

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Apple Inc.,

Petitioner

v.

Rally AG LLC,

Patent Owner

Case IPR2024-01446

U.S. Patent No. 11,361,107

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	SUMMARY OF THE '107 PATENT	6
	A. The State Of The Art	6
	B. An Example Of Personal Data Sharing Before The '107 Patent	7
	C. The Invention Claimed In The '107 Patent	8
	D. Claim Construction	24
	E. Person Of Ordinary Skill In The Art	24
III.	THE ASSERTED PRIOR ART	25
	A. Lee	25
IV.	THE PETITION FAILS TO SHOW A REASONABLE LIKELIHOOD THAT ANY CLAIMS OF THE '107 PATENT ARE UNPATENTABLE	33
	A. Claim 13	33
	1. The Petition fails to show that a POSITA would have found it obvious to “determine whether the end user profile contains a previous association between the relying party email address and a cloaked relying party email address . . . ; [and] in response to determining the end user profile does not contain a previous association between the relying party address and the cloaked relying party email address, generate a new cloaked relying party email address”	33
	2. The Petition fails to show that a POSITA would have found it obvious to “send the email to the identified end user specified address, wherein the email is configured with a reply-to email address comprising the new cloaked relying party email address”	40
	B. The Challenges To The Other Claims Are Similarly Deficient	45
V.	THE BOARD SHOULD DENY INSTITUTION IN VIEW OF THE PARALLEL DISTRICT OF DELAWARE CASE	45
VI.	CONCLUSION	49

EXHIBIT LIST

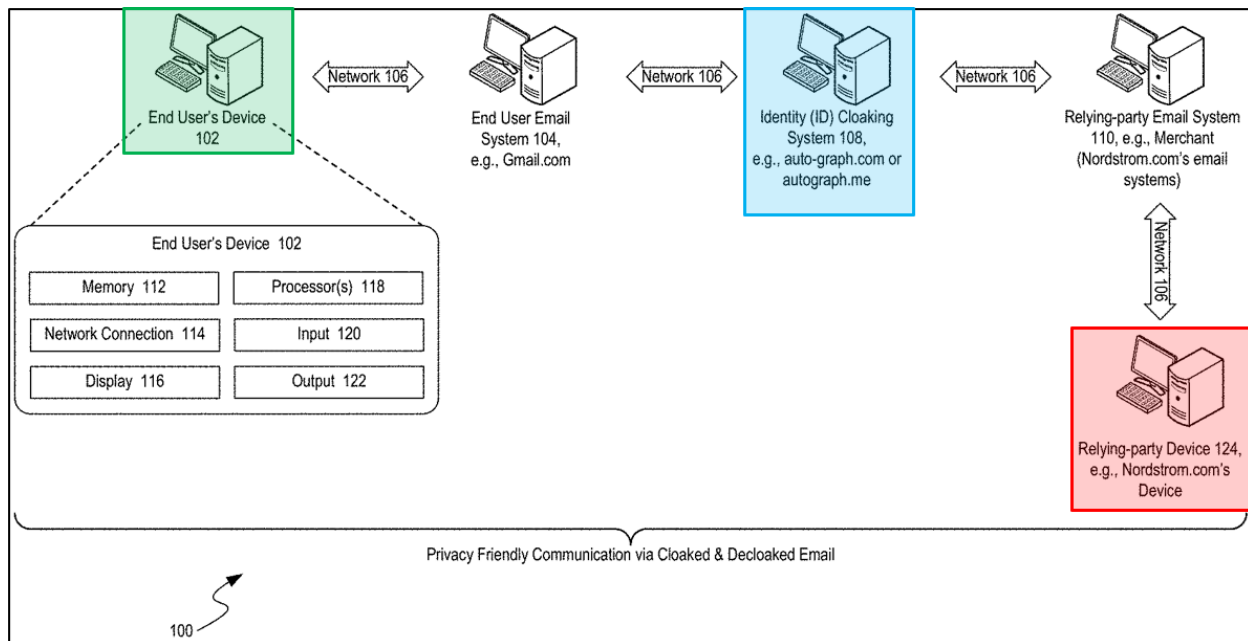
Exhibit No.	Description
Ex. 2001	<i>Rally AG LLC v. Apple, Inc.</i> , 123-cv-01106 (D. Del.), Docket as of January 16, 2025
Ex. 2002	Memorandum Opinion, 123-cv-01106 (D. Del.), Paper No. 52

All emphasis has been added and all internal citations have been omitted unless otherwise indicated.

I. INTRODUCTION

The realities of Internet communication and modern e-commerce result in a constant barrage of third-party requests for sensitive personal information. Some form of personal data is requested for almost any online activity. In some instances (*e.g.*, for delivery of an online purchase), transfer of some personal data may be legitimate and necessary. But often, requested personal information is not really required. The inventor of U.S. Patent No. 11,361,107 (“’107 Patent”) recognized this and sought to (i) limit the amount of personal information shared with third parties and (ii) decrease the risk of sharing when that sharing was necessary. In particular, the ’107 Patent enhances a user’s ability to utilize email in a way that maximizes privacy while enjoying the familiarity of their chosen email system.

The ’107 Patent provides an unobtrusive ID cloaking system that serves as a bulwark between a user’s email system and a third party’s email system. The ID cloaking system defends the user’s privacy by augmenting emails sent between the user and the third party (referred to in the ’107 Patent as the “relying party”).



Ex. 1001, FIG. 1. By assigning unique “cloaked” email addresses that are associated with the ID cloaking system to the user and to each relying party, the ID cloaking system can keep itself in the communication loop. When forwarding a message from the user (green) to the relying party (red), the ID cloaking system (blue) “cloaks” certain content, such as the user’s private email address, so that the relying party does not obtain that personal information. Further, the ID cloaking system may “de-cloak” emails forwarded from the relying party to the user. De-cloaking re-inserts information into user-received emails, adding essential context back into those emails.

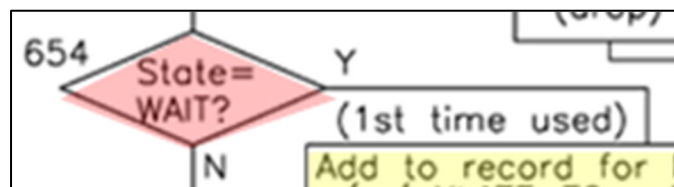
The Petition requests *inter partes* review (IPR) of claims 1-19 of the '107 Patent based on U.S. Patent No. 8,458,264 (Lee, “Email Proxy Server with First Respondent Binding”). Lee’s system allows a user to create a “single-sender public

email address.” Ex. 1004, 3:33-42. The first third party to send a message to that public email address is “bound” to that address such that future messages from that third party are relayed to the user. *Id.*, Title, FIG. 6D. Emails from any other third party are blocked. *Id.*

The Board should decline to institute IPR of the ’107 Patent for at least three reasons:

First, the claims of the ’107 Patent require “generat[ing] a new cloaked relying party email address” when it is “determined that the end user profile does not contain a previous association between the relying party address and [a] cloaked relying party email address.” Ex. 1001, Claim 13, Limitations 13(c), 13(d). These steps identify instances where relying parties have not yet been assigned a unique cloaked address that is associated with the ID cloaking system. In those instances, the ID cloaking system assigns the new relying party a cloaked relying party address.

That determination of whether a relying party needs to have a cloaked relying party address assigned to it is not present in Lee. The Petition cites to Lee’s step 654 as purportedly disclosing this functionality. Petition, 28-31. But Lee’s step 654 is looking at a STATE variable associated with a public email address.



Ex. 1004, FIG. 6D. That STATE variable indicates whether that “single-sender public email address” has been previously used (*i.e.*, whether a “first respondent” has been “bound” to that email address). Lee’s step 654, discussed at column 7:1-7, does not evaluate any email addresses, let alone describe a “determin[ation of] whether the end user profile contains a previous association between the relying party email address and a cloaked relying party email address” as required by the claims. Because Lee never makes the required “determin[ation]” and never subsequently “generat[es] a new cloaked relying party email address” based on that determination, institution should be denied.

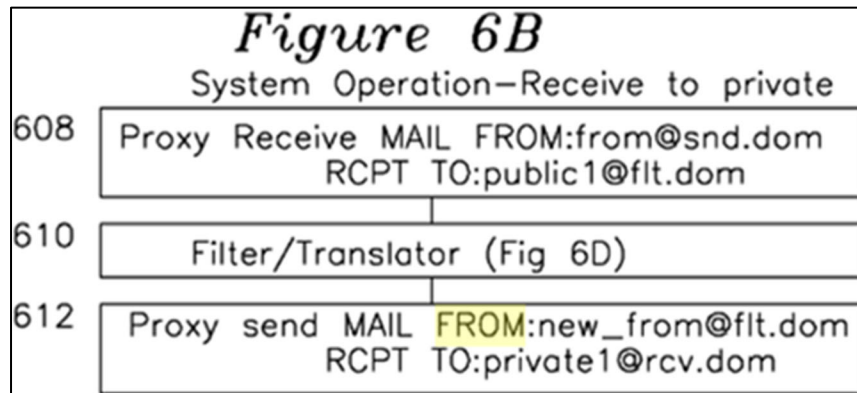
Second, the Petition fails to show that Lee and the knowledge of a POSITA renders obvious using the Reply-To field of emails to maintain email routing through the ID cloaking system. Ex. 1001, Claim 13, Limitation 13(e).



Id., FIG. 4 (annotated); 17:21-24. The From field (info@Nordstrom.com) is used for addressing a reply email when used without an overriding Reply-To field. The '107 Patent utilizes that overriding Reply-To field (cloak2@auto-graph.com), which is typically not displayed to the user, to direct the user’s reply back through

the ID cloaking system. The intact From field (info@Nordstrom.com) then provides the user context regarding the sender of the email that they are viewing.

Lee discloses use of the From field for selectively forwarding emails.



Ex. 1004, FIG. 6B. Petitioner and its expert admit that Lee does not contemplate use of the “Reply-To” field. They further admit that “[a] POSITA would have understood that these two fields serve distinct roles.” Petition, 33-34; Ex. 1003, ¶83. Despite Lee not discussing use of the Reply-To field, which Petitioner has admitted has a “distinct role” from the From field, the Petition provides no additional facts or reasoning to back its cursory claim that a POSITA would have found it obvious to utilize the Reply-To field as claimed. Based on this failure of proof, the institution should again be denied.

Third, the Board should deny the IPR in light of the parallel district court litigation, where an unpatentability determination could occur before the Final Written Decision in this case.

The Petition falls short of its burden to show that the claims of the '107 Patent are obvious. Institution should thus be denied.

II. SUMMARY OF THE '107 PATENT

A. The State Of The Art

Data sharing over computer networks has existed for decades. The dawn of the Internet exponentially increased that data sharing. Personal computing and network communication channels, such as email, facilitate easy sharing by users. But data sharing, particularly with third parties that a user does not completely trust, comes with risk. Ex. 1001, 2:59-61. Transmission of personal data exposes a user to the possibility of misuse by the third party or other entities. *Id.* Personal data might be intercepted, or even sold by the third party with which the user intended to communicate, enabling malicious or other unintended uses. *Id.* The user's name, email address, phone number, mailing address, age, social security number, credit card numbers, and other contact information might then be utilized in undesirable ways that range from annoying (spam marketing) to harmful (identity theft). *Id.*, 2:59-65.

