

**No. 21-2203**

---

**IN THE UNITED STATES COURT OF APPEALS  
FOR THE FEDERAL CIRCUIT**

---

**BLIX, INC.**

*Plaintiff-Appellant*

v.

**APPLE, INC.**

*Defendant-Appellee.*

On Appeal from the United States District Court for the District of Delaware  
in Case No. 1:19-cv-1869  
Hon. Leonard P. Stark

---

**CORRECTED OPENING BRIEF FOR PLAINTIFF-APPELLANT BLIX  
INC.**

---

MARK C. RIFKIN  
THOMAS H. BURT  
LILLIAN R. GRINNELL  
**WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP**  
270 Madison Avenue, 9<sup>th</sup> Floor  
New York, New York 10016

GUY YONAY  
DANIEL J. MELMAN  
SARAH BENOWICH  
**PEARL COHEN ZEDEK LATZER BARATZ LLP**  
7 Times Square, 19<sup>th</sup> Floor  
New York, NY 10036

*Attorneys for Plaintiff-Appellant Blix Inc.*

**INDEPENDENT CLAIMS 1-5, 7-11, 13-15, 18, 21-24, 28-30, 33-37  
OF U.S. PATENT NO. 9,749,284 B2**

1. A method of performing controlled reciprocating communication, wherein said controlled reciprocating communication comprises an incoming and outgoing communications, between a first party and at least one second party, said method comprises: (a) providing at least one private interaction address of said first party; (b) defining at least one manageable public interaction address for said first party; (c) forming a record, wherein said manageable public interaction address is associated with said private interaction address for said first party; (d) receiving an incoming communication, said incoming communication comprises a communication from said second part to said first party; wherein said incoming communication is initiated by said second party to said manageable public interaction address of said first party; (e) identifying that said incoming communication was received to said manageable public interaction address; (f) accessing said record and performing at least one step selected from the group consisting of: (I) determining said respective identity associated with said manageable public interaction address identified in said incoming communication, and (II) determining said private interaction address of said first party associated at said record with said manageable public interaction address identified in said incoming communication; said method is characterized by: (g) generating at least one reverse list entry, wherein an interaction address of said second party is

associated at least with said manageable public interaction address of said first party; (h) performing a pre-interaction act, said pre-interaction act comprises: (I) accessing said reverse list; (II) identifying said interaction address of said second part in said reverse list; (III) determining that said manageable public interaction address of said first party is associated, at said reverse list, with said interaction address of said second party; (i) performing an outgoing communication, said outgoing communication comprises a communication from said first party to said second party, said outgoing communication is initiated by said first party; (j) said outgoing communication is characterized by that said outgoing communication, to said interaction address of said second party, is performed from said manageable public interaction address of said first party; wherein upon performing said outgoing communication, said second party is exposed merely to said manageable public interaction address of said first party; wherein said interaction address of said second party is obtainable from a third party or external services provider, wherein said at least one reverse list entry is formed by synchronizing said interaction address of said second party with said manageable public interaction address.

2. The method of performing controlled reciprocating communications as set forth in claim 1, wherein said steps of defining and forming further comprise: (a) defining a respective identity of said first party, for said manageable

public interaction address of said first party, and (b) forming a record associating said respective identity of said first party with said manageable public interaction address of said first party.

3. The method of performing controlled reciprocating communication as set forth in claim 2, wherein said step of determining further comprises determining that said interaction address of said second party is associated, at said reverse list, with said respective identity of said first party.

4. The method of performing controlled reciprocating communication, as set forth in claim 1, wherein said communication comprises a communication selected from the group consisting of: an attempted communication, incomplete communication, rejected communication, interrupted communication and abrupted communication.

5. The method of performing controlled reciprocating communication, as set forth in claim 1, wherein said interaction address selected from the group consisting of: a line telephone number, line facsimile number, cellular/mobile phone number, instant messaging (IM) name, e-mail address, presence screen name, service handle, universal resource identifier (URI), universal resource name (URN), universal resource locator (URL), extensive resource identified (XRI), SIP identifier, any type of user identifier for sharing or and any type of user identifier communication.

7. The method of performing controlled reciprocating communication, as set forth in claim 1, wherein said step of determining said private interaction address, during said step of accessing said record, further comprises performing at least one step selected from the group consisting of: (a) forwarding said incoming communication to said at least one private interaction address associated with said manageable public interaction address at said record; (b) forwarding information regarding said incoming communication to said at least one private interaction address associated with said manageable public interaction address at said record; (c) presenting said manageable public interaction address to which said incoming communication was received; (d) presenting at least one information item selected from the group consisting of: (I) a name assigned to said manageable public interaction address; (II) metadata assigned to said manageable public interaction address (III) public identity assigned to said manageable public interaction address; (e) applying a notification rule to said incoming communication; (f) selecting contents for said notification.

8. The method of performing controlled reciprocating communication, as set forth in claim 1, wherein said reverse list further comprises at least one constituent selected from the group consisting of: a name assigned to said manageable public interaction address; metadata assigned to said manageable public interaction address; a public identity assigned to said manageable public

interaction address; a rule relating to a notification; a content for said notification; a default communication preference; an overruling alternative for said default communication preference; personal information of said second party; contact information of said second party.

9. The method of performing controlled reciprocating communication, as set forth in claim 1, wherein generating said reverse list is performed by at least one selected from the group consisting of: said first party; a user of the system for controlled reciprocating communication; an operator of said system for controlled reciprocating communication; a third party related to said system for sustaining a controlled reciprocating communication, and external services providers for said system of sustaining a controlled reciprocating communication.

10. The method of performing controlled reciprocating communication, as set forth in claim 1, wherein said reverse list entry is generated in at least one manner selected from the group consisting of: manually by inputting said interaction address of said second party; upon receiving said incoming communication; upon performing said outgoing communication; by external services providers for a system for sustaining a controlled reciprocating communication.

11. The method of performing controlled reciprocating communication, as set forth in claim 1, wherein said interaction address of said second party is

unavailable to said first party, wherein at least a portion of said reverse list entry is confidential to said first party.

13. The method of performing controlled reciprocating communication, as set forth in claim 1, further comprises performing at least one predefined rule, said rule comprises at least one instruction for a predefined response, wherein said response selected from the group consisting of: rejecting a communication; recording a communication; converting a communication to another format; forwarding a communication to said private interaction address of said first party.

14. The method of performing controlled reciprocating communication, as set forth in claim 1, further comprises prescribing at least one communication preference selected from the group consisting of: a default communication preference and overruling alternative for said default communication preference, said communication preference is assigned to at least one selected from the group consisting of: (a) said private interaction address of said first party, contained in said record (b) said manageable public interaction address of said first party, contained in said record or said reverse list, and (c) said interaction address of said second party, contained in said reverse list.

15. The method of performing controlled reciprocating communication, as set forth in claim 1, further comprises prescribing at least one default communication preference, wherein said default communication preference

indicates said manageable public interaction address of said first party, determined at said step of determining during said pre-interaction act.

18. The method of performing controlled pre-interaction, as set forth in claim 17, wherein said method is not followed by a communication.

21. The method of performing controlled pre-interaction, as set forth in claim 17, further comprises performing at least one predefined rule, said rule comprises at least one instruction for a predefined response, wherein said response selected from the group consisting of: recording a communication, converting a communication to another format; forwarding a communication to said private interaction address of said first party.

22. The method of performing controlled pre-interaction, as set forth in claim 17, further comprises performing at least one predefined rule, said rule is assigned to at least one selected from the group consisting of: said private interaction address of said first party, contained in said record; said manageable public interaction address of said first party, contained in said record or said reverse list, and said interaction address of said second party, contained in said reverse list.

23. The method of performing controlled pre-interaction, as set forth in claim 17, further comprises prescribing at least one communication preference selected from the group consisting of: a default communication preference and



overruling alternative for said default communication preference said communication preference is assigned to at least one selected from the group consisting of: said private interaction address of said first party, contained in said record, said manageable public interaction address of said first party, contained in said record or said reverse list, and said interaction address of said second party, contained in said reverse list.

24. The method of performing controlled pre-interaction, as set forth in claim 17, further comprises prescribing at least one communication preference, wherein said default communication preference indicates said manageable public interaction address of said first party, determined at said step of determining during said pre-interaction act.

28. The system for performing a controlled pre-interaction, as set forth in claim 27, further comprises a networking terminal configured for a controlled outgoing communication, said controlled outgoing communication comprises a communication from said first party to said second party, said controlled outgoing communication is initiated by said first party, wherein initiating of said controlled outgoing communication, to said interaction address of said second party, is performed from said manageable public interaction address of said first party.

29. The system for performing a controlled pre-interaction, as set forth in claim 27, further comprises a networking terminal configured to receive said

incoming communication, wherein said receiving of said incoming communication is performed by at least one networking terminal selected from the group consisting of: (a) a networking terminal configured for receiving said incoming communication from said second party to said first party; wherein said incoming communication is initiated by said second party to said manageable public interaction address of said first party; (b) a networking terminal configured identifying that said incoming communication was received to said manageable public interaction address; (c) a networking terminal configured accessing said record and determining said respective identity associated with said manageable public interaction address identified with said means of identifying.

30. The system for performing a controlled pre-interaction, as set forth in claim 27, wherein said controlled pre-interaction is not followed by a communication.

33. The system for performing a controlled pre-interaction, as set forth in claim 27, further comprises at least one microprocessor configured for executing at least one pre-defined rule selected from the group consisting of: recording a communication, converting a communication to another format, forwarding a communication to said private interaction address of said first party.

34. The system for performing a controlled pre-interaction, as set forth in claim 27, further comprises at least one microprocessor configured for executing at

least one pre-defined rule, said rule is assigned to at least one member selected from the group consisting of: said private interaction address of said first party, contained in said record; said manageable public interaction of said first party, contained in said record or said reverse list, and said interaction address of said second party, contained in said reverse list.

35. The system for performing a controlled pre-interaction, as set forth in claim 27, further comprises at least one non-transitory computer storage memory configured to store therein at least one communication preference selected from the group consisting of: a default communication preference and overruling alternative for said default communication preference, said communication preference is assigned by said means of prescribing to at least one selected from the group consisting of: said private interaction address of said first party, contained in said record; said manageable public interaction address of said first party, contained in said record or said reverse list, and said interaction address of said second party, contained in said reverse list.

36. The system for performing a controlled pre-interaction, as set forth in claim 27, further comprises at least one non-transitory computer storage memory configured to store therein a preset content for a notification, said preset content for said notification selected from the group consisting of: text, alphanumeric data,

audio files, video files, graphics, hyperlinks and a template comprising at least one empty field, which is filled-in with content thereafter.

37. The system for performing a controlled pre-interaction, as set forth in claim 27, further comprises at least one non-transitory computer storage memory configured to store therein at least one default communication preference wherein said default communication preference indicates said manageable public interaction address of said first party, determined by said means of determining during said pre-interaction act.

**CERTIFICATE OF INTEREST**

Pursuant to Federal Circuit Rule 47.4, counsel for Plaintiff-Appellant, certifies the following:

1. The full name of the party represented by me is Blix, Inc.
2. The name of the real party in interest (if the party named in the caption is not the real party in interest) represented by me: N/A.
3. Parent corporations and publicly held companies that own 10% or more of stock in the party: N/A.
4. The names of all firms and the partners or associates that appeared for the party now represented by me in the trial court or are expected to appear in this Court (and who have not or will not enter an appearance in this case) are:

Shaoul Sussman (Pearl Cohen Zedek Latzer Baratz)  
Adam B. Wolfson (Quinn Emanuel Urquhart & Sullivan, LLP)  
Patrick Curran (Quinn Emanuel Urquhart & Sullivan, LLP)  
Stephen R. Neuwirth (Quinn Emanuel Urquhart & Sullivan, LLP)  
Stephen C. Cherny (Quinn Emanuel Urquhart & Sullivan, LLP)  
Andrew Colin Mayo (Ashby & Geddes, P.A.)  
John G. Day (Ashby & Geddes, P.A.)  
John W. Shaw (Shaw Keller LLP)  
David M. Fry (Shaw Keller LLP)  
Karen Elizabeth Keller (Shaw Keller LLP)

5. The title and number of any case known to counsel to be pending in this or any other court or agency that will directly affect or be directly affected by this court's decision in the pending appeal: N/A.
6. The organizational victims and bankruptcy cases applicable to this appeal: N/A.

