

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner

v.

Rally AG LLC
Patent Owner

Case No. IPR2024-01446
U.S. Patent No. 11,361,107

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,361,107**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	SUMMARY OF THE '107 PATENT	1
A.	THE '107 PATENT'S ALLEGED INVENTION	1
B.	THE '107 PATENT'S PROSECUTION.....	6
C.	A PERSON OF ORDINARY SKILL IN THE ART	7
III.	OVERVIEW OF THE PRIOR ART AND PROPOSED GROUNDS ..	7
A.	OVERVIEW OF <i>LEE</i>	8
B.	OVERVIEW OF <i>HARDT</i>	16
C.	OVERVIEW OF <i>LE JOUAN</i>	17
IV.	PROCEDURAL REQUIREMENTS UNDER 37 C.F.R. § 42.104	18
A.	STANDING UNDER 37 C.F.R. § 42.104(A).....	18
B.	CHALLENGE UNDER 37 C.F.R. § 42.104(B) AND RELIEF REQUESTED.....	19
C.	CLAIM CONSTRUCTION UNDER 37 C.F.R. § 42.104(B)(3)	19
V.	THE CHALLENGED CLAIMS ARE UNPATENTABLE	20
A.	GROUND 1: CLAIMS 13 AND 14 ARE OBVIOUS UNDER AIA 35 U.S.C. § 103 OVER <i>LEE</i> IN VIEW OF THE KNOWLEDGE OF A POSITA.	20
B.	GROUND 2: CLAIMS 1, 2, 7, 8, AND 19 ARE OBVIOUS UNDER AIA 35 U.S.C. § 103 OVER <i>LEE</i> IN VIEW OF <i>HARDT</i>	36
C.	GROUND 3 & 4: CLAIMS 15-18 ARE OBVIOUS UNDER AIA 35 U.S.C. § 103 OVER <i>LEE</i> IN VIEW OF <i>LE JOUAN</i> AND CLAIMS 3-6 AND 9-12 ARE OBVIOUS UNDER AIA 35 U.S.C. § 103 OVER <i>LEE</i> IN VIEW OF <i>HARDT</i> AND IN FURTHER VIEW OF <i>LE JOUAN</i>	52
VI.	THE <i>FINTIV</i> FACTORS FAVOR INSTITUTION.....	67
VII.	CONCLUSION.....	71
IX.	MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(A)(1).....	72
A.	REAL PARTY-IN-INTEREST.....	72
B.	RELATED MATTERS.....	72
C.	LEAD AND BACK-UP COUNSEL	72

I. INTRODUCTION

Petitioner Apple Inc. (“Petitioner”) requests *Inter Partes* Review (“IPR”) of Claims 1-19 (the “Challenged Claims”) of U.S. Patent No. 11,361,107 (“the ’107 Patent”).

II. SUMMARY OF THE ’107 PATENT

A. The ’107 Patent’s Alleged Invention

The ’107 Patent is generally directed to an email system capable of protecting an end user’s (e.g., a consumer’s) personal information from being revealed to a relying party (e.g., a merchant).¹ Ex. 1001, Abstract. The described system comprises an ID cloaking system that “serves as an intermediary between the end user’s email system and the relying-party’s email system.” *Id.*, 4:5-8. The ID cloaking system provides consumers with a cloaked address they can provide to a merchant. *Id.*, 6:8-14. When the ID cloaking system receives an email sent to this cloaked consumer address, it processes the email and sends it to the consumer’s personal email address, hiding the consumer’s actual (i.e., non-cloaked) email address from the merchant. *Id.*, 12:1-12. In addition to hiding the consumer’s actual

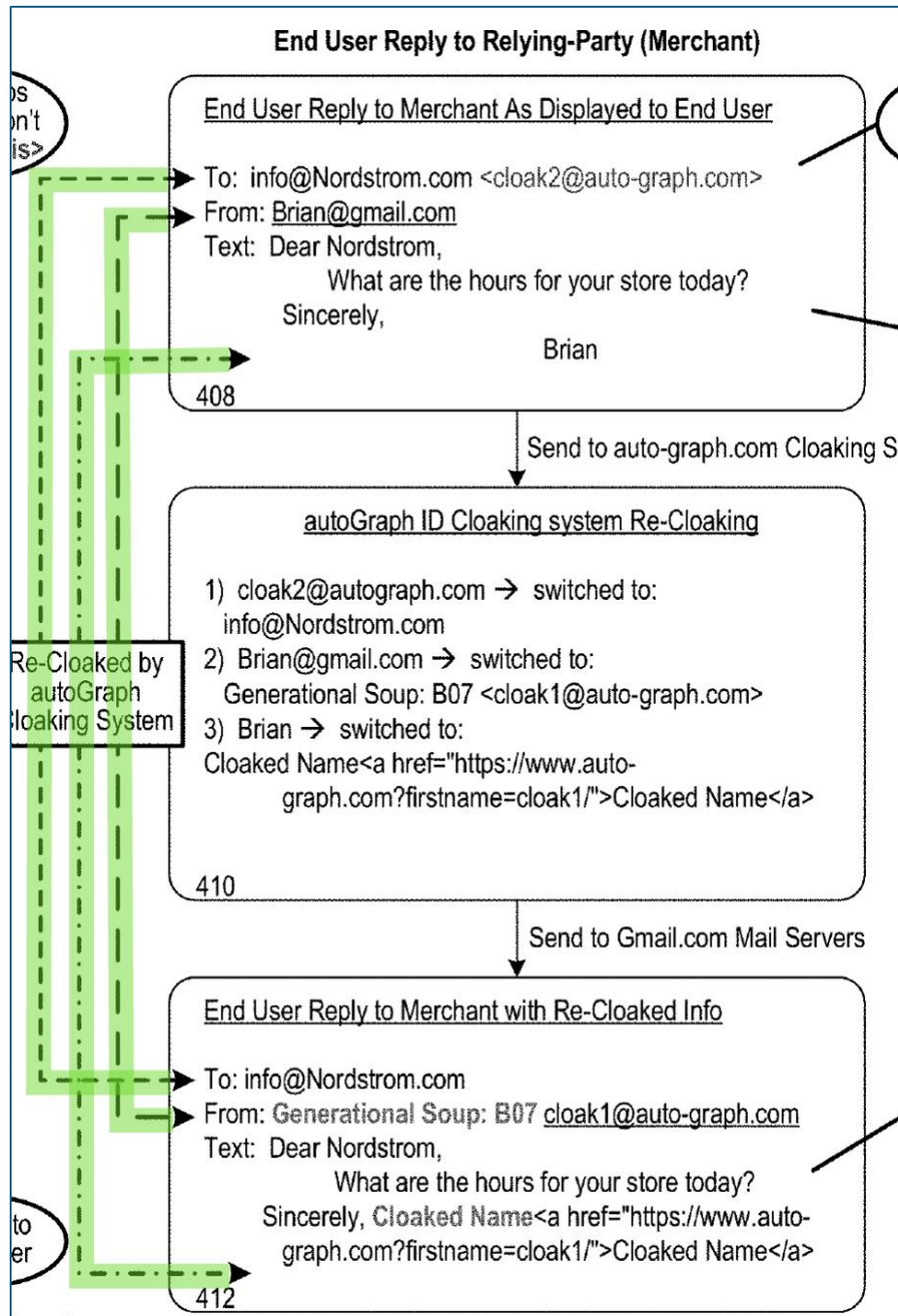
¹ The ’107 Patent refers to the user who seeks to protect his or her personal information as an “end user” and the entity that emails the end user as a “relying party.” Because the patent often uses the example of a potential customer receiving marketing emails from a merchant, the Petition will use “consumer” interchangeably with “end user” and “merchant” interchangeably with “relying party.”

email address from the merchant, the ID cloaking system creates a cloaked merchant address and inserts this cloaked address in the “from” field when the message is passed along to the consumer. *Id.* As a result, if the consumer responds to the email, the ID cloaking server will receive the reply and will replace the consumer’s actual email address with a cloaked address before sending the reply to the merchant. *Id.*, 12:17-64.

The ’107 Patent teaches that a consumer creates a profile with the ID cloaking system that allows the consumer to “specify what information she wants to keep confidential from others[.]” *Id.*, 7:60-64. This information is stored on the profile along with the consumer’s actual email address, cloaked values, and the associations between the cloaked values and the consumer’s actual information. *Id.*, 11:4-17.

The ID cloaking system is capable of “cloaking” and “decloaking” information found in emails to and from the consumer. *Id.*, 6:42-49. As an example of cloaking, when the ID cloaking system receives emails from the consumer’s email system to the merchant’s email system, it *cloaks* the private information of the consumer by swapping this information with cloaked values before routing the email to the merchant. *Id.*, 4:16:21. And, as an example of de-cloaking, when an email is sent from the merchant to the consumer, the private information is *de-cloaked* by the ID cloaking system (returned to the actual values) before being delivered to the consumer’s actual email address. *Id.*, 4:32-39.

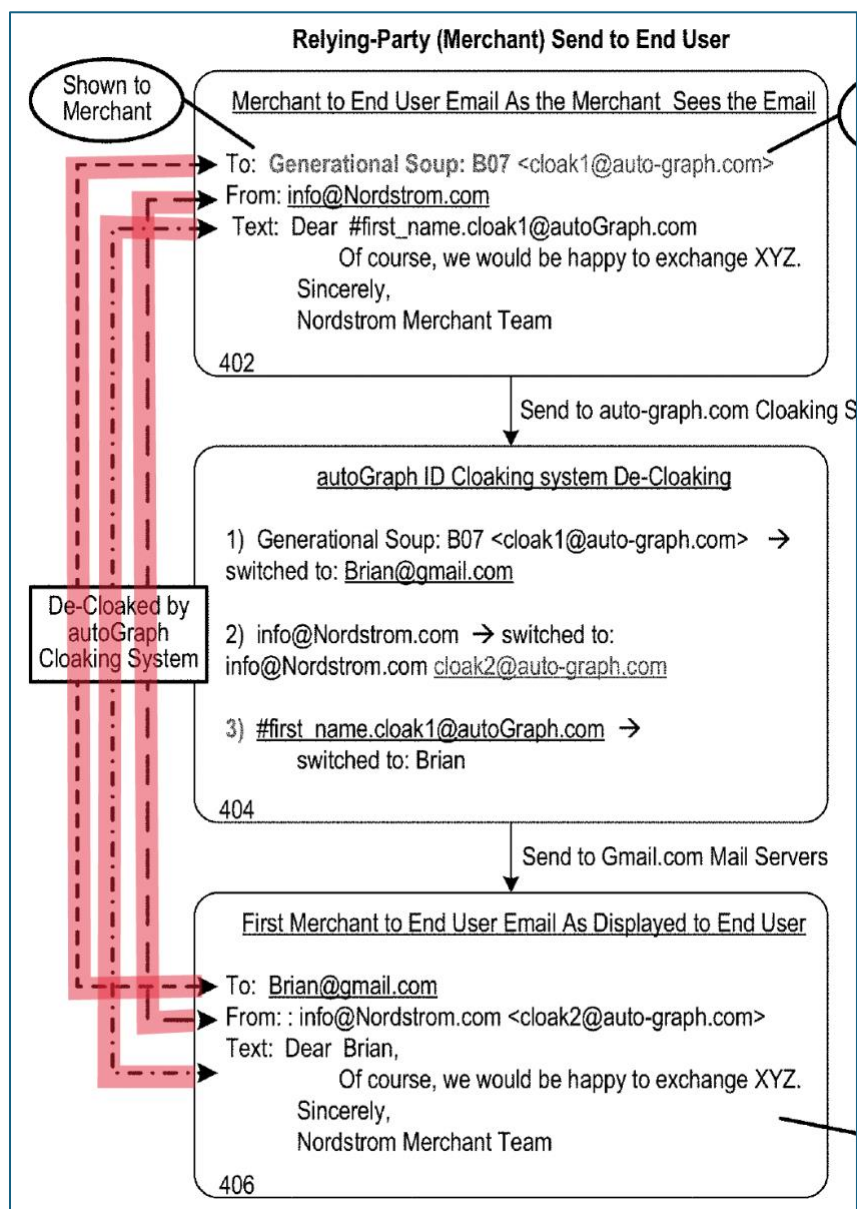
FIG. 4 illustrates the ID cloaking system cloaking (or re-cloaking) emails sent from a consumer to a merchant. In this example, the consumer's email address, brian@gmail.com, is replaced with a cloaked consumer address, cloak1@auto-graph.com. *Id.*, 12:54-64. The cloaked merchant email address, cloak2@auto-graph.com is replaced with the merchant's email address info@nordstrom.com. *Id.*, 12:64-66. Finally, the consumer's first name, Brian, is also cloaked when the system replaces it with the cloaked placeholder, "Cloaked Name." *Id.*, 12:54-64. The green arrows illustrate which data fields are modified by the ID cloaking system:



Id., FIG. 4 (annotated).

When the system receives an email from a merchant, the ID cloaking system decloaks the information in the manner shown below. The cloaked consumer email, cloak1@auto-graph.com is replaced with the consumer's personal email,

Brian@gmail.com. *Id.*, 11:32-35. The merchant email address info@nordstrom.com is replaced with the cloaked merchant address cloak2@auto-graph.com. *Id.*, 11:56-57. Finally, the cloaked name placeholder is replaced with the consumer's name, Brian. *Id.*, 11:46-51. As with the example above, the red arrows illustrate which data fields are modified by the ID cloaking system:



Id. at FIG. 4 (annotated).

In certain embodiments, the consumer may use the email cloaking system to contact a merchant via a webform, initiating contact without revealing the consumer's actual/private email address. *Id.*, 7:42-57. In this scenario, the ID cloaking system generates an association between the URL of the webform and the cloaked consumer email address. *Id.*, 8:58-65. When an email is received from a merchant email address, the ID cloaking system identifies a consumer profile associated with the cloaked consumer email address and any merchant URLs associated with that profile. *Id.* In one example, storing merchant URLs in a consumer profile allows the consumer to identify unauthorized/unwanted merchants using a cloaked email the consumer created for a more limited use. *Id.*, 18:53-59 (“[I]f the end user notices that a cloaked email address she created with one merchant (related to the merchant email/URL when created etc.) is being misused, she can cancel, disable or delete the cloaked email address.”).

B. The '107 Patent's Prosecution

The '107 Patent issued from U.S. Application Serial No. 16/865,053 (the “'053 Application”), filed on May 1, 2020, which claims priority to two provisional applications, Provisional Application No. 62/841,726 filed on May 1, 2019 and Provisional Application No. 62/850,459 filed on May 20, 2019. '107 Patent (Ex. 1001). For purposes of this proceeding only, Petitioner applies May 1, 2019 as the priority date.

The '107 Patent was allowed without an office action. In the Notice of Allowance, the Examiner cited a single prior art reference, U.S. Patent Application No. 2017/0032344 to Attolini et al. ("Attolini"), noting Attolini failed to teach the claimed subject matter. Ex. 1002, 43.

C. A Person of Ordinary Skill in the Art

A person of ordinary skill in the art ("POSITA") at the time of the '107 Patent 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. A POSITA would have had an understanding of the privacy concerns relevant to electronic communications. Additional education or experience might substitute for the above requirements. *Dec.*, ¶24.²

III. OVERVIEW OF THE PRIOR ART AND PROPOSED GROUNDS

U.S. Patent No. 8,458,264 to Lee et al. ("Lee") describes an email alias system starkly similar in functionality to the '107 Patent. Lee's system not only generates an alias for the user/recipient, protecting her identity, but also generates an alias for the sender, ensuring the user cannot inadvertently reply directly to the sender,

² Citations to "Dec." correspond to the supporting declaration of Dr. Loren Terveen, Exhibit 1003.

revealing the user's private email address. As set forth in Ground 1 below, Lee renders obvious claims 13 and 14.

Independent claims 1 and 7 are nearly identical to independent claim 13, but additionally require storing a sender's URL in the user's profile. As set forth in Ground 2 below, a POSITA would have been motivated to add URL functionality to Lee's system pursuant to U.S. Patent No. 7,783,741 to Hardt ("Hardt"). Such a modification would have improved Lee's system, allowing users to define which senders are permitted to use a generated alias, rather than simply assuming by default, as Lee does, that the first sender is permitted.