At the time of the '107 Patent, Internet users could hardly access a website or shop online without their email address being required to log in or otherwise communicate. *Id.*, 2:61-65. To avoid the undesired use of personal information, there was a need for a user-friendly system that protected email addresses and

personal information from predatory actors while maintaining the familiar conveniences and user experience of modern email systems. *Id.*, 3:57-59; 3:61-66.

B. An Example Of Personal Data Sharing Before The '107 Patent

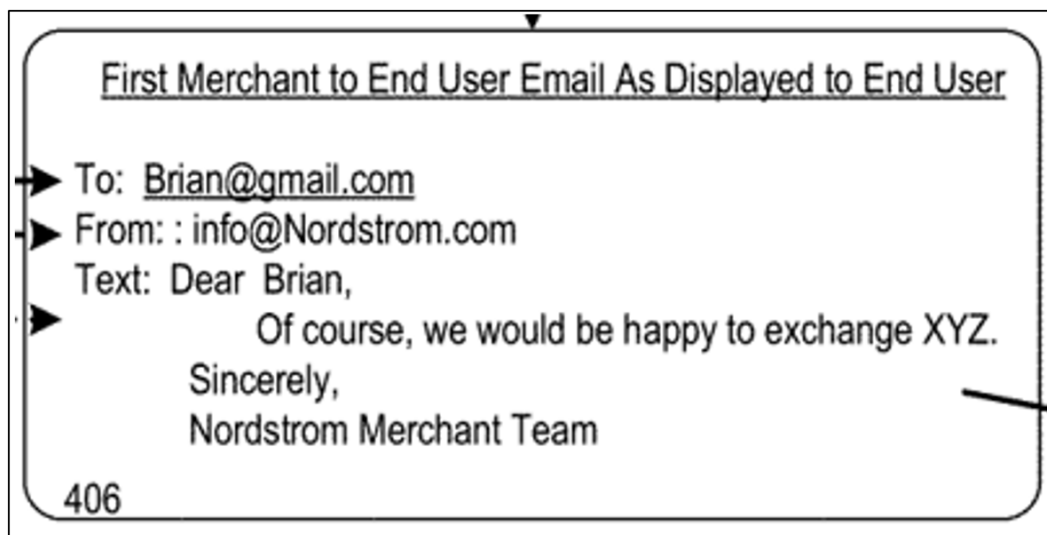
As noted above, websites, online stores, and other platforms have required users to divulge personal information to create accounts, transact commerce, and access information for many years. *Id.*, 2:61-65. These portals required users to provide personal information as a prerequisite to fully accessing their functionality. *Id.* Often, personal information was provided via web forms or other input methods. *Id.*, 6:52-55; 8:20-26. FIG. 2 depicts an example of a blank and completed web form on a third-party website:

FIG. 2 shows two versions of a web form 200. The left version is a blank form with fields for First Name, Last Name, Job title, Email Address, Phone, Address, Employees, United States, and State. The right version is the same form filled out with the name Brian Smith, job title Attorney, email Brian@gmail.com, phone 555-867-5309, and address 121 Gigawatt Street. Both forms include a checkbox for 'Employees', a dropdown for 'United States', and a dropdown for 'State'. A vertical line 208 separates the two forms, and a curved arrow 200 points to the bottom of the right form.

Id., FIG. 2 (edited). The web form 200 requested that the user, Brian, provide his name, occupation, email address, phone number, and mailing address. *Id.* When

the form was submitted, the website owner received and stored Brian's personal information on a remote server, leaving the confidentiality of Brian's personal information out of his control.

In an example, after sharing his personal information with the untrusted third party via the form above, Brian received an email from that third party:

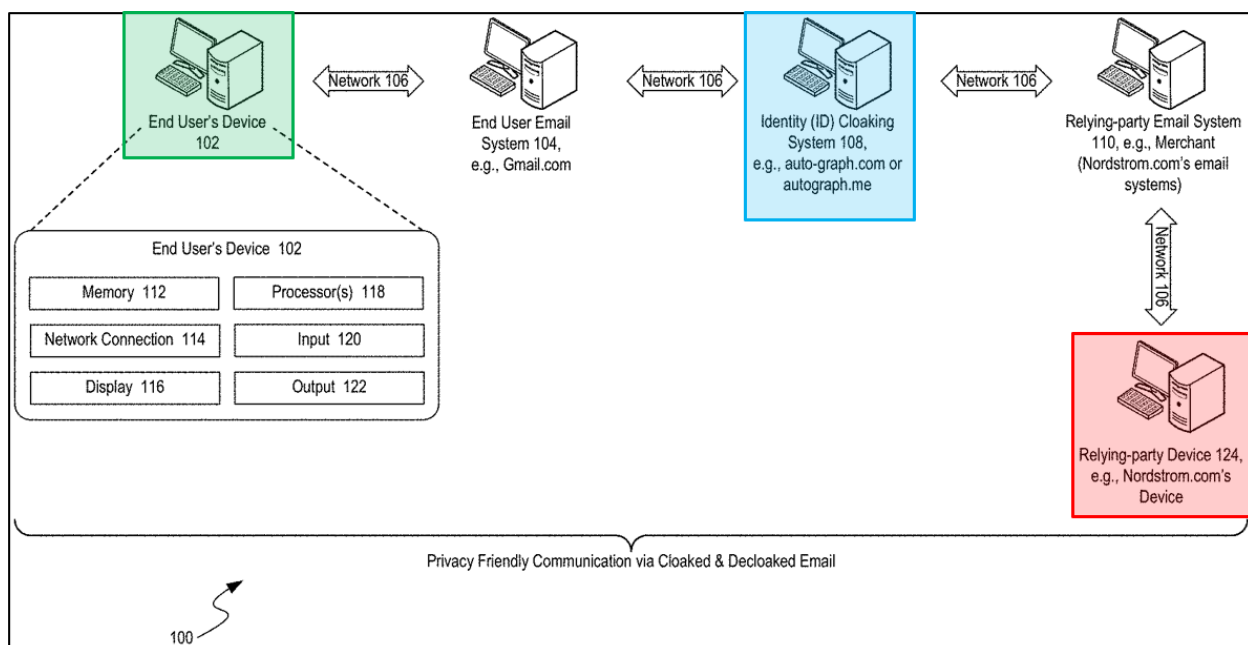


Id., FIG. 4 (edited). As shown, the third party possesses and is using Brian's name and personal email address to communicate. Ideally, Brian would have been able to transact with the third party without divulging his personal information.

C. The Invention Claimed In The '107 Patent

Recognizing that need, the '107 Patent provided a "tool[]" to efficiently protect privacy for end users and others on the Internet when communicating with others" in the form of an ID cloaking system. *Id.*, Abstract. An ID cloaking system 108 (highlighted in blue below) is inserted into the communication path between an end

user's device 102 (highlighted in green) and a relying party's¹ device 124 (highlighted in red). *Id.*, 4:5-10. The ID cloaking system receives and relays emails between the communicating parties in a way that is substantially transparent to the user. An email from a relying party appears to the user to be substantially similar to an email that did not traverse the ID cloaking system. The ID cloaking system protects the user's personal information by relaying emails in both directions through the ID cloaking system, cloaking, and, in some instances, de-cloaking the user's personal information in the relayed emails. *Id.*, 4:8-13.



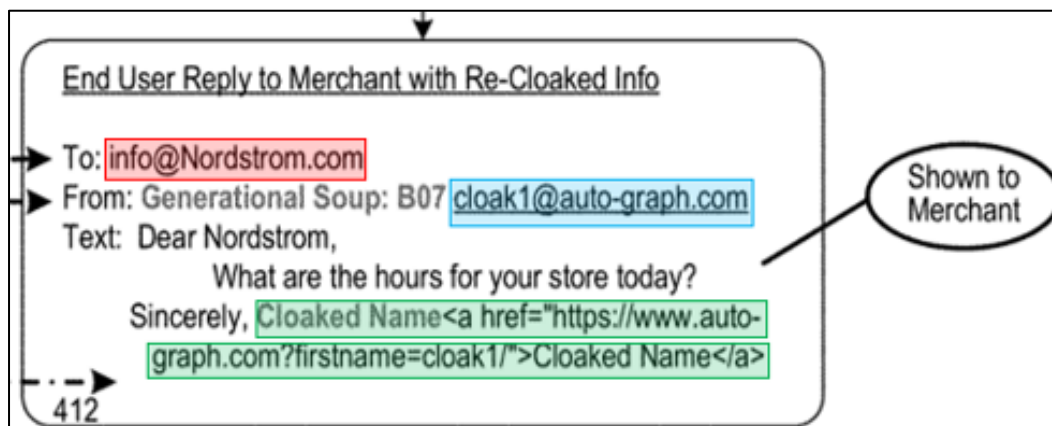
Id., FIG. 1.

¹ As noted above, third parties are referred to in the '107 Patent as "relying parties."

The ID cloaking system may augment emails in both directions (*i.e.*, from the user to the relying party; and from the relying party to the user) in multiple ways. First, the ID cloaking system adjusts certain email addresses (*i.e.*, Reply-To addresses) in forwarded emails so that a subsequent reply to the forwarded email again traverses the ID cloaking system before being directed to its destination. Second, the system revises emails from the user to the relying party to remove some or all personal information that the user does not want to share with the relying party, “cloaking” that information. And third, the system may further revise emails from the relying party to the user to restore certain personal information that was hidden from the relying party, “de-cloaking” that information. De-cloaking in emails relayed to the user provides improved context to the user, making those emails look similar to an email that they would expect to receive had that email not traversed the ID cloaking system on its way to the user.

Regarding the first augmentation, in relaying emails from the user to the relying party, the ID cloaking system changes the Reply-To address (blue below) from the user’s real email address to a cloaked end user address. More specifically, the ID cloaking system (operating on a server at auto-graph.com) replaces the user’s real address (Brian@gmail.com) with a cloaked end user address (cloak1@auto-graph.com). That cloaked end user address in the Reply-To field routes reply emails

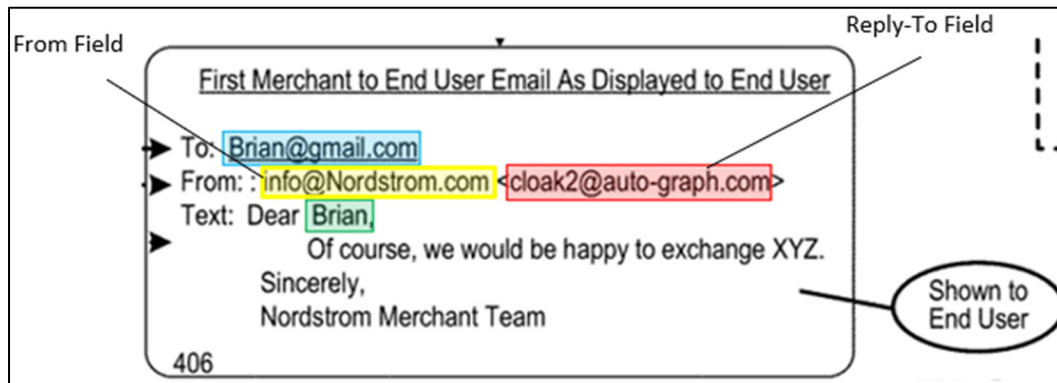
from the relying party back through the ID cloaking system (operating at auto-graph.com) for processing. *Id.*, 4:19-22.



Id., FIG. 4. In the example above, personal information is also removed. Specifically, the user's name in the From field is cloaked from "Brian" to "Generational Soup: B07," and the user's name in the body of the email is cloaked from "Brian" to "Cloaked Name." Thus, neither the user's real email address nor the user's name are provided to the relying party.