Dated: November 3, 2021

/s/ Thomas H. Burt

THOMAS H. BURT

WOLF HALDENSTEIN  
ADLER FREEMAN & HERZ LLP  
270 Madison Avenue, 9<sup>th</sup> Floor  
New York, New York 10016  
(212) 545-4600

## **TABLE OF CONTENTS**

TABLE OF AUTHORITIES .....	iv
STATEMENT OF RELATED CASES .....	ix
JURISDICTIONAL STATEMENT .....	2
STATEMENT OF ISSUES .....	2
STATEMENT OF THE CASE.....	2
A.    Blix’s Asserted Patent .....	2
B.    The District Court Litigation .....	6
C.    The PTAB Has Denied Apple’s Request to Institute an IPR.....	7
D.    The Competitive Implications of Blix’s Technology.....	8
SUMMARY OF THE ARGUMENT .....	10
ARGUMENT .....	16
I.    STANDARD OF REVIEW.....	16
II.    THE DISTRICT COURT’S DISMISSAL OF THE ’284 PATENT CLAIM SHOULD BE REVERSED .....	17
A.    Determination of Patent Eligibility Under 35 U.S.C. § 101 .....	17
B.    The District Court Erred at Both Steps One and Two by Legally Determining Factual Questions .....	19
1.    The District Court’s Error at Step 1 .....	19
2.    The District Court’s Error at Step 2.....	24
III.    THE DISTRICT COURT’S DISMISSAL OF THE MONOPOLY MAINTENANCE CLAIM SHOULD BE REVERSED .....	28

A.	Apple’s Infringement of the ’284 Patent Constitutes Anticompetitive Conduct.....	31
B.	Apple Uses A “Moat” Around Its User Base to Preserve Its Mobile OS Monopoly .....	32
1.	Apple’s Sherlocking is the Entry Point of Its “Embrace and Extend Strategy” .....	34
2.	Apple Uses Its Monopoly to Bind Developers .....	37
C.	Apple’s Conduct Towards Blix Was Part of Its Anticompetitive “Sand in the Gears” Strategy” .....	40
1.	Apple’s Pretextual Exclusion and Audits of Blix.....	42
2.	Apple’s Pretextual Assertion of Privacy and Security Flaws.....	43
3.	Apple’s Pretextual Blocking of Publishing Updates .....	43
4.	Apple’s Refusal to Recognize Blix’s Name Change.....	44
D.	Apple’s Implementation of SIWA Is Anticompetitive .....	45
1.	Apple’s SIWA Implementation Prevents Competition by Impermissibly Bundling Its Offerings.....	47
2.	Apple’s Forcing of SIWA On Blix and Other Developers Blocks Messaging Bridge’s Disruptive Potential.....	49
IV.	THE DISMISSAL OF THE TYING CLAIM SHOULD BE REVERSED.....	49
A.	Standard .....	49
1.	Operating Systems and SSOs are Distinct Products.....	51
2.	Apple Has Monopoly Power in the OS Market.....	52
3.	Apple’s Tying Affected a Substantial Amount of Commerce .....	52
B.	A Free Product Can Result in Antitrust Liability.....	53



CONCLUSION.....	57
ADDENDUM	

## TABLE OF AUTHORITIES

### Cases

<i>Aatrix Software, Inc. v. Green Shades Software, Inc.</i> , 890 F.3d 1354 (Fed. Cir. 2018).....	16
<i>Aatrix Software, Inc. v. Green Shades Software, Inc.</i> , 882 F.3d 1121 (Fed. Cir. 2018).....	19, 24
<i>Abbott Labs. v. Teva Pharm. USA, Inc.</i> , 432 F. Supp. 2d 408 (D. Del. 2006).....	47
<i>Alice Corp. Pty. Ltd. v. CLS Bank Int'l</i> , 573 U.S. 208 (2014).....	<i>passim</i>
<i>Ancora Techs. v. HTC Am., Inc.</i> , 908 F.3d 1343 (Fed. Cir. 2018).....	22, 28
<i>Apple Inc. v. Blix Inc.</i> , No. IPR2020-01635 at 4, 2021 Pat. App. LEXIS 3259 (P.T.A.B. Apr. 19, 2021) .....	8, 27
<i>Apple Inc. v. Pepper</i> , 139 S. Ct. 1514 (2019).....	54, 57
<i>Avaya Inc., RP v. Telecom Labs, Inc.</i> , 838 F.3d 354 (3d Cir. 2016).....	50
<i>Behrend v. Comcast Corp.</i> , No. 03-6604, 2012 U.S. Dist. LEXIS 51889 (E.D. Pa. Apr. 12, 2012).....	55
<i>Berkheimer v. HP Inc.</i> , 881 F.3d 1360 (Fed. Cir. 2018).....	18, 23
<i>Bronowicz v. Allegheny Cty.</i> , 804 F.3d 338 (3d Cir. 2015).....	16
<i>In re Burlington Coat Factory Sec. Litig.</i> , 114 F.3d 1410 (3d Cir. 1997).....	16

<i>CardioNet, LLC v. InfoBionic, Inc.</i> , 955 F.3d 1358 (Fed. Cir. 2020).....	18
<i>Cellspin Soft, Inc. v. Fitbit, Inc.</i> , 927 F.3d 1306 (Fed. Cir. 2019).....	12
<i>Centocor Ortho Biotech, Inc. v. Abbott Labs.</i> , 636 F.3d 1341 (Fed. Cir. 2011).....	16
<i>Cosmokey Sols. GMBH &amp; Co. KG v. Duo Sec. LLC</i> , No. 2020-2043, 2021 U.S. App. LEXIS 29808 (Fed. Cir. Oct. 4, 2021) .....	<i>passim</i>
<i>Data Engine Techs. LLC v. Google LLC</i> , 906 F.3d 999 (Fed. Cir. 2018).....	22
<i>DDR Holdings, LLC v. Hotels.com, L.P.</i> , 773 F.3d 1245 (Fed. Cir. 2014).....	26
<i>Enfish, LLC v. Microsoft Corp.</i> , 822 F.3d 1327 (Fed. Cir. 2016).....	17
<i>Free Freehand Corp. v. Adobe Sys.</i> , 852 F. Supp. 2d 1171 (N.D. Cal. 2012).....	41, 54
<i>Glen Holly Entm't, Inc. v. Tektronix Inc.</i> , 352 F.3d 367 (9th Cir. 2003) .....	41
<i>IQVIA Inc. v. Veeva Sys.</i> , Civil Action No. 17-00177 (CCC), 2018 U.S. Dist. LEXIS 171456 (D.N.J. Oct. 3, 2018) .....	55
<i>Kickflip, Inc. v. Facebook, Inc.</i> , 999 F. Supp. 2d 677 (D. Del. 2013).....	49
<i>LePage's, Inc. v. 3M</i> , 324 F.3d 141 (3d Cir. 2003).....	29, 30

<i>Maio v. Aetna</i> , 221 F.3d 472 (3d Cir. 2000).....	16
<i>MAZ Encryption Techs. LLC v. Blackberry Corp.</i> , No. 13-304-LPS, 2016 U.S. Dist. LEXIS 134000 (D. Del. Sep. 29, 2016).....	21
<i>McRO, Inc. v. Bandai Namco Games Am. Inc.</i> , 837 F.3d 1299 (Fed. Cir. 2016).....	21
<i>Meijer, Inc. v. Ranbaxy Inc.</i> , No. 15-11828-NMG, 2016 U.S. Dist. LEXIS 120780 (D. Mass. June 16, 2016).....	45
<i>In re Neurontin Antitrust Litig.</i> , No. MDL No. 1479, 2013 U.S. Dist. LEXIS 111587 (D.N.J. Aug. 8, 2013) .....	30
<i>New York v. Actavis PLC</i> , 787 F.3d 638 (2d Cir. 2015).....	29
<i>Packet Intelligence LLC v. NetScout Sys.</i> , 965 F.3d 1299 (Fed. Cir. 2020).....	17, 18, 21
<i>Presque Isle Colon &amp; Rectal Surgery v. Highmark Health</i> , 391 F. Supp. 3d 485 (W.D. Pa. 2019).....	30, 42
<i>Prism Techs. LLC v. T-Mobile USA, Inc.</i> , 696 F. App'x 1014 (Fed. Cir. 2017) .....	5
<i>Rochester Drug Co-operative v. Braintree Labs.</i> , 712 F. Supp. 2d 308 (D. Del. 2010).....	14, 29
<i>Roxul USA, Inc. v. Armstrong World Indus.</i> , No. 17-1258, 2019 U.S. Dist. LEXIS 37926 (D. Del. Mar. 8, 2019).....	52, 53
<i>Spruill v. Gillis</i> , 372 F.3d 218 (3d Cir. 2004).....	16

<i>SRI Int'l, Inc. v. Cisco Sys.</i> , 930 F.3d 1295 (Fed. Cir. 2019).....	17, 23
<i>In re Suboxone (Buprenorphine Hydrochloride &amp; Naloxone) Antitrust Litig.</i> , 64 F. Supp. 3d 665 (E.D. Pa. 2014) .....	43
<i>TecSec Inc. v. Adobe Inc.</i> , 978 F.3d 1278 (Fed. Cir. 2020).....	10, 12, 19
<i>TQP Dev., LLC v. Intuit Inc.</i> , No. 2:12-CV-180-WCB, 2014 U.S. Dist. LEXIS 20077 (E.D. Tex. Feb. 19, 2014) .....	23
<i>Uniloc USA, Inc. v. LG Elecs. USA, Inc.</i> , 957 F.3d 1303 (Fed. Cir. 2020).....	17
<i>United States v. Microsoft Corp.</i> , 253 F.3d 34 (2001).....	<i>passim</i>
<i>Walgreen Co. v. Organon, Inc.</i> , 335 F. Supp. 2d 522 (D.N.J. 2004) .....	30

## **Statutes & Rules**

Federal Rules of Civil Procedure	
Rule 12 .....	12, 15
Rule 12(b)(6).....	16
Sherman Antitrust Act of 1890, 15 U.S.C. § 1, <i>et seq.</i>	
15 U.S.C. § 1 .....	<i>passim</i>
15 U.S.C. § 2 .....	<i>passim</i>
28 U.S.C. § 1295(a)(1).....	1
28 U.S.C. § 1331 .....	1
28 U.S.C. § 1338(a) .....	1
28 U.S.C. § 101 .....	1, 17

## **Other Authorities**

Assistant Att’y Gen. Makan Delrahim, <i>“I’m Free”: Platforms and Antitrust Enforcement in the ZeroPrice Economy</i> , Address at Silicon Flatirons Annual Tech. Policy Conference at the Univ. of Co. L. Sch. (Feb. 11, 2019).....	56
Guilio Federico, Fiona Scott Morton, and Carl Shapiro, <i>Antitrust and Innovation: Welcoming and Protecting Disruption</i> , Innovation Policy and the Economy, Vol 20 (NBER 2020) .....	36-37
Terrell McSweeney & Brian O’Dea, <i>Data, Innovation, and Potential Competition in Digital Markets—Looking     Beyond Short-Term Price Effects in Merger Analysis</i> , Fed. Trade Comm’n 2-3 (Feb. 22, 2018).....	56
John M. Newman, <i>Antitrust in Zero-Price Markets: Foundations</i> , 164 U. Pa. L. Rev. 149 (Dec. 2015).....	32
John M. Newman, <i>Antitrust in Zero-Price Markets: Applications</i> , 94 Wash. U. L. Rev. 49 (2016).....	56
Daniel L. Rubinfeld & Michael Gal, <i>The Hidden Costs of Free Goods: Implications for Antitrust Enforcement</i> , 80 Antitrust L.J. 521, 551 (2015-2016) .....	56
U.S. Dept. of Justice, <i>Competition and Monopoly: Single-Firm Conduct Under Section 2 of the     Sherman Act</i> , Sept. 2008.....	33
Tim Wu, <i>Blind Spot: The Attention Economy and the Law</i> , 82 Antitrust L.J. 771 (2019).....	56

**STATEMENT OF RELATED CASES**

Pursuant to Fed. Cir. R. 47.5(a), counsel for Blix Inc. states that no other appeal in or from the same case in the district court was previously before this or any other appellate court. Pursuant to Fed. Cir. R. 47.5(b), counsel is not aware of any other cases pending in this or any other court of agency that will directly affect or be directly affected by this Court's decision in the pending appeal.

### **JURISDICTIONAL STATEMENT**

In this patent infringement and antitrust matter brought by Plaintiff-Appellant Blix Inc. (“Blix”) against Defendant-Appellee Apple, Inc. (“Apple”) the United States District Court for the District of Delaware had jurisdiction under 28 U.S.C. §§ 1331 and 1338(a). The district court also had jurisdiction under 28 U.S.C. § 1331 over the monopoly maintenance claim brought under 15 U.S.C. § 2 and the monopoly tying claim based on 15 U.S.C. §§ 1 and 2.

After issuing an order holding that Blix’s asserted patent, U.S. Patent No. 9,749,284 (the “284 Patent” or the “Asserted Patent”), lacked patent-eligible subject matter pursuant to 35 U.S.C. § 101, the district court entered final judgment of ineligibility of the asserted claims. (*See Appx1*). It then entered final judgment as to the monopoly maintenance claim and monopoly tying claim, holding that the patent claim had been a fundamental premise of the claims brought under 15 U.S.C. § 2, and that the tying claim did not satisfy the requirements of 15 U.S.C. § 1.

The final judgments being appealed from were entered into on March 18, 2021, and July 9, 2021, and disposed of all issues in this case. Blix filed a timely notice of appeal on August 3, 2021. This Court has jurisdiction under 28 U.S.C. § 1295(a)(1).