Finally, Ground 3 proposes further modifying Lee's system to not only cloak the user's private email address, but to additionally cloak personal/private information within the email (e.g., the user's actual name) pursuant to U.S. Patent Pub. No. 216/0323229 to Le Jouan ("Le Jouan").

A. Overview of *Lee*

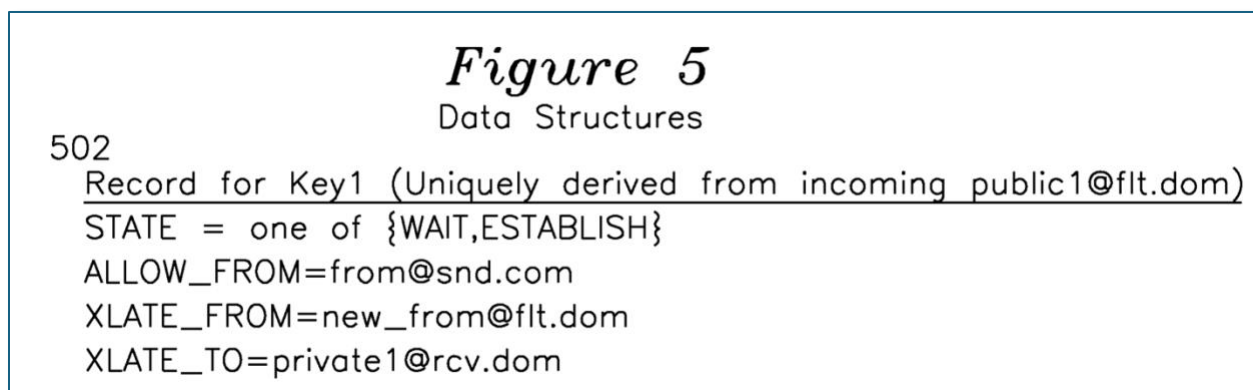
Lee issued on June 4, 2013 and is prior art to the '107 Patent under 35 U.S.C. § 102(a)(1). Lee was not cited or considered during the '107 Patent's prosecution.

Lee describes an email proxy server that protects a user's private email address from receiving unwanted messages by generating and managing proxy emails. *Lee*, Abstract, 1:61-2:14. In a first step, the user requests a proxy email from the server that the user can provide to a third party. *Id.*, 2:36-45. Once a proxy is

generated and provided by the user to a third party, the email proxy server receives and forwards emails sent to the proxy email according to a filter/translate algorithm. *Id.*, 4:46-51, 6:48-52.

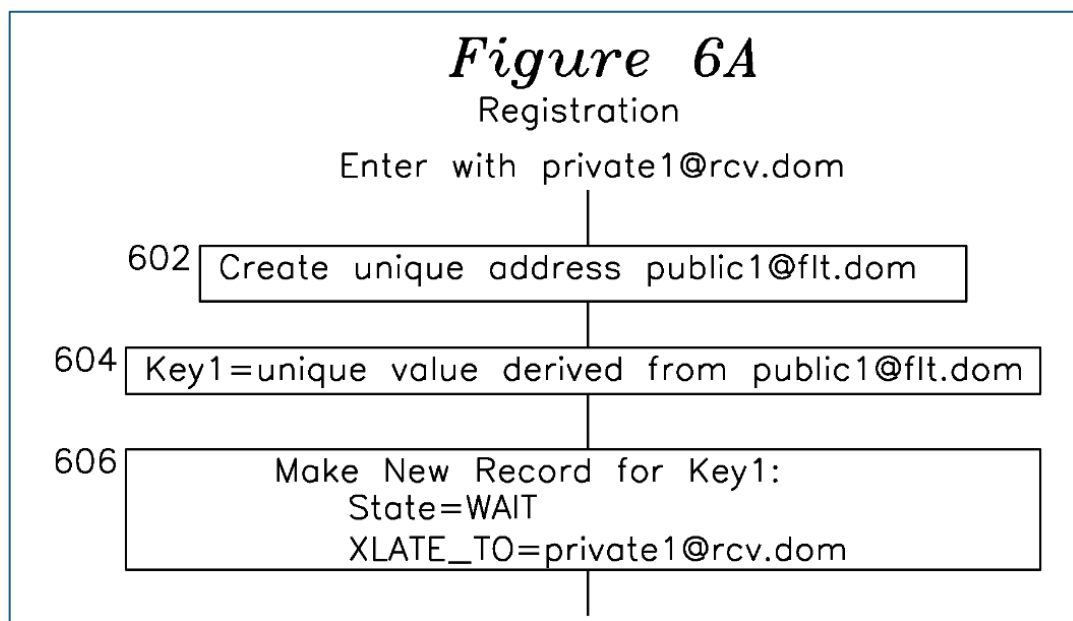
Lee teaches that a user profile is generated when the user creates an email alias. Namely, first data structure 502 is “generated upon registration of a user private email address ... addressable using a first key[.]” *Lee*, 6:10-12. The first key is associated with a public email address and contains a record³. *Id.*, 6:9-14, FIG. 5. The key 1 record is stored “using either a database with database records, or they may be stored in a lookup memory such as any random access memory (RAM), a disk file, or in any manner known for maintaining records.” *Id.*, 7:44-47. The key 1 record contains various fields, including those illustrated in FIG. 5:

³ The first key is a unique value derived from the public email address generated in step 604 of FIG. 6A. The first key has a record that contains fields and associated values. For simplicity, when this Petition refers to the “key 1 record” it is referring to the stored data contained within and associated with the first key, including the public address used to generate the unique key and the entire record of the key. *Dec.*, fn4.



Lee, FIG. 5 (cropped to show the key 1 record).

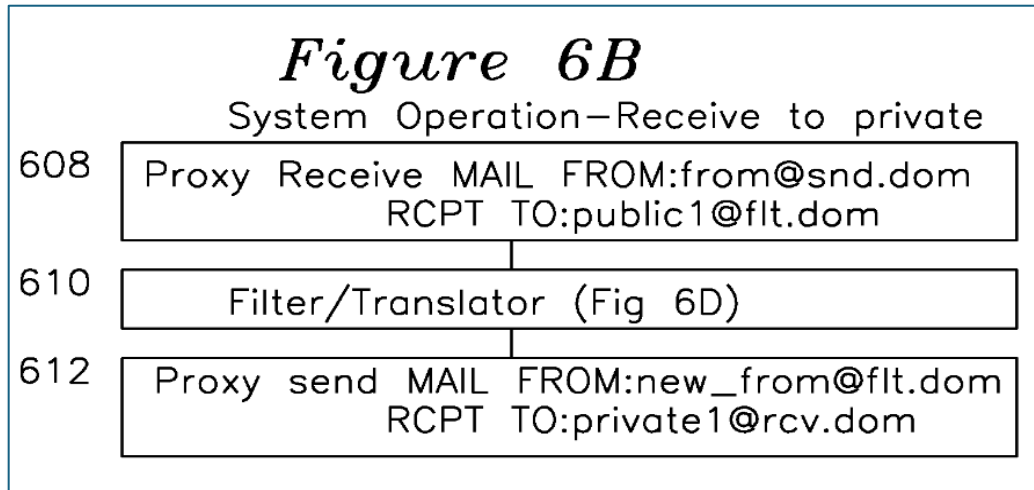
When the key 1 record is initially created, it includes two important data fields: the STATE field is set to “WAIT” and the XLATE_TO field is the user’s private email address:



Id., FIG. 6A, 6:33-37 (describing the same).

As illustrated in Fig. 6B, when an email is received to the public email address associated with the key 1 record (e.g., the generated alias email address, public1@flt.dom), a filter/translator process is run by the email proxy server prior

to the proxy sending the email to the user's private address (e.g., private1@rcv.dom):



Id., FIG. 6B, 6:47-52 (describing the same).

In the filter/translate step, the server checks the value of the STATE field. If the value is WAIT, it indicates that no prior emails have been received to the associated alias email:

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,***⁴ 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.

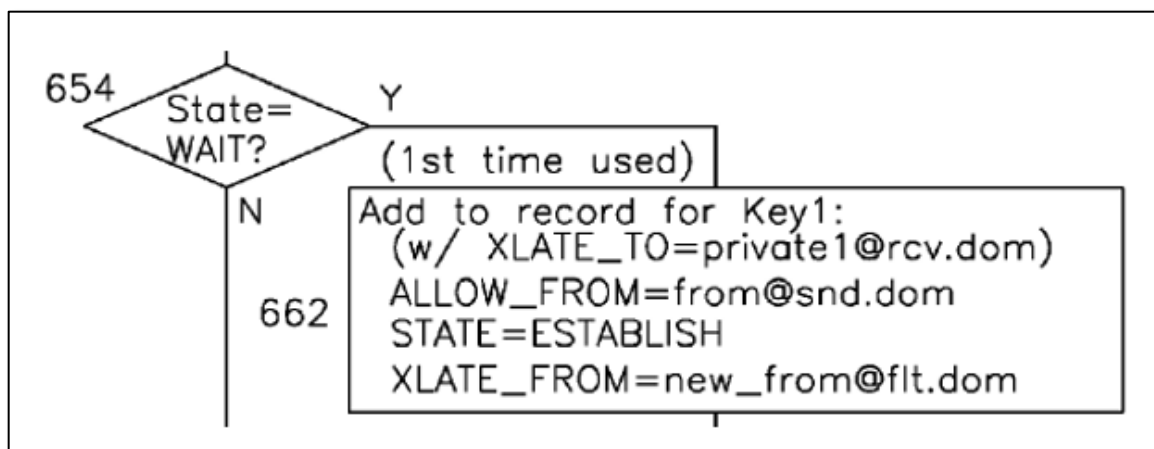
Id., 7:1-7; *Dec.*, ¶46. Upon detecting that the alias has never before been used, an alias email address is generated for the sending party (e.g., new_from@flt.dom), the

⁴ All emphases added unless noted otherwise.

sending party's email is optionally stored in the key 1 record and the state is updated to ESTABLISH, which indicates to the system moving forward that the user's email alias has been previously used and that a sender alias has been previously generated:

In step 662, the XLATE_FROM value is updated with a unique value, shown as "new_from@[flt].dom",⁵ 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., 7:7-13. This process of updating the user profile in response to receiving a first email is depicted in the Fig. 6D excerpt below:



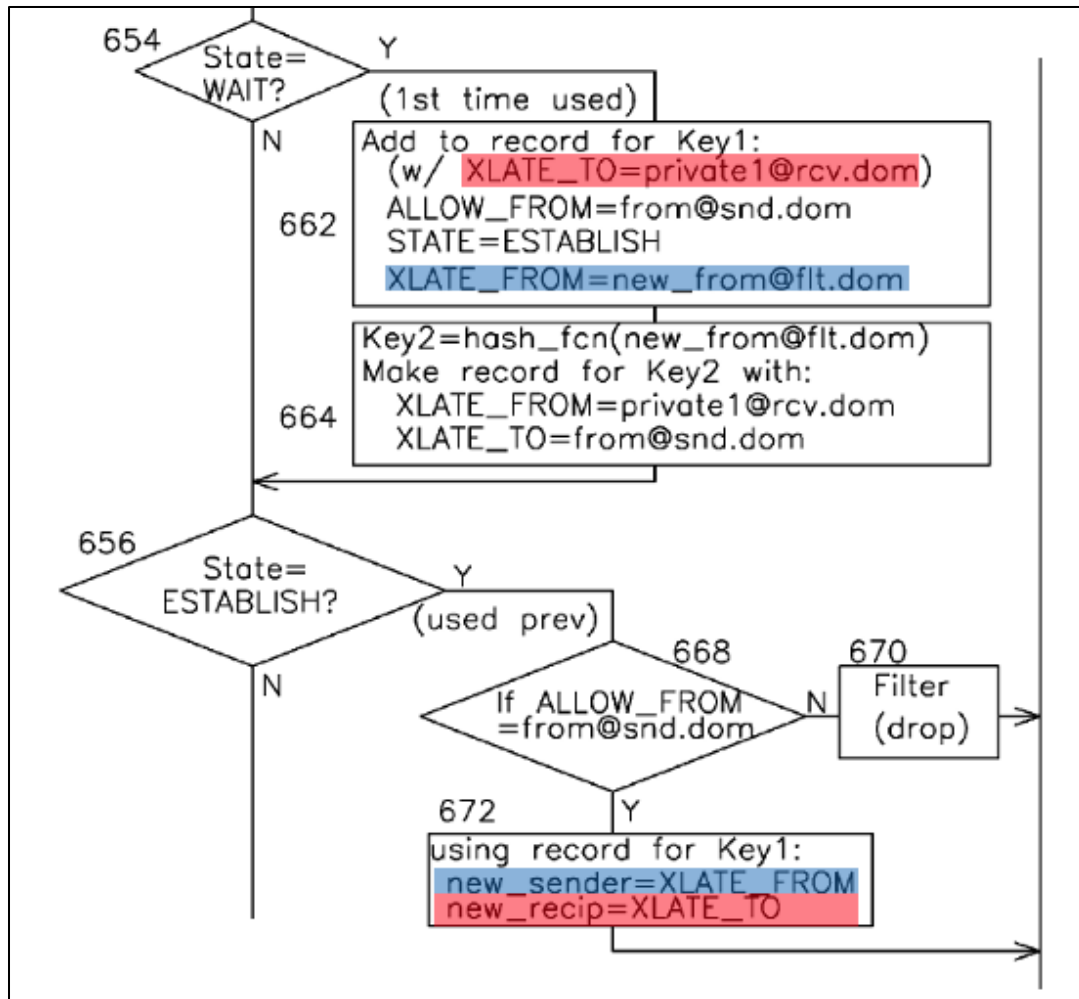
⁵ The specification incorrectly states that the newly generated sender alias is new_from@snd.dom. As illustrated in Fig. 6D, and consistent with the remainder of the disclosure, a POSITA would understand that the alias should instead be new_from@flt.dom, using the "flt.dom" domain Lee associates with all aliases generated by its system. *Dec.*, fn5.

Id., Fig. 6D (excerpt).

With a sender alias generated and stored in Key1, the system then passes the email to the intended recipient by (1) checking to ensure the sender is allowed, (2) replacing the recipient's alias with her private email address in the "to" field, and (3) replacing the sender's private email address with the newly generated sender alias in the "from" field:

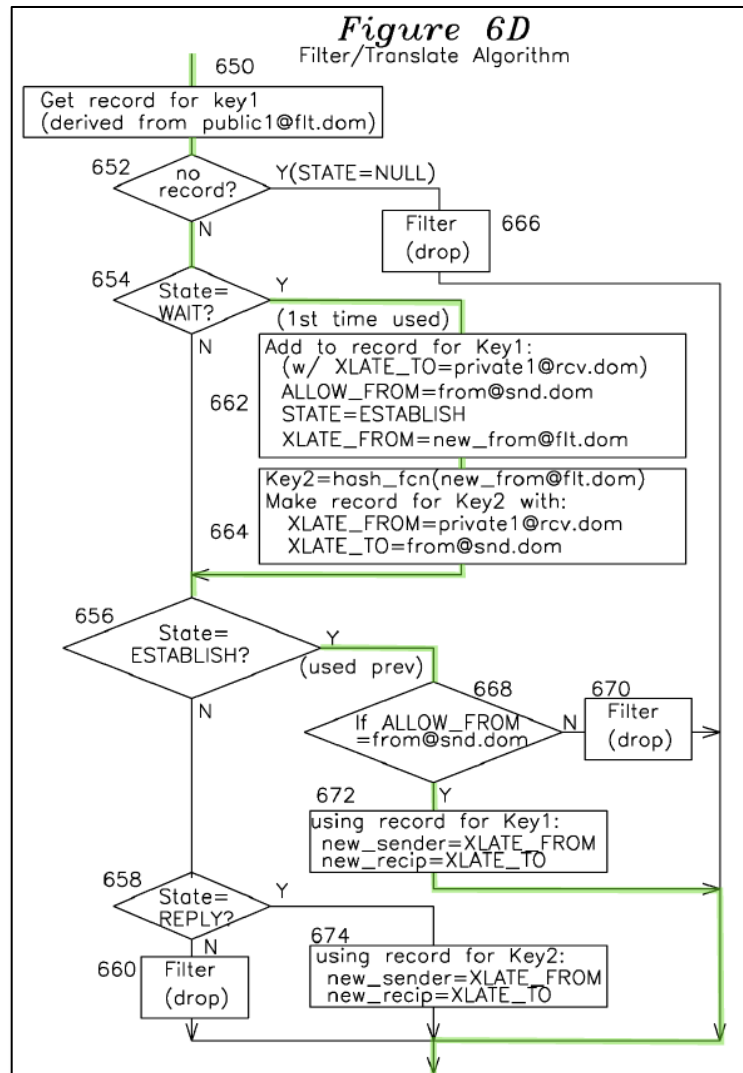
If the record for the key associated with the public email address as [sic] STATE=ESTABLISH 656, the associated ALLOW_FROM field is compared 668 with the sender address, and if there is no match, the message is filtered 670, otherwise ***the translation fields XLATE_FROM and XLATE_TO associated with the received public address*** (first key) are extracted from the associated record, and these fields ***are used for the new_sender and new_recipient address translations***, respectively.