In the reverse direction, when relaying emails from the relying party to the user, the ID cloaking system again adjusts the Reply-To address from the relying party address (info@Nordstrom.com) to a cloaked relying party address (cloak2@auto-graph.com) (red) to ensure that a user's reply to the relayed email traverses the ID cloaking system. *Id.*, 10:64-11:3. Each relying party is associated with a unique cloaked relying party address. *Id.*, 9:4-7. That unique address indicates to the ID cloaking system to which relying party the user's reply should be

forwarded (*i.e.*, the user's reply should be routed to the relying party associated with cloak2@auto-graph.com). *Id.*, 12:64-13:3.

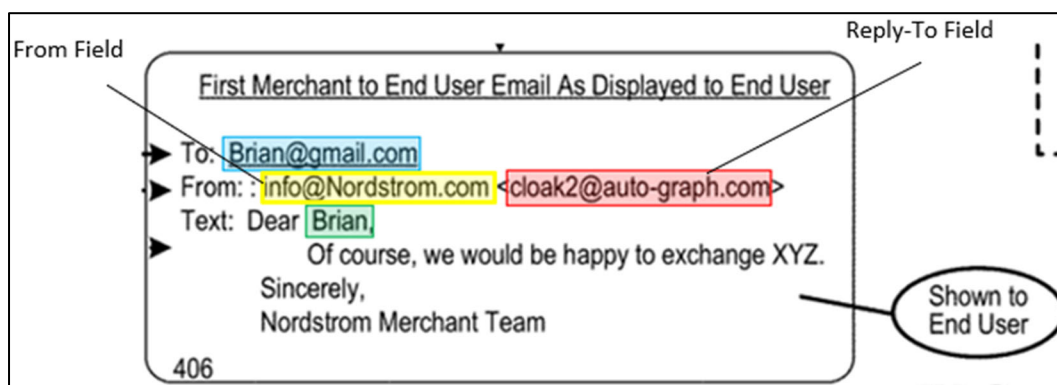


Id., FIG. 4. The ID cloaking system may further de-cloak certain information in the email to increase the amount of context provided to the user. In the above example, the user's name (**green**) is de-cloaked from "Cloaked Name" to "Brian."

Cloaked email addresses have a domain name that is associated with a server implementing the ID cloaking system. By adjusting real email addresses to cloaked addresses in Reply-To fields (*i.e.*, changing the user's real email address to a cloaked user address; and the relying party's email address to a cloaked relying party address), the system ensures that all replies are directed back through the ID cloaking system. When the ID cloaking system receives an email addressed to a particular cloaked address, that cloaked address is used to determine the destination to which the email should be forwarded. For example, when an email is received at a cloaked user address, user profiles are queried to determine to which real user email address that email should be forwarded. And when an email is received at a cloaked relying party

address, that cloaked relying party address is used to determine the relying party address to which that email should be forwarded. *Id.*, 12:52-13:3. Thus, the cloaked email addresses provide unique identifiers that direct the ID cloaking system to forward emails to the correct destination email addresses. *Id.*, 9:4-7 (“[Cloaked addresses] serve as a Globally Unique IDs (GUID) to identify [a party] when [the party’s] real information needs to be re-associated and/or to re-route information such as emails back to [the party].”).

The ID cloaking system seeks to maintain the familiar user experience of the user’s chosen email system while protecting the user’s personal information. De-cloaking personal information, which was hidden from the relying party, in emails forwarded to the user can assist in mimicking a typical email user experience (*e.g.*, a user experience where an ID cloaking system is not used). Further, not augmenting certain fields can help to maintain context and normalcy of operations.



Id., FIG. 4. As shown above in the email forwarded to the user, the Reply-To email address (red above) is changed (from info@Nordstrom.com to cloak2@auto-

graph.com) to ensure that the user's reply is routed back through the ID cloaking system operating at auto-graph.com. But, in that example, the From field (info@Nordstrom.com) (yellow) is not changed. The maintained From field (which is typically displayed to the user, where the Reply-To field is not) helps to provide context for the user by indicating the original sender of the forwarded email. *Id.*, FIG. 4.

Example Use Case

The ID cloaking system may be introduced into communications between the user and a relying party in a variety of ways. In one example, an email string between the user and the relying party is initiated by the user providing information into a web form. Instead of providing their real email address, the user requests a cloaked end user email address to submit with the form. This cloaked end user address routes a subsequent email from the relying party to the user through the ID cloaking system.

An example of a user requesting a cloaked end user address and initiating communications with a relying party using that cloaked end user address is shown in the example of FIGS. 2-4.

we'll be in touch right away.
Please fill out all fields.

First Name

Last Name

Job title

Email Address

Phone

Address

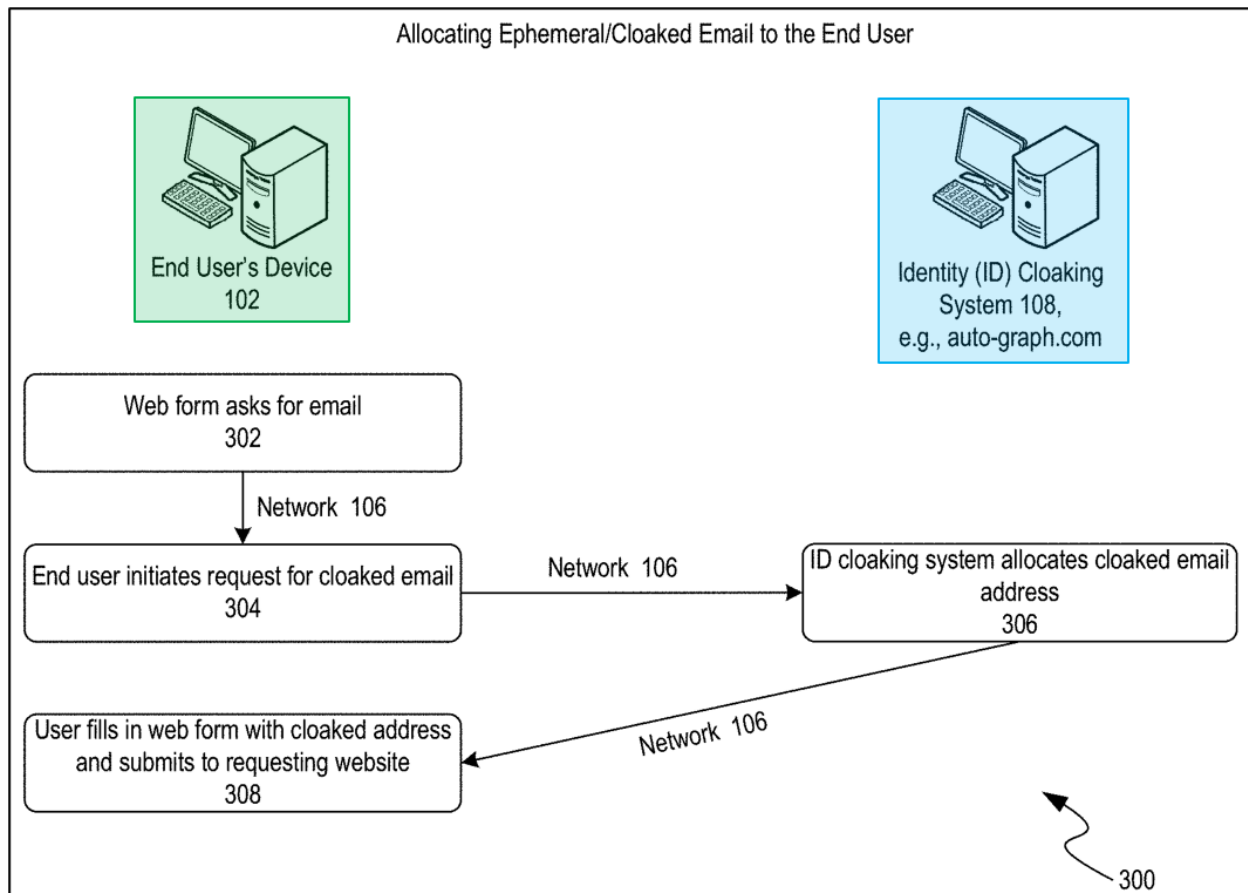
Employees

United States

State

By registering I confirm that I have read and agree to the [Privacy Statement](#).

Id., FIG. 2 (edited). In that example, the user traverses the Internet to a web form associated with the relying party, like the one shown above in FIG. 2, which requests the user's email address to facilitate a subsequent communication to the user. *Id.*, FIG. 2; FIG. 3.

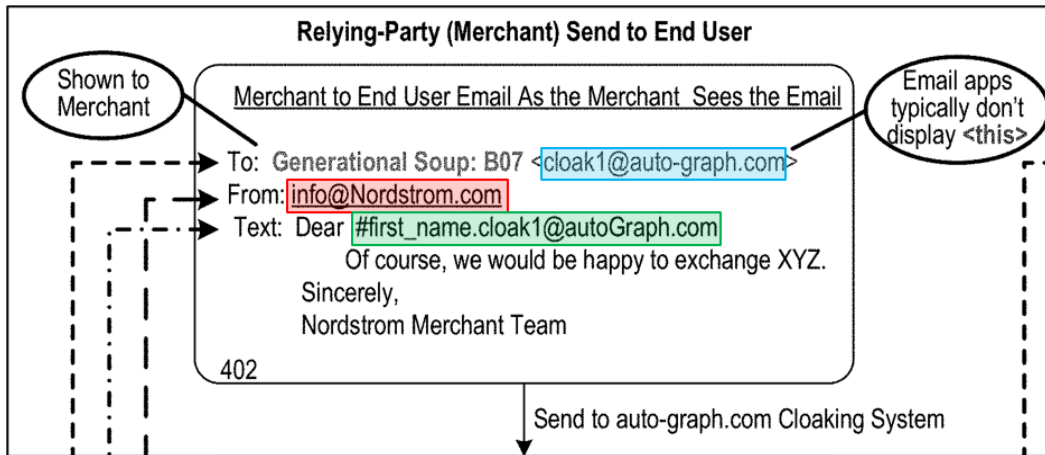


Id., FIG. 3. Because the user does not fully trust the relying party, the user does not want to communicate their actual email address via the form. Instead, the user requests a cloaked email from the ID cloaking system at 304 via a manual request, an application plugin, or other mechanism. *Id.*, 9:30-31. The ID cloaking system allocates a cloaked end user address to the user by generating a unique cloaked end user address that is entered into the form at 206. That cloaked end user address includes a domain associated with the ID cloaking system (auto-graph.com) such that emails to the user via that cloaked address traverse the ID cloaking system. *Id.*, 9:31-34; 19:13-15; 5:41-45.