### **STATEMENT OF ISSUES**

1. Whether the district court erred in determining that Blix's patent was directed to an abstract idea lacking an inventive concept, and thereby directed to patent-ineligible subject matter despite disputed questions of fact?
2. Whether Apple's infringement of Blix's patent constitutes anticompetitive conduct?
3. Whether a valid patent was necessary for Blix to establish a monopoly maintenance claim and a tying claim under Section 2 of the Sherman Act?
4. Whether the district court erred in dismissing Blix's tying claim under Sherman 1 of the Sherman Act by holding that because developers do not pay to buy iOS there cannot be an illegal tying arrangement?

### **STATEMENT OF THE CASE**

#### **A. Blix's Asserted Patent**

Blix is the owner of the '284 patent, entitled "Systems and Methods of Controlled Reciprocating Communication," (Appx1064) which was filed on May 13, 2013, and issued on August 29, 2017. The claims of the '284 Patent describe an innovative improvement to communications networks, and specifically, to managing secure interactions by employing private and public interaction addresses. This

innovation allows an ongoing two-way conversation, maintaining the user's anonymity, and with no intermediary having access to the user's real identity or control of the communication. It is a critical step forward in mobile technology.

The innovation covered by the '284 patent solves a problem caused by the fact that smartphone and mobile device users interact through their devices with a limitless variety of applications. This creates potentially conflicting needs for different aliases for each application to preserve the user's anonymity. To manage this situation, users and developers need privacy and efficiency in managing multiple aliases. The innovation covered by the '284 patent solves the potential conflict while also making the sign-in process easier and more efficient, thus ensuring both privacy and efficiency.

Complex multiple aliases for different applications raise the issue of "alias confusion," meaning: difficulty in determining which alias to use for which communication. In a conventional alias system, each user's private identity is matched with one single, fixed public identity for *all* communications. That system lacks full anonymity and is inefficient for two main reasons. *First*, the user must expose a public identity to the world that is the same for multiple recipients. Any one or more of those recipients who can cross-reference the public alias can then identify the private individual user. *Second*, the conventional alias system relies on a trusted human intermediary who becomes privy not only to the private identities

of both the first and second users, but also to the mosaic of information that comes from knowing the who, what, when, where, and how a person chooses to communicate. In other conventional systems, multiple or manageable aliases may be employed. While such variability improves security, it sacrifices constancy and caller recognition, which impedes efficient reciprocating electronic communication. The oversimplified analogies Apple presented, and which the district court erroneously accepted, exemplify these conventional systems but do not reflect the innovations of the '284 Patent.

The '284 Patent solves the problem of alias confusion and caller recognition using innovative technological means, by creating an entirely new data structure: the “reverse list” (*see, e.g.*, claim element 1(g)). The reverse list is a persistent memory that tracks corresponding aliases (first party manageable public addresses) with actual contact details (second party interaction address), so the anonymous sender knows from which alias to route outgoing communications, thereby making it recognizable to recipients without exposing confidential information (*see, e.g.*, claim elements 1(h), (j)). This solution reconciles the opposing demands of flexible addressing and caller recognition, a problem unsolved until the '284 Patent (by conventional or technical means).

Unlike the '284 Patent, other alias systems have several major flaws: (1) they sacrifice transparency – for example, the recipient is unable to recognize the caller

at all; (2) they are not perfectly anonymous – for example, they may have a single, fixed alias which can be revealed through cross-referencing; (3) they rely on trusted human intermediaries to manage the interactions; and (4) they are not flexible – *i.e.*, they do not allow for anonymous and reciprocal/two-way communication. Prior to the '284 Patent, there was no known way – conventional or otherwise – to efficiently provide secure reciprocal communications using a single alias that is anonymous, and both flexible (“manageable public interaction address”) and recognizable (known by the contacts in the “reverse list”).

This complex system of aliases devised by the '284 Patent is not simply a technological analogue to an age-old human activity. *See Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App'x 1014, 1017 (Fed. Cir. 2017) (there was no “pre-computer-age corollar[y]” for the encryption mechanism disclosed and claimed in the asserted patent). The subject matter of the patent claims is something that humans could not and cannot do, and that is achieved using specific inventive steps. Nevertheless, the district court found the '284 Patent to be abstract. The district court misunderstood or failed to appreciate that the hypothetical possibility of human performance – indeed, Apple *never* claimed that this was ever actually performed conventionally by humans – is not dispositive here, and practically irrelevant in this scenario. In any event, the impossibility of human performance raised a disputed

factual question, which the district court erred by resolving in Apple's favor on a threshold motion.

Accordingly, because the '284 Patent claims disclose steps that humans cannot perform, and that improve the security and efficiency of computer functionality, the district court erred in granting Apple's motion to dismiss, at least without conducting further fact-finding as to the issue of human performance, among other open factual questions.

**B. The District Court Litigation**

Blix's original Complaint (Appx44) against Apple asserted infringement of U.S. Patent No. 9,749,284 and illegal monopolization. Blix's First Amended Complaint (Appx88), added monopolization allegations about the iOS App Store. Regarding Section 101, the district court granted Apple's motion to dismiss, only as to claim 17 (which it declined to find representative of all claims) (Appx492). While reserving its right to appeal as to claims 17 and 27, Blix filed the Second Amended Complaint (Appx494, the "SAC"), specifically identifying claims 1-5, 7-11, 13-15, 18, 21-24, 28-30, 33-37 (the "SAC Asserted Claims"). The SAC also established a monopoly maintenance claim under Section 2 of the Sherman Act, 15 U.S.C. § 2 and a tying claim under Sections 1 and 2 of the Sherman Act, 15 U.S.C. §§ 1-2. The district court granted Apple's motion to dismiss.

On the first round of briefing, the district court held that “claim 17 was directed to an abstract idea at *Alice* Step 1, specifically, **facilitating anonymous communication using a proxy**. At [*Alice*] Step 2, [the district court] found that claim 17 did not capture any inventive concept, explaining claim 17’s method for controlling pre-interaction merely recites the conventional steps of gathering, categorizing, organizing, and comparing data . . . [and] that the ordered combination of limitations consists of performing conventional steps with conventional computer components.” *See* Appx1405 (emphasis added).

Although the district court permitted briefing on the SAC Asserted Claims, it found “no material difference in any of the other 26 remaining asserted claims that would lead to a conclusion that any of them are directed to something other than that same abstract idea that [it] found claim 17 to be directed to.” *See* Appx1407.

### **C. The PTAB Has Denied Apple’s Request to Institute an IPR**

After the filing of Blix’s First Amended Complaint, Apple filed a request to institute an *inter partes* review (“IPR”) challenging the validity of the claims of the ’284 Patent. After the district court dismissed Plaintiff’s patent claim, the Patent Trial and Appeal Board (“PTAB”) found that the Asserted Patent claims a non-obvious advancement over the prior art, denied Apple’s motion on the merits, and upheld the validity of the ’284 Patent claims. The PTAB explained the technological advancement as follows: “Upon receiving an incoming communication and/or

attempted incoming communication in step 18, the system determines the private interaction address associated with the manageable public interaction address to which the incoming communication was directed and determines the private interaction address associated with that public interaction address in steps 20 and 22.” *Apple Inc. v. Blix Inc.*, No. IPR2020-01635 at 4, 2021 Pat. App. LEXIS 3259, at \*2-3 (P.T.A.B. Apr. 19, 2021). The PTAB further found – focusing on claim 1’s limitation of “generating at least one reverse list entry, wherein an interaction address of said second party is associated at least with said manageable public interaction address of said first party” (*id.* at \*4) – that the ’284 Patent was not obvious over prior art’s “accept call list”, which is generally typified in the overly simplified analogies that Apple promoted and the district court accepted, in error.

#### **D. The Competitive Implications of Blix’s Technology**

By making a matrix of individual aliases possible for each of an end user’s communications with applications developers, the ’284 Patent enabled radical change to the competitive landscape in mobile communications.

Apple has a monopoly in mobile operating systems (“Mobile OS”), as it conceded in moving to dismiss the antitrust claims. Appx1441 (21:11-12). Certain kinds of middleware – those that flatten the differences between one Mobile OS and others, and allow users the same experience with applications no matter what operating system they use – threaten this monopoly. The ’284 Patent is such a

technology. Apple’s ecosystem builds a “moat” of high transactions costs to deter its users from leaving. The ’284 Patent technology, particularly if embodied in a Consumer Single Sign-On authentication system (“SSO”) which creates a credentialing relationship through a single user portal, builds a bridge over that moat.

Blix first released the SSO technology as Messaging Bridge, as part of BlueMail’s “Share Email” feature. But Messaging Bridge was capable of, and was intended to, form the basis of a full-featured SSO. Appx540 (¶170); Appx547 (¶196); Appx551-552 (¶¶218, 222). A fully anonymous encrypted SSO outside Apple’s control would link the user to each developer in a way that Apple could not disrupt, and could not surveil, significantly threatening Apple’s hold over its developers and allowing a competitive alternative to Apple’s highly lucrative payment processing system for in-app purchases. Appx547-548 (¶¶198, 200-01). Before Blix could gain sufficient traction to launch its fully encrypted SSO in this capacity, however, Apple took measures to (1) prevent the threat to its Mobile OS monopoly; and (2) guard its competitive flank by rolling out Apple’s own SSO, called Sign In With Apple (“SIWA”), which it improperly tied to its Mobile OS monopoly so that developers were required to implement it, like it or not. Appx554 (¶¶226-27); Appx559 (¶¶243-44). SIWA is a trap: its users unknowingly give over control of all their account relationships to Apple. Because SIWA creates an anonymous and *unknown* sign-in, to leave Apple’s iOS ecosystem after using SIWA



just once, a user needs to recreate all his or her accounts from scratch, while developers lose all their Apple users if they run afoul of Apple, a weapon Apple already threatened to deploy against Epic Games. Appx572 (¶296). Blix was and is a tiny developer in the Apple ecosystem, but Apple deployed extraordinary harassing measures: kicking BlueMail out of the Mac App Store, blocking it on multiple pretexts, stonewalling Blix's updates for weeks, and even refusing to recognize Blix's name change, all timed to coincide with the launch of SIWA. Appx500-501 (¶16); Appx564-565 (¶¶265, 269); Appx1230 (¶171). The SIWA launch infringed the '284 Patent, but from a competitive standpoint, it also neutralized it. Using its monopoly power and tying scheme, Apple forced into the marketplace a SSO that did much of what the '284 Patent was designed to do, but that kept the communications under Apple's control, where they could be revoked to control developers and keep them from forming a separate, secure relationship to users. By attacking Blix, Apple neutralized a disruptive nascent competitor with the technology to alter the competitive landscape. Appx537 (¶152).

### **SUMMARY OF THE ARGUMENT**

The district court erred in ruling as a matter of law that the '284 Patent claimed non-patentable subject despite the existence of four key factual disputes.

*First*, at *Alice* steps one and two, there was a question of fact as to whether the Asserted Claims effect an improvement to computer and system network

functionality and technology. Throughout its decision, the district court further improperly misinterpreted and misapplied this Court’s precedent regarding Section 101 cases involving relevant encryption and authentication technologies, such as *TecSec Inc. v. Adobe Inc.*, 978 F.3d 1278, 1293 (Fed. Cir. 2020) (holding that claims were patent eligible because they solved “a problem specifically arising in the realm of computer networks or computers” and they identify “specific” improvements to computer functionality and technology) (internal quotation omitted). Like the *TecSec* encryption mechanisms, the Asserted Claims provide secure yet recognizable reciprocal communications without requiring any human action. Further, the Asserted Claims improve communication privacy technology by solving the problem of integrating previously incompatible features of manageable addressing (improving security and flexibility) and caller recognition (improving transparency and supporting caller recognition functionality such as caller-ID, call screening, firewalls, for example). In fact, quite recently, this Circuit has reversed a dismissal of a software patent in a substantially similar case to the one here, finding that its claims and specification “recite[d] a specific improvement to authentication that increases security, prevents unauthorized access by a third party, is easily implemented, and can advantageously be carried out with mobile devices of low complexity.” *CosmoKey Sols. GMBH & Co. KG v. Duo Sec. LLC*, No. 2020-2043, 2021 U.S. App. LEXIS 29808, at \*14 (Fed. Cir. Oct. 4, 2021). Regardless, the

district court erred by not crediting any of Blix's allegations and the '284 Patent specification demonstrating those points.

In particular, the Asserted Claims solve “a problem specifically arising in the realm of computer networks or computers” and they identify “specific” improvements to computer functionality and technology. *See TecSec*, 978 F.3d at 1293 (collecting cases). These disclosed improvements at the very least should have merited factual finding as to whether the Asserted Claims teach specific, inventive improvements to computer functionality and communication privacy technology at *Alice* steps one and two.

*Second*, at *Alice* step one, the district court accepted Apple's attorney arguments without crediting Blix's allegations and foreclosed any fact finding as to whether a human intermediary could accomplish the completely anonymous, transparent, and manageable system of communication without vitiating privacy and efficiency.

*Third*, the district court ignored Blix's un rebutted allegations that the Asserted Claims are unconventional inventive improvements over the prior art. *See Cellspin Soft, Inc. v. Fitbit, Inc.*, 927 F.3d 1306, 1315-18 (Fed. Cir. 2019) (Rule 12 dismissal was inappropriate where “allegations in the complaint” supported plausible inferences that the limitations “were potentially inventive”).