Id., 7:27-35. The annotated FIG. 6D excerpt below illustrates the process of translating both the sender and recipient emails prior to forwarding the message to the recipient, ensuring the sender/from field is populated with the newly generated **sender's alias** and the recipient/to field is populated with the **user's private address**:



Id., Fig. 6D (excerpt and annotated).

The full Fig. 6D below, illustrates the complete filter/translate algorithm that is performed when the first email to a user's alias is generated:



Id., FIG. 6D (annotated).

Because Lee, like the '107 Patent, discloses an email alias system, Lee is in the same field of endeavor as the '107 Patent. *Compare* '107 Patent, 4:5-15, 4:44-54, *with* Lee, 3:33-4:11.

Further, the '107 Patent and Lee are both directed to the problem of protecting user privacy in email communications. *Compare* '107 Patent, Abstract, *with* Lee, 6:53-64. Accordingly, Lee is analogous art to the '107 Patent. *Dec.*, ¶49-50.

B. Overview of *Hardt*

Hardt issued on August 24, 2010 and is prior art to the '107 Patent under 35 U.S.C. § 102(a)(1). *Hardt* was not cited or considered during the '107 Patent's prosecution.

Hardt is directed to a method and system of automated pseudonymous email address (also called an alias) generation and creation to prevent unsolicited email messages from reaching a user. *Hardt*, Abstract. Relevant to the Proposed Grounds, *Hardt* creates aliases “for web pages, mailing lists, untrusted recipients and online forms” and “creat[es] rules that determine the routing associated with the alias.” *Id.*, 8:32-36.

Users can complete a webform to initiate the email alias process. *Id.*, 19:67-20:4. When an alias is generated pursuant to the webform embodiment, the “form filler provides the URL of the form in which the information will be entered, so that the alias generator 100 can store the information to later determine if privacy policies have been breached.” *Id.*, 20:4-9. This privacy policy enforcement mechanism allows the system to ensure emails originating from senders unaffiliated with the stored URL can be rejected. *Id.*, 15:2-6 (“[A]lias generator 100 obtains, either directly from the plug-in, or from the website privacy policy, a set of email addresses that mail will be received from, so that any message received from another address can be discarded.”).

Because Hardt, like the '107 Patent, discloses an email alias system, Hardt is in the same field of endeavor as the '107 Patent. *Compare* '107 Patent, 4:5-15, 4:44-54, *with Hardt*, 5:21-42.

Further, the '107 Patent and Hardt are both directed to the problem of protecting user privacy in email communications. *Compare* '107 Patent, Abstract, *with Hardt*, Abstract. Accordingly, Hardt is analogous art to the '107 Patent. *Dec.*, ¶¶53-54.

C. Overview of *Le Jouan*

Le Jouan published on November 3, 2016 and is prior art to the '107 Patent under 35 U.S.C. § 102(a)(1). *Le Jouan* was not cited or considered during the '107 Patent's prosecution.

Le Jouan is directed to protecting personal information by generating entity-specific aliases for use in communications with third parties. *Le Jouan*, Abstract. In one embodiment relevant to the grounds of this Petition, *Le Jouan* discloses an alias-aware email server system. *Id.*, [0136], FIG. 5. The email server system contains an email personalization engine 514 and an email server 504. *Id.*, [0144]. When a user sends an email to a third party, the email personalization engine 514 “can remove sensitive information [and] replace the sensitive information with dummy values or aliases, or the like.” *Id.*, [0144]. *Le Jouan* specifies sensitive information “is intended to mean personal information that is useful for contacting or identifying the user

outside of the system [], such as an email address, a physical address, a phone number, or the like.” *Id.*, [0077]. This email personalization engine also performs standard email alias functionalities, including replacing “the user’s email alias . . . with the user’s actual email address” when a third party sends an email to the user. *Id.*, [0145].

Because Le Jouan, like the ’107 Patent discloses an email alias system, Le Jouan is in the same field of endeavor as the ’107 Patent. *Compare* ’107 Patent, 4:5-15, 4:44-54, *with Le Jouan*, [0144]-[0145].

Further, the ’107 Patent and Le Jouan are both directed to the problem of protecting user privacy in email communications. *Compare* ’107 Patent, Abstract, *with Le Jouan*, Abstract. Accordingly, Le Jouan is analogous art to the ’107 Patent. *Dec.*, ¶¶57-58.

IV. PROCEDURAL REQUIREMENTS UNDER 37 C.F.R. § 42.104

A. Standing Under 37 C.F.R. § 42.104(A)

Petitioner certifies that the ’107 Patent is available for IPR and that Petitioner is not barred or estopped from requesting an IPR challenging the claims of the ’107 Patent. Specifically, (1) Petitioner is not the owner of the ’107 Patent, (2) Petitioner has not filed a civil action challenging the validity of the claim of the ’107 Patent, and (3) this Petition is filed less than one year after the Petitioner was served with a complaint alleging infringement of the ’107 Patent.

B. Challenge Under 37 C.F.R. § 42.104(B) and Relief Requested

In view of the prior art and evidence presented, claims 1-19 of the '107 Patent are unpatentable and should be cancelled. 37 C.F.R. § 42.104(b)(1). Further, based on the prior art references identified below, IPR of the Challenged Claims should be granted. 37 C.F.R. § 42.104(b)(2).

Proposed Grounds of Unpatentability	Exhibits
Ground 1: Claims 13 and 14 are obvious under AIA 35 U.S.C. § 103 over <i>Lee</i> in view of the knowledge of a POSITA.	Ex. 1004
Ground 2: Claims 1, 2, 7, 8, and 19 are obvious under AIA 35 U.S.C. § 103 over <i>Lee</i> in view of <i>Hardt</i> .	Ex. 1004 Ex. 1005
Ground 3: Claims 15-18 are obvious under AIA 35 U.S.C. § 103 over <i>Lee</i> in view of <i>Le Jouan</i> .	Ex. 1004 Ex. 1006
Ground 4: Claims 3-6 and 9-12 are obvious under AIA 35 U.S.C. § 103 over <i>Lee</i> in view of <i>Hardt</i> and in further view of <i>Le Jouan</i> .	Ex. 1004 Ex. 1005 Ex. 1006

Section V identifies where each element of the Challenged Claims is found in the prior art. 37 C.F.R. § 42.104(b)(4). The exhibit numbers of the evidence relied upon to support the challenges are provided above and the relevance of the evidence to the challenges raised is provided in Section V. 37 C.F.R. § 42.104(b)(5). **Exhibits 1001-1016** are also attached.

C. Claim Construction Under 37 C.F.R. § 42.104(B)(3)

In this proceeding, claims are interpreted under the same standard applied by Article III courts (i.e., the *Phillips* standard). *See* 37 C.F.R § 42.100(b); *see also* 83 Fed. Reg. 197 (Oct. 11, 2018); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed.

Cir. 2005) (*en banc*). Under this standard, words in a claim are given their plain meaning, which is the meaning understood by a person of ordinary skill in the art in view of the patent and file history. *Phillips*, 415 F.3d 1303, 1312–13. Petitioner proposes that no express constructions are required to resolve the invalidity challenges set forth herein.⁶

V. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 13 and 14 are obvious under AIA 35 U.S.C. § 103 over *Lee* in view of the knowledge of a POSITA.

i. Claim 13⁷

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

To the extent the preamble is limiting, *Lee* discloses this feature or at least renders it obvious. *Dec.*, ¶¶59-60. *Lee* discloses an email proxy server (“ID cloaking system”) that allows a user to create a public/alias email address. *Lee*, 6:33-46. A key 1 record is generated upon creating the alias that includes the user’s private email

⁶ Petitioner reserves all rights to propose express claim constructions in district court as relevant and necessary to those proceedings. Petitioner also reserves all rights to raise invalidity issues under 35 U.S.C. §112 in the district court proceeding.

⁷ The independent Challenged Claims are largely similar in scope, but independent Claim 13 lacks the URL limitations recited in Claims 1 and 7. Ground 1 maps the prior art to broader independent Claim 13, and the subsequent grounds capture the URL concepts of the narrower independent claims and their dependents.

address, the newly generated alias, and additional information that is populated as the public email alias is used. *Id.*, 3:33-45. A filter/translate algorithm (“instructions”) on the email proxy server processes and modifies emails sent to the public email address, allowing the user to receive communications from third parties without revealing the user’s private email address. *Id.*, 6:9-26.

Lee acknowledges standard server electronics for the system, including that the key values generated by the system are stored in a “database with database records, or they may be stored in a lookup memory such as any random access memory (RAM), a disk file, or in any manner known for maintaining records.” *Id.*, 7:43-47. Lee does not expressly describe that these processor electronics are used for executing its filter/translate algorithm or the specific memory on which the filter/translate algorithm is stored. However, a POSITA would have understood that this RAM or disc file constitutes a non-transitory computer readable medium and would further have understood or at least found it obvious that Lee’s filter/translate algorithm is stored on this same or similar memory within the email proxy server. *Dec.*, ¶60.

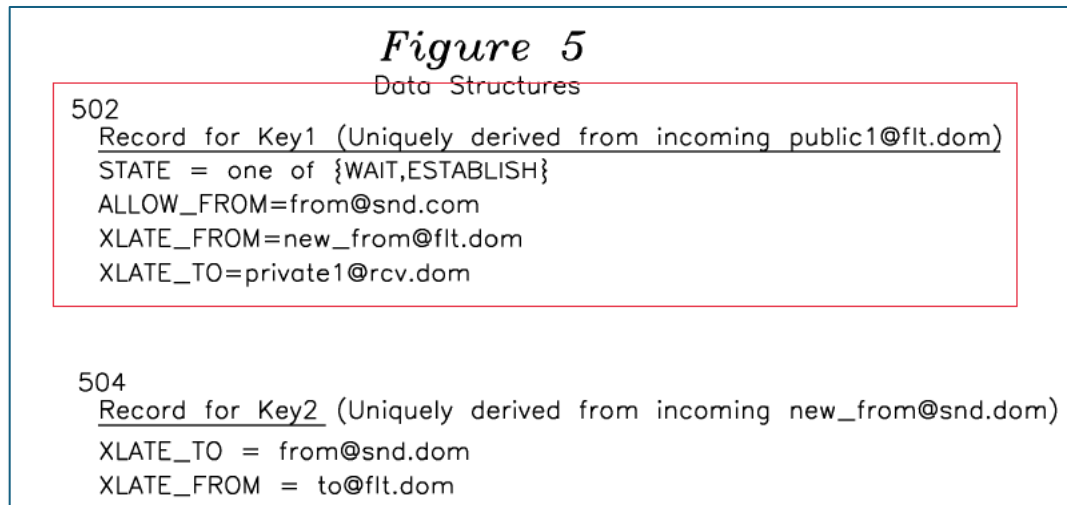
[13(a)] receive an email addressed to a cloaked end user address, wherein the email is sent from a relying party email address, and wherein the domain of the cloaked end user address and the domain associated to the cloaked ID system are the same domain;

Lee discloses this limitation, teaching an ID cloaking system that shares its domain with the cloaked consumer email addresses it generates.

Lee discloses a user providing their private email address during registration to create a public email address (“cloaked end user address”), which has the domain of the email proxy server, for communication with a third party. *Lee*, 6:9-26, 2:36-45. A key 1 record is created that contains the public email address, private email address, and other information. *Id.*, 6:33-46. When a third party sends an email from its email address (“relying party email address”) to the public email address, the email proxy server receives the email, runs a filter/translate algorithm to modify the key 1 record, and sends the email to the user. *Id.*, 6:47-52.

In the relevant embodiment, a first data structure 502 (key 1 record) “is generated upon registration of a user private email address, and is addressable using a first key, which may be generated from the public email address associated with the record[.]” *Id.*, 6:10-13, FIG. 5. This public email address is “a cloaked end user address” since the public address is not the end user’s private email and is provided to a sender in order to contact the end user. *Id.*, 4:47-51.

The key 1 record contains fields that include STATE, ALLOW_FROM, XLATE_FROM, and XLATE_TO, each of which can have values set and updated by the email proxy server. *Id.*, 6:40-46, 7:7-13. FIG. 5 illustrates the information stored in the record of the first key, outlined in red.



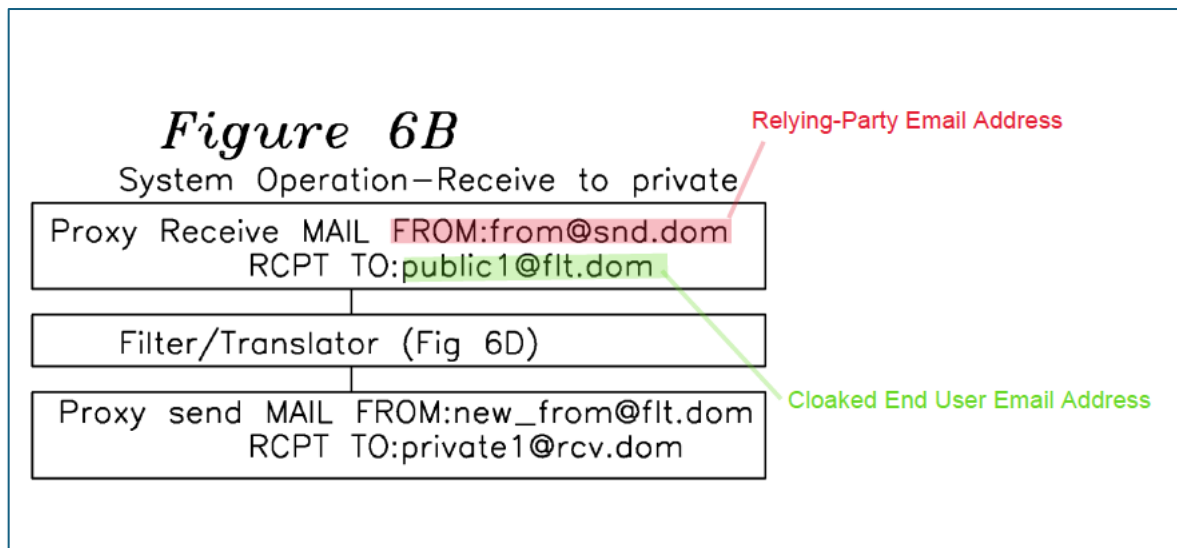
Id., FIG. 5 (annotated).

When “an email message to a public address is received” the sender private email address and recipient public email address are sent to the filter/translator step 610 “which either rejects the email, or sends the email in step 612 using the translated values.” *Id.*, 6:47-52, FIG. 6B. In this embodiment, the email received by the email proxy server is sent from a sender email address, namely “from@snd.dom”, to a public email address (which may be associated with a recipient, i.e., a user who registered with Lee’s email proxy system), namely “public1@flt.dom.” *Id.*, FIG. 6B.