In this example, the user, Brian, has a private end user address, Brian@gmail.com, and the relying party has a relying-party address, info@Nordstrom.com. *Id.* When Brian requested a cloaked end user address and cloaked first name at FIG. 3, step 304, the ID cloaking system allocated Brian a cloaked end user address of cloak1@auto-graph.com and a cloaked name of #first_name.cloak1@autoGraph.com. *Id.*

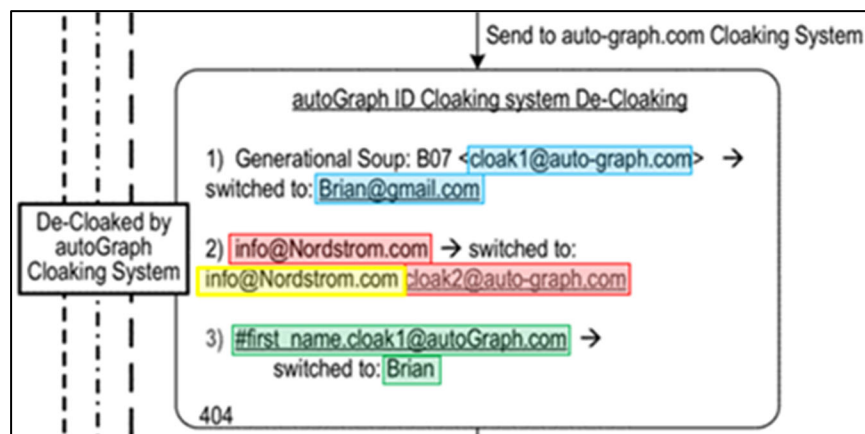
As Brian shopped on the relying party's website, that website prompted Brian to enter an email address via the form of FIG. 2 to continue shopping or to complete a transaction. Wishing to avoid providing the relying party with his name and private end user address (Brian@gmail.com), Brian provided his cloaked name (#first_name.cloak1@autoGraph.com) and cloaked end user address (cloak1@auto-graph.com) in the web form 308.

The following excerpt illustrates an email sent from the relying party (Nordstrom) to the user (Brian) using the cloaked end user address (cloak1@auto-graph.com) that Brian provided in the form:



Id., FIG. 4.

When the above email to cloak1@auto-graph.com is sent by the relying party, the ID cloaking system operating at auto-graph.com receives that email. The system identifies Brian's end user profile based on its association with the cloaked end user address (cloak1@auto-graph.com). The system uses that user profile to ascertain Brian's real email address (Brian@gmail.com) to relay the email, as shown in step 1 below. *Id.*, 10:58-61.



Id., FIG. 4.

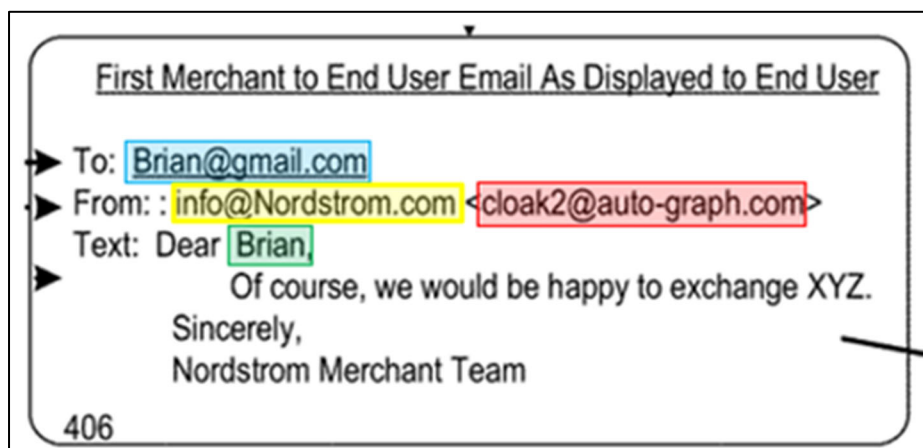
The ID cloaking system requires each relying party to be associated with a unique cloaked relying party address. The ID cloaking system uses that cloaked relying party address to determine where to forward the reply message from the user. *Id.*, 9:4-7. In step 2, the ID cloaking system determines whether Brian's end user profile contains a previous association between Nordstrom's relying-party address (info@Nordstrom.com) and an existing cloaked relying-party address for Nordstrom. *Id.*, 27:35-39. If the ID cloaking system determines that there is no previous association between Nordstrom's relying-party address (info@Nordstrom.com) and a cloaked relying-party address, then the system generates a new cloaked relying-party address. *Id.*, 27:40-45. In the FIG. 4 example, the cloaked relying-party address generated for info@Nordstrom.com is **cloak2@auto-graph.com**. *Id.*, FIG. 4. Step 2 above shows the augmenting of the From/Reply-To fields of the email that will be forwarded to the user. In the message received by the ID cloaking system from the relying party, the From field contained info@Nordstrom.com. In step 2, the Reply-To field is changed to **cloak2@auto-graph.com** without changing the From field, which remains info@Nordstrom.com (yellow). Retaining the From field as info@Nordstrom.com (yellow) in the email to Brian helps to maximize context provided to the user. Augmenting the Reply-To address to **cloak2@auto-graph.com** ensures that a user reply to the message is routed back through the ID cloaking system operating at auto-graph.com.

The ID cloaking system further de-cloaks Brian's name (#first_name.cloak1@autoGraph.com to Brian) in Step 3 above to maximize context in the email presented to the user. *Id.*, 4:40-44.



Id., FIG. 4 (annotated). “The email is then sent to the end user’s real email address by end user email system 104, with the ‘from’/reply-to address of info@nordstroms.com <cloak2@autograph.me >[.]” *Id.*, 17:21-24.

FIG. 4 at 406 depicts the email that is forwarded to Brian based on the message received by the ID cloaking system at 402. *Id.*

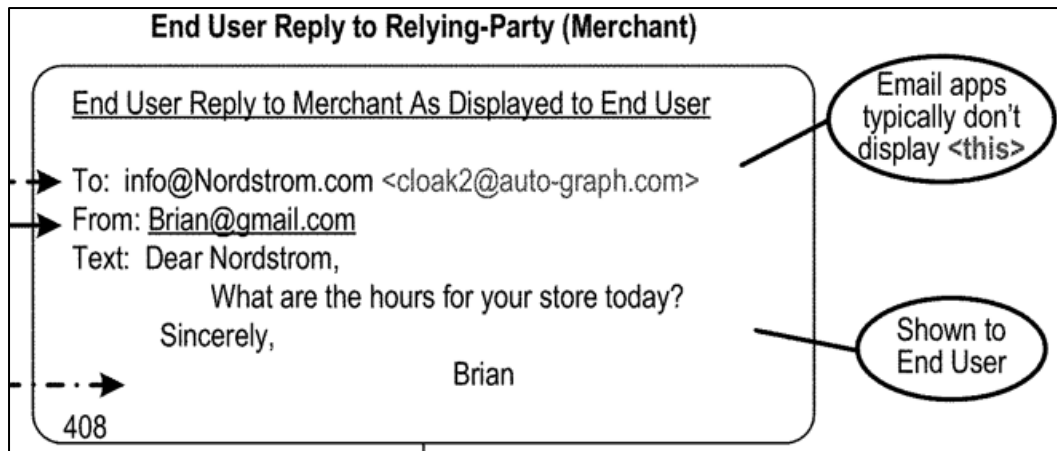


Id., FIG. 4. The system modified the email received from the relying party by (1) swapping out Brian’s cloaked end user address (cloak1@auto-graph.com) with Brian’s private end user address (Brian@gmail.com); (2) adding Nordstrom’s

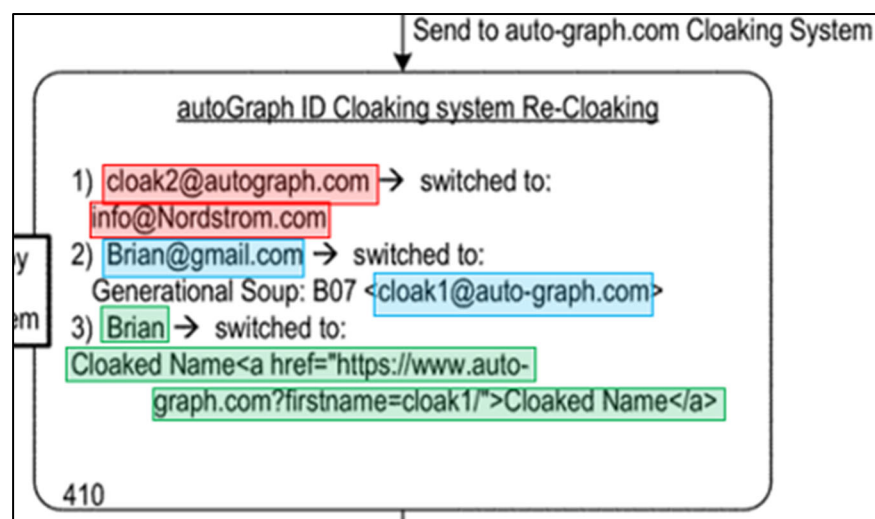
cloaked relying-party address (**cloak2@auto-graph.com**) to the email's Reply-To field without augmenting the From field (info@Nordstrom.com); and (3) swapping out Brian's cloaked first name (**#first_name.cloak1@autoGraph.com**) with Brian's actual name. *Id.*

As noted above, the ID cloaking system maintains routing of the user's reply to the relying party through the ID cloaking system by modifying the Reply-To field of the message 406 that the user receives (*i.e.*, changing **info@Nordstrom.com** to **cloak2@auto-graph.com**). *Id.*, 10:64-11:3. This adjustment of the Reply-To address prevents Brian from unintentionally sending a reply directly to the relying party without that reply traversing the ID cloaking system, avoiding the desired re-cloaking of his personal information. *Id.* However, the From field (info@Nordstrom.com (yellow)) is not augmented so that the email shown at 406 indicates the identity of the relying party (Nordstrom). *Id.* As noted in FIG. 4's annotations, many email applications only display the From field by default, without displaying the Reply-To field. Thus, from Brian's point of view, the relying party name in the From field (info@Nortstrom.com) appears the same regardless of whether that message at 406 traversed the ID cloaking system.

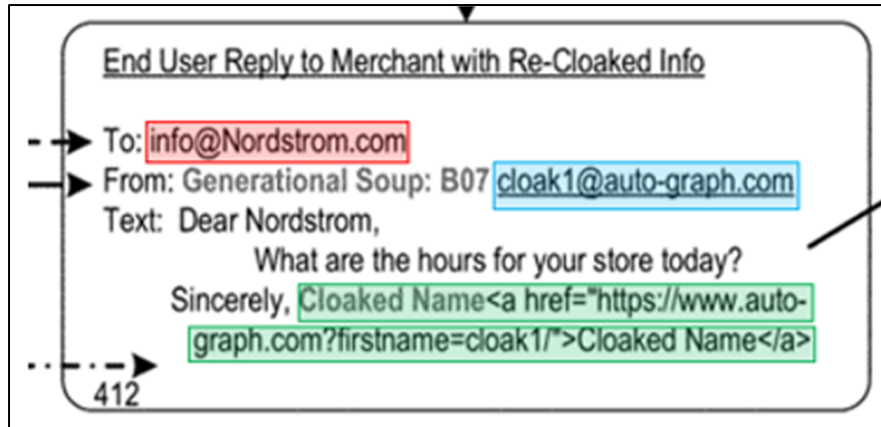
When Brian sends the reply shown below, the ID cloaking system receives and augments Brian's reply before forwarding it to the relying party.



Id., FIG. 4. Specifically, at 410 Step 1, the system uses the cloaked relying party address (**cloak2@auto-graph.com**) to determine the relying party's real email address (**info@Nordstrom.com**) and substitutes the To field accordingly. At Step 2, the system cloaks Brian's private end user address (**Brian@gmail.com**) with the cloaked end user address (**cloak1@auto-graph.com**) in the Reply-To field so that a subsequent reply from the relying party again traverses the ID cloaking system. And at Step 3, the system cloaks Brian's name in the body of the email. *Id.*, 4:19-22.



Id., FIG. 4.