*Fourth*, the district court entirely ignored the factual question as to whether the Asserted Claims preempt every solution to the problem of private communications or, as explained in Blix's opposition to Apple's motion to dismiss, there are other systems that could achieve private communications utilizing solutions different than those claimed in the '284 Patent.

And, despite the '284 Patent's clear advances over the prior art, as Blix alleged and the PTAB later found, the district court found the patent invalid under *Alice* steps one and two, and in so doing, it improperly:

1. Oversimplified and inaccurately broadened the claim language to formulate a purported abstract idea;
2. Ignored specific allegations pointing to the claims' technical elements;
3. Ignored – and thus decided – issues of material fact, and did so incorrectly without favoring Blix, the non-movant; and
4. Overlooked the claims' improvements over the prior art.

The district court's flawed legal analysis and disregard of factual questions constitutes reversible error.

With regard to the antitrust claims, the primary error made by the district court was disregarding Apple's entire pattern of anticompetitive conduct after dismissing the patent infringement claim. Apple's infringement of the '284 Patent was done to crowd Blix out of the market by offering consumers a cheaper if inferior option, and thereby constituted anticompetitive conduct on which the monopoly maintenance and tying claims were based in part.

But Apple also engaged in a series of other strategies and maneuvers that together also constitute anticompetitive conduct through which a viable monopoly maintenance claim based on Section 2 of the Sherman Act was made. It made several hostile actions towards Blix as part of a “sand in the gears” strategy, including the refusal to recognize Blix’s name change, defamatory statements about Blix’s stance on privacy, and pretextual exclusions of Blix’s product from the App Store. Appx500-501 (¶16); Appx564 (¶265); Appx1230 (¶171)

Apple furthermore engages in the practice of “Sherlocking,” which the district court erroneously found was indistinguishable from the charge of patent infringement (Appx24 n.1) but is rather the practice of using its review process to collect data about third party apps so that Apple is able to steal their technology for itself. Appx500 (¶15); Appx527 (¶¶113-14). This was a preliminary step to Apple’s infringement of the ’284 Patent, but is also anticompetitive in itself. The effects of all of these actions were exacerbated by the high-walled moat constructed around Apple’s user base. Courts in the Third Circuit must look at alleged anticompetitive actions together as a whole, and not piecemeal. *See e.g. Rochester Drug Co-op v. Braintree Labs.*, 712 F. Supp. 2d 308, 317-19 (D. Del. 2010). Here, the district court came to the erroneous conclusion that if there was no valid patent at issue, Apple could not have acted anticompetitively, despite all of the facts to the contrary.

This fallacy bled into the district court's analysis of the monopoly tying claim, and it summarily dismissed the portion of it based on Section 2 as it had been predicated on the monopoly maintenance claim. Appx27. In its rejection of the tying claim insofar as it was predicated on Section 1 of the Sherman Act, the district court erred in neglecting to consider that a tying arrangement could exist without a paid product. Here, Apple tied a mandatory inclusion of SIWA to any developer's use of a SSO – in order to put one's product using an SSO onto Apple's mobile OS, a developer must also showcase Apple's free SIWA alongside any other options. Appx501 (¶19); Appx559 (¶244). This tying arrangement serves to quash any nascent rival SSOs by forcing them to compete against a free, seemingly similar competitor, keeping them from gaining any sort of meaningful foothold in the market. Worse still, SIWA also gives Apple more control over both users and developers because it owns the channel between the two. Zero-price transactions should not be excluded and are able to compete in factors like price and quality; the fact that SIWA is free should not be a defense against Apple's illegal tying of SIWA to its monopoly mobile OS product.

The district court's failure to distinguish these anticompetitive actions from the patent infringement claim, as well as the failure to recognize that a free product could be used in a monopoly tying arrangement, constitute reversible error.

## **ARGUMENT**

### **I. STANDARD OF REVIEW**

This Court “review[s] a district court’s ultimate conclusion on patent eligibility *de novo*.” *See CosmoKey Sol’ns GmbH*, 2021 U.S. App. LEXIS 29808, at \*8-9 (citation omitted) (reversing the district court’s Rule 12 dismissal of patent claims for lack of patent-eligible subject matter).

When issues arise that are “not unique to patent law,” this Circuit applies “the law of the regional circuit in which the appeal would otherwise lie.” *Centocor Ortho Biotech, Inc. v. Abbott Labs.*, 636 F.3d 1341, 1347 (Fed. Cir. 2011). In this case, that would be the Third Circuit. When reviewing dismissals for failure to state a claim under 12(b)(6), the Third Circuit applies a *de novo* standard of review. *See Bronowicz v. Allegheny Cnty.*, 804 F.3d 338, 344 (3d Cir. 2015); *see also Aatrix Software, Inc. v. Green Shades Software, Inc.*, 890 F.3d 1354, 1357 (Fed. Cir. 2018) (“If patent eligibility is challenged in a motion to dismiss for failure to state a claim pursuant to Rule 12(b)(6), we must apply the well-settled Rule 12(b)(6) standard which is consistently applied in every area of law.”).

In evaluating 12(b)(6) motions to dismiss, courts must accept as true all material allegations of the complaint. *See Spruill v. Gillis*, 372 F.3d 218, 223 (3d Cir. 2004). “The issue is not whether a plaintiff will ultimately prevail but whether the claimant is entitled to offer evidence to support the claims.” *In re Burlington*

*Coat Factory Sec. Litig.*, 114 F.3d 1410, 1420 (3d Cir. 1997) (internal quotation marks omitted). Only after “accepting all well-pleaded allegations in the complaint as true, and viewing them in the light most favorable to plaintiff, [and finding that the] plaintiff is not entitled to relief” may a court dismiss the claim. *Maio v. Aetna, Inc.*, 221 F.3d 472, 481-82 (3d Cir. 2000) (quoting *Burlington*, 114 F.3d at 1420).

## **II. THE DISTRICT COURT’S DISMISSAL OF THE ’284 PATENT CLAIM SHOULD BE REVERSED**

### **A. Determination of Patent Eligibility Under 35 U.S.C. § 101**

The legal standard governing patent eligibility is well-established. To determine whether a patent claims ineligible subject matter, the Supreme Court has established a two-step framework. *See generally Alice Corp. v. CLS Bank Int’l*, 573 U.S. 208, 217 (2014). First, the court “must determine whether the claims at issue are directed to a patent-ineligible concept such as an abstract idea.” *See SRI Int’l, Inc. v. Cisco Sys., Inc.*, 930 F.3d 1295, 1303 (Fed. Cir. 2019) (citing *Alice*, 573 U.S. at 217)). Claims are not drawn to abstract ideas when they are focused on “an improvement to computer functionality itself.” *See Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335-36 (Fed. Cir. 2016). “[S]oftware-based innovations can make ‘non-abstract improvements to computer technology’ and be deemed patent-eligible subject matter at step 1.” *Packet Intelligence LLC v. NetScout Sys.*, 965 F.3d 1299, 1309 (Fed. Cir. 2020) (internal citations and quotations omitted); *see also Uniloc USA, Inc. v. LG Elecs. USA, Inc.*, 957 F.3d 1303, 1306 (Fed. Cir. 2020) (for software



innovations, the *Alice* step 1 inquiry “often turns on whether the claims focus on specific asserted improvements in computer capabilities or instead on a process or system that qualifies an abstract idea for which computers are invoked merely as a tool”).

If the court finds the claims are not drawn to abstract ideas, then the inquiry stops there. Otherwise, at *Alice* step 2, the court considers “the elements of each claim both individually and ‘as an ordered combination’ to determine whether the additional elements ‘transform the nature of the claim’ into a patent-eligible application.” *See CosmoKey*, 2021 U.S. App. LEXIS 29808, at \*13 (quoting *Alice*, 573 U.S. at 217)). The court must “accept[] as true all well-pleaded facts alleged in the complaint and draw[] all reasonable inferences in favor of the non-moving party.” *See CardioNet, LLC v. InfoBionic, Inc.*, 955 F.3d 1358, 1367 (Fed. Cir. 2020). In the “eligibility analysis, [the court must] consider the claim as a whole... and read it in light of the specification.” *See Packet Intelligence*, 965 F.3d at 1309 (citations omitted).

“Patent eligibility under § 101 is a question of law that may contain underlying questions of fact.” *CosmoKey*, 2021 U.S. App. LEXIS 29808, at \*8. “Any fact [. . .] that is pertinent to the invalidity conclusion must be proven by clear and convincing evidence” because patents are entitled to a presumption of eligibility. *See Berkheimer v. HP Inc.*, 881 F.3d 1360, 1368 (Fed. Cir. 2018).

**B. The District Court Erred at Both Steps  
One and Two by Legally Determining Factual Questions**

The district court erred at both *Alice* steps by ruling as a matter of law despite unresolved factual questions. On a motion to dismiss, courts may only invalidate patents “when there are no factual allegations that, taken as true, prevent resolving the eligibility question as a matter of law.” *See Aatrix*, 882 F.3d at 1125. The district court failure to credit factual disputes as to whether humans could perform the invention claimed in the Asserted Patent and whether the invention as claimed provides a technical, unconventional and non-routine improvement to reciprocal electronic communication led to erroneous rulings as to abstractness and the presence of an inventive concept.

**1. The District Court’s Error at Step 1**

*First*, the district court erred by dismissing the claims despite factual disputes as to whether the claims represent an improvement to computer and network functionality. Like the many patents that this Court recently has found to be patent-eligible, the Asserted Claims are not directed to abstract subject matter because they solve “a problem specifically arising in the realm of computer networks or computers” and identify “specific” improvements to computer functionality. *See TecSec*, 978 F.3d at 1293 (collecting cases). The Asserted Claims here are particularly analogous to the claims in *TecSec* *because* they are likewise directed to privacy which, like encryption, prevents human exposure to secret data. The problem

that the '284 Patent solves arises specifically in computer and network functionality, and the '284 Patent presents a unique technological solution to this technological problem. The reverse list is not simply a spreadsheet or table that a human could control, even assuming, *arguendo*, a human *could* actually devise and manipulate what would need to be a three-dimensional spreadsheet. Instead, as the PTAB recognized, the '284 Patent, teaches an improvement to reciprocal communication by increasing security (full anonymity) while allowing for flexibility (enabling two-directional communications) in a completely private environment.

The claims and specifications explain the benefits of utilizing manageable addressing, the importance of caller recognition, and how claim 1 of the patent in particular reconciles the apparent dissonance between these two technical features. Generally, a fixed public address assigns one alias to each user, through which the user communicates with all third parties. Because the user communicates through the same public address, the entire system is less private and less secure because the recipients of communication from the use employing the alias could cross-reference the user's communications and uncover the user's true identity and patterns of behavior. In contrast, a *manageable* public addressing system introduces variability. While this creates a more private and secure communication environment, it sacrifices caller recognition. Specifically, if the user communicates with an outside source or application (e.g., Expedia) using variable public addresses (or aliases) for

each communication, Expedia may lose the ability to recognize or identify the user and risks sending reciprocal communication (e.g., travel discount information unique to the user) to an unknown public address.

To solve this problem, unique to computer electronic communication systems, the '284 Patent's reverse list reconciles manageable public addresses and caller recognition, yielding significant benefits, including increased security and efficiency. *See* Appx1080 (21:25-28; 21:20-32, 22:3-12; 22:17-26; 22:44-53); Appx554-557 (¶¶227, 229, 231-233, 236); *see also Packet Intelligence*, 965 F.3d at 1309 (claims were not directed to abstract subject matter where they “purport[ed] to meet a challenge unique to computer networks, identifying disjointed connection flows in a network environment”); *McRO Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1314 (Fed. Cir. 2016) (claims were not abstract where they disclosed specific steps for improving the “existing technological process” of “computer animation” unsolved by the prior art). At the very least, Blix has sufficiently pleaded an unconventional improvement to the field and prior art to require fact finding on the issue. The district erred by offering nothing more than a cursory dismissal of the application of this binding Federal Circuit precedent to the '284 Patent or even its own. *See MAZ Encryption Techs. LLC v. Blackberry Corp.*, No. 13-304-LPS, 2016 U.S. Dist. LEXIS 134000, at \*22 (D. Del. Sept. 29, 2016) (finding that a method for creating a transparent encryption system was an eligible technological improvement

because it obviated “the need for user input, eliminating interruption and inefficiency – as well as human action – in a technology process.”)

*Second*, the district court committed reversible error by adopting Apple’s inaccurate and misleading analogies and an overly broad characterization of the “abstract idea” of “facilitating anonymous communication using a proxy.” Appx12. *See Data Engine Techs. LLC v. Google LLC*, 906 F.3d 999, 1011 (Fed. Cir. 2018) (rejecting defendant’s argument that “humans have long used tabs to organize information” in spreadsheets, because “[i]t is not enough, however, to merely trace the invention to some real-world analogy,” instead “[t]he question of abstraction is whether the claim is ‘directed to’ the abstract idea itself.”) In contrast to Apple’s mere lawyer argument, Blix proffered tens of pages of allegations, supported by specific references to the claims, specifications, and prosecution history showing that this broad characterization is incorrect. As in *CosmoKey*, the claims, specification, and written description of the Asserted Patent suggest that the focus of the “claimed advance” is far more technologically-driven and nuanced: the use of a reverse list to allow for reciprocal, anonymous communications. “The critical question then is whether this correct characterization of what the claims are directed to is either an abstract idea or a specific improvement in computer verification and authentication techniques.” *See CosmoKey*, 2021 U.S. App. LEXIS 29808, at \*12 (citing *Ancora Techs. v. HTC Am., Inc.*, 908 F.3d 1343, 1347 (Fed. Cir. 2018)).