The public email address and the mail proxy system (cloaked ID system) have the same domain—flt.dom. Lee expressly teaches that the “domain flt.dom resolves to the IP address of the mail proxy system[.]” *Id.*, 6:37-38. When a user requests a public email address, they are assigned an “flt.dom” address, e.g.,

“public1@flt.dom”. *Id.*, 6:33-38, FIG. 6B. Therefore, the “cloaked end user address and the domain associated to the cloaked ID system are the same domain[.]”

FIG. 6B, illustrated below, shows an operation of the email proxy server where the server receives an email from a sender email address, **from@snd.dom**, sent to a public email address, **public1@flt.dom**. The mail proxy system goes through the filter/translator steps of FIG. 6D (*See infra* Section V.A.i.13(b), V.A.i.13(c)) and sends the email to the end user, private1@rcv.dom.



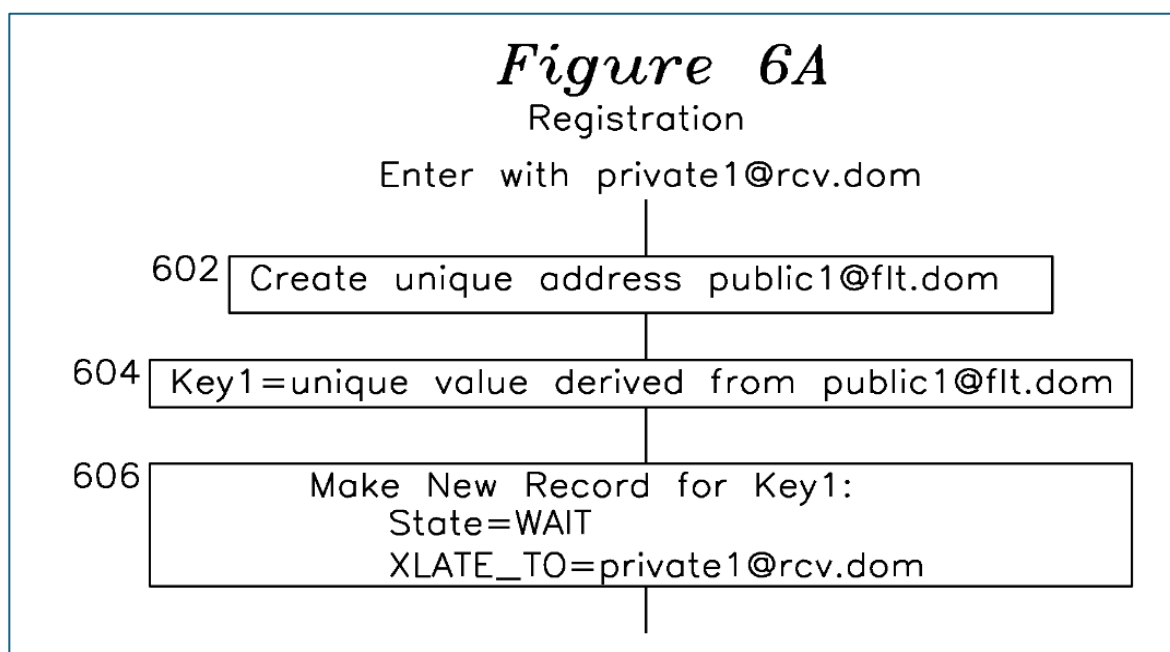
Lee, FIG. 6B (annotated).

[13(b)] identify an end user specified address associated to the cloaked end user address by an end user profile;

Lee discloses a key 1 record (“end user profile”) that associates a private email address of the user (“end user specified address”) with a public alias email address (“cloaked end user address”). When the server receives an email to the user’s alias

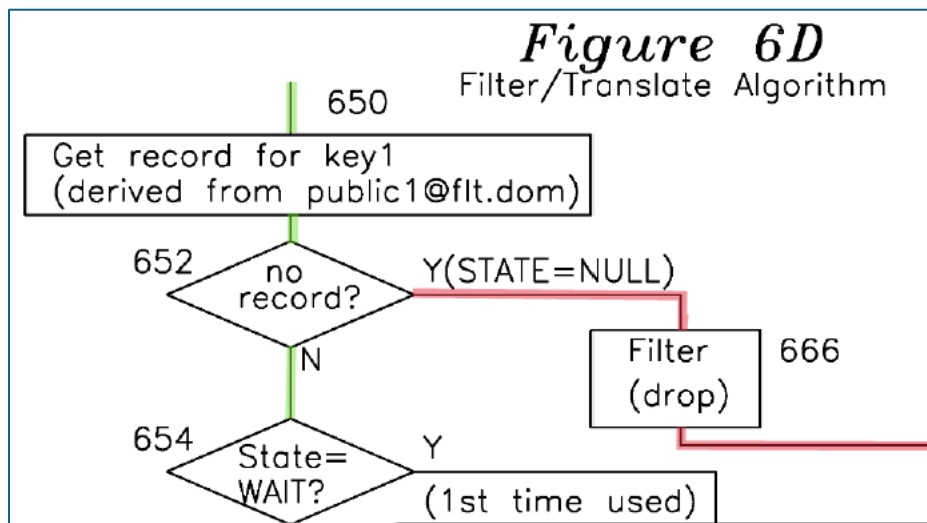
address, it checks to see if a key 1 record exists. Accessing this key 1 record identifies the private email and the public email linked to the user, as claimed.

Lee discloses the creation of a key 1 record (“end user profile”) during a registration upon request by the user. FIG. 6A, below, illustrates the registration step of a new public email address including the creation of a key 1 record. *Lee*, 6:33-46. The key 1 record has a key value related to the created public email address, e.g., “public1@flt.dom” (“cloaked end user address”) and an XLATE_TO field with a value of the user’s private address, e.g., “private1@rcv.dom” (“end user specified address”).



Lee, FIG. 6A. A POSITA would understand that the key 1 record is an “end user profile” at least because it contains information relating to the user’s cloaked and private address. *Dec.*, ¶69.

Lee teaches that when an email is sent to a user's public email address, the sender email address and public email address "are furnished to the filter/translator step[.]" *Lee*, 6:47-52, FIG. 6B. In the initial step of the filter/translator algorithm, the system checks to see if there is a record associated to the key 1 record. *Id.*, 6:65-67, FIG. 6D (shown below). If there is not a record, it means the public email address does not exist (e.g. was not created by a user), and the server filters out the email. FIG. 6D (shown in red). If a record for the key is found, the public email associated with the key was previously generated and the filter/translate algorithm continues to perform additional steps. FIG. 6D (shown in green).



Lee, FIG. 6D (annotated). The key 1 record contains an XLATE_TO field with the value of the user's private email address, private1@rcv.dom, initialized at the time of registration of the public/alias email address. *Id.*, 7:1-7, FIG. 6A, FIG. 5.

Because the key 1 record associates the user's private email ("end user specified address") and alias email ("cloaked end user address"), a POSITA would

have recognized that determining that the key 1 record exists satisfies the claimed step of “identify[ing] an end user specified address associated to the cloaked end user address by an end user profile[.]” Dec., ¶71.

[13(c)] 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;

Lee discloses this limitation or at least renders it obvious. When an initial email is received to a user’s alias, Lee’s system checks to see if an alias has been previously generated for the sender by checking the value of the STATE field in the key 1 record (“end user profile”). As explained below, the value WAIT means the system has *not* previously associated the sender with the user’s alias email address.

When the STATE value is WAIT, it indicates to the system that there has not been a previous communication to the user’s alias address:

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.

Lee, 7:1-7, FIG. 6D. In other words, when STATE=WAIT, there is *no information about any sender’s email address*, and therefore when the STATE=WAIT is encountered, it indicates that it is “determine[d]” that the end user profile ***did not***

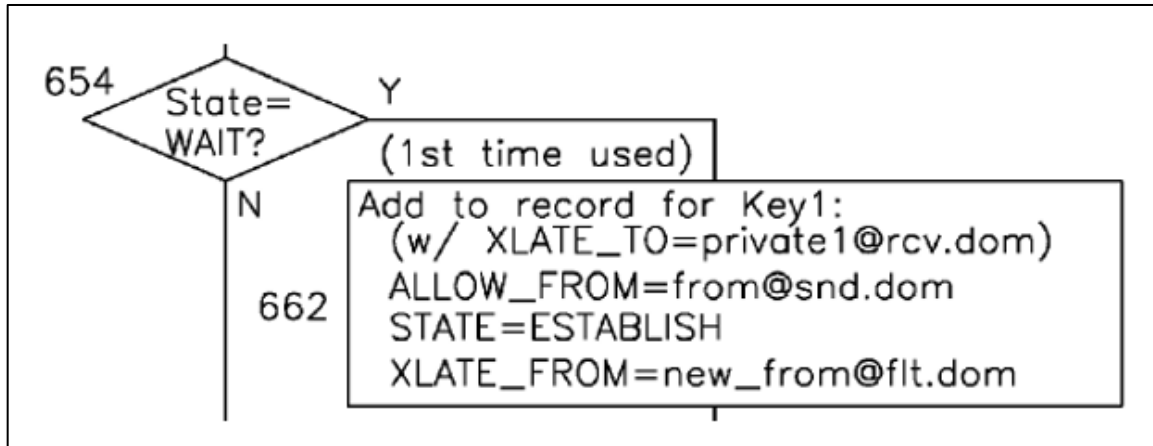
contain a “previous association between the relying party address and the cloaked relying party email address”.

Upon detecting that the alias has never before been used, an alias email address is generated for the sending party (e.g., new_from@flt.dom) (“a cloaked relying party email address”), that cloaked relying party email address is stored in the XLATE_FROM field, and the state is updated to ESTABLISH, which indicates to the system moving forward that the user’s email alias has been previously used and that an alias email address has been previously generated for this sender:

In step 662, *the XLATE_FROM value is updated with a unique value, shown as “new_from@[flt].dom”*,⁸ 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., 7:7-13. At this point, Lee’s key 1 record (“end user profile”) is updated to contain an association between a sender’s (“relying party”) email address and a cloaked version of that address (“a cloaked relying party email address”). This process of updating the user profile in response to receiving a first email is depicted in the Fig. 6D excerpt below:

⁸ See fn5.



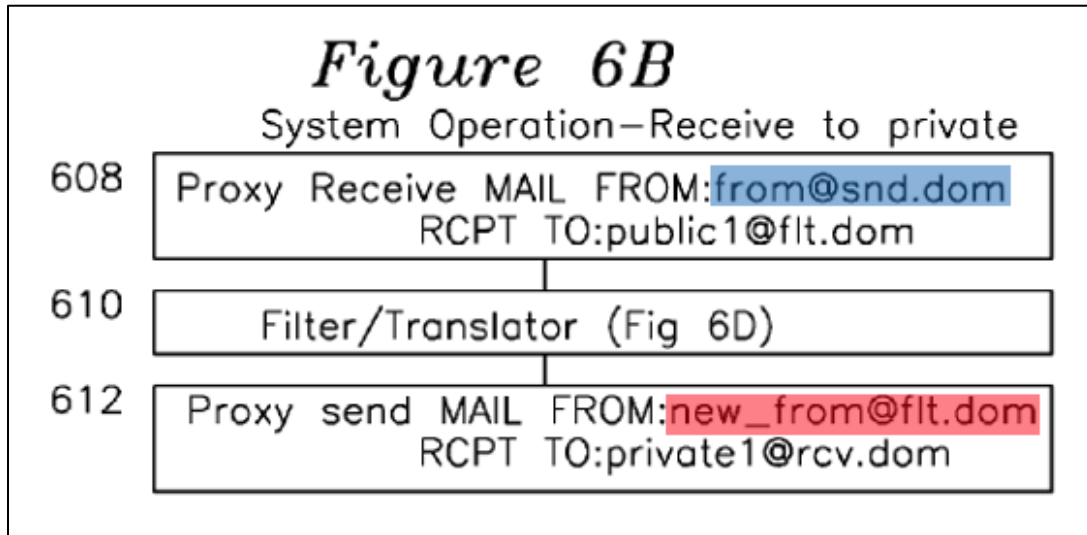
Id., Fig. 6D (excerpt).

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. *Dec.*, ¶¶72-75.

Lee’s sender alias has a different domain than the sender’s native email address

As discussed above, Lee teaches that its mail proxy system uses the domain flt.dom and that all alias addresses also use this domain. *Lee*, 5:30-36 (describing a user’s alias address “public1@flt.dom, and a sender’s alias addresses, “new_from@flt.dom”), 6:37-38 (teaching the “domain flt.dom resolves to the IP address of the mail proxy system”). Lee also teaches that the sender address has a different domain, e.g., “snd.dom.” *Id.* Fig. 6B below has been annotated to highlight

the different domains of the sender's native email address and the sender's generated alias:



Id., Fig. 6B (annotated). Accordingly, “the relying party address has a different domain than the cloaked relying party email address.” *Dec.*, ¶76.

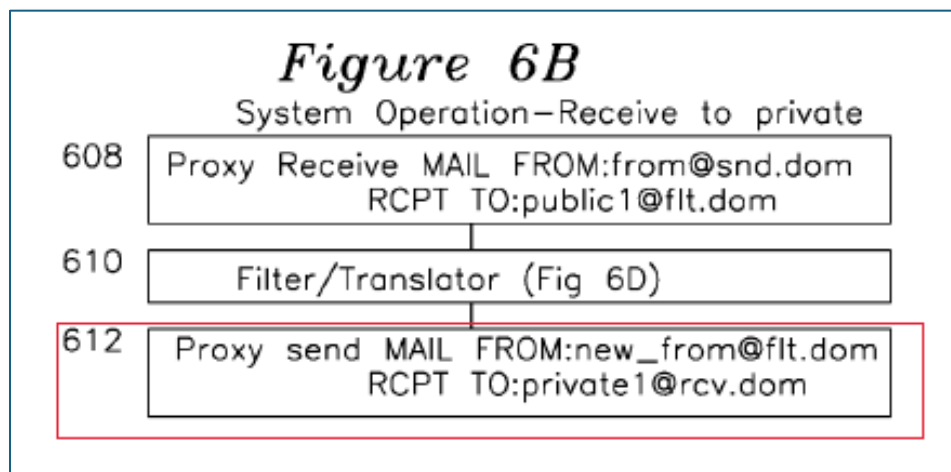
[13(d)] where the end user profile does not contain a previous association between the relying party address and the cloaked relying party email address, then generate a new cloaked relying party email address and associate the new cloaked relying party email address to the end user profile, the cloaked end user address, wherein the new cloaked relying party email address is generated with a domain different than the relying party address; and

As discussed above, Lee discloses this limitation, teaching that, upon receiving a first email from the sender, the system (1) confirms that no sender alias exists, (2) generates an alias email for the sender, and (3) stores this new sender alias in the end user's profile along with the user's alias. *Lee*, 7:1-13; *see supra* Section V.A.i.13(c); *Dec.*, ¶¶77-80. A POSITA would understand that storing the sender's new alias (“new cloaked relying party email address”) in the key 1 record (“the end

user profile”), which already contains the user’s alias (“the cloaked end user address”), “associates” the newly generated sender alias with the user alias. *Dec.*, ¶80. Further, as set forth with reference to the preceding limitation, the sender’s native email address and the sender’s generated alias use different domains. See *supra* Section V.A.i.13(c); *Dec.*, ¶81.