Id. The cloaked email is then forwarded to the relying party at info@Nordstrom.com as shown at 412.

Claim 13 is representative, describing an ID cloaking system processing an email from a relying party that is addressed to a cloaked end user address.

13. A non-transitory computer readable medium for a ID cloaking system having instructions stored thereon that are executable by processor electronics to:

receive an email addressed to a **cloaked end user address**, wherein the email is sent from a **relying party email address**, and wherein the domain of the cloaked end user address and the domain associated to the cloaked ID system are the same domain;

identify an end user specified address associated to the **cloaked end user address** by an end user profile;

determine whether the end user profile contains a previous association between the **relying party address** and a **cloaked relying party email address**, wherein the relying party address has a different domain than the cloaked relying party email address;

where the end user profile does not contain a previous association between the **relying party address** and the **cloaked relying party email address**, then generate a new **cloaked relying party email address** and associate the new cloaked relying party email address to the end user profile, the **cloaked end user address**, wherein the new

cloaked relying party email address is generated with a domain different than the relying party address; and
send the email to the identified **end user specified address**, wherein the email is configured with a reply-to email address comprising the new **cloaked relying party email address**.

D. Claim Construction

Claim terms are to be construed in accordance with the standard set forth in *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-24 (Fed. Cir. 2005) (en banc). But “[o]nly terms which are in controversy need to be construed, and then only to the extent necessary to resolve the controversy and material to the decision.” *Facebook, Inc. v. Sound View Innovations, LLC*, IPR2017-01005, Paper No. 13 at 6 (PTAB Sept. 1, 2017) (citing *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). As detailed below, reasons exist for denial of institution that do not require addressing the construction of claim terms at this time. If the Board nonetheless institutes trial, then Rally AG reserves its right to put forth constructions for any claim terms, including terms for which Petitioner formally or otherwise relies on for construction of a term.

E. Person Of Ordinary Skill In The Art

Petitioner states that a person having ordinary skill in the art (“POSITA”) as of the claimed priority date “would have had a bachelor’s degree in computer science, electrical engineering, computer engineering or equivalent from an accredited academic program with at least two years of work experience with electronic

communications.” Petition, 7. And that “[a] POSITA would have had an understanding of the privacy concerns relevant to electronic communications.” *Id.* At this stage of the proceeding, Rally AG does not propose a different level of skill in the art but reserves the right to propose a level of ordinary skill in the art in this proceeding should it be instituted, or in other proceedings.

III. THE ASSERTED PRIOR ART

Petitioner asserts three references across its four grounds:

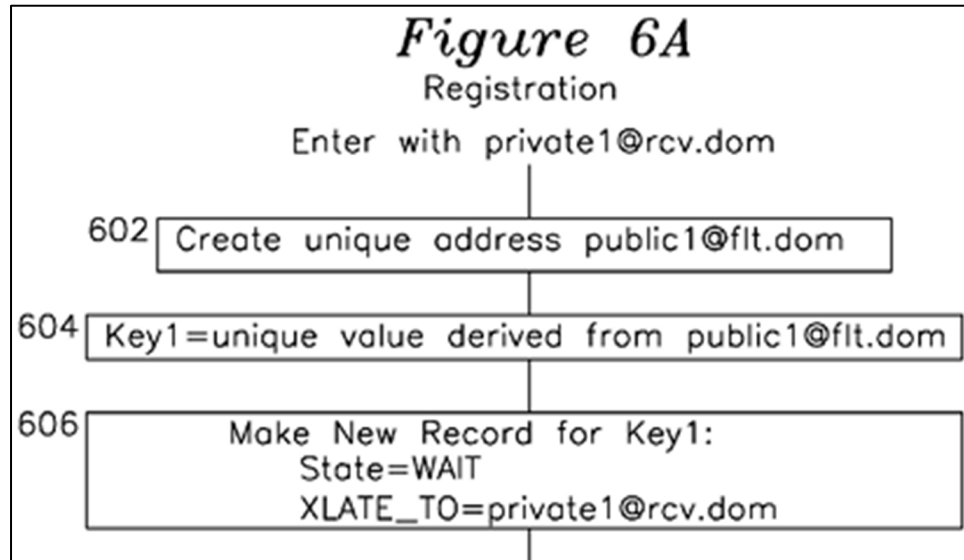
- U.S. Patent No. 8,458,264 to Lee, et al. (“Lee”);
- U.S. Patent No. 7,783,741 to Hardt (“Hardt”); and
- U.S. Patent Publication No. 2016/0323229 to Le Jouan (“Le Jouan”).

A. Lee

Lee is titled “Email Proxy Server With First Respondent Binding[.]” Ex. 1004, Title. Lee discloses an email proxy server where a user can register for “a single-sender public email address[.]” *Id.*, 3:33-36. Once an email to the user from a particular sender is received at that public email address, future emails to that public address from that particular sender are forwarded to the user. Emails addressed from any other sender are blocked from reaching the user. *Id.*, 7:27-35.

Lee “relates to an email proxy server for filtering unwanted communications from a sender to a recipient.” *Id.*, 1:6-8. Lee aims to reduce the number of spam

emails sent to a user's address. Lee achieves this goal by allowing only one sender to communicate with each registered public address.



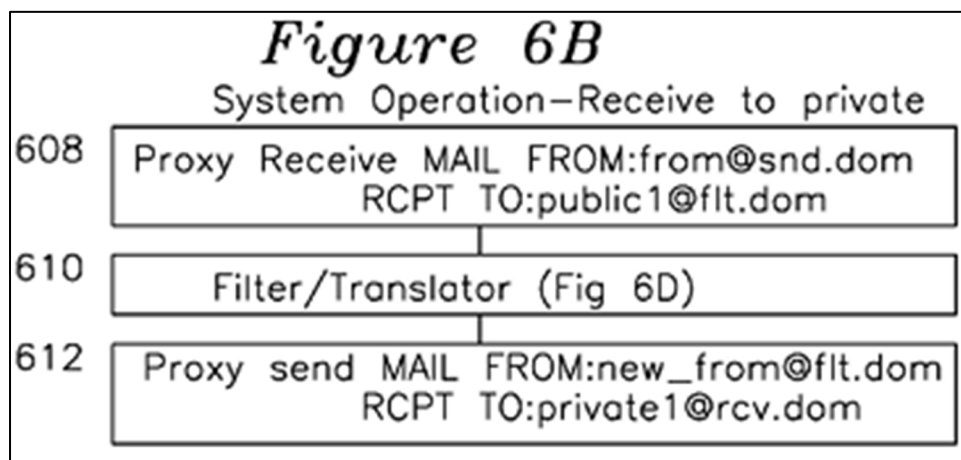
Id., FIG. 6A. “FIG. 6A shows an overview of the registration process.” *Id.*, 6:33.

On request, “[a] user having a private email address [of] ‘private1@rcv.dom’ requests a public email address[.]” *Id.*, 6:33-35. The user receives a unique public email address (public1@flt.dom) that routes emails from a single third party through the email proxy server and then to the user.

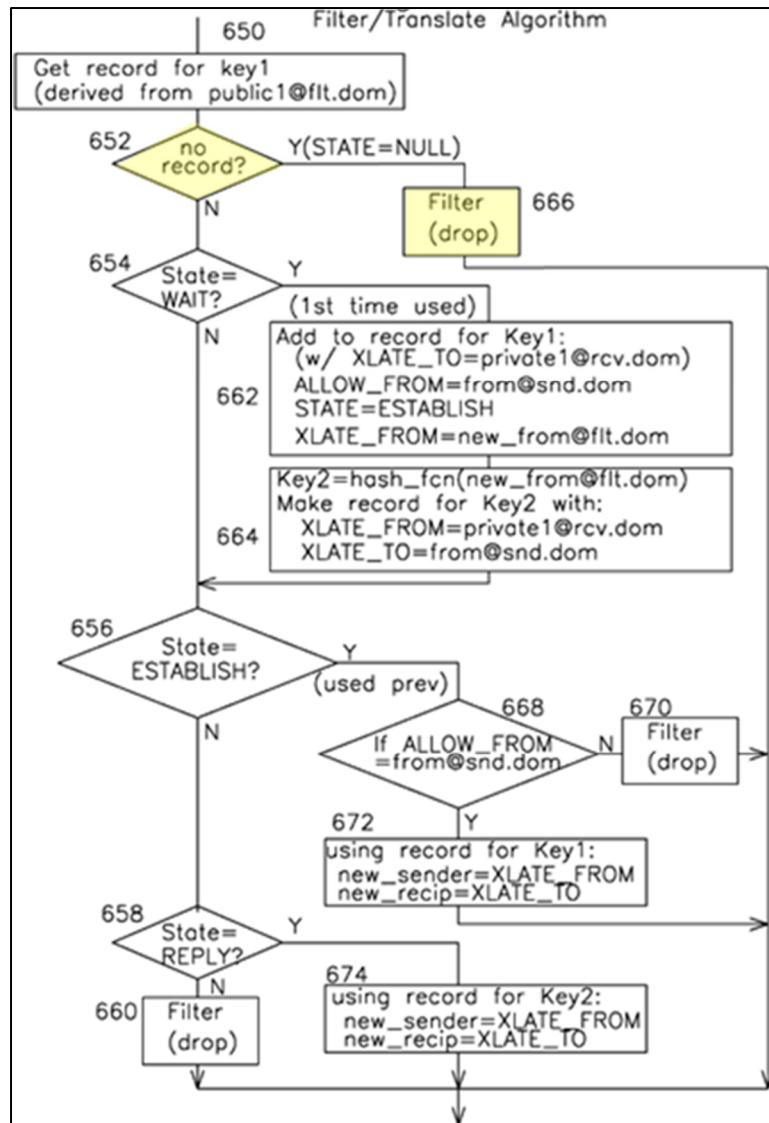
When the single-sender public email address is allocated, Lee generates a first data structure for tracking data associated with that address. *Id.*, 6:10-15. As shown at 606, that Key1 data structure indicates the user's private email address (private1@rcv.dom) to forward emails from the single sender. The Key1 data structure further includes a STATE field that indicates whether the identity of the single third party has been determined yet. The initial value for the STATE field is

set to WAIT. “Usable STATE values are WAIT, indicating that a private recipient has registered an address that has not yet been used, and ESTABLISH, which means a message has been received, and all fields in the record are complete.” *Id.*, 6:22-26. At that ESTABLISH point, the “single-sender public email address” has been bound to the “first respondent” to that address. *Id.*, 3:33-36; Title.

