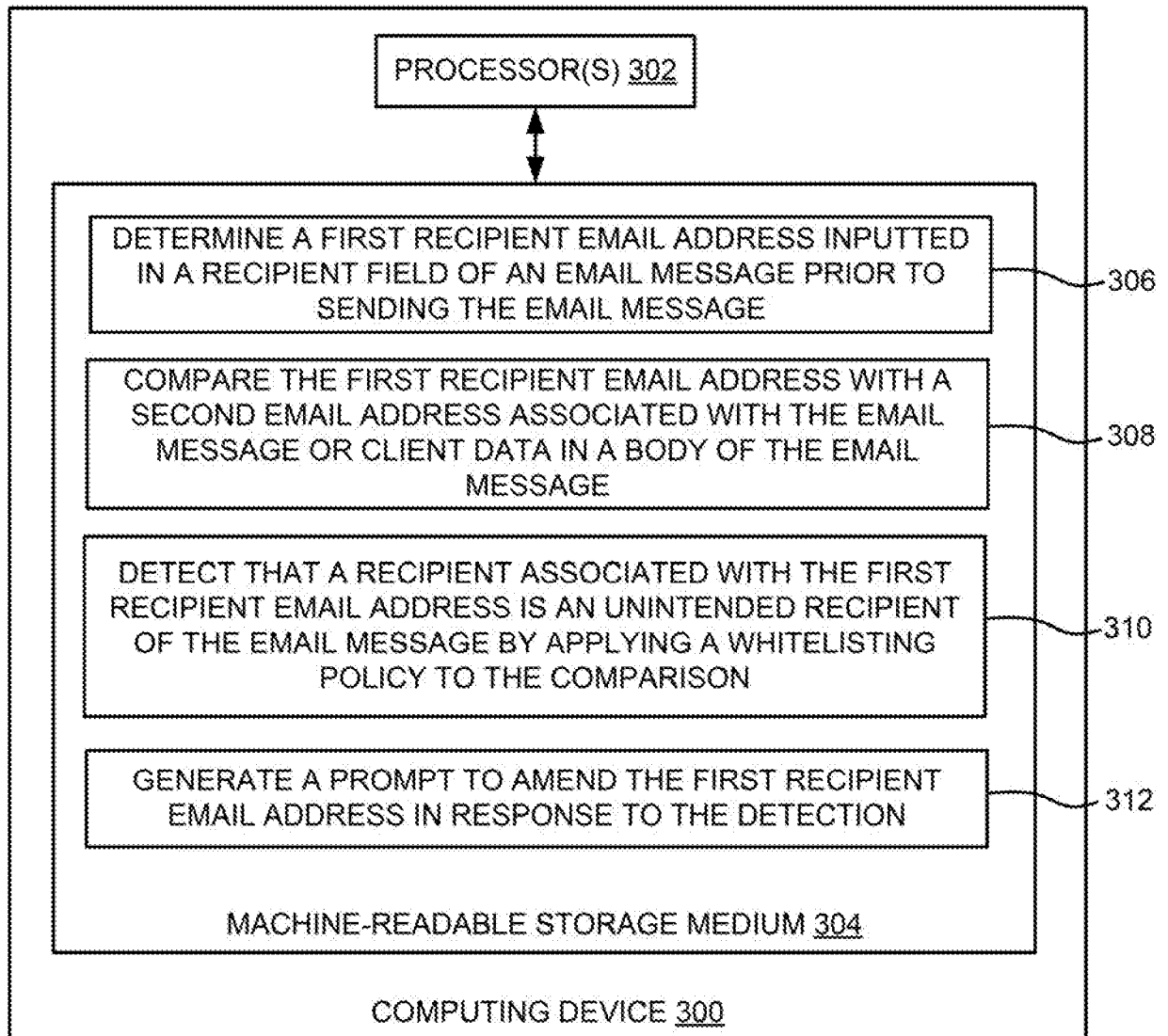


FIG. 3

FILEMESSAGEINSERTFORMAT TEXTHELP

UNTITLED – MESSAGE (HTML)

FILE

FROM

TO

CC

MIKE.RRR@XYZ.COM

JOHN@ABC.COM

408

404

406

SUBJECT RE: REF. NO. 12345: FIRST DRAFT

PRIVILEGED AND CONFIDENTIAL

412

HI JOHN,
PLEASE FIND THE ATTACHED DRAFT AGREEMENT OF
"LMN COMPANY LTD" FOR YOUR REVIEW.
KINDLY CONTACT US IF YOU HAVE ANY QUESTIONS.
REGARDS,
MIKE