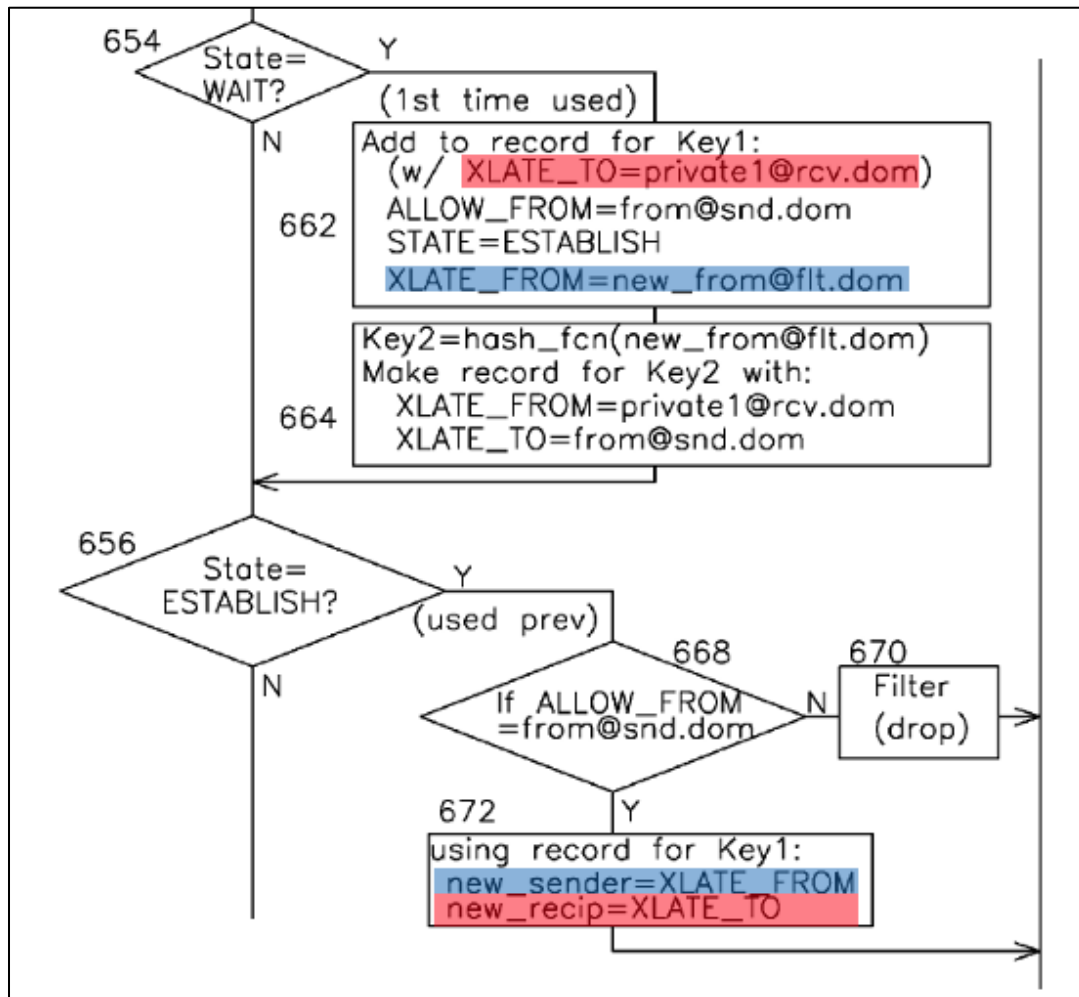
[13(e)] send the email to the identified end user specified address, wherein the email is configured with a reply-to email address comprising the new cloaked relying party email address.

After the filter/translator algorithm has processed as described with reference to the preceding limitations, Lee teaches sending the “email in step 612 using the *translated values*.” *Lee*, 6:51-52, FIG. 6B.



Lee, FIG. 6B (annotated to show the MAIL FROM and RCPT TO addresses). The annotated FIG. 6D excerpt below illustrates this process of translating both the sender and recipient emails prior to forwarding the message to the recipient, ensuring

the sender/from field is populated with the newly generated **sender's alias** and the recipient/to field is populated with the **user's private address**:



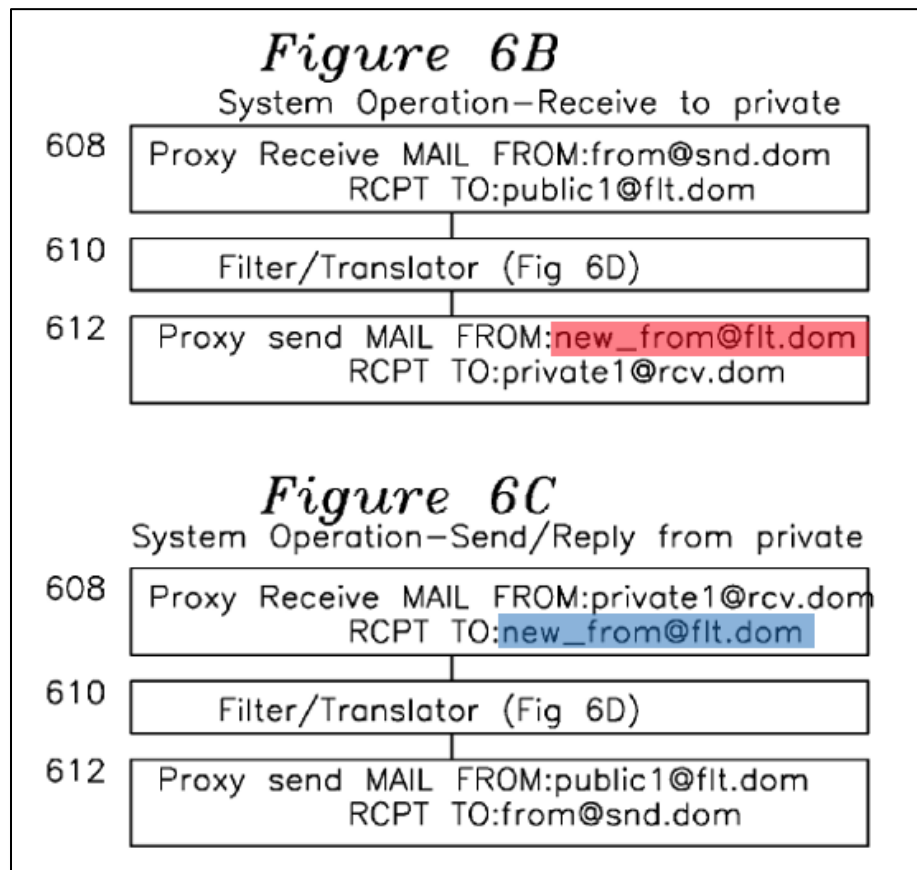
Id., Fig. 6D (excerpt and annotated), 7:31-35 (“[T]ranslation fields XLATE_FROM and XLATE_TO associated with the received public address (first key) are extracted from the associated record, and these fields are used for the new_sender and new_recipient address translations, respectively.”) Accordingly, 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.

Lee's system configures the forwarded email with a reply-to email address comprising the sender's alias

As described in the '107 Patent, an email can contain distinct “from” and “reply-to” fields. '107 Patent, 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>[.]”). A POSITA would have understood that these two fields serve distinct roles. Namely, the “from” field indicates an address of the sender and the “reply-to” field is an optional field that defines which address will populate the “to” field in a responsive communication when the recipient replies to the email that is only used in case the sender wishes a reply to be sent to a different address than that found in the “from” field. Dec., ¶83. 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.* (noting that the standard approach is to direct a responsive email to the “from” address in the received email, but acknowledging that an express “reply-to” field in the received email can override this standard process, dictating the destination of a responsive email).

Lee does not expressly discuss distinct “from” and “reply-to” fields, but it does expressly teach that, when an end user responds to an email received pursuant to the embodiment described above, the responsive email will be addressed to the sender’s alias address. For example, Figs. 6B and 6C below, show that the sender’s

alias address (i.e., `new_from@flt.dom`) populates the “from” field in an email to the user’s private address and also is the “to” address in responsive communications. Namely, Fig. 6B shows that the sender’s alias (`new_from@flt.dom`) populates the “from” field in a translated email sent to the user’s private email address (`private1@rcv.dom`). And Fig. 6C shows that the user’s responsive email is addressed to the same sender’s alias (`new_from@flt.dom`).



Lee, Figs. 6B-6C (annotated).

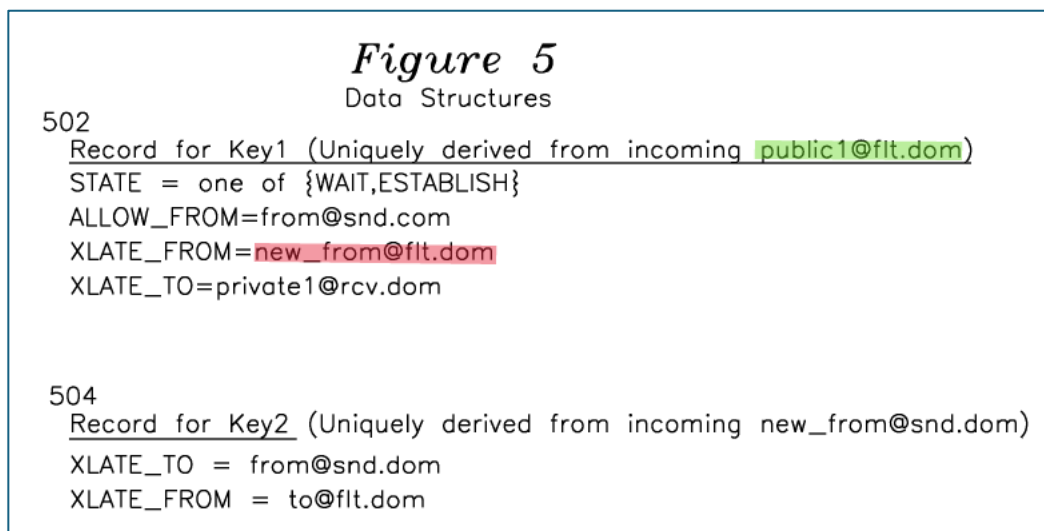
Accordingly, a POSITA would have understood that it would have been obvious to populate a “reply-to” field with the sender’s alias. *Dec.*, ¶85 (noting that

Lee's described functionality accomplishes the same result as populating a "reply-to" field with the sender's alias).

ii. Claim 14

The non-transitory computer readable medium 13, wherein the new cloaked relying party email address has a domain that is the same as the cloaked end user address.

Lee discloses the XLATE_FROM value (cloaked relying party email address) as having a flt.dom domain, for example **new_from@flt.dom**. *Lee*, FIG. 5, 6D. Lee also discloses the user's public email address as having a flt.dom domain, for example **public1@flt.dom**. *Id.* Therefore, Lee discloses the cloaked relying party email address has the same domain as the cloaked end user address.



Lee, FIG. 5 (annotated to highlight public email address and XLATE_FROM values with same domain).

B. Ground 2: Claims 1, 2, 7, 8, and 19 are obvious under AIA 35 U.S.C. § 103 over *Lee* in view of *Hardt*.

As set forth in Ground 1 above, *Lee* teaches or renders obvious all limitations of independent Claim 13. Independent Claims 1 and 7 are similar in scope to Claim 13, but further recite storing, in the end user profile, URLs associated with the relying party. As set forth below, a POSITA would have been motivated to supplement *Lee*'s email alias system with *Hardt*'s functionality that (1) allows a user to create an email alias using a web form, (2) stores the URL of the web form in the user's profile, and (3) uses the stored URL to enforce privacy policies that ensure emails are received to the alias address only from user-intended senders.

i. Claim 1

[1(P)] A processor-based ID cloaking system, comprising:

To the extent the preamble is limiting, *Lee* discloses this feature. *Lee* discloses an email proxy server (ID cloaking system) that allows a sender to send email to a user's primary email address via a public address which is provided to the sender. *Lee*, 2:36-45. A POSITA would understand that an email proxy server would consist of at least one processor in order to perform the functions of an email proxy server. *Dec.*, ¶88; see *supra* Section V.A.i.13(P).

[1(a)] memory configured to store contents that are executable by processor electronics;

Lee discloses storage of values associated with keys using "either a database with database records, or they may be stored in a lookup memory such as any random

access memory (RAM), a disk file, or in any manner known for maintaining records.” *Lee*, 7:43-47. A POSITA would understand that the contents of the memory disclosed by *Lee* would be executable by the processor electronics of the email proxy server. *Dec.*, ¶89; *see supra* Section V.A.i.13(P).

[1(c)] processor electronics configured to execute the contents in order to:

Lee discloses this element for at least the same reasons as presented above for limitation 13(P). *See supra* Section V.A.i.13(P).

[1(c)(i)] 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 processor-based cloaked ID system are the same domain;

Lee discloses this limitation for at least the same reasons as presented above for 13(a). *See supra* Section V.A.i.13(a).

[1(c)(ii)] identify an end user specified address as well as any URLs associated to the cloaked end user address based on an end user profile;

Lee in view of *Hardt* renders this limitation obvious. This limitation narrows the concept recited in Claim 13 (mapped in Ground 1) by further requiring the ID cloaking system identify any URLs stored in the user profile. Referred to as “associated relying-party URLs” in claim 1(c)(iv), consistent with the ’107 Patent specification, the URLs recited in claim 1 correspond to the relying-party (e.g., they identify the merchant’s URL) and are associated with the end user’s alias and stored in the end user’s profile. Indeed, the ’107 Patent describes an embodiment in which a consumer fills out a webform using a cloaked consumer address. *Id.*, 9:13-26. The

ID cloaking system may then associate “the URL [of] the webform” with the consumer’s profile. *Id.*, 9:34-40. In one example, storing merchant URLs in a consumer profile allows the consumer to identify unauthorized/unwanted merchants using a cloaked email the consumer created for a more limited use. *Id.*, 18:53-59 (“[I]f the end user notices that a cloaked email address she created with one merchant (related to the merchant email/URL when created etc.) is being misused, she can cancel, disable or delete the cloaked email address.”).

Hardt teaches a similar process through which webform URLs are used to ensure only intended senders/merchants are able to reach the end user via that user’s email alias. Namely, Hardt teaches that users can complete a webform to initiate its email alias process. *Hardt*, 19:67-20:4. When an alias is generated pursuant to the webform embodiment, the “form filler provides the URL of the form in which the information will be entered, so that the alias generator 100 can store the information to later determine if privacy policies have been breached.” *Id.*, 20:4-9. This privacy policy enforcement mechanism allows the system to ensure emails originating from senders unaffiliated with the stored URL can be rejected. *Id.*, 15:2-6 (“[A]lias generator 100 obtains, either directly from the plug-in, or from the website privacy policy, a set of email addresses that mail will be received from, so that any message received from another address can be discarded.”).

Lee discloses an end user specified address associated to cloaked end user address based on an end user profile. *See supra* Section V.A.i.13(b). But Lee does not describe identifying “URLs associated to the cloaked end user[.]” As set forth below, however, a POSITA would have been motivated to supplement Lee’s teachings with such URL functionality pursuant to Hardt.

a. Lee’s Teachings

As discussed above, Lee’s email proxy server generates a key 1 record for a public email generated upon a user request. *Lee*, 6:9-14. When initially generated, the key 1 record contains the user’s private email address, a uniquely generated public email address, and a STATE field. *Lee*, 6:33-46. Upon receiving a first ever email from a third-party sender to the public address (as indicated by STATE=WAIT), an optional ALLOW_FROM field is initialized with the sender’s address and the STATE is then updated to ESTABLISH. *Id.*, 7:1-13. Once the STATE is updated to ESTABLISH, the ALLOW_FROM field is used to filter out future emails from different senders. *Id.*, 7:27-35, FIG. 6D. A POSITA would have understood that this mechanism prevents the abusive email behavior Lee identifies as problematic in which an alias email address is sold and used by any number of undesired senders. *Dec.*, ¶95; *Lee*, 1:65-2:6 (describing a scenario in which a merchant “resells customer lists to other promoters, or uses the list for their own

unrequested promotions[,]” which causes “[t]he user [to] receive[] increasing amounts of email wholly unrelated to the original transaction”).

Importantly, Lee does not identify any security mechanism that prevents the ALLOW_FROM field from being populated with an email address from an undesired sender. *Dec.*, ¶96. The Lee system simply assumes that the first party to send a message to the public address is a desired sender and populates the ALLOW_FROM field with that party’s email address. *Id.* A POSITA would have recognized that Lee’s process creates a security flaw, allowing potentially undesired senders to communicate with a user simply by being the first party to communicate with a newly generated user alias email. *Id.*

Additionally, Lee recognizes that a user may wish to authorize more than one sending party, i.e., to populate multiple addresses in the ALLOW_FROM field. *See Lee*, 7:53-56 (“In another embodiment of the invention, a new state ESTABLISH_ADD could be used to indicate that additional qualified ALLOW_FROM and XLATE_FROM senders should be added to the record 502.”). But Lee does not describe *how* a user may configure the system to permit multiple desired senders while filtering out all others.