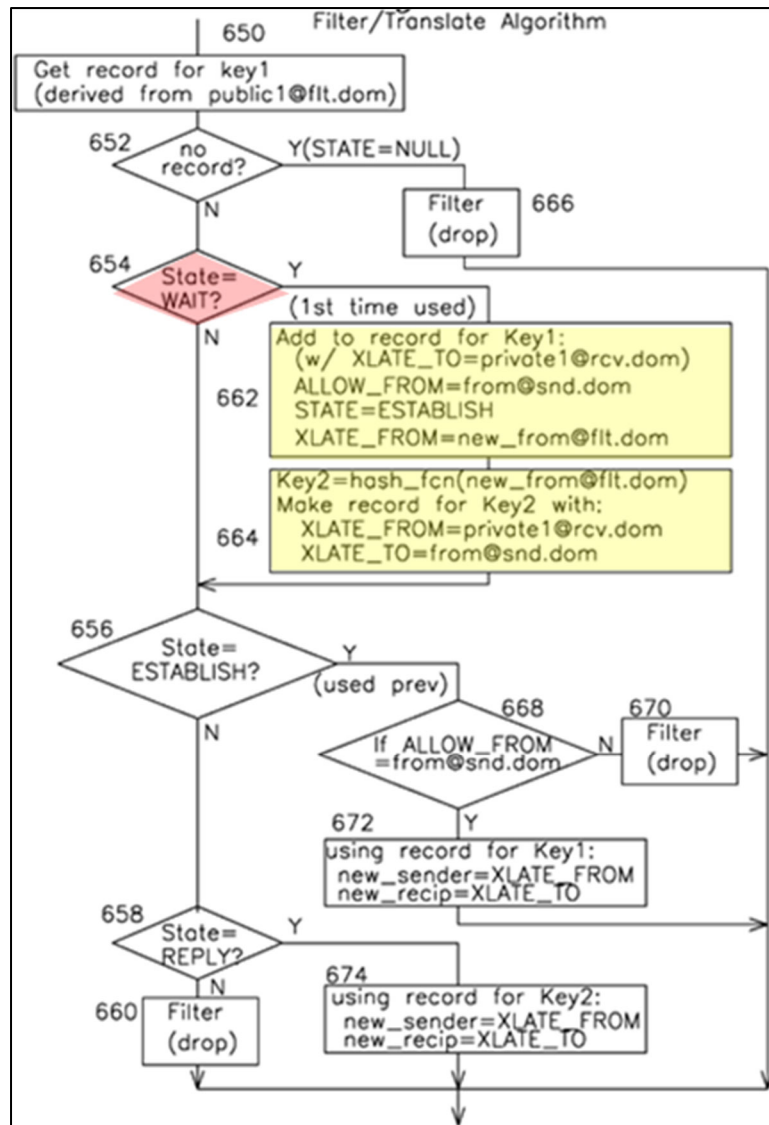
When an email is received at the single-sender public email address (public1@flt.dom), a filter/translator step 620 is performed “which either rejects the email, or sends the email in step 612” to the user’s private email address (private1@rcv.dom).



Id., FIG. 6B; 6:51-52. FIG. 6D depicts “operation of the filter and translator.” *Id.*, 6:60-61. When an email is received at public1@flt.dom, an initial check is performed at 652 to determine whether a Key1 record exists for public1@flt.dom.



Id., FIG. 6D. If no record exists, then the received email is filtered because “the sender attempted to send to a non-existent public email address.” *Id.*, 6:65-67.



Id., FIG. 6D.

Steps 654, 662, 664 illustrate steps performed when an email is received at an existing public email address (public1@flt.dom) that is in the WAIT state because it has not previously received an email. *Id.*, 7:1-6. When the public email address (public1@flt.dom) receives its first email, its Key1 data record is further initialized at 662. There, the “ALLOW_FROM [field] is initialized with the sender’s email

address, shown as ‘from@snd.dom[,]’ to establish the sender as the “single sender” associated with the public email address. *Id.*, 7:9-11. Further, “the XLATE_FROM value is updated with a unique value, shown as ‘new_from@[flt].dom[,]’ and the STATE of the Key1 data record is updated to “ESTABLISH, which indicates that the public address is ready to process the first and any subsequent emails directed to it.” *Id.*, 7:7-13. Specifically, Lee at 7:1-13, states:

If a record for the associated public email address exists and the STATE value is WAIT 654, this indicates that the user has registered this public email address, but it has not been used yet, so the record contains only STATE=WAIT and XLATE_TO=private1@rcv.dom, which were initialized at the time of registration of the public email address, as described in FIG. 6A. In step 662, the XLATE_FROM value is updated with a unique value, shown as “new_from@[flt].dom”, and an optional field ALLOW_FROM is initialized with the sender's email address, shown as “from@snd.dom”. The STATE value is updated to ESTABLISH, which indicates that the public address is ready to process the first and any subsequent emails directed to it.

Id., 7:1-13.

This “First Respondent Binding” functionality treats the public email address as analogous to an open door of a house. *Id.*, Title. A first third-party sender who transmits an email to the public email address enters the open front door and takes ownership of the house, locking the door behind them. Subsequent emails from that third party sender to the public email address will be forwarded to the user’s private

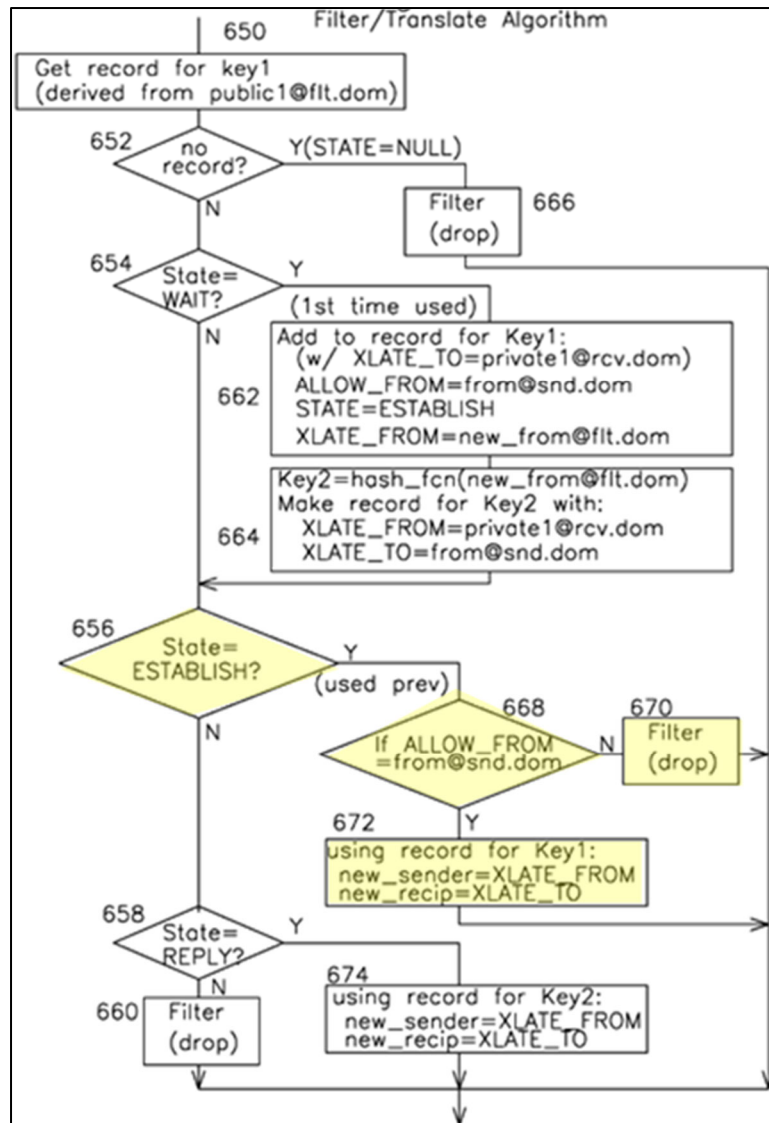
email address (private1@rcv.dom), while emails from other third parties to that public address will be blocked at the locked door.

An additional data structure set-up operation is performed at 664. “In order to process reply messages which will be directed to the translated recipient ‘new_from@flt.dom’, a second key is generated in step 664 from the unique value ‘new_from’, which is used to make a second record containing the translation fields for replies, which contain values for the fields XLATE_FROM and XLATE_TO.” *Id.*, 7:13-19.

504 Record for Key2 (Uniquely derived from incoming new_from@snd.dom) XLATE_TO = from@snd.dom XLATE_FROM = to@flt.dom
--

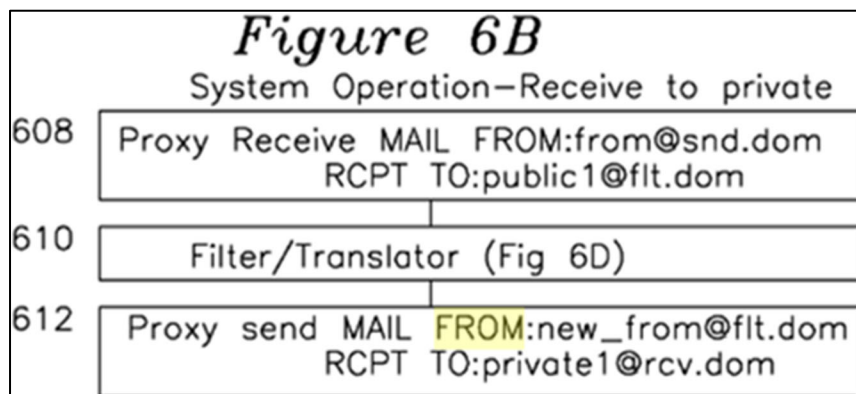
Id., FIG. 5. This second key “allows for replies from the private email to be translated back to addresses which correspond to the original sender.” *Id.*, 7:24-26.

Steps 656, 668, 670, 672 illustrate steps performed when an email is received at an existing public email address (public1@flt.dom) that has previously received an email and is thus in the ESTABLISH state. *Id.*, 7:27-35.



Id., FIG. 6D. At 668, the “ALLOW_FROM field is compared 668 with the sender address” to see whether the sender is the “single sender” associated with the “single-sender public email address.” *Id.*, 7:28-30; 3:33-36. “[I]f there is no match, the message is filtered 670[.]” *Id.*, 7:30. If the sender is the “single sender” and a match is indicated, then the From field of the message is changed to match the XLATE_FROM field of the Key1 data record (new_from@flt.dom) and the To field

of the message is changed to match the user's private email address in the XLATE_TO field of that Key1 data record (private1@rcv.dom). *Id.*, 7:31-35.



Id., FIG. 6B.

Following operations by the filter/translator in FIG. 6B at 610, the message, if not filtered, is sent as indicated by the From field (new_from@flt.dom) to the address indicated by the user's private email address indicated by the To field (private1@rcv.dom). *Id.*, 6:47-52.

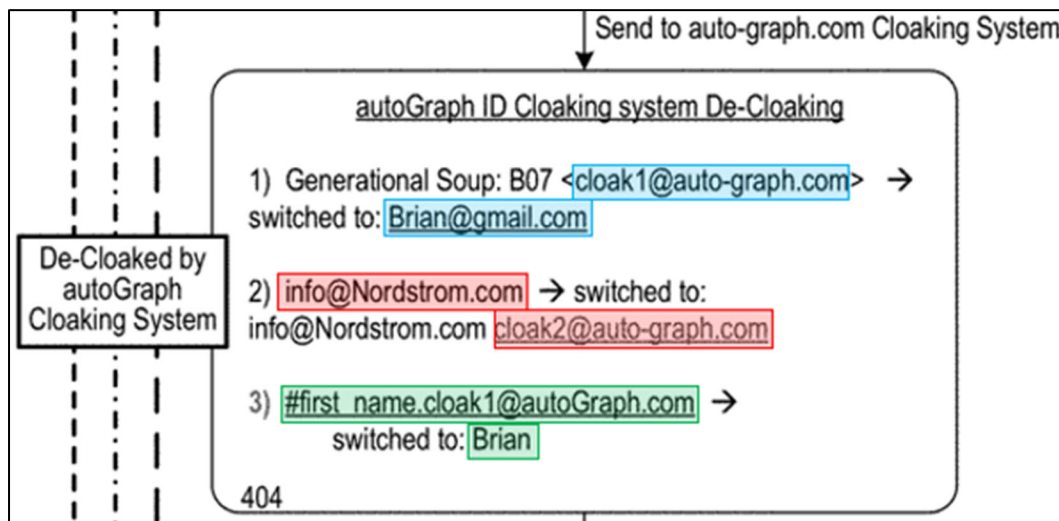
IV. THE PETITION FAILS TO SHOW A REASONABLE LIKELIHOOD THAT ANY CLAIMS OF THE '107 PATENT ARE UNPATENTABLE

A. Claim 13

1. *The Petition fails to show that a POSITA would have found it obvious to “determine whether the end user profile contains a previous association between the relying party email address and a cloaked relying party email address . . . ; [and] in response to determining the end user profile does not contain a previous association between the relying party address and the cloaked*

relying party email address, generate a new cloaked relying party email address”

Claim 13 describes a scenario where an ID cloaking system “receive[s] an email addressed to a cloaked end user address[.]” Ex. 1001, Claim 13, Limitation 13(a). “[T]he email is sent from a relying party email address[.]” *Id.* In order to “send the email to the... user[’s] specified address” in Limitation 13(e), Limitation 13(b) “identif[ies] an end user specified address associated to the cloaked end user address[.]” *Id.*, Claim 13, Limitations 13(e), 13(b); *see*, example of Step 1 below:



Id., FIG. 4.