414

ALERT
THE WHITELISTING POLICY DOES NOT
PERMIT TO SEND THIS EMAIL MESSAGE
TO "RANDY@MMM.COM". DO YOU WANT
TO PROCEED?
SEND
CANCEL

402

FROM: JOHN@ABC.COM
SENT: 08 AUGUST 20XX
TO: 'MIKE' <MIKE.RRR@XYZ.COM>; JOY.KR@ABF.COM
SUBJECT: REF. NO. 12345: FIRST DRAFT

410

400

402

FIG. 4

6/8

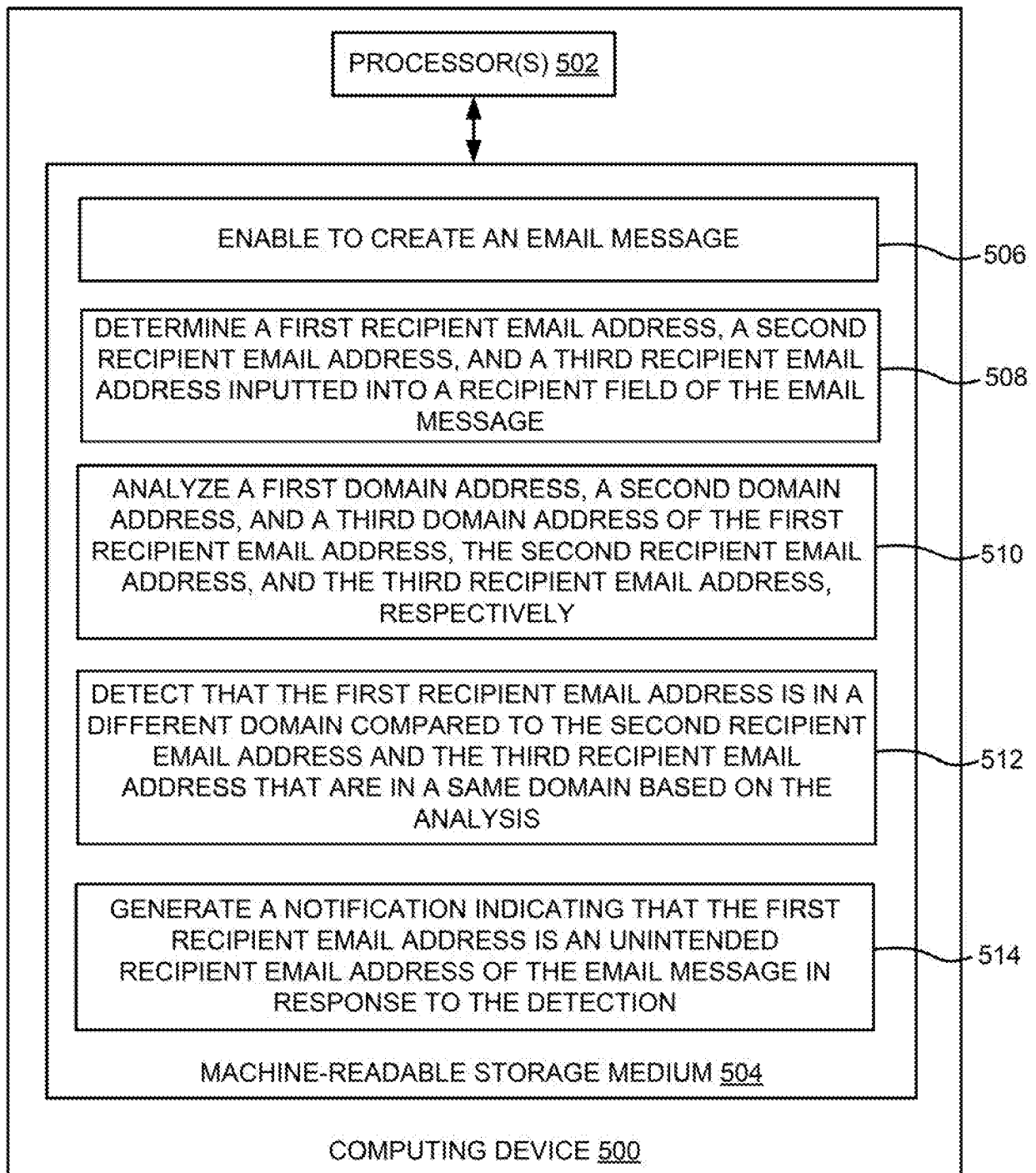


FIG. 5

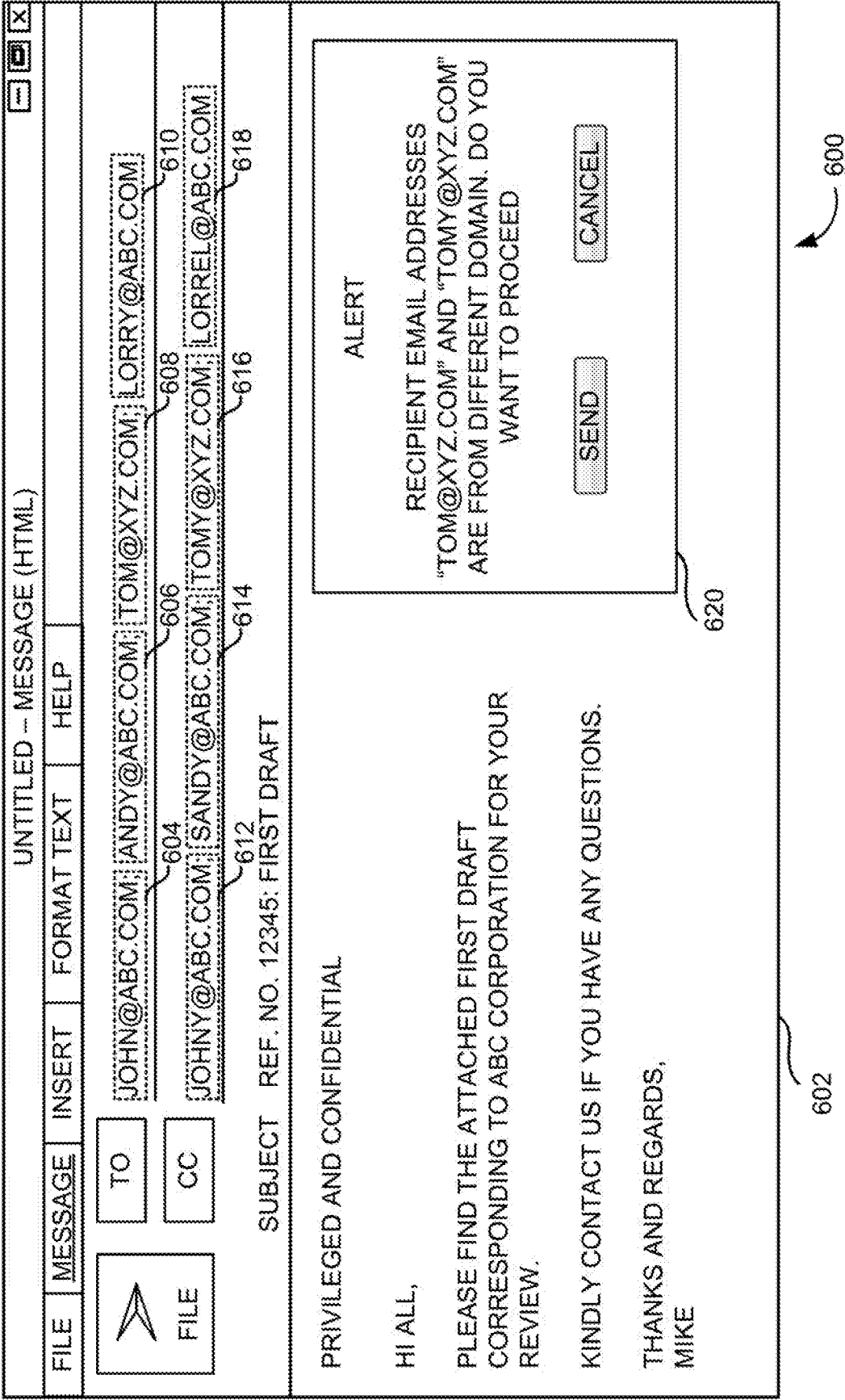


FIG. 6

8/8

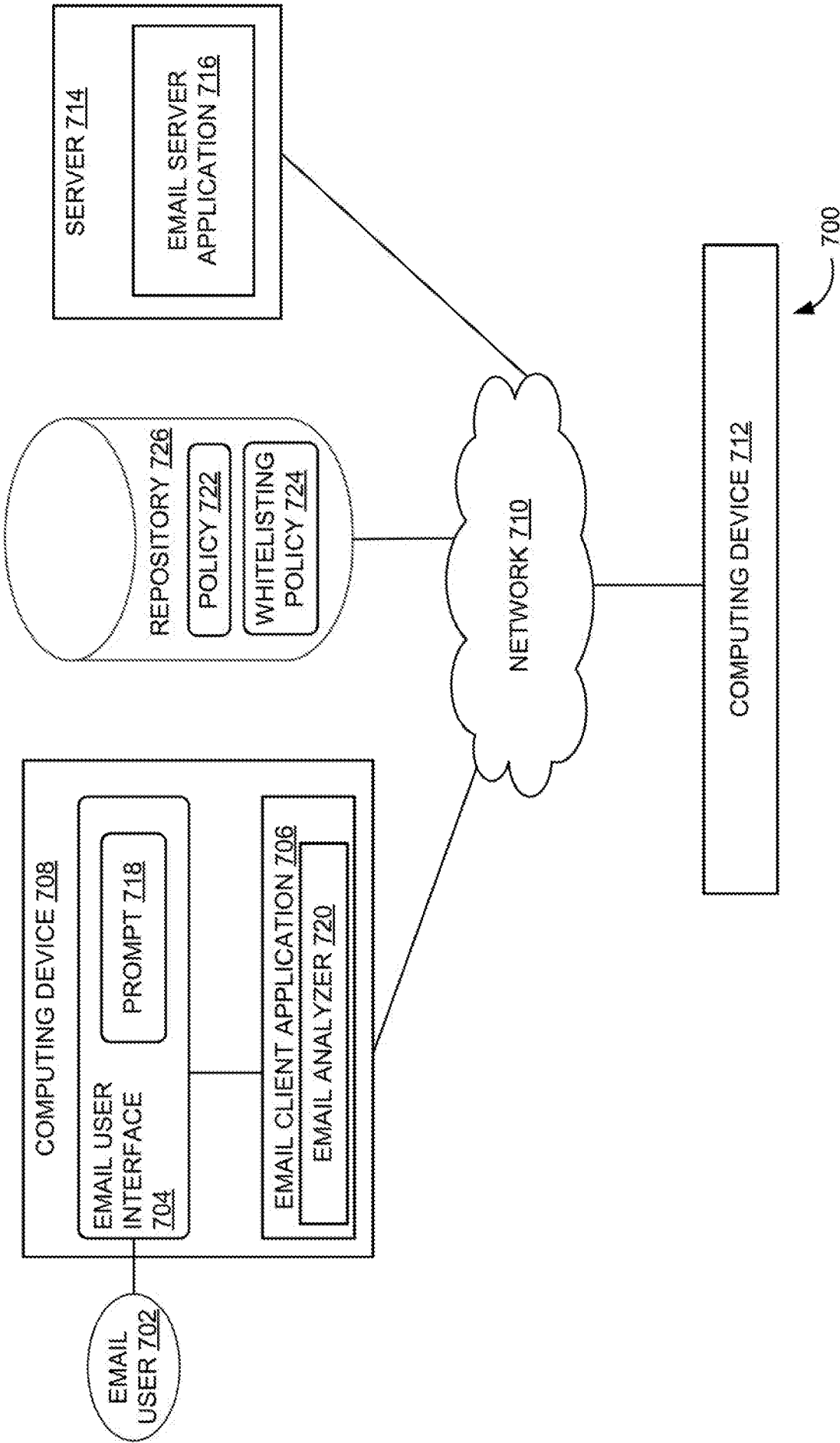


FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 2020/047731

A. CLASSIFICATION OF SUBJECT MATTER		
<i>H04L 12/58 (2006.01)</i> <i>H04L 12/859 (2013.01)</i> <i>G06F 21/16 (2013.01)</i>		