As set forth below, a POSITA would have been motivated to implement Hardt’s URL teachings in Lee’s system, allowing a user to define authorized senders by storing URLs for those senders in the user profile upon its generation. *Dec.*, ¶98.

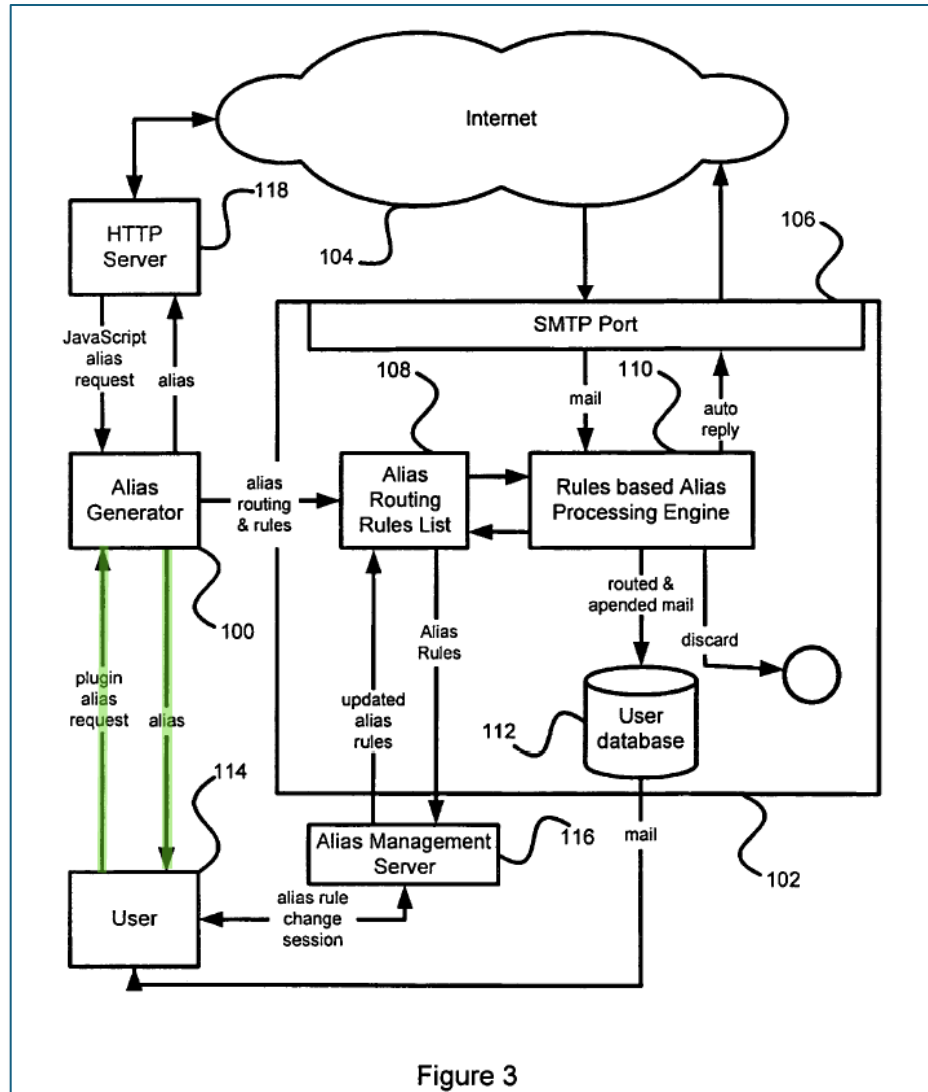
This modification improves Lee's system in multiple ways. First, it solves the security flaw in Lee's native system, allowing the user to define a desired sender with specificity, rather than simply assuming the first sender is a desired sender. *Id.* Second, it provides implementation details for the multiple allowed senders feature that Lee expressly contemplates, defining how a user may configure the system to permit multiple desired senders while filtering out all others. *Id.*

b. Hardt's Teachings

Hardt teaches an identity management system that includes a form filling application that can request an alias from an alias generator 100 and provide it to the web-based form. *Hardt*, 19:61-65, FIG. 3. The form filler may provide the URL of the form to the alias generator 100 to be stored to help determine if privacy policies are later breached. *Id.*, 20:4-9. The alias generator 100 (and as a result, the URL) is associated with a user profile. *Id.*, 20:13-15. The alias generator 100 may obtain from the website privacy policy associated with the URL "a set of email addresses that mail will be received from, so that any message received from another address can be discarded." *Id.*, 15:2-6. Hardt does not mandate *when* the URL is used by the alias generator to pull email addresses from the website's privacy policy, but a POSITA would have understood that the addresses could either be pulled at the creation of the alias, when the webform is completed, or subsequently when an email is received by the alias. *Dec.*, ¶99. A POSITA would have recognized that there are benefits

realized by waiting until an email is received to the generated alias. *Id.* Namely, storing the URL and pulling emails associated with the privacy policy at the time the email is received ensures that the most recent privacy policy is checked (e.g., the system receives the most recent list of allowed emails per the associated security policy). *Id.*

The annotated FIG. 3 below shows the architecture of the identity management system of Hardt. The green pathways show the request from the user to generate an alias through the webform plugin and the alias generator 100 providing the alias back to the user.



Hardt, Fig. 3 (annotated).

Although Hardt does not specify what exact data is stored as the “URL,” a POSITA would have understood that Hardt teaches or at least renders obvious storing the full URL associated with the webform. *Dec.*, ¶101. A URL (unique resource locator) is a unique identifier used to locate a specific resource on the Internet. *Id.* Three main parts of a URL are the scheme, domain, and path. *Id.* The scheme is the protocol used to establish a connection between a browser and a

service, the domain is the unique name of a website, and the path shows the specific location of the resource the user is accessing. *Id.* Using <https://www.nordstrom.com/browse/customer-service> as an example, the scheme is “https”, the domain is “nordstrom.com”, and the path is “browse/customer-service”. *Id.* A POSITA would have understood that a full URL—including a scheme, domain, and likely a path—is associated with the webform described by Hardt. *Id.* And, while Hardt does not specify whether the entire URL or a partial URL is stored, a POSITA would have understood the most straightforward manner with which to store the webform URL pursuant to Hardt’s teachings is to store the full URL. *Id.* Indeed, while it is certainly possible to filter components of the URL, retaining only the information necessary to implement an associated privacy policy, a POSITA would have understood that Hardt does not teach or suggest such filtering. *Id.* (concluding that Hardt fairly conveys storing the full URL at least based on its failure to teach or suggest filtering any URL data).

c. The Lee-Hardt Combination

In the proposed Lee-Hardt combination, the email proxy server of Lee is supplemented with the webform filler and URL association of Hardt as a means of providing a public email address to a third-party sender. A user requests a public email (i.e., an alias) in the process of filling a webform. When requesting a public email using a webform, Lee’s key 1 record will be supplemented with a URL field

that is automatically populated with the URL of the webform, and the URL is then used to enforce privacy functions disclosed in Hardt. *Hardt*, 15:2-6 (describing a privacy policy associated with the URL that defines “a set of email addresses that mail will be received from, so that any message received from another address can be discarded”). The proposed combination relies on Lee’s existing ALLOW_FROM field to enforce such privacy policies. Per Lee’s native functionality, the ALLOW_FROM field is used to reject emails from undesired senders, and Lee expressly acknowledges that the ALLOW_FROM field can support multiple desired senders. Accordingly, Hardt’s URL-based privacy policy teachings seamlessly merge with Lee’s system, populating Lee’s ALLOW_FROM field with email addresses associated with the privacy policy of the stored URL.

For example, a user filling out a webform at ford.com could request the email proxy server provide a public email to be used in the messages between Ford and the user to protect the user’s private email address. *Dec.*, ¶103. The URL https://www.ford.com would be stored in the key 1 record URL field. *Id.* When an email is received by Lee’s email proxy server to the user’s alias associated with key 1, the server examines the URL field to enforce Hardt’s privacy policy. *Id.* For example, the privacy policy at ford.com may show emails at Ford may come from email1@ford.com or email2@ford.com. *Id.* The email proxy server could subsequently add these emails to ALLOW_FROM fields contained in the key 1

record. *Id.* This would allow the email proxy server to filter out emails to the public address that are not from these emails and ensure only ford.com may contact the user through the public address. *Id.*

In sum, the Lee-Hardt combination utilizes a web form filler that “provides the URL of the form in which the information will be entered” to the email proxy server to “store the information” as part of the creation of a public email address and associated key 1 record. The email proxy server then uses the URL to find email address in the privacy policy and to forward emails from senders only if they have an address that matches one of those in the privacy policy.

d. Motivation to Combine Lee and Hardt

For a number of reasons, a POSITA would have been motivated and found it obvious to supplement Lee’s email proxy server with Hardt’s form filler plugin. *Dec.*, ¶¶105-108. A POSITA would have recognized that the form filler disclosed by Hardt would benefit the email proxy server of Lee in the same way it benefits Hardt, allowing the user the ability to create a public email address via a webform and using the URL of the webform to ensure emails are received only from intended senders. *Dec.*, ¶105; *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007) (“[I]f a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious[.]”). This addresses an apparent problem of Lee—that the

user cannot limit which sender(s) uses a public address when registering the public address because Lee's system simply assumes that the first received email is desired regardless of sender. *Dec.*, ¶105. A POSITA would have recognized that limiting intended senders to email addresses associated with one or more user-approved URLs solves the security problem of Lee, benefitting Lee's system in the same way the URL feature benefits Hardt's system. *Id.*

Supporting the conclusion that it would have been obvious to supplement Lee's system with Hardt's form filler, Lee and Hardt describe "similar devices." *Dec.*, ¶106. For example, each reference discloses a system that can generate an aliased email to hide the end user's actual email address (the email proxy server of Lee and the alias generator of Hardt). *Compare Lee*, Abstract, *with Hardt*, Abstract. Each system has the capability to route an email sent to an aliased email to the end user, and to replace the "from" address with a generated email that shares a domain of the system. *Compare Lee*, Abstract, *with Hardt*, 10:41-44. Finally, each teaches a profile that is associated with the end user that stores information including the user's personal email address and one or more cloaked addresses. *Compare Lee*, 6:9-32 (discussing the key 1 record), *with Hardt*, 10:1-3.

These similarities in function and architecture would also have led a POSITA to expect success in making the proposed combination. *Dec.*, ¶107. The proposed modifications to Lee's filter translate algorithm and key 1 record are also

straightforward and would have been well within the capabilities of a POSITA at the time, further supporting a reasonable expectation of success in making the proposed modification. *Id.* Indeed, adding a field for a URL is technically similar to adding an additional ALLOW_FROM field. *Id.* Because Lee already filters undesired emails using the ALLOW_FROM field's value, a POSITA would understand the proposed modification seamlessly merges with Lee's existing functionality. *Id.*

Additionally, a POSITA would have recognized that Hardt was a known and predictable solution for implementing Lee's expressly contemplated feature of populating ALLOW_FROM with multiple permitted senders. *Dec.*, ¶108. As noted above, Lee recognizes that a user may wish to authorize more than one sending party (i.e., to populate multiple addresses in the ALLOW_FROM field), but does not describe how a user may configure the system to accomplish this functionality. *Lee*, 7:53-56. A POSITA would have been motivated to look to known methods for accomplishing such functionality and would have recognized Hardt as an obvious solution that aligns with Lee's native teachings and that was well within a POSITA's technical grasp. *KSR Int'l Co.*, 550 U.S. 398 at 421 ("When there is a design need . . . and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense."); *see also In re Translogic*

Technology, Inc., 504 F.3d 1249, 1262 (Fed. Cir 2007) (“[I]n looking for a multiplexer circuit for the individual 2:1 multiplexers disclosed in Gorai, a person of ordinary skill in the art would have solved this design need by ‘pursu[ing] known options within his or her technical grasp.’”).

[1(c)(iii)] determine whether the end user profile contains a previous association between the relying party email address and a cloaked relying party email address, wherein the relying party email address has a different domain than the cloaked relying party email address;

Lee discloses this limitation for at least the same reasons as presented for limitation 13(c). *See supra* Section V.A.i.13(c).

[1(c)(iv)] 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 and associate the new cloaked relying party email address to the end user profile, the cloaked end user address and any of the said associated relying-party URLs, wherein the new cloaked relying party email address is generated with a domain different than the relying party address; and

Lee in combination with Hardt discloses this limitation. Lee discloses this limitation with the exception of “and any of the said associated relying-party URLs[.]” *See supra* Section V.A.i.13(d). The Lee-Hardt combination teaches adding a URL to the key 1 record. *See supra* Section V.B.i.1(c)(ii).c. Since the URL is contained in the key 1 record which also has an XLATE_FROM value (cloaked relying party email address) (*See supra* Section V.A.i.13(d)) this element is satisfied by the Lee-Hardt combination. *Dec.*, ¶110.

[1(c)(v)] 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.

Lee discloses this limitation for at least the same reasons presented above for 13(e). *See supra* Section V.A.i.13(e).

ii. Claim 2

The ID cloaking system of claim 1, wherein the new cloaked relying party email address has a domain that is the same as the cloaked end user address.

Lee discloses this limitation for at least the same reasons presented above for claim 14. *See supra* Section V.A.ii.14.

iii. Claim 7

[7(P)] A non-transitory computer readable medium for a ID cloaking system having instructions stored thereon that are executable by processor electronics to:

To the extent the preamble is limiting, Lee discloses this limitation for at least the same reasons presented above for 13(Preamble). *See supra* Section V.A.i.13(P).

[7(a)] 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;

Lee discloses this limitation for at least the same reasons presented above for limitation 13(a). *See supra* Section V.A.i.13(a).

[7(b)] identify an end user specified address as well as any URLs associated to the cloaked end user address by an end user profile;

Lee in combination with Hardt teaches this limitation for at least the same reasons presented above for limitation 1(c)(ii). *See supra* Section V.B.i.1(c)(ii).

[7(c)] 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;

Lee discloses this limitation for at least the same reasons presented above for limitation 13(c). *See supra* Section V.A.i.13(c).

[7(d)] 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 and any of the said associated relying-party URLs, wherein the new cloaked relying party email address is generated with a domain different than the relying party address; and

The combination of Lee and Hardt teaches this limitation for at least the same reasons presented above for limitation 1(c)(iv). *See supra* Section V.B.i.1(c)(iv).

[7(e)] 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.

Lee discloses this limitation for at least the same reasons presented above for limitation 13(e). *See supra* Section V.A.i.13(e).

iv. Claim 8

The non-transitory computer readable medium of claim 7, wherein the new cloaked relying party email address has a domain that is the same as the cloaked end user address.

Lee discloses this limitation for at least the same reasons presented above for claim 14. *See supra* Section V.A.ii.14.

v. Claim 19

The non-transitory computer readable medium of claim 13, wherein the user profile is further comprised of at least one URL associated to the cloaked end user address.

The combination of Lee and Hardt teaches this limitation. Where a user registers a key 1 record using the Lee-Hardt combination by filling in a webform, the “form filler provides the URL of the form” to the key 1 record as a value to a URL field. *Hardt*, 20:4-9; *See supra* Section V.B.1(c)(ii).c. Because the key 1 record contains both the URL of the webform and the user’s private address, the Lee-Hardt combination discloses this limitation. *Dec.*, ¶120.

C. Ground 3 & 4: Claims 15-18 are obvious under AIA 35 U.S.C. § 103 over *Lee* in view of *Le Jouan* and claims 3-6 and 9-12 are obvious under AIA 35 U.S.C. § 103 over *Lee* in view of *Hardt* and in further view of *Le Jouan*.