Limitation 13(c) then determines whether a “cloaked relying party email address” has been set up for the “relying party email address” indicated by the received email. *Id.*, Claim 13, Limitation 13(c). Specifically, Limitation 13(c) “determine[s] whether the end user profile contains a previous association between the relying party address and a cloaked relying party email address[.]” *Id.* Then in

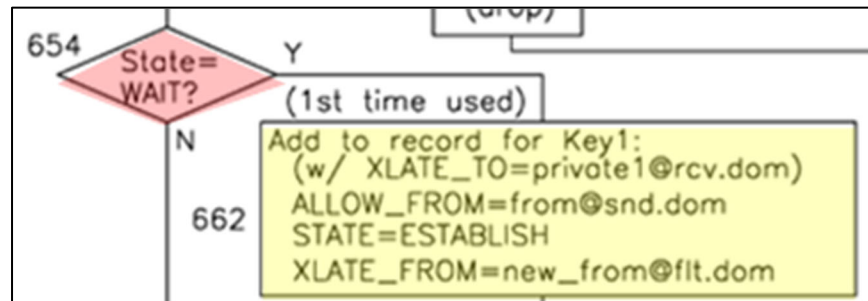
Limitation 13(d), “where the end user profile does not contain a previous association between the relying party address and the cloaked relying party email address,” “a new cloaked relying party email address [is generated] and associate[d with]” “the end user profile.” *Id.*, Claim 13, Limitation 13(d); *see*, example of Step 2 below:



Id., FIG. 4.

As described above, the cloaked relying party address serves two purposes. First, that cloaked address is associated with the server implementing the ID cloaking system (*i.e.*, auto-graph.com), which ensures that the user’s replies to the email are directed back to the ID cloaking system. Further, the cloaked relying party address is used for determining where to route those replies from the user. *Id.*, 12:52-13:3. Each relying party is associated with a unique cloaked relying party email address. Cloaked addresses “serve as a Globally Unique IDs (GUID) to identify [a party] when [the party’s] real information needs to be re-associated and/or to re-route information such as emails back to [the party].” *Id.*, 9:4-7. Limitations 13(c) and (d) ensure that each relying party that communicates with the cloaked end user address is associated with a unique cloaked relying party address so that user replies can be appropriately directed back to the correct relying party.

The Petition cites to Lee step 654 as disclosing “determin[ing] whether the end user profile contains a previous association between the relying party address and a cloaked relying party email address[.]” Petition, 28-29.



Id., 29 (citing Ex. 1004, FIG. 6D).² And the Petition further cites to Lee step 662 as allegedly disclosing “generat[ing] a new cloaked relying party email address” “where the end user profile does not contain a previous association between the

² The Petition cites to paragraphs 72-76 of the Ex. 1003 Declaration in support of its case for Limitation 13(c). Those declaration paragraphs are nothing more than a copy of the corresponding Petition paragraphs. “Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.” 37 C.F.R. § 42.65(a); *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper No. 9 at 15 (Aug. 24, 2022) (Precedential) (“[T]he cited declaration testimony is conclusory and unsupported, adds little to the conclusory assertion for which it is offered to support, and is entitled to little weight.”)

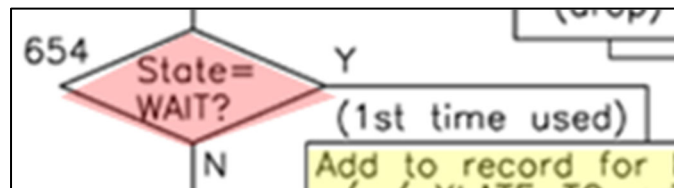
relying party address and the cloaked relying party email address.” *Id.*, 30-31.

Citing to Lee, 7:1-13, the Petition argues that:

A STATE value of WAIT means no prior email has been received to the user’s alias address and therefore no sender alias has been generated; a STATE value of ESTABLISH means that a prior email has been received to the user’s alias address, and an alias has been created for the sender’s email address. Therefore, checking the value of this STATE variable “determine[s] whether the end user profile contains a previous association between the relying party address and a cloaked relying party email address,” as claimed.

Id., 29.

The Petition’s assertion is wrong. FIG. 6D’s illustration of step 654 immediately illustrates that fact.



Ex. 1004, FIG. 6D. Step 654 is an evaluation of Key1’s STATE variable, which indicates whether Lee’s public address has previously received an email. Lee, 7:1-7, cited by the Petition for Limitation 13(c), states:

If a record for the associated public email address exists and the STATE value is WAIT 654, this indicates that the user has registered this public email address, but it has not been used yet, so the record contains only STATE=WAIT and XLATE_TO=private1@rcv.dom, which were initialized at the time of registration of the public email address, as described in FIG. 6A.

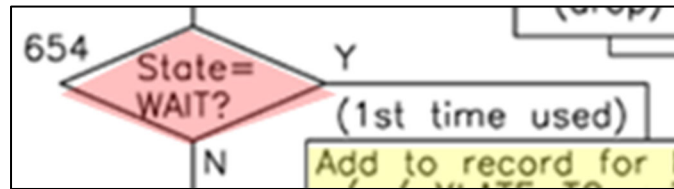
Id., 7:1-7.

The depiction of Lee 654 in FIG. 6D and its associated discussion in column 7:1-7 make no mention of “a relying party address” or “a cloaked relying party email address,” let alone describe a “determin[ation of] whether the end user profile contains a previous association between the relying party address and a cloaked relying party email address” as required by the claims. Ex. 1001, Claim 13, Limitation 13(c). Lee steps 654, 662 set up an XLATE_TO address when a public email address receives its first message. That operation is not based on a “determin[ation of] whether the end user profile contains a previous association between the relying party email address and a cloaked relying party email address” as required by claim 13. *Id.* Step 662 is performed based the determination at 654 of whether the incoming email is the first to the public email address, via a determination that the STATE variable indicates the “WAIT” state.

Petitioner argues at page 29 that Lee step 654’s check on the Key1 STATE variable is the same as the claimed determining of step 13(c). Petition, 29. But this logic is flawed. Limitation 13(c), (d) require that the “new cloaked relying party email address” is generated each time “the end user profile does not contain a previous association between the relying party address and the cloaked relying party email address[.]” Ex. 1001, Claim 13, Limitations 13(c), 13(d). This establishes a unique cloaked relying party email address for each relying party. Lee 664, 662

assigns an XLATE_FROM address that is, at best, associated with a first party that sends an email to the public address.³

Cited step 654 of Lee is agnostic as to whether there is a “previous association between the relying party address and a cloaked relying party email address.” *Id.*



Ex. 1004, FIG. 6D. This step of Lee is only looking at whether the public email address (public1@flt.dom) has been used before to bind that public address to the first sender who uses the public email address (in this case from@snd.dom).

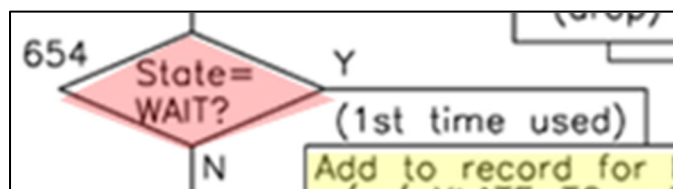
“[E]very word in a claim limitation is [] presumed to have meaning[.]” *Square, Inc. v. Think Comput. Corp.*, CBM2014-00159, Paper No. 47 at 8 (PTAB Nov. 27, 2015); *see Bicon, Inc. v. Straumann Co.*, 441 F.3d 945, 950 (Fed. Cir. 2006)

³ Both the Petition and Dr. Terveen’s declaration admit that Lee lacks disclosure regarding how its system could be configured to permit multiple desired senders:

But Lee does not describe *how* a user may configure the system to permit multiple desired senders while filtering out all others.

Petition, 40 (emphasis in original); Ex. 1003, ¶97.

("[C]laims are interpreted with an eye toward giving effect to all terms in the claim."); *see also Stumbo v. Eastman Outdoors, Inc.*, 508 F.3d 1358, 1362 (Fed. Cir. 2007). Petitioner's mapping of Lee onto claim 13 violates this rule of claim interpretation. Lee's step 654 functionality, which in no way considers "whether the end user profile contains a previous association between the relying party address and a cloaked relying party email address," is insufficient. Ex. 1001, Limitation 13(c). Such a mapping reads the "determinat[ion of] whether the end user profile contains a previous association between the relying party address and a cloaked relying party email address" out of both Limitations 13(c) and 13(d) and cannot be correct. *Id.*



Ex. 1004, FIG. 6D.

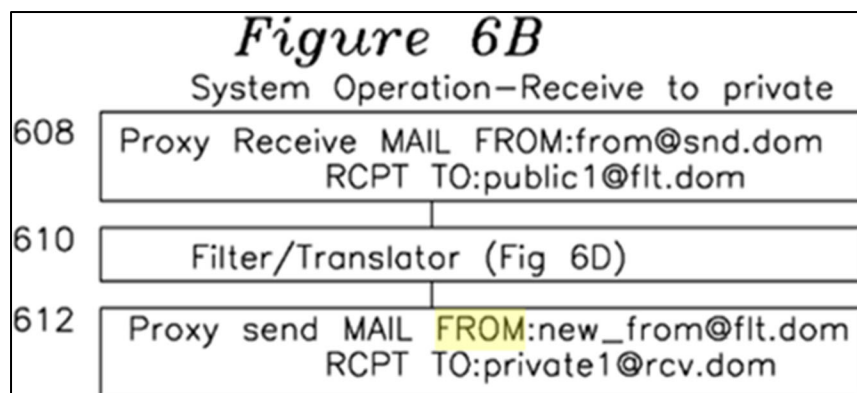
Because the Petition fails to identify any disclosure of the claimed determining that is explicitly required by Limitations 13(c) and 13(d), the Petition fails to meet its burden for institution of trial based on grounds asserted against claim 13. 37 C.F.R. § 42.108(c).

2. *The Petition fails to show that a POSITA would have found it obvious to “send the email to the identified end user specified address, wherein the email is configured with a reply-to email*

address comprising the new cloaked relying party email address”

The Petition further fails to show the obviousness of Limitation 13(e)’s “send[ing] the email to the identified end user specified address, wherein the email is configured with a reply-to email address comprising the new cloaked relying party email address.” Ex. 1001, Claim 13, Limitation 13(e). The Petition cites to Lee but admits that Lee fails to disclose the above emphasized feature. Petition, 33 (“Lee does not expressly discuss distinct ‘from’ and ‘reply-to’ fields[.]”). Rather than citing to a reference to fill that admitted gap, the Petition appeals to the knowledge of a POSITA.