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)		
H04L 12/00 -12/859, G06F 21/00-21/16		
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 practicable, search terms used)		
PatSearch (RUPTO Internal), USPTO, PAJ, Espacenet, Information Retrieval System of FIPS		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 9736100 B2 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 15.08.2017, abstract, column 2, lines 36-67, column 4, line 55-column 6, line 20, column 8, lines 14-67, column 10, line 4-column 11, line 26, figures 1, 2	1-5, 7-15
Y		6
Y	US 2016/0294755 A1 (TRISHA N. PRABHU) 06.10.2016, paragraph [0060]	6
A	US 2012/0011192 A1 (MARK MEISTER et al.) 12.01.2012	1-15
A	US 2009/0158430 A1 (KEVIN R. BORDERS) 18.06.2009	1-15
☐ Further documents are listed in the continuation of Box C. ☐ 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 "D" document cited by the applicant in the international application "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 22 March 2021 (22.03.2021)	Date of mailing of the international search report 08 April 2021 (08.04.2021)	
Name and mailing address of the ISA/RU: Federal Institute of Industrial Property, Berezhkovskaya nab., 30-1, Moscow, G-59, GSP-3, Russia, 125993 Facsimile No: (8-495) 531-63-18, (8-499) 243-33-37	Authorized officer E. Krivtsova Telephone No. 8(495)531-65-15	