The remaining claims recite limitations directed to identifying and processing “cloaked placeholders” within emails. For example, Claim 6 recites an additional step in which the user profile is configured to remove the user’s name from an email, replacing it with cloaked/alias information and protecting the privacy of the user. As set forth in Grounds 1 and 2, Lee alone and the combination of Lee and Hardt disclose all the limitations of the independent claims underlying the additional claims addressed here in Grounds 3 and 4, including limitations directed to cloaking both the end user’s email address and the sender’s email address. As set forth in detail below, a POSITA would have been motivated to modify Lee (alone or in

combination with Hardt) to additionally cloak the user's personal information pursuant to Le Jouan. Le Jouan discloses a controlled data management system with an email personalization engine 514 that is capable of creating dummy values for personal user information and to cloak and de-cloak that information, protecting the user's privacy. *Le Jouan*, [0144-45] ("When a user sends an email to a third party entity, the email personalization engine 514 can remove sensitive information, replace the sensitive information with dummy values or aliases, or the like."). Further, Le Jouan discloses that user's personal information can include a name, among other identifying information. *Id.*, [0030].

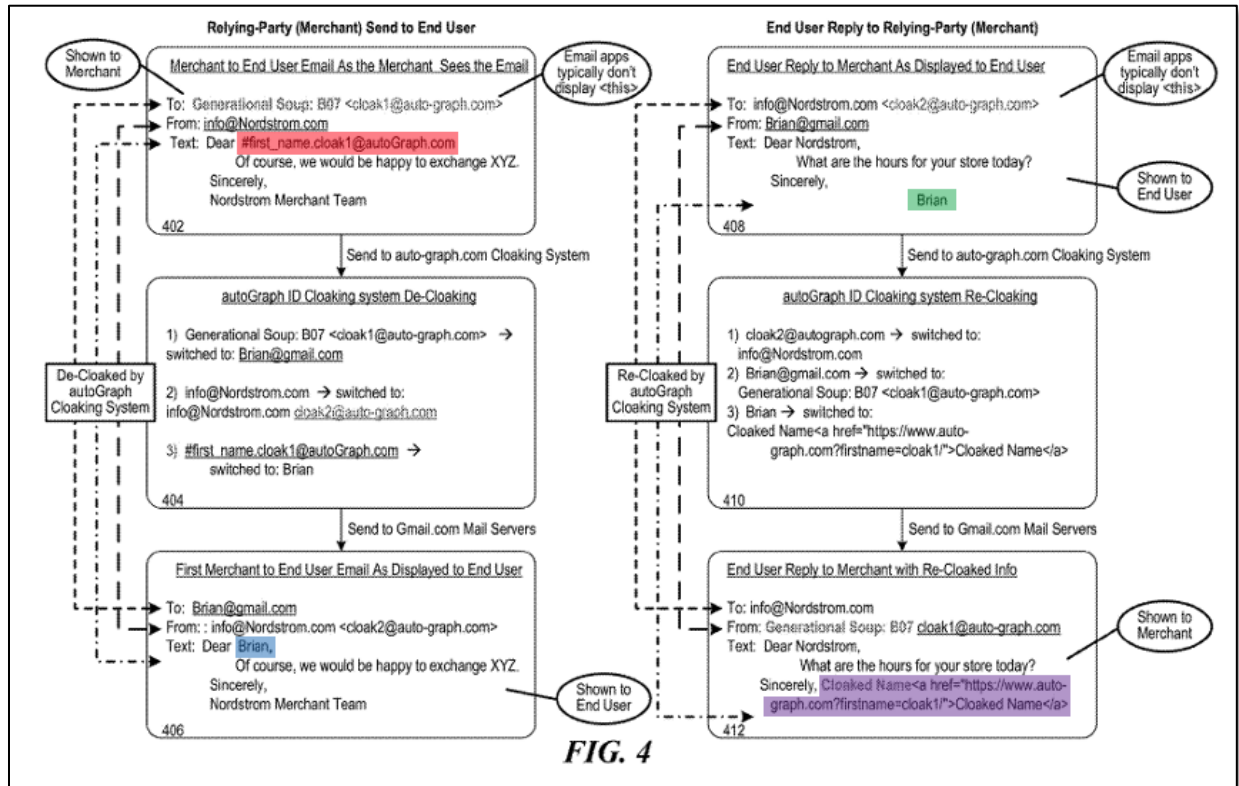
Ground 3: Claims 15-18 are obvious over Lee in view of Le Jouan

i. Claim 15

The non-transitory computer readable medium of claim 13, further comprising instructions that are executable by the processor electronics to cause the processor electronics to determine if the email comprises a cloaked placeholder.

The combination of Lee and Le Jouan render obvious this limitation. The '107 Patent teaches that "cloaked placeholders" may be used to cloak personal information contained in an email. '107 Patent, 11:39-51. Fig. 4 illustrates this process in both the merchant->consumer direction and the consumer->merchant direction. As illustrated on the left, a merchant may send an email to the consumer, using a **placeholder for the consumer's name**, which the cloaking system will replace with the **user's actual name** when the email is delivered. In the opposite direction, as illustrated on the right, a consumer may draft an email including their **actual name**,

which the system can identify and replace with a **cloaked placeholder** before delivering the message to the merchant.



Id., Fig. 4 (annotated).

a. *Le Jouan's Teachings*

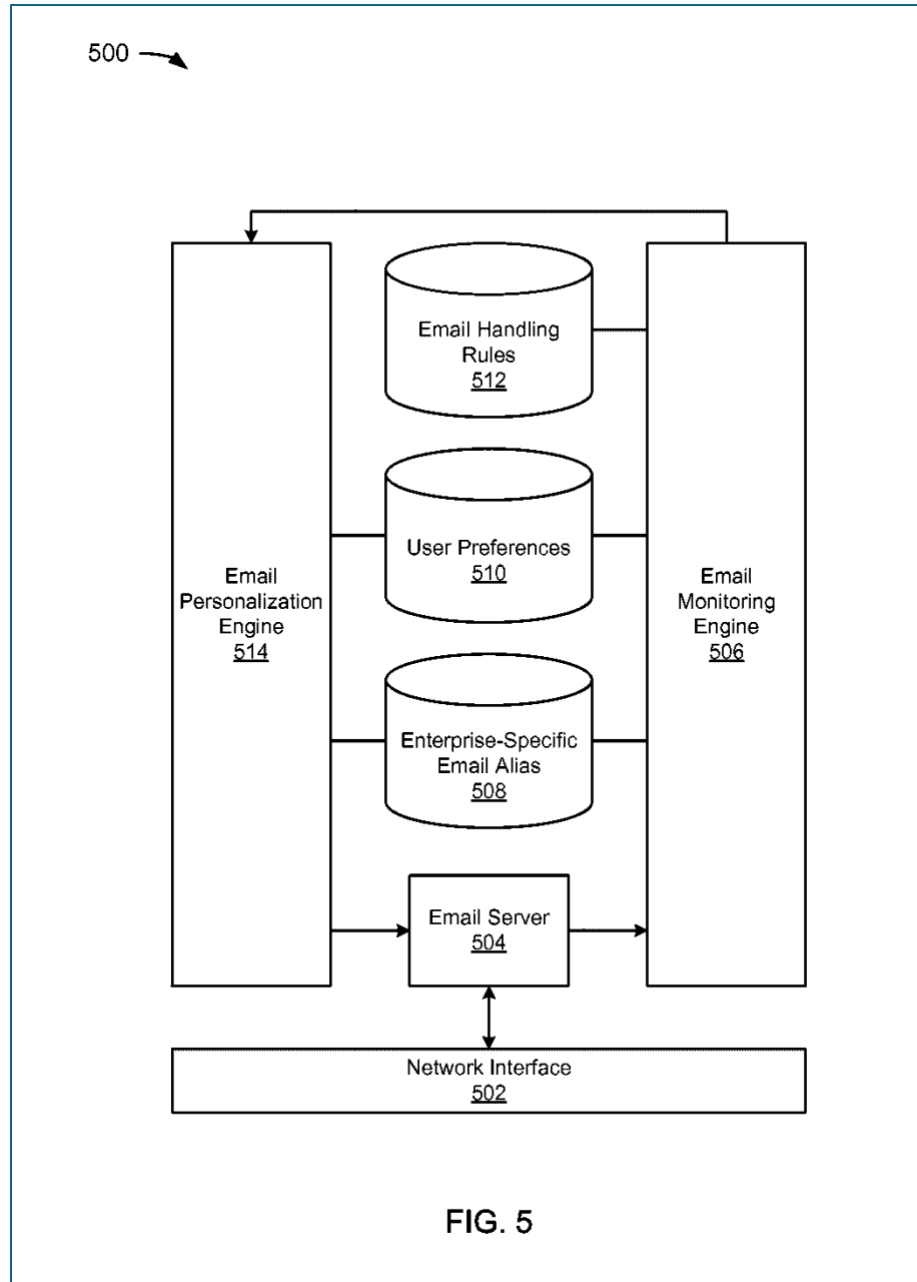
Like the '107 Patent, Le Jouan describes a system that “[protects] personal information by generating entity-specific aliases for use in communication with third parties[.]” *Le Jouan*, Abstract. “[P]ersonal information can include name, important anniversaries, home address, business address, home phone, home fax, cell phone, business phone, business fax, personal email” among other information that is associated with a user. *Le Jouan*, [0033]. Le Jouan teaches that, not only can a user’s

email address be cloaked with an email alias, but a user's personal information can also be cloaked, maintaining more comprehensive anonymity:

In a specific implementation, ***the aliased information includes an email alias***. In alternative implementations, the aliased information could include ***an aliased phone number, an aliased name*** (e.g., a doing-business-as "DBA" name), ***an aliased address*** (e.g., a post office box), or the like.

Id., [0066].

Relevant to this petition, Le Jouan discloses an embodiment of an alias-aware email server system 500. *Id.*, [0136], FIG. 5. The architecture of the email server system is shown in FIG. 5 below.



Le Jouan, FIG. 5. The alias aware email server system 500 includes an email personalization engine 514 that can replace sensitive personal information with aliases or dummy values in an outgoing email from a user to a third party:

When a user sends an email to a third party entity, ***the email personalization engine 514 can remove sensitive information, replace***

the sensitive information with dummy values or aliases, or the like.

While the email personalization engine 514 can be configured to automatically identify certain character strings that are likely to include sensitive information, *such as email addresses, URLs, phone numbers, credit card numbers*, or other character strings that have distinctive formats[.]

Id., [0144]. The email personalization engine also works for incoming emails, replacing dummy values or aliases in an email from a third party with actual values:

When a user receives email from a third party entity, *the email personalization engine 514 can update the email with useful information*. For example, the user's email alias can be replaced with the user's actual email address so that the message can be sent to the user . . . [and] *aliases or dummy values could be replaced or the actual values could be added parenthetically next to the aliases or dummy values*[.]

Id., [0145].

Although Le Jouan does not expressly mention a user's name as sensitive information that may be anonymized within this Fig. 5 embodiment, a POSITA would have understood that a user's name falls within the category of sensitive information to which this embodiment is directed (or at least would have been motivated to anonymize a user's name consistent with this embodiment). *Dec.*, ¶125. Indeed, Le Jouan defines “‘sensitive information’ [as] *personal information that is useful for* contacting or *identifying the user outside of the system* 300, such as an

email address, a physical address, a phone number, or the like.” *Le Jouan*, [0077].

Le Jouan contrasts such user-identifying “sensitive information” with data fields like a user ID from which the user’s identity cannot be ascertained. *Id.* (“Perhaps most information that a user would store in an address book could be considered sensitive information, but ***a userid that identifies the user only within a controlled data management system would not be considered sensitive information***, since ***that information would not enable a third party to identify the user*** without more.”). A POSITA would have understood that a user’s name (e.g., first name, last name, or full name) falls within the category of user-identifying sensitive information of the type Le Jouan’s email personalization engine is intended to cloak. *Dec.*, ¶125. (further noting that Le Jouan at [0066] expressly describes cloaking a name).

b. The Lee-Le Jouan Combination

The Lee-Le Jouan combination modifies the email proxy server of Lee with personal information aliasing taught by Le Jouan. Per this proposed modification, Lee’s key 1 record would contain fields for personal information (e.g. a NAME field) and associated aliases (e.g. a NAME_XLATE_TO field). *Dec.*, ¶126. When the user requests a public email address (i.e., Lee’s initial alias generation process), the user would be prompted to provide sensitive information (i.e., information to be cloaked) directly to the email proxy server. *Id.* Per Le Jouan’s teachings, dummy values would be created for each item of personal information in the same manner the public email

address is created. *Id.* For example, when a user requests a public email, the user would provide their name by filling in a NAME field, the proxy server would generate a dummy value for this name (e.g., “Name1”) and store it in a key 1 data field (e.g., NAME_XLATE_TO). *Id.* When an email is received, the email proxy server would run a modified filter/translate algorithm that searches for character string matching a dummy value (e.g., Name1) and replaces the dummy value with the correct personal information (e.g., the user’s name) in the manner disclosed by Le Jouan. *Id.*

Relevant to claim 15, in the proposed combination, when an email is received by the email proxy server, the email personalization engine 514 identifies any dummy values in the email (“cloaked placeholder”) and “update[s] the email with useful information” such as the user’s actual name, rather than the public/alias name. *Le Jouan*, [0145].

c. Motivation to Combine Lee with Le Jouan

A POSITA would have been motivated and found it obvious to combine the email proxy server of Lee with the functions of the email personalization engine 514 taught by Le Jouan. *Dec.*, ¶128. First, a POSITA would have recognized that replacing sensitive information with dummy values when sending emails to a third party and replacing those dummy values with the actual values when receiving emails from a third party as taught by Le Jouan would benefit the email proxy server

of Lee in the same way it benefits Le Jouan. Namely, as Le Jouan expressly teaches, this protects personal information included in the body of emails. *Dec.*, ¶128; *KSR Int'l Co.*, 550 U.S. 398 at 417 (“[I]f a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious[.]”); *see Le Jouan*, [0144] (system automatically identifies character strings in emails that include sensitive information and replaces the strings with dummy values). A POSITA would have recognized that such functionality desirably provides users the ability to protect personal information included in emails received and processed by the email proxy server of Lee. *Dec.*, ¶128 (describing the widely acknowledged issue of preventing web-based bad actors from obtaining personal information and noting these concerns were not limited to private email addresses, but instead acknowledged the need to protect any information from which a user’s identity may be ascertained).

Supporting the conclusion that it would have been obvious to benefit Lee’s system with the protection of other information as taught by Le Jouan, Lee and Le Jouan describe “similar devices.” For example, each reference discloses a system to hide the end user’s actual email address from third parties (the email proxy server of Lee and the email server system 500 of Le Jouan). *Compare Lee*, Abstract, with *Le Jouan*, [0136]. Each system also teaches storing personal information and aliases associated to the user including the user’s personal email address and one or more

public/aliased addresses. *Compare Lee*, 6:9-32 (discussing the key 1 record), with *Le Jouan*, [0132].

Based on these similarities and the straightforward nature of the proposed combination, a POSITA would also have had a reasonable expectation of success in making the proposed combination. Indeed, improving *Lee* to store additional values for personal information, associated dummy values, and to recognize and replace the dummy values with actual information would be well within the skill of a POSITA. *Dec.*, ¶130. Adding additional fields to the key 1 record and replacing dummy values with actual values are both simple changes implemented via software—the nature of which would have been well within the capabilities of a POSITA. *Id.*

ii. Claim 16

The non-transitory computer readable medium of claim 15, further comprising instructions that are executable by the processor electronics to cause the processor electronics to replace the cloaked placeholder with end user specified information from the end user profile.

Le Jouan discloses replacing aliases or dummy values with actual values. See *supra* Section V.C.i.b. In the *Lee-Le Jouan* combination, the key 1 record includes fields for personal information and fields for dummy values relating to said personal information (end user specified information). See *supra* Section V.C.i.b. When an email is received the email proxy server identifies any dummy values included in the email and replaces each dummy value with the associated value from the key 1

record (“end user profile”). See *Le Jouan*, [0145]. A POSITA would understand that this function is implemented via the processor electronics of Lee. *Dec.*, ¶131.

iii. Claim 17

The non-transitory computer readable medium of claim 13, wherein the user profile is further comprised of an end user first name.