Although the *CosmoKey* Court did not resolve the issue of abstractness, because regardless the claims there survived step two, the Court took issue with the district court's inaccurate characterization of the asserted claims.

*Third*, the district court erred by legally resolving the factual question of whether humans would be capable of performing the invention. *See SRI*, 930 F.3d at 1304 (“This is not the type of human activity that § 101 is meant to exclude. Indeed, we tend to agree with SRI that the human mind is not equipped to detect suspicious activity by using network monitors and analyzing network packets as recited by the claims.”); *see also TQP Dev. LLC v. Intuit Inc.*, No. 2:12-CV-180-WCB, 2014 U.S. Dist. LEXIS 20077, at \*15 (E.D. Tex. Feb. 19, 2014) (Bryson, J.) (the possibility for human performance of a multi-step encrypted communication system required findings of fact because “except perhaps in its most simplistic form, [the claimed invention] could not conceivably be performed in the human mind or with pencil and paper.”) The district court erred by ruling as a matter of law a question that should have been left to a factfinder and directly contradicting this Court's recent precedent in case regarding encryption- and authentication-directed patents. *See, e.g., Aatrix and Berkheimer, supra.*

*Fourth*, the district court misunderstood the implication of human performance, namely whether the reverse list and other innovative technological methods improved computer functionality such that the Asserted Patent is not

directed to an abstract idea. First, introducing human eyes at the intermediary level would vitiate privacy, and undermine efficiency. Second, the human mind, as a practical matter, could not perform these tasks because it requires coordination of multiple parties who are not allowed to know each other. Including even one human link in the chain bridging public and private identities would breach confidentiality. At the very least, the district court should have credited this factual dispute and allowed the parties to proffer fact and expert evidence.

## **2. The District Court's Error at Step 2**

At step 2, the district court rejected Blix's well-pled allegations that the disclaimed methods and steps were neither conventional nor well-understood, but rather provided an inventive concept. *See generally Aatrix*, 882 F.3d at 1128. Rather than accept factual and expert evidence, the district court rendered its own fact finding that:

[t]he purported inventive concepts are not in the claim[s]. The remaining asserted claims are not directed to anything more than the abstract idea and the conventional steps of communicating, that is, including gathering, categorizing, organizing, and comparing data. [...] I have found that none of these limitations make a difference in Step 2. The additional limitations are results-oriented and functional; they are not specific to computers.

(Appx14). This finding was erroneous considering the many citations to the record, on which the PTAB ultimately relied, explaining the unique nature of the reverse list as a specific technological solution to a computer-based problem.

On October 4, 2021, in a nearly identical case, this Court reversed the dismissal of a similar software patent, holding that the district court's step 2 analysis was flawed. *See CosmoKey*, 2021 U.S. App. LEXIS 29808, at \*14 (“We disagree with the district court’s analysis and conclusion. The patent claims and specification recite a specific improvement to authentication that increases security, prevents unauthorized access by a third party, is easily implemented, and can advantageously be carried out.”) In *CosmoKey*, looking to the claims and specifications, this Court ruled that the asserted patent there “recite[d] a specific improvement to authentication that increases security, prevents unauthorized access by a third party, is easily implemented, and can advantageously be carried out with mobile devices of low complexity. Contrary to the district court’s conclusion, the [asserted patent] discloses a technical solution to a security problem in networks and computers.” *See id.* at \*14-15.

Nearly the exact same thing can be said here. The '284 Patent claims and discloses specific improvements to authentication carried out in nonconventional and advantageous technical steps. The claim language includes specific steps which limit the invention to a narrow use of those particular steps: (a) rendering the public addresses manageable (as opposed to conventionally fixed) provides a security feature that prevents cross-correlating identity patterns to expose parties (all Asserted Claims); (b) routing incoming communication via addresses found in the



“record” provides privacy (Appx1080 (21:24-40); *see also* Appx1080-1081 (22:49-23:07); Appx1082 (26:39-56)); and (c) routing outgoing communication via aliases associated in the reverse list provides privacy (obfuscating private addresses) as well as caller recognition (a recognizable alias associated with the contact) (Appx1080 (21:49-52; 21:66-22:11); *see also* Appx1081 (23:30-37); Appx1082 (26:29-38)). *See, e.g., DDR Holdings, LLC v. Hotels.com, LP*, 773 F.3d 1245, 1258-59 (Fed. Cir. 2014) (claims provided an inventive concept where pleadings and record alleged specific steps to achieve the combined look and feel of a host website with embedded third-party merchant content).

As Blix plausibly alleged, the ’284 Patent provides novel techniques which improve on known forms of electronic communications, pointing to several prior art references that described the state of the art. *See* Appx1070 (1:23-40); Appx1075 (12:17-18); *see, e.g.,* Appx1504 (1:50-62) (explaining that a need exists to protect privacy in electronic voice communication, such as to ensure the caller’s privacy when calling from certain locations); Appx1531 (1:8-38) (explaining the need “for preventing a leakage of personal information such as a telephone number while establishing a telephone call quickly and efficiently,” including when using “a provisional telephone number corresponding to a regular telephone number”); Appx1541 (1:20-23) (explaining “[t]here are particular situations wherein a person would like to make their private phone number available to the other party for only

a limited time, or reserve the ability to block future phone calls from a specific person altogether”); *see, e.g.*, Appx 1549 (May 5, 2016 Office Action) (identifying 24 patents and patent applications the Examiner considered as prior art). The prior art included Sprint patents “for masquerading the identity of a communication device returning a missed call” (*id.* at 5-6, discussing U.S. Patent No. 7,995,730 to Zhang) and Fujitsu patents for managing “a provisional telephone number corresponding to the regular telephone number” (*id.*, discussing U.S. Patent App. Pub. No. 2006/0233551 to Oshika, discussed *infra*).

In denying Apple’s request to institute an IPR, the PTAB specifically held that the reverse list mechanism was a nonobvious improvement over prior art, which relied on a one-way list. *See Blix*, 2021 Pat. App. LEXIS 3259, at \*12-14. The district court neither credited Blix’s well-supported allegations, nor even permitted any fact finding, as to the ’284 Patent’s solution to the alias confusion problem by integrating the data structure (the reverse list) to route outbound communications (*e.g.*, claim 1(g)-(j)). The reverse list provides persistent memory tracking of which alias (first party manageable public address) to associate with which contacts (second party interaction address), so the confidential party knows which of its identities to use in order to be recognizable to other parties. This provides a technical solution or inventive step that reconciles the facially contradictory features of flexible addressing and caller recognition, a problem unsolved until the ’284 Patent. The

above inventive steps are manifested in the claims of the '284 Patent, particularly claim 1(g)-(j).

The district court's resolution of this fact-intensive inquiry as a matter of law conflicts with Federal Circuit precedent that improving computer or network security can constitute "a non-abstract computer-functionality improvement if done by a specific technique that departs from earlier approaches to solve a specific computer problem." *See Ancora*, 908 F.3d at 1348.

Here, as Blix alleged with specific cites to the record, the claims and specification make clear that the Asserted Patent recites an inventive concept by requiring a specific combination of steps far beyond the artificially broad abstract idea the district court identified and that improve upon the prior art by providing a simple method that yields unprecedented privacy and efficiency.

For all of the foregoing reasons, the District Court erred in dismissing Blix's patent infringement claim and ruling as a matter of law that the claims of the '284 Patent constitute ineligible subject matter.

### **III. THE DISTRICT COURT'S DISMISSAL OF THE MONOPOLY MAINTENANCE CLAIM SHOULD BE REVERSED**

In ruling on Apple's motion to dismiss, the District Court failed to take account of the entire interlocking pattern of anticompetitive conduct by Apple to maintain its OS monopoly, and the effect that its actions towards Blix had on competition in general. Courts distinguish between a monopolist who maintains

dominance by “a superior product, business acumen, or historic accident,” and one whose actions disadvantage not only competitors, but competition itself. *United States v. Microsoft Corp.*, 253 F.3d 34, 58 (2001) (internal quotation omitted). Anticompetitive or exclusionary conduct that harms competition, not just a competitor, and is harm “of the type that the statute was intended to forestall.” *Microsoft*, 253 F.3d at 59, citing *Brunswick Corp. v. Pueblo Bowl-O-Mat, Inc.*, 429 U.S. 477, 487-88 (1977). If a monopolist engages in conduct that “has a substantial effect in protecting [the monopolist’s] market power, and does so through means *other than competition on the merits*, it is anticompetitive.” *Microsoft*, 253 F.3d at 62 (emphasis added); see *LePage’s, Inc. v. 3M*, 324 F.3d 141, 147 (3d Cir. 2003) (“monopolist willfully acquires or maintains monopoly power when it competes on some basis other than the merits”); *New York v. Actavis PLC*, 787 F.3d 638, 652 (2d Cir. 2015). Apple has engaged in precisely such anticompetitive conduct.

Importantly, under Third Circuit precedent, the court should not compartmentalize the various allegations of a monopolization scheme by assessing each piece of conduct in isolation. To the contrary, “[p]laintiffs may make their antitrust case by establishing an overall scheme ...” *Rochester Drug Co-op*, 712 F. Supp. 2d at 317-19. Courts “must look to the monopolist’s conduct taken as a whole rather than considering each aspect in isolation.” *Id.* (quotation and citation omitted). A series of actions taken in furtherance of a plan to improperly defend a monopoly

may trigger liability, even where the components in isolation might not. *Id.* at 318; *see LePage's*, 324 F.3d at 162 (*en banc*) (actions examined “as a whole rather than considering each aspect in isolation”); *Presque Isle Colon & Rectal Surgery v. Highmark Health*, 391 F. Supp. 3d 485, 498 (W.D. Pa. 2019) (quoting *LaPage's*); *In re Neurontin Antitrust Litig.*, MDL No. 1479, 2013 U.S. Dist. LEXIS 111587, at \*19-20 (D.N.J. Aug. 8, 2013) (actions “in furtherance of and as an integral part of a plan to violate the antitrust laws” can trigger liability as a scheme.); *Walgreen Co. v. Organon, Inc.*, 335 F. Supp. 2d 522, 532 (D.N.J. 2004) (denying motion to dismiss as to “overall scheme”).

Contrary to this precedent, in dismissing the monopoly maintenance claim, the district court centered its analysis on the patent infringement issue. Having already dismissed the patent infringement claim, the Court predicated its dismissal of the monopoly maintenance claim on its prior dismissal of the patent infringement claim, treating the patent claim as a “fundamental premise” of the monopoly maintenance claim. Appx24. While Blix stands by its claim for patent infringement and its allegation that said patent infringement was one particular weapon Apple deployed in a series of anticompetitive actions towards Blix (Appx585 (¶¶350-351)), it was not a “fundamental premise” or necessary element of its monopoly maintenance claim. The other examples of Apple’s anticompetitive behavior are so extensive and egregious that when properly considered together they form a viable

monopoly maintenance claim even if Apple's infringement of the '284 Patent is not considered.

**A. Apple's Infringement of the '284 Patent  
Constitutes Anticompetitive Conduct**

Apple's infringement of the '284 Patent constitutes anticompetitive conduct in the form of an "embrace and extend" strategy – a modus operandi in which Apple, a large monopolist, copied (or "embraced") the technology of its smaller, nascent competitor, and then proceeded to publish ("extend") it throughout its vast ecosystem and user base – forcing third-party app developers who wished to employ a SSO solution to use SIWA either alone or as an equal option to any competing SSOs. Appx568 (¶279). As the market predictably became flooded with Apple's infringing and self-entrenching version of its technology, Blix was left far less able to compete with its own, more privacy- and competition-friendly version of the product.

Moreover, Apple's removal of the BlueMail app from its App Store mere days before launching the infringing SIWA (Appx583 (¶340)) evinces a clear anticompetitive intent: by holding back the original patented technology, Apple was able to cut open a hole in the market to insert its inferior, infringing product. This was a premeditated theft of a novel technology that would otherwise have threatened Apple's grip on its user base and monopoly.

**B. Apple Uses A “Moat” Around Its  
User Base to Preserve Its Mobile OS Monopoly**

A key element of Apple’s anticompetitive conduct is the nearly impenetrable “moat” it has constructed around its user base by a series of actions that, individually and especially together, make it difficult and expensive for iOS users to leave the coordinated technological ecosystem which is grounded and protected by Apple’s monopoly power in its OS. In analyzing this argument, the district court focused particularly on the forcing of SIWA alongside other SSOs – which it regarded as *procompetitive* – disregarding many other actions Apple took to build its moat (Appx24-26), ultimately failing to consider that Apple’s customers become dependent on its immense and interconnected ecosystem, it becomes prohibitively expensive to leave, forcing consumers to stay in Apple’s ecosystem.