In addressing Limitation 13(e), Petitioner rehashes the steps of Lee’s filter/translator to conclude that “the sender’s alias, new_from@flt.dom, populates the ‘From’ address of the email sent by the email proxy server to the end user.” *Id.*, 32. As the Petition admits, that Lee disclosure fails to meet Limitation 13(e)’s requirement that “the email is configured with a reply-to email address comprising the new cloaked relying party email address.” Ex. 1001, Claim 13, Limitation 13(e).



Ex. 1004, FIG. 6B.

To account for Lee's missing disclosure, the Petition alleges that a POSITA would understand the functionalities of the From and Reply-To fields of an email. Petition, 33-34. The Petition notes that "[a] POSITA would have understood that these two fields serve distinct roles" and that "[a] POSITA would also understand that, while the 'from' and 'reply-to' fields are distinct, either may be used to control the destination of a reply email." *Id.* But rather than providing a reason why a POSITA would be motivated to make the alleged modification regarding the From and Reply-To fields, which admittedly are "distinct" fields that have "distinct roles," the Petition makes only a conclusory assertion that "a POSITA would have understood that it would have been obvious to populate a 'reply-to' field with the sender's alias" without elaboration. *Id.*, 34.

This bald assertion is plainly insufficient. Separate configuration of From and Reply-To addresses provides a significant functional benefit to users of the '107 Patent. The '107 Patent's inventor recognized the need for increasing data privacy while minimizing effects on the user's email experience. Limitation 13(e)'s configuration of the email to the user "with a reply-to email address comprising the new cloaked relying party email address" facilitates the functionality of the ID cloaking system with limited effects on user experience. Ex. 1001, Claim 13, Limitation 13(e). After the relying party sends an email to the user's cloaked address

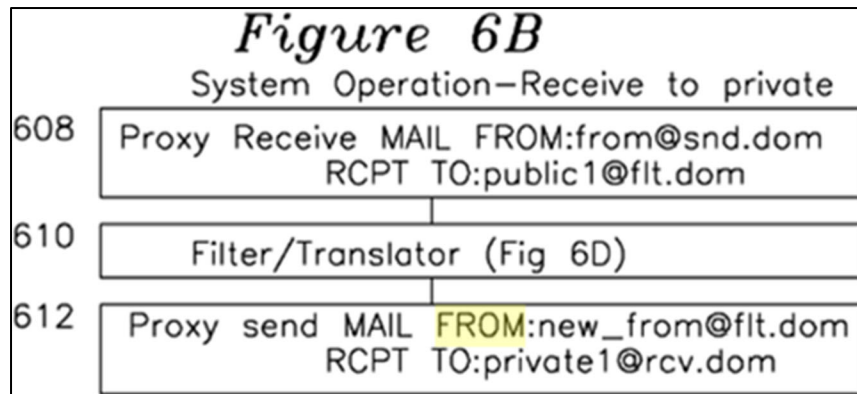
but before the email is forwarded the user, the ID cloaking system configures the Reply-To field of the email to contain the cloaked relying party address. This configuration of the Reply-To field (cloak2@auto-graph.com below) ensures that a user's reply is addressed to the cloaked relying party address and traverses the ID cloaking system before being forwarded to the relying party.



Id., FIG. 4 (annotated); 17:21-24 (“The email is then sent to the end user’s real email address by end user email system 104, with the ‘from’/reply-to address of info@nordstroms.com <cloak2@autograph.me>[.]”)

Furthermore, augmenting the Reply-To field configuration does not disrupt a user’s email experience because email applications by default display the From field, without displaying the content of the Reply-To field. By configuring an email’s Reply-To field with the cloaked relying party address without adjusting the From field, the user is informed of the relying party’s identity (info@Nordstrom.com), providing context to the email.

Lee replaces the From field of the email with the XLATE_FROM field, as shown in FIG. 6B. The user-received message thus indicates that it is from “new_from@flt.dom” as opposed to indicating the true sender “from@snd.dom.”



Ex. 1004, FIG. 6B. This From field (new_from@flt.dom) provides no context regarding from where the email received by the user actually originated (from@snd.com).



Ex. 1001, FIG. 4. In contrast, the '107 Patent's use of the Reply-To field shows the user that the received message is from Nordstrom's. By utilizing the Reply-To field, Limitation 13(e) provides important context to the user that is not provided by Lee.

Lee fails to disclose separate configuration of From and Reply-To fields in an email sent to the user. Lee only discloses use of the From field. The Petition does nothing to explain why a POSITA would find it obvious to modify Lee to utilize the Reply-To field, beyond noting that a POSITA would have known of the existence of the Reply-To field and the Reply-To field's "distinct role." An understanding of the existence of the "distinct" From and Reply-To fields and their "distinct role[s]" is not a motivation to modify Lee to meet Limitation 13(e). Use of the Reply-To

field in Limitation 13(e) facilitates the ID cloaking system's functionality while retaining user context as to the origin of a received email. This context is lost in Lee. Because the Petition lacks any motivation to augment Lee beyond hindsight reconstruction of claim 13, the Petition's case for Limitation 13(e) is deficient such that institution should be denied.

B. The Challenges To The Other Claims Are Similarly Deficient

The challenges to independent claims 1 and 7 fail for the same reasons as independent claim 13. Those independent claims contain analogous limitations as those for which deficiencies were noted above. The Petition does not provide any additional facts or reasoning for those limitations beyond what was presented for claim 13. Thus, institution should be denied for similar reasoning. The dependent claims are not unpatentable at least by virtue of dependency.

V. THE BOARD SHOULD DENY INSTITUTION IN VIEW OF THE PARALLEL DISTRICT OF DELAWARE CASE

The Petition should be denied under 35 U.S.C. § 314(a) because a pending district court case could address validity of the challenged claims before a Final Written Decision here. *See* Katherine K. Vidal, U.S. Pat. & Trademark Off., *Memorandum: Interim Procedure For Discretionary Denials In AIA Post-Grant Proceedings With Parallel District Court Litigation* (2022); Ex. 2001. For this independent efficiency reason, the Petition should be denied.

In prior precedential decisions, the Board recognized an independent basis for denying institution of IPR for inefficiencies and duplication of effort for cases in which another tribunal will likely resolve the same issues raised by a petition at an earlier date than the Board. *See NHK Spring Co. v. Intri-Plex Techs., Inc.*, IPR2018-00752, Paper No. 8 (PTAB Sept. 12, 2018); *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper No. 11 (PTAB Mar. 20, 2020). *Fintiv* introduced six factors relevant to deciding whether to deny institution in light of co-pending proceedings:

1. whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted;
2. proximity of the court's trial date to the Board's projected statutory deadline for a final written decision;
3. investment in the parallel proceeding by the court and the parties;
4. overlap between issues raised in the petition and in the parallel proceeding;
5. whether the petitioner and the defendant in the parallel proceeding are the same party; and
6. other circumstances that impact the Board's exercise of discretion, including the merits.

Fintiv, IPR2020-00019 at Paper No. 11 at 6.

Factor 1

Regarding factor 1, no stay has been requested and there has not been any indication from the court that a stay would likely be granted. Thus, this factor counsels in favor of denial.

Factor 2

Regarding factor 2, the June 2022 memorandum from the USPTO Director states that “[p]arties may present evidence regarding the most recent statistics on median time-to-trial for civil actions in the district court in which the parallel litigation resides[.]” Vidal, *supra*, 8-9.

In this case, Patent Owner Rally AG asserted the ’107 Patent against the Petitioner in the U.S. District Court for the District of Delaware, filing the Complaint on October 5, 2023. *See* Ex. 2001, Paper No. 1. During the twelve-month period ending September 30, 2024, the median time-to-trial for a civil case in the District of Delaware was 32.2 months. U.S. Dist. Cts., *Combined Civil and Criminal Federal Court Management Statistics* (2024). Using this figure, the parallel district court proceeding can be expected to reach trial 32.2 months after the complaint was filed, around June 2026.

The Petition in the present case was filed at the very end of Petitioner’s Section 315(b) window. The Final Written Decision of this IPR could be issued as late as October 2026 when considering the three months to make the institutional

decision (April 2025), the twelve months to complete the IPR (April 2026), and the potential for a six-month extension for good cause (October 2026).

Because of Petitioner's delay and because the Final Written Decision here could occur after the district court trial, this factor counsels in favor of denial.

Factor 3

Regarding factor 3, the district court has put material effort into litigating the '107 Patent, including providing a detailed ruling finding that the Petitioner failed to make its case that the '107 Patent's claims are patent ineligible. Ex. 2002. Petitioner's delay in filing this Petition has resulted in the district court case exhausting additional resources, such that factor 3 counsels in favor of denial.

Factor 4

Regarding factor 4, the Petitioner has not made an indication that they will decline to pursue overlapping arguments at the PTAB and district court. Thus, this factor weighs in favor of denial.

Factor 5

Regarding factor 5, the Petitioner and the defendant in the parallel proceeding are the same party. Ex. 2001. Thus, factor 5 also counsels in favor of denial.

Factor 6

And finally regarding factor 6, the Petition contains serious flaws, including those noted above, which span all of the challenged claims. These weaknesses indicate that factor 6 also weighs in favor of denial of institution.

With all factors indicating that institution should be denied, the Panel should exercise its discretion to deny institution under § 314(a) and the *Fintiv* guidance.

VI. CONCLUSION

For the reasons set forth above, the Board should decline to institute IPR of the '107 Patent.

Respectfully submitted,

Date: January 22, 2025

/Matthew W. Johnson/

Matthew W. Johnson
Reg. No. 59,108
JONES DAY
500 Grant Street, Suite 4500
Pittsburgh, PA 15219
(412) 394-9524
mwjohnson@jonesday.com

John V. Biernacki
Reg. No. 40,511
Lorenz & Kopf, LLP
26300 Crocker Landing
Columbia Station, Ohio 44028
(480) 361-0462
jbiernacki@lkglobal.com

Joshua R. Nightingale
Reg. No. 67,865
JONES DAY
500 Grant Street, Suite 4500
Pittsburgh, PA 15219
(412) 394-7950
jrnightingale@jonesday.com

Attorneys for Patent Owner

CERTIFICATE OF WORD COUNT

Pursuant to Rule 37 C.F.R. 42.24(d), the undersigned hereby certifies that, based upon the word count of the word-processing system used to prepare this Preliminary Response, the number of words in this Preliminary Response is 8,081.

Date: January 22, 2025

/Matthew W. Johnson/

Matthew W. Johnson
Reg. No. 59,108
JONES DAY
500 Grant Street, Suite 4500
Pittsburgh, PA 15219
(412) 394-9524
mwjohnson@jonesday.com

Attorney for Patent Owner

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §42.6(e), I certify that I caused to be served on the counsel for Petitioner a true and correct copy of the foregoing by email on January 22, 2025, at the following addresses:

Paul.Hart@eriseip.com
Adam.Seitz@eriseip.com
PTAB@eriseip.com

Date: January 22, 2025

/Matthew W. Johnson/

Matthew W. Johnson
Reg. No. 59,108
JONES DAY
500 Grant Street, Suite 4500
Pittsburgh, PA 15219
(412) 394-9524
mwjohnson@jonesday.com

Attorney for Patent Owner