The combination of Lee and Le Jouan teaches this element. The Lee-Le Jouan combination teaches storing a variety of personal information of a user’s choice in the key 1 record. See *supra* Section V.C.i.b. Le Jouan discloses that “personal information can include name,” and a POSITA would understand that the name can be any part of a user’s full name, including a first name. *Le Jouan*, [0033], *Dec.*, ¶132. Therefore, the Lee-Le Jouan combination can include a field for first name in the key 1 record. *Id.*

iv. Claim 18

The non-transitory computer readable medium of claim 17, wherein the user profile was configured by the end user to associate the end user first name with a cloaked end user first name placeholder.

The Lee-Le Jouan combination teaches the user providing personal information to the email proxy system, which includes the functionality of the email personalization engine 514 of Le Jouan. *Le Jouan* [0144]. The user can choose what information to provide to key 1 record. See *Le Jouan*, [0144]; See *supra* Section V.C.i.b. The information provided by the user may include first name. See *supra* Section V.C.i. A POSITA would understand that the user’s first name would be

associated with a dummy value (“cloaked end user first name placeholder”) in the key 1 record so that the dummy value can be replaced with the actual value. *Dec.*, ¶133; *See supra* Section V.C.i.b. Further, the user may configure the key 1 record to store a first name and cloaked first name placeholder in the Lee-Le Jouan combination. *See supra* Section V.C.i.b.

Ground 4: Claims 3-6 and 9-12 are obvious over *Lee* in view of *Hardt* and in further view of *Le Jouan*

As set forth in Ground 3 above, a POSITA would have been motivated to modify Lee pursuant to Le Jouan, satisfying the personal information cloaking limitations of Claims 15-18. Claims 3-6 and 9-12 are materially identical to Claims 15-18, but for their respective underlying independent claims. As noted above, independent claims 1 and 7 are substantively identical to independent claim 13, but for their addition of URL limitations. Ground 2 established that independent claims 1 and 7 are obvious over Lee in view of Hardt, pointing to Hardt’s URL teachings, but otherwise relying on the same Lee teachings as set forth in Ground 1 for independent claims 13.

Relevant to dependent Claims 3-6 and 9-12, a POSITA would have been motivated and found it obvious to modify the Lee-Hardt combination set forth in Ground 2 pursuant to Le Jouan’s personal information cloaking teachings for the same reasons set forth in Ground 3 above. *See Intell. Ventures II LLC v. Ericsson Inc.*, 685 F. App’x 913, 917 (Fed. Cir. 2017) (nonprecedential) (noting “[t]here is no

per se rule that requires each subset of prior art references to be independently combined” where each secondary reference can be combined through the primary reference). Indeed, a POSITA would recognize the addition of Hardt’s URL functionalities in Lee’s system would have no impact on the motivation to also add Le Jouan’s personal information cloaking teachings. *Dec.*, ¶135 (explaining that the URL functionalities from Hardt and personal information cloaking functionalities from Le Jouan function independently of one another and the inclusion of one would have no bearing on the inclusion of the other). A POSITA would have had little difficulty modifying the structure of the key 1 record and the filter/translate algorithm of Lee to contain the desired functionality of both Hardt and Le Jouan. *Id.* Accordingly, Ground 4 renders obvious Claims 3-6 and 9-12 over Lee in view of Hardt and Le Jouan for the same reasons as set forth in Ground 3 above, discussing Lee in view of Le Jouan.

v. Claim 3

The ID cloaking system of claim 1, further comprising instructions that are executable by the processor electronics to cause the processor electronics to determine if the email comprises a cloaked placeholder.

The combination of Lee, Hardt, and Le Jouan discloses this limitation for at least the same reasons presented above for claim 15. *See supra* Section V.C.i; *see also* Section V.B.i.

vi. Claim 4

The ID cloaking system of claim 3, further comprising instructions that are executable by the processor electronics to cause the processor electronics to replace the cloaked placeholder with end user specified information from the end user profile.

The combination of Lee, Hardt, and Le Jouan discloses this limitation for at least the same reasons presented above for claim 16. *See supra* Section V.C.ii; *see also* Section V.B.i.

vii. Claim 5

The ID cloaking system of claim 1, wherein the user profile is further comprised of an end user first name.

The combination of Lee, Hardt, and Le Jouan discloses this limitation for at least the same reasons presented above for claim 17. *See supra* Section V.C.iii; *see also* Section V.B.i.

viii. Claim 6

The ID cloaking system of claim 5, wherein the user profile was configured by the end user to associate the end user first name with a cloaked end user first name placeholder.

The combination of Lee, Hardt, and Le Jouan discloses this limitation for at least the same reasons presented above for claim 18. *See supra* Section V.C.iv; *see also* Section V.B.i.

ix. Claim 9

The non-transitory computer readable medium of claim 7, further comprising instructions that are executable by the processor electronics to cause the processor electronics to determine if the email comprises a cloaked placeholder.

The combination of Lee, Hardt, and Le Jouan discloses this limitation for at least the same reasons presented above for claim 15. *See supra* Section V.C.i; *see also* Section V.B.ii.

x. Claim 10

The non-transitory computer readable medium of claim 9, further comprising instructions that are executable by the processor electronics to cause the processor electronics to replace the cloaked placeholder with end user specified information from the end user profile.

The combination of Lee, Hardt, and Le Jouan discloses this limitation for at least the same reasons presented above for claim 16. *See supra* Section V.C.ii; *see also* Section V.B.ii.

xi. Claim 11

The non-transitory computer readable medium of claim 7, wherein the user profile is further comprised of an end user first name.

The combination of Lee, Hardt, and Le Jouan discloses this limitation for at least the same reasons presented above for claim 17. *See supra* Section V.C.iii; *see also* Section V.B.ii.

xii. Claim 12

The non-transitory computer readable medium of claim 11, wherein the user profile was configured by the end user to associate the end user first name with a cloaked end user first name placeholder.

The combination of Lee, Hardt, and Le Jouan discloses this limitation for at least the same reasons presented above for claim 18. *See supra* Section V.C.iv; *see also* V.B.ii.

VI. THE *FINTIV* FACTORS FAVOR INSTITUTION

Under the “*Fintiv* factors,” the Board may consider parallel litigation, including an early trial date, in determining whether to institute under 35 U.S.C. § 314(a). *NHK Spring Co., Ltd., v. Intri-Plex Technologies, Inc.*, IPR2018-00752, Paper 8 at 19–20 (PTAB Sept. 12, 2018) (precedential); *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 at 2–3, 6 (PTAB Mar. 20, 2020) (precedential).

Those factors strongly favor institution here. Indeed, the parallel litigation has not yet progressed beyond the pleadings stage. *See* Ex. 1007. Petitioner filed a motion to dismiss the initial Complaint for failure to state a claim, arguing that the ’107 Patent claims are directed to patent ineligible subject matter under 35 U.S.C. §101. *Id.* (*see* Dkt. Nos. 12 and 13). Patent Owner then amended its complaint, rendering that motion to dismiss moot. *Id.* (*see* Dkt. No. 20). Petitioner filed a motion to dismiss the first amended complaint, again based on patent ineligibility under 35 U.S.C. §101. *Id.* (*see* Dkt. Nos. 23 and 24). A hearing was held on the motion to dismiss on March 21, 2024, and the Court issued an order granting Patent Owner

leave to amend its complaint yet again. *Id.* (see Dkt. Nos. 32 and 33). Patent Owner did so on May 3, 2024, and Petitioner filed another motion to dismiss for patent ineligibility under 35 U.S.C. §101. *Id.* (see Dkt. Nos. 35, 41 and 42). A hearing on the motion to dismiss for the second amended complaint was held on August 15, 2024. *Id.* (see Dkt. No. 51). The Court has not issued an order regarding the motion to dismiss as of the filing of this Petition. *Id.*

A. Stay

Parallel litigation is ongoing. While no stay has been requested, Petitioner may seek a stay if institution is granted, thus favoring institution. District statistics strongly suggest such a request would be granted. *Stay Article* (Ex. 1016) (noting that 79% of stay motions are granted and that stay motions may be denied if the IPR challenges only some asserted claims). Because the instant IPR is filed early in the litigation schedule and challenges all asserted claims, a stay is likely to be granted.

B. Proximity of the Court’s Trial Date

“This factor looks at the *proximity* of the trial date to the date of [FWD] to assess the weight to be accorded a trial date set earlier than the expected [FWD] date.” *Shenzhen Carku Tech. Co., Ltd. v. The Noco Co.*, IPR2020-00944, Paper 20 at 61 (PTAB Nov. 12, 2020). Because the parallel litigation has not advanced beyond the pleadings stages, no schedule exists, and this factor weighs heavily in favor of institution.

C. Investment in Parallel Proceeding

The district court case is in its infancy. Petitioner filed motions to dismiss each of Patent Owner's three complaints. The Petitioner has challenged the patentability of the '107 Patent's claims under 35 U.S.C. § 101 in each of its motions to dismiss. So far, the Patent Owner has twice amended its complaint to address this argument to no avail. No other investments have been made in the parallel proceeding, strongly favoring institution.

D. Overlap

No contentions have been served in the parallel proceeding, so there is currently no overlap in prior art. Further, this petition challenges all of the claims of the '107 Patent, and Patent Owner has alleged only that Apple infringes claim 13 in the parallel litigation. Ex. 1008, 20. Therefore, it is likely the District Court will not address the validity of a significant number of the '107 Patent claims. *See Apple Inc. v. Seven Networks, LLC*, No. IPR2020-00506, Paper 11 at 14-15 (P.T.A.B. Sept. 1, 2020) (finding overlap weighs against denying institution when petition challenges twenty-six claims and only four claims are asserted in litigation); *see also Samsung Bioepis Co., Ltd. v. Regeneron Pharms., Inc.*, No. IPR2023-00884, Paper 13 at 70-72 (P.T.A.B. Nov. 17, 2023) (finding petition where every claim is at issue while only a few claims are actively litigated weighs against denying institution).

E. Same Party

The Parties are the same. However, members of the Board have noted *Fintiv* addresses only the scenario where the petitioner is unrelated to the defendants in litigation, which weighs against denying institution, but *Fintiv* “says nothing about situations in which the petitioner is the same as, or is related to, the district court defendant.” *Cisco Sys., Inc. v. Ramot at Tel Aviv Univ. Ltd.*, IPR2020-00122, Paper 15 at 10-11 (PTAB May 15, 2020) (APJ Crumbley, dissenting) (disfavoring a “defendant in the district court” is “contrary to the goal of providing district court litigants an alternative venue to resolve questions of patentability”).

F. Other Circumstances

“[W]here the PTAB determines that the information presented at the institution stage presents a compelling unpatentability challenge, **that determination alone** demonstrates that the PTAB should not discretionarily deny institution under *Fintiv*.” *Hewlett Packard Enterprise Co., et al. v. Billjco LLC*, IPR2022-00420, Paper 17, at 6 (PTAB July 12, 2022) (“[c]ompelling, meritorious challenges are those in which the evidence, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence”). The strength of Petitioner’s Proposed Grounds weighs strongly in favor of institution. *Id.* (refusing to deny institution under *Fintiv* based solely on the strength of Petitioner’s grounds).

VII. CONCLUSION

For the foregoing reasons, Petitioner respectfully requests *inter partes* review of Claims 1-19 of the '107 Patent.

Respectfully submitted,

By: /s/ Paul R. Hart
Paul R. Hart, Reg. No. 59,646
Adam P. Seitz, Reg. No. 52,206

COUNSEL FOR PETITIONER

IX. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(A)(1)

A. Real Party-In-Interest

Petitioner is the real party-in-interest. 37 C.F.R. § 42.8(b)(1).

B. Related Matters

Pursuant to 37 C.F.R. § 42.8(b)(2), Petitioner is aware of the following matter involving the '107 Patent:

- *Rally AG LLC v. Apple Inc.*, No. 1-23-cv-01106 (D. Del.).

C. Lead and Back-Up Counsel

Petitioner provides the following designation and service information for lead and back-up counsel. 37 C.F.R. § 42.8(b)(3) and (b)(4).

Lead Counsel	Back-Up Counsel
Paul R. Hart (Reg. No. 59,646) Paul.Hart@eriseip.com PTAB@eriseip.com <u>Postal and Hand-Delivery Address:</u> Erise IP, P.A. 717 17 th St., Suite 1400 Denver, Colorado 80202 Telephone: (913) 777-5600 Fax: (913) 777-5601	Adam P. Seitz (Reg. No. 52,206) Adam.Seitz@eriseip.com PTAB@eriseip.com <u>Postal and Hand-Delivery Address:</u> Erise IP, P.A. 7015 College Blvd., Ste. 700 Overland Park, Kansas 66211 Telephone: (913) 777-5600 Fax: (913) 777-5601

APPENDIX OF EXHIBITS

Exhibit 1001	U.S. Patent No. 11,361,107 (the “’107 Patent”)
Exhibit 1002	File History for U.S. Patent No. 11,361,107
Exhibit 1003	Declaration of Dr. Loren Terveen
Exhibit 1004	U.S. Patent No. 8,458,264 to Lee, et al. (“ <i>Lee</i> ”)
Exhibit 1005	U.S. Patent No. 7,783,741 to Hardt (“ <i>Hardt</i> ”)
Exhibit 1006	U.S. Patent Publication No. 2016/0323229 to Le Jouan (“ <i>Le Jouan</i> ”)
Exhibit 1007	<i>Rally AG LLC v. Apple, Inc.</i> , 1:23-cv-01106 (D. Del.), Docket as of September 27, 2024
Exhibit 1008	Second Amended Complaint, 1:23-cv-01106 (D. Del.), No. 35
Exhibit 1009	Joon S. Park, Hsin-Yang Lu, and Chia-Jung Tsui, <i>Anti-Spam Approaches: Analyses and Comparisons</i> , The Open Information Systems Journal 3, 36-47 (2009).
Exhibit 1010	<i>Basics: What is a URL?</i> , https://zvelo.com/anatomy-of-full-path-url-hostname-protocol-path-more/ (Last visited July 26, 2024)
Exhibit 1011	U.S. Patent Publication No. 2019/0288987 to Paulramachandran et al.
Exhibit 1012	U.S. Patent No. 7,558,829 to Perlman et al.
Exhibit 1013	U.S. Patent No. 9,401,886 to Bastide et al.
Exhibit 1014	U.S. Patent Publication No. 2007/0180039 to Sutidze et al.
Exhibit 1015	RFC 2822, <i>Internet Message Format</i> , The Internet Society, Apr. 2001
Exhibit 1016	“Trending at the PTAB: When to Ask Court for Litigation Stay,” March 30, 2023 (“ <i>Stay Article</i> ”)

CERTIFICATION OF WORD COUNT

The undersigned certifies pursuant to 37 C.F.R. § 42.24 that the foregoing Petition for *Inter Partes* Review, excluding any table of contents, mandatory notices under 37 C.F.R. § 42.8, certificates of service or word count, or appendix of exhibits, contains 13,924 words according to the word-processing program used to prepare this document (Microsoft Word).

Dated: October 2, 2024

By: /s/ Paul R. Hart
Paul R. Hart, Reg. No. 59,646

COUNSEL FOR PETITIONER

CERTIFICATE OF SERVICE ON PATENT OWNER
UNDER 37 C.F.R. § 42.105

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105, the undersigned certifies that on October 2, 2024, a complete and entire copy of this Petition for *Inter Partes* Review including exhibits was provided via Federal Express to the Patent Owner by serving the correspondence address of record for the '107 Patent as listed on PAIR:

LKGLOBAL/Rally AG, LLC.
7501 East McCormick Parkway
Suite 105 South
Scottsdale, AZ 85258

Further, a courtesy copy of this Petition for *Inter Partes* Review was sent via email to Patent Owner's litigation counsel:

Rodger Dallery Smith, II (rsmith@morrisnichols.com)
Lucinda Cole Cucuzzella (ccucuzzella@morrisnichols.com)
Bruce J. Rose (brucerose@mvalaw.com)
Samuel C. Merritt (sammerritt@mvalaw.com)
Clara G. Ilkka (clarailkka@mvalaw.com)

By: /s/ Paul R. Hart
Paul R. Hart, Reg. No. 59,646

COUNSEL FOR PETITIONER