The high cost of escaping Apple’s ecosystem begins with the purchase of its hardware. Apple’s OS is exclusive to Apple’s hardware, Appx514 (¶61), and Apple’s hardware is expensive, Appx519 (¶85). Because the hardware can no longer be used if the user decides to stop using the iOS operating system, this cost makes it “prohibitively expensive” to leave. *Id.* This interplay between the nominally free operating system and the expensive hardware that is both necessary to use it, and only works with it, is neither accidental nor innocuous. *See* John M. Newman, *Antitrust in Zero-Price Markets: Foundations*, 164 U. Pa. L. Rev. 149, 154 (Dec. 2015) (“To profitably offer products at a price of \$0 in the long term, a rational firm

must intend to turn a profit in some manner not involving those products.”); *see id.* at 156 (“the interrelated nature of complementary products does create multiple avenues for anticompetitive behavior by a firm with market power in at least one of the relevant product markets.”). *See also Competition and Monopoly: Single-Firm Conduct Under Section 2 of the Sherman Act*, U.S. Dept. of Justice, Sept. 2008, ch. 5 at p.84 (recognizing the incentive to extract switching costs or future upgrades, so that “a monopolist may tie to earn monopoly profits in the tied-good market that are not currently available but will be in the future.”)

Even a user willing to sacrifice the hardware expense faces other barriers to departure. For example, Apple facilitates family members’ access to each other’s purchased apps or subscription media such as music, movies, and books. Communication apps like FaceTime are proprietary to Apple, so that a family using all Apple devices must continue to all use Apple devices to maintain their same pattern of use. Appx519-521 (¶¶86-87, 90). Switching often means migrating the entire family to an OS on the competitive fringe, and even then, users lose at least some functionality. Appx520-521 (¶90). For example, a high school student whose friends have a running group message that cannot easily add an Android user has a strong incentive to pressure their parents into staying within the Apple ecosystem.

SIWA redoubles this effect. Because SIWA is both opaque (meaning that the anonymous sign-in is not shared with the user) and exclusive (meaning that the sign-



in is only valid for iOS devices and apps), any iOS customer who uses SIWA to authenticate his or her accounts through Apple and later wishes to leave the iOS ecosystem for another platform must recreate all those sign-ins for the new platform.

**1. *Apple’s Sherlocking is the Entry Point of Its “Embrace and Extend Strategy”***

Apple steals developers’ ideas – a tactic admitted to by Apple’s storied co-founder Steve Jobs. Appx526 (¶110). Apple’s tactic of using its review process of apps built for its operating systems to decide whether or not to steal them is so pervasive that it has been given its own name: “Sherlocking.” Appx527 (¶113). Moreover, Apple does not even deny that it uses its app review process to “peek at apps under review” and decide what to steal. Appx526 (¶112). Apple’s own personnel admit the practice, and indeed the Developer Agreement codifies Apple’s “right” to do this (Appx526 (¶111)) – a provision reviled by developers who are nevertheless powerless to fight back against Apple’s overwhelming monopoly.

The District Court failed to consider the anticompetitive effect of Sherlocking after dismissing the validity of the patent infringement claim, overlooking the fact that the Sherlocking is a distinct step *prior* to the actual act of patent infringement in Apple’s embrace and extend scheme to shut Blix out as a viable competitor. Sherlocking is not a mere “exercise of business acumen” (Appx24 n.1, citation omitted); in fact, it is an exercise of maintaining of monopoly power.

While Sherlocking may indeed lead to the theft of a patent, by itself it is not patent infringement – though to be sure, Apple’s Sherlocking of Blix’s technology was a precursor step to its act of patent infringement. And even if the ’284 patent were found to be invalid, the district court erred by linking both Apple’s Sherlocking and embrace and extend strategies to the patent infringement. Apple can steal an idea – and do so as an anticompetitive tactic – whether or not the idea has the protection of a valid patent. Certainly, the technology described in the ’284 Patent was and is a novel and valuable idea. That there is a valid patent here which Apple has infringed only adds to Apple’s list of anticompetitive actions; it does not diminish the rest. Thus, the district court’s ruling dismissing the patent claim did not merge into an examination of the impact of stealing ideas on the competitive landscape, and said dismissal should not have barred consideration of this part of the monopoly maintenance claim (*see* Appx24).

Importantly, Sherlocking allows Apple to control new technologies that threaten its OS monopoly – in particular, middleware. Middleware refers to any technology that, by sitting between applications and an operating system, flattens any differences between operating systems. This in turn allows interoperability of apps across operating systems, creating common and seamless user experiences across operating systems and the hardware they run on. Operating systems are thus transformed into invisible background mechanics – and ultimately, commoditized.

Middleware is familiar to antitrust law. In *Microsoft Corp.*, 253 F.3d 34, the middleware at issue was the internet browser. Microsoft had a monopoly desktop operating system, Windows. The operating system exposed application programmer interfaces (“APIs”), the code with which the applications software interacted. Netscape’s competing browser also exposed APIs with which apps interacted. The DC Circuit reasoned that browsers were an emerging threat to Microsoft’s Windows monopoly because if applications developers began using browser APIs instead of operating system APIs to connect their application, the browser as middleware could commoditize the operating system: “If a consumer could have access to the applications he desired – regardless of the operating system he uses ... then he would no longer feel compelled to select Windows in order to have access to those applications.” *Microsoft*, 253 F.3d at 60. If that happened, the user “could select an operating system other than Windows based solely upon its quality and price. In other words, *the market for operating systems would be competitive.*” *Id* (emphasis added).

The parallel to Apple’s OS monopoly is nearly exact. If users could use whatever apps they want regardless of their phone hardware or OS, they could choose their phone OS based only on quality and price. Apple thus seeks to thwart such a threat to maintain its monopoly and avoid competition. Such “[e]xclusion of a disruptive entrant inherently harms the competitive process, even if that disruptive

entrant is (currently) less efficient than the dominant firm. ... If consumers have limited options, then even a small chance of the arrival of an effective second choice can be very valuable to them.” Guilio Federico, Fiona Scott Morton and Carl Shapiro, *Antitrust and Innovation: Welcoming And Protecting Disruption*, Innovation Policy and the Economy, Vol. 20, p. 159 (NBER 2020).

Sherlocking provides a critical link between Apple’s current monopoly power, and its ability to keep that monopoly by means other than competition on the merits (making it exclusionary conduct, *see Microsoft*, 253 F.3d at 62). Apple requires new apps to be submitted to it for review. Appx516 (¶73); Appx523 (¶101). It can then take any idea and use it however it wants because its Developer Agreement dictates its ability to do so. Appx526 (¶111). If a submission contains middleware that poses the threat described by the *Microsoft* court, Apple is able to preemptively “embrace” the idea by coming up with its own proprietary copy. Apple can then “extend” by disseminating that copied technology in a proprietary version, under its control so as to neutralize any possibility of the middleware.

## **2. Apple Uses Its Monopoly to Bind Developers**

Apple uses its mobile OS monopoly to control its developers, as a means to keep captive its user base. Apple binds its developers with its Developer Agreement, in which it creates and enforces policies which it can and does deploy as it sees fit to force its developers to shun technologies that Apple sees as threatening. Appx522

(¶¶97-99). Because of the power disparity created by Apple's monopoly, developers are unable to object. One example of such a technology is Microsoft's xCloud software, another version of middleware that sat between the operating system and applications. It allowed users to access games software from the cloud and play it effectively, smoothing the functional gap between native and web applications. When Apple saw the danger of this middleware it banned it in the Developer Agreement. *Id.*

Apple's OS monopoly gives it the power to review any app before authorizing distribution, Appx516-518 (¶¶70-75, 81-82); Appx523 (¶101). It can and does use its review process to either remove developers' apps from the app store, or simply to bury them in the search function that the vast majority of its users depend on to find apps for any particular purpose. For all but the best-established apps, unfavorable search treatment cuts off the developer's avenue for growth. This lets Apple maintain its dominance over any nascent rival emerging through its own ecosystem. Appx523 (¶101); Appx524 (¶106, n.36). This blocks out third party developers who would otherwise build a following for core apps that are able to function across operating systems, which could in turn tempt users to leave Apple's monopoly. Appx524 (¶¶105-06).

Another aspect of Apple's control over its developers is that it makes them depend on Apple for payment processing for digital content and subscriptions

purchased in those apps. In *Epic v. Apple*, the United States District Court recently found that Apple's anti-steering provisions locking developers into this system were unfair, and issued a permanent injunction which is currently on appeal to the Ninth Circuit. Case No. 4:20-cv-05640-YGR (N.D. Cal. Sept. 10, 2021) [ECF Nos. 812-13].

Apple charges a large commission on both the sale of apps as well as in-app purchases – typically 30%, which in turn forces developers to charge more for their apps to earn a sustainable profit. Appx523 (¶103). Developers cannot refuse because of Apple's monopoly share of the OS market. In this way, Apple has inserted itself between the developer and the customer as the primary payment processor for every developer that sells in-app content. Apple's payment requirements thus prevent developers and users from forming financial relationships that it cannot surveil or control. Appx537 (¶154); Appx547 (¶195); Appx569 (¶284); Appx570-573 (¶¶291-96, 299).

Apple tends to claim that it is attempting to ensure its users' privacy when its control of app distribution is challenged. But this claim has been found to be pretextual, and specifically deployed to protect Apple's monopoly. The House Committee on Energy and Commerce report found that Apple's privacy efforts were often inadequate, evidencing a lackluster commitment. In fact, it found, Apple uses the notion of privacy to insulate its own apps against competitors by affixing privacy

labels to competing developers' products, while exempting its own pre-installed proprietary apps. Appx525 (¶109). The added advantage for apps that only Apple offers further entrenches the Apple user base: if Apple succeeds in making them believe that Apple's proprietary apps better safeguard their privacy (even if this is not objectively true), giving up that perceived (but illusory) privacy advantage is another cost of switching away from Apple's monopoly.

**C. Apple's Conduct Towards Blix Was Part of Its Anticompetitive "Sand in the Gears" Strategy**

When Apple launched SIWA, it was embarking on a conscious strategy of entrenching its own SSO, which it controlled, before Blix's Messaging Bridge could establish a footing and launch (as the technology was obviously designed to facilitate) as an independent SSO. To help this strategy, Apple attacked Blix's flagship product, its email client, BlueMail. While BlueMail was largely unrelated to the battle over SSO, by attacking BlueMail, Apple could distract and disarm Blix while it launched SIWA to blunt the threat that the Blix Messaging Bridge presented.

Blix Messaging Bridge was available to end users only in the proxy email feature of BlueMail. This was the route through which Blix had to gain user familiarity with and acceptance of the Messaging Bridge product, and the '284 Patent, before expanding it to a complete SSO.

Apple, before and immediately upon the launch of SIWA, which copied the '284 Patent technology, began a campaign of harassment and delay designed to

marginalize and neutralize the Messaging Bridge in the marketplace. Meanwhile, as Blix struggled to defend itself against Apple's onslaught of defamation and arbitrary hurdles, Apple promulgated (with the force of its control over developers) its own version of the technology.

The district court rejected this argument because "the Complaint fails to adequately and plausibly allege that Apple has thrown 'sand in the gears' of competition as opposed to just in the gears of a single competitor." Appx27. In this, the district court applied the wrong standard. Harm to innovation is harm to competition, even if the operative acts are directed at one competitor in particular, and can indeed form the basis of antitrust injury. *See, e.g., Glen Holly Entm't, Inc. v. Tektronix, Inc.*, 352 F.3d 367, 374 (9th Cir. 2003), quoting *Amarel v. Connell*, 102 F.3d 1494, 1509 (9th Cir. 1996) (antitrust injury includes stifling innovation or coercive activity that "prevents its victims from making free choices between market alternatives"); *Free FreeHand Corp. v. Adobe Sys. Inc.*, 852 F. Supp. 2d 1171 (N.D. Cal. 2012) (where Adobe's stifling of a single competitor to boost sales for its own product, was found to harm innovation in general for the purposes of antitrust injury). Blix is a market disruptor, offering innovation in the form of middleware which has the potential to remove Apple from the developer-consumer relationship, and drastically transform and innovate the market. Apple could crush any small developer; it has chosen to turn its weapons on Blix not merely to harm Blix, but to



prevent the emergence of technology that would foster competition. Apple’s target is therefore not its competitor, to thwart a competitive technology that could outflank its monopoly. The district court was bound to, but did not, review Apple’s actions against Blix in light of the well-pleaded allegation that Apple specifically intended these acts to keep an emerging technology from bringing competition to its monopoly in mobile OS.

**1. Apple’s Pretextual Exclusion and Audits of Blix**

Two weeks before announcing SIWA on June 3, 2019, Apple abruptly flagged BlueMail and threatened to kick it out of the Mac App Store, its only foothold for distribution that Apple controlled, despite Apple’s prior approval. Appx1230 (¶171). Between then and SIWA’s launch, Apple provided multiple, transparently pretextual (Appx1236 (¶¶198-200)) reasons for its targeted scrutiny of BlueMail before ultimately removing it altogether on June 5, 2018 (Appx541-545 (¶¶172-188)). Then Apple just went silent. Appx1235 (¶197). Blix’s BlueMail product was locked out of the Mac App Store and Blix had no way to popularize its Messaging Bridge technology to Apple’s user base or provide iOS users any experience with it. Such unnecessary audits and pretextual scrutiny constitute anticompetitive conduct. *Presque Isle*, 391 F. Supp. 3d at 499-500 (“unnecessary audits” to claw back prior payments, and “inefficient procedure codes” that imposed added costs were part of a pattern by the monopolist to drain the resources of a potential competitive threat).

## 2. **Apple's Pretextual Assertion of Privacy and Security Flaws**

When questioned by the trade press about BlueMail, on Feb 12, 2020, Apple made precisely the kind of false assertion that the House Committee has identified: “Blix is proposing to override basic data security protections ... and threaten [users’] privacy.” Appx565 (¶267). Blix sent a cease and desist letter informing Apple that this accusation was false. Appx565 (¶268). The Third Circuit recognizes that “such defamation, which plainly is not competition on the merits, can give rise to antitrust liability, especially when it is combined with other anticompetitive acts.” *In re Suboxone Antitrust Litig.*, 64 F. Supp. 3d 665, 682 (E.D. Pa. 2014) *quoting* *W. Penn Allegheny Health Sys. Inc. v. UPMC*, 627 F.3d 85, 109 n.14 (3d Cir. 2010) (as part of a concerted scheme to thwart a new entrant, the monopolist raised “false safety concerns and disparag[ed] Suboxone tablets”).

## 3. **Apple's Pretextual Blocking of Publishing Updates**

In August 2020, after a year of Apple's arbitrary barriers, Blix had its BlueMail client available on both the Mac and iOS App Stores. Then, on August 13, 2020, Apple suddenly decided that Blix was required to offer SIWA to its own users, and on this basis, blocked Blix from using publishing updates to support its own end-users. Appx565 (¶269). This rationale was particularly ironic: SIWA copied the functionality of Messaging Bridge, and Apple had acted to ensure that SIWA, which it controlled, propagated in the market, while Blix scrambled to stay available to end

users at all. Then, Apple decided that its rules required that Blix was obligated to give Apple’s product significant space on its own sign-in screen, allowing Apple to control and intermediate the relationship, when the entire point of Blix’s technology was to prevent a communication from being intermediated. The literal terms of Apple’s own Developer Guidelines did not require this of Blix, Appx566 (¶271). The overt singling out of Blix caused scrutiny in the trade press, and as a result Apple relented at the end of September, 2020 – though it still suspended users’ ability to make BlueMail their default email client for another week thereafter. Appx567 (¶¶274-75).

#### 4. *Apple’s Refusal to Recognize Blix’s Name Change*

As part of a longstanding expansion plan, Blix attempted to change the name of the company on iOS from BlueMail to Blix. Without explanation Apple refused the request for approximately 18 months, eventually relenting only four days before Plaintiffs’ SAC was due to be filed. Appx564-565 (¶265)

If the district court had taken all of the above allegations of anticompetitive conduct together as required, it would have found that Apple’s pretextual exclusions, disabling of updates, insistence on Blix’s own implementation of SIWA, false allegations of privacy and security flaws, and refusal even to accept Blix’s name change amount to a “scheme of deception and delay” by Apple in order to maintain

its exclusive position in the market. *See, e.g., Meijer Inc. v. Ranbaxy Inc.*, No. 15-11828-NMG, 2016 U.S. Dist. LEXIS 120780, at \*50-51 (D. Mass. June 16, 2016).

**D. Apple’s Implementation of SIWA Is Anticompetitive**

SIWA bundled a SSO with its monopoly OS, but Apple did not offer the product and allow developers to choose it on merit. Rather, Apple both forced developers to choose its SSO, if not in preference to all others, then by using its monopoly to require that they offer it on equal footing; and also acted to block Blix’s earlier and superior Messaging Bridge, which would preempt Apple’s control over developer-user relationships and fosters frictionless cross-OS interoperability.

The District Court erred in concluding that “it appears to be undisputed that the requirement to offer Sign In With Apple actually expands consumer choice in the SSO market.” Appx26 (emphasis removed). This misinterprets the allegations Blix has made. By imposing SIWA either as an equal choice to other SSOs or as the only SSO for a given app (Appx561 (¶252)), consumers are driven towards using SIWA above other SSOs because they become more dependent on this piece of the ecosystem, committing their accounts to Apple’s control. If a developer wishes to offer an SSO, it must offer SIWA. No other SSO is mandated; therefore, it is exceptionally unlikely that any other SSO will prevail over SIWA in consumer choice. When the products of smaller developers are left unable to compete because

they must be offered alongside a cheaper inferior one, they are pushed out of the market altogether and consumer choice is thus limited.

Apple's implementation of SIWA is just another instance of Apple spotting and thwarting disruptive new technology by means other than competition on the merits, before it can challenge Apple's monopoly. Like Microsoft before it, Apple identified an emerging middleware that threatened increased cross-platform functionality, reduced switching costs, and would force iOS into a competitive battle on the basis of price and quality. Rather than contest this battle, Apple instead turned a rival technology that threatened its dominance into one that entrenched it.

Apple's primary goal is to limit customer exposure to Blix's Messaging Bridge. Appx563-564 (¶263). Prior to and after SIWA's launch, Apple threw up hurdles to Blix's then-available product that incorporates the Messaging Bridge. Apple then forced SIWA upon its entire developer base, conduct that again tracks with what the Microsoft court described as anticompetitive. *See Microsoft*, 253 F.3d at 74-77 (Microsoft violated § 2 of the Sherman Act where it took various steps "to exclude Java from developing as a viable cross-platform threat"). Additionally, Microsoft's exclusive agreements with internet service providers helped "keep usage of Navigator below the critical level necessary for Navigator or any other rival to pose a real threat to Microsoft's monopoly." *Id.* at 71. In that case the Court found that Microsoft did not need to totally foreclose distribution or use of Navigator in

order to violate Section 2 of the Sherman Act. *Id.* at 70. It merely needed to ensure that Navigator did not achieve widespread popularity that would then translate into pervasive cross-platform usage that would decouple the choice of operating systems from the selection of applications. Likewise, here Apple does not need to foreclose all distribution of Blix Messaging Bridge, only to stifle its ability to become a widespread middleware which could threaten Apple's OS dominance. Blix has the potential to end-run Apple's payment processing system, Appx547 (¶195), reduce its control over developers, Appx570-572 (¶¶290-96), and form a SSO which would authenticate users to applications directly – thus flattening the user experience across operating systems, Appx548 (¶201); Appx551 (¶215), and forcing iOS to compete with other operating systems on the basis of quality and price, rather than by being necessary to participate in the largest ecosystem.

**1. *Apple's SIWA Implementation Prevents Competition by Impermissibly Bundling Its Offerings***

A monopolist may bundle its offerings to make its own product more attractive, but cannot bundle its own products merely to discourage distribution of a rival product. *Abbott Labs. v. Teva Pharms. USA, Inc.*, 432 F. Supp. 2d 408, 422 (D. Del. 2006), interpreting *Microsoft*, 253 F.3d at 65-67. Apple mandates through contract that any developer who wishes or needs to integrate a SSO into their iOS app must also integrate SIWA into their product. This mandate is enforced notwithstanding any individual developers' preference. But Apple's forcing of

SIWA upon developers has anticompetitive effects on the OS market. Blix not only alleges that Apple's conduct harmed it as a competitor in the SSO market, but that Apple's anticompetitive scheme harms competition both in the SSO market and the OS market.

By mandating SIWA either as the only SSO offered, or as an equal alternative to any other SSO integrated into a given app, Apple injects itself as an intermediary between the developer and the user of its app, allowing it to shut off the developer's access to its own customers. A developer, furthermore, must test and manage each SSO relationship, and SIWA takes up space on a login page that developers will not clutter with numerous offerings. As a result, the mandatory inclusion of SIWA makes a developer more likely to reject smaller or nascent rivals. *See Microsoft*, 253 F.3d at 63-64 (mandatory inclusion of Internet Explorer took up scarce hard drive space and committed testing costs). Even if SIWA ultimately occupies less than a dominant share in the SSO market, its mandatory inclusion in every app login page would still successfully crowd out Blix's Messaging Bridge, a competing offering that neither requires consumers to trade away their data, nor forces developers to allow the SSO maker to control their user relationships – a maverick middleware product that poses a fundamental threat to the Mobile OS monopoly in ways that other SSOs do not. *See, e.g.*, Appx550 (¶212).

**2. Apple’s Forcing of SIWA On Blix and Other Developers  
Blocks Messaging Bridge’s Disruptive Potential**

Apple has interpreted its Developer Guidelines to place Blix in a quandary when offering Messaging Bridge as a SSO, or in any application as an authenticator. Apple requires SIWA “as an equivalent option”, Appx561 (¶252), if an application uses another SSO. For Blix to offer its SSO to authenticate customers with other developers, those developers are then forced to offer SIWA as an equal choice – even though Blix’s most likely developer partners are those who are uncomfortable with SIWA and the control it gives Apple over the relationship between developer and end user. Apple effectively blunts Blix’s best pitch, its alternative to SIWA, because Apple does not allow any developer to partner with a Blix SSO alone.

**IV. THE DISMISSAL OF THE TYING CLAIM SHOULD BE REVERSED**

**A. Standard**

The antitrust concern with tying is that the maker can exploit market power in one market, to force the acceptance of a product in a different market. *See, e.g., Kickflip, Inc. v. Facebook, Inc.*, 999 F. Supp. 2d 677, 688-89 (D. Del. 2013) (Stark, J.). In order to establish a tying claim, a plaintiff must show (1) that the defendant offers two distinct products; (2) the defendant’s market power in the tying market; and (3) that a substantial amount of commerce is affected. *Id.*

In addition, the Third Circuit has defined an unlawful tying as “as an agreement by a party to sell one product [or service] but only on the condition that



the buyer also purchases a different (or tied) product [or service], or at least agrees that he will not purchase that product [or service] from any other supplier.” *Avaya Inc., RP v. Telecom Labs, Inc.*, 838 F.3d 354, 397 (3d Cir. 2016) (quotation omitted). Contrary to the District Court’s holding (Appx27-28), *Avaya*’s standard is satisfied here. Blix is forced to incorporate SIWA into its system if it wishes to offer its product on Apple’s mobile OS. The District Court pointed out that “[i]t is only when the application offers the additional choice of a single sign in that the application developer is required to also offer Sign In With Apple as a choice” (Appx28, emphasis removed) – but this disregards the utter vitality of an SSO to Blix’s technology. Blix has no real choice in the matter because to remove its own SSO – the consequence of not using SIWA – would be to destroy a key functionality from its app. Thus, this “choice” of whether or not to implement SIWA is in fact more of a death threat; in order for Blix to operate at all on Apple’s mobile OS it must use SIWA.

The District Court also found that insofar as the tying claim under Section 2 of the Sherman Act was “predicated on the deficient Section 2 [monopoly maintenance] claim” it “must also fail.” Appx27. Thus, for the reasons that the monopoly maintenance claim’s dismissal should be reversed, so too should the portion of the tying claim based on Section 2 – the patent claim’s dismissal should have been allowed such a domino effect. With respect to the tying claim based on

Section 1 of the Sherman Act, the Court erred in concluding that simply because Sign In With Apple did not follow every single purchase of iOS, there is no tie. But this analysis ignores the fact that if iOS is purchased, then SIWA will inevitably be tied with any developer's product that uses an SSO. Indeed, the elements of tying are easily satisfied.

**1. Operating Systems and SSOs are Distinct Products**

The threshold requirement that the products at issue be distinct products, in distinct markets, is easily satisfied here. Blix pleaded that the SSO is a new market. Appx532-535 (¶¶132-43). *Microsoft* guides courts to make the analysis not merely on the basis of historical products. *Microsoft*, 253 F.3d at 87, citing *Jefferson Parish Hosp. Dist. No. 2 v. Hyde*, 466 U.S. 2, 21 n.33 (1984). To avoid the backward-looking problem, *Microsoft* held “that the rule of reason, rather than per se analysis, should govern the legality of tying arrangements involving platform software products,” as in situations involving “novel categories of dealings... simplistic application of per se tying rules carries a serious risk of harm.” *Microsoft*, 253 F.3d at 84

The SSO is clearly separate from the OS market. In *Microsoft*, the trial court found that other operating system makers also bundled browsers with them, though on different terms than Microsoft. *Id.* at 89. But here, aside from Apple, several participants in the tied market are not operating system makers but social media

companies. They do not, and cannot, bundle a SSO with an operating system. Appx534 (¶140). SSO is not an outgrowth of operating systems that naturally suggests an integrated product, nor does competitive efficiency dictate that it be offered as a bundle with an operating system.

## 2. **Apple Has Monopoly Power in the OS Market**

Apple has monopoly power in the tied market (Apple accepted this *arguendo*, see Appx1441 (21:11-12), and without that monopoly power, it could not force SIWA on the market. Except for Apple's contractual ability to require developers to offer it, developers would not do so. Appx538 (¶155); Appx568 (¶280); Appx588-589 (¶¶365-367).

## 3. **Apple's Tying Affected a Substantial Amount of Commerce**

Apple's tie affected a substantial amount of commerce. Appx589 (¶367). In this young market for SSO, Apple can displace the early entrants because it offers a different business model, and because it can force developers to accept its product through the power of its OS monopoly in the tying market. Appx534-536 (¶¶139-149). Apple has specifically used its tie to exclude Blix, which offers all of the privacy benefits that Apple claims, but with neither the intent nor the history of threatening developers. See Appx537 (¶152); Appx550-551 (¶¶213); Appx572 (¶296). Blix is positioned to offer a new business model to the market; it is a maverick entrant. Appx537 (¶151); Appx550-551 (¶¶212, 215-16). In *Roxul USA*,

*Inc. v. Armstrong World Indus.*, Civ. No. 17-1258, 2019 U.S. Dist. LEXIS 37926 (D. Del. Mar. 8 2019), the Court held in considering the analogous element of substantial foreclosure that even if anticompetitive agreements “do not foreclose a substantial number of rivals, exclusivity severely restricts the market’s ambit by preventing a ‘maverick’ ... from achieving a footing in the market.” *Id.* at \*29 (citing Department of Justice Vertical Merger Guidelines).

The effect warned of in *Roxul* is pertinent to the forced implementation of SIWA in this case – if a developer wants to use an SSO, it must offer SIWA. If it does not wish to do so, it is foreclosed from offering any SSO. The key lesson of *Roxul* is that if a maverick like Blix is constrained then competition in general is harmed. Monopoly power overcomes and quells innovation. The fact that SIWA is a “free” alternative to other SSOs that may be paid, like Blix’s, means that such SSOs are inevitably constrained and excluded from the market even if they are superior.

**B. A Free Product Can Result in Antitrust Liability**

Much is made in the district court’s opinion of the fact that developers do not “purchase” either iOS or SIWA (Appx28) – and to be sure, neither do consumers. As mentioned previously, however, developers do pay a \$99 annual program fee and Apple takes a 30% cut off most purchases from its App Store. It is thus incorrect to state that developers do not purchase iOS – they do, in the form of paying the

developer program fee and surrendering to Apple the sizeable (and, in fact, supracompetitive<sup>1</sup>) prices from what have become largely subscription based services.

The nominal “free” nature of both Apple’s mobile OS and SIWA does not foreclose tying liability. Products that are “free” or have a non-monetary price can serve as the basis for antitrust claims. Apple is a monopolist of a particular kind, one running a “closed ecosystem,” and it can (and has attempted to) manipulate where it takes its monopoly profit to avoid antitrust scrutiny before, most notably failing to persuade the U.S. Supreme Court. *Apple Inc. v. Pepper*, 139 S. Ct. 1514 (2019). In *Pepper*, Apple faced a challenge to the pricing in its iOS App Store, and argued that its own end-users were not direct purchasers of apps from the App Store simply because they allowed the developers of these apps to set prices. Justice Kavanaugh, writing for the Court, held that Apple’s argument elevated form over substance, but worse, that if accepted, it would provide a roadmap to allow monopolistic retailers to structure their transactions to evade antitrust scrutiny. *Id.* at 1522-23.

In a similar situation to this case, in *Free FreeHand Corp.*, 852 F. Supp. 2d 1171, the defendant, Adobe, allegedly purchased FreeHand in order to take certain of its features, thereby decreasing innovation and injuring the end consumers who brought suit, but with no allegation of increased prices. *See id.* at 1188-89. With

---

<sup>1</sup> *See Epic v. Apple* [ECF No. 812 at pp. 118, 137, 147]

respect to tying, the court found that “[i]f, as alleged, Adobe ceased the development of FreeHand while steering existing FreeHand users to a bundled product, thereby further raising already high barriers to entry, it is plausible to infer that this conduct tended ‘to impair the opportunities of rivals’ and ‘did not further competition on the merits.’” *Id.* at 1184.

In *IQVIA Inc. v. Veeva Sys.*, Civ. No. 17-00177, 2018 U.S. Dist. LEXIS 171456, at \*8-9 (D.N.J. Oct. 3, 2018), a software developer alleged that an incumbent monopolist both defended its existing monopoly, and blocked plaintiff’s product in another market which it was attempting to monopolize. There, the alleged monopolist argued “that it does not charge for TPA Agreements” and so any refusal to offer such an agreement to the plaintiff was ultimately harmless. *Id.* But the Court was not persuaded given that the plaintiff’s pleading argued that absence of revenue’s purpose was to bar a rival. *Id.* at \*10. *See also Behrend v. Comcast Corp.*, Civ. No. 03-6604, 2012 U.S. Dist. LEXIS 51889, at \*126-27 (E.D. Pa. Apr. 12, 2012) (Monopolist can trade “part of its monopoly profits, at least temporarily, for a larger market share, by making it unprofitable for other sellers to compete with it.”).

The district court headed in the wrong direction by sweeping aside the possibility of a tying claim for transactions at a zero monetary price. *See Appx28.* It is widely accepted that firms that offer products at zero price and monetize in other

ways benefit from consumers’ data and attention. *See e.g.*, Tim Wu, *Blind Spot: The Attention Economy and the Law*, 82 Antitrust L.J. 771 (2019); John M. Newman, *Antitrust in Zero-Price Markets: Applications*, 94 Wash. U. L. Rev. 49, 166-72 (2016). And zero-price products and services still can compete on a variety of nonprice dimensions such as quality and privacy. Antitrust law can act to protect such competition and by extension consumers. *See* Daniel L. Rubinfeld & Michael Gal, *The Hidden Costs of Free Goods: Implications for Antitrust Enforcement*, 80 Antitrust L.J. 521, 551 (2015-2016); Terrell McSweeney & Brian O’Dea, *Data, Innovation, and Potential Competition in Digital Markets—Looking Beyond Short-Term Price Effects in Merger Analysis*, Fed. Trade Comm’n 2-3 (Feb. 22, 2018); Assistant Att’y Gen. Makan Delrahim, *“I’m Free”: Platforms and Antitrust Enforcement in the ZeroPrice Economy*, Address at Silicon Flatirons Annual Tech. Policy Conference at the Univ. of Co. L. Sch. (Feb. 11, 2019), (antitrust law applies “in full” to zero-price markets because firms offering “free” products and services compete on a variety of dimensions other than price).

Apple is the exclusive seller of devices that use its mobile OS, which it conceded for the purposes of the motion to dismiss is a monopoly. It sells these devices at a premium, and they require iOS to be operable. Thus whether the device is free and the OS is expensive, or the OS is free and the device is expensive, Apple simply elects how it chooses to extract revenue – from the transaction. While Apple

may choose to make iOS free to users, it is hardly out of generosity. Free iOS steers users to paid portions of the Apple ecosystem and, furthermore, undermines paid competitors.

To compound this effect, Apple, the monopoly maker of mobile operating system software, also gives away SIWA specifically to preempt competitors that could dilute the value of its OS monopoly, Appx536-537 (¶¶147, 152); Appx548 (¶¶200-01); Appx551 (¶¶214-15); Appx568 (¶282), or else reduce its ability to monetize its monopolistic control over developers, Appx537-538 (¶154); Appx547 (¶195); Appx569 (¶284); Appx571-573 (¶¶292-96, 299). Clever structuring of transactions should not be allowed to immunize Apple from antitrust scrutiny, as Justice Kavanaugh warned. *Pepper*, 139 S. Ct. 1522-23.

### **CONCLUSION**

For the foregoing reasons, the decisions dismissing Blix's claims for patent infringement, monopoly maintenance, and monopoly tying should be reversed.

Dated: November 3, 2021

**WOLF HALDENSTEIN  
ADLER FREEMAN &  
HERZ LLP**

By: /s/ Thomas H. Burt  
THOMAS H. BURT  
*Principal Attorney*



Mark C. Rifkin  
Lillian R. Grinnell  
270 Madison Avenue, 9<sup>th</sup> Floor  
New York, New York 10016

**PEARL COHEN ZEDEK  
LATZER BARATZ LLP**

Daniel J. Melman  
Guy Yonay  
Sarah Benowich  
7 Times Square, 19<sup>th</sup> Floor  
New York, NY 10036

*Attorneys for Plaintiff-  
Appellant Blix Inc.*

## **ADDENDUM**

**INDEX TO THE ADDENDUM**

<b>Filing Date</b>	<b>Doc. No.</b>	<b>Description</b>	<b>Page No.</b>
03/18/2021	69	Memorandum Order Granting Motion to Dismiss	Appx 1
07/09/2021	79	Memorandum Opinion Granting Motion to Dismiss	Appx 19
07/09/2021	80	Order Granting Motion to Dismiss	Appx 30
02/12/2021	59-1	Patent No. 9,749,284	Appx 1064

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

CONTENT SQUARE SAS and  
CONTENT SQUARE ISRAEL LIMITED  
(f/k/a Clicktale Limited),

Plaintiffs,

V.

C.A. No. 20-832-LPS

QUANTUM METRIC, INC.,

Defendant.

MOXCHANGE LLC,

Plaintiff,

V.

C.A. No. 20-1123-LPS

ALE USA INC.,

Defendant.

MOXCHANGE LLC,

Plaintiff,

v.

C.A. No. 20-1440-LPS

AVIGILON USA CORPORATION,

Defendant.

**BLIX INC.,**

Plaintiff,

V.

C.A. No. 19-1869-LPS

APPLE INC.,

Defendant.

# MEMORANDUM ORDER

At Wilmington, this 18th day of March, 2021:

WHEREAS, Defendants in the above-listed cases filed Rule 12 motions to dispose of patent infringement claims on the bases that certain patent claims are invalid under 35 U.S.C. § 101, because they are allegedly directed to patent ineligible subject matter;

WHEREAS, the above-listed cases brought by Content Square SAS and Content Square Israel Limited (together, “Content Square”), Moxchange LLC (“Moxchange”), and Blix Inc. (“Blix”) are unrelated to one other;

WHEREAS, the Court heard oral argument in all of the above-listed cases on March 12, 2021, and has considered the parties' respective briefs and related filings;<sup>1</sup>

WHEREAS, the Court continues to find that its experimental procedure of addressing multiple Section 101 motions from separate cases in one hearing is an efficient use of judicial resources and a beneficial tool for resolving the merits of Section 101 motions;

**NOW, THEREFORE, IT IS HEREBY ORDERED** that, with respect to the above-listed Content Square case, Defendant's Rule 12 motion (C.A. No. 20-832 D.I. 11) is **GRANTED IN PART and DENIED IN PART**, and Defendant's motion to stay pending *inter partes* review (D.I. 22) is **DENIED**;

**IT IS FURTHER ORDERED** that, with respect to the above-listed Moxchange cases, Defendants' Rule 12 motions (C.A. No. 20-1123 D.I. 8; C.A. No. 20-1440 D.I. 11) are **DENIED**; and

<sup>1</sup> Chief Judge Leonard P. Stark and Magistrate Judge Sherry R. Fallon jointly presided throughout the argument. The Court adopts the full bench ruling.

**IT IS FURTHER ORDERED** that, with respect to the above-listed Blix case, Defendant's Rule 12 motion (C.A. No. 19-1869 D.I. 50) is GRANTED.

The Court's Order is consistent with the bench ruling announced at the hearing on March 12, 2021, pertinent excerpts of which follow:

Initially, let me note, all of the motions today present Section 101 patent eligibility issues arising in a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim upon which relief can be granted. I have, of course, applied the well-known standard applicable to Rule 12(b)(6) motions, which is not disputed in any of the cases argued today.

I've also, of course, applied the now very familiar two-step framework for patent eligibility under Section 101. That is set out by the Supreme court in *Alice*. . . .<sup>[2]</sup>

In brief, under Section 101, an invention directed to laws of nature, physical phenomena, or abstract ideas is not patentable. To determine if an invention is patent ineligible, the Court must first determine if claims are directed to a patent ineligible concept. If the claim is directed to a patent ineligible concept, then the Court will look for an element or a combination of elements that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the ineligible concept itself. If, but only if, the defendant prevails at both Steps 1 and 2, the Court may declare the patent not eligible for patenting and dismiss the patent infringement claim.

Because the legal standards are not in dispute, for simplicity, the Court incorporates by reference the legal standards outlined in previous decisions, such as my *DiStefano Patent Trust* decision,<sup>[3]</sup> . . . which the Federal Circuit summarily affirmed in 2019, as well as the legal standards as set out in the motion to dismiss opinion in the *Blix v. Apple* case, one of the cases argued today. . . .<sup>[4]</sup>

The Court also incorporates by reference the legal standards for Section 101 and motions to dismiss under Rule 12(b)(6) as outlined in the Federal Circuit's recent decision in *Simio v. FlexSim* . . . .<sup>[5]</sup> That was from last year as well.

...

---

<sup>2</sup> *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208 (2014).

<sup>3</sup> *DiStefano Patent Trust III, LLC v. LinkedIn Corp.*, 346 F. Supp. 3d 616, 620-23 (D. Del. 2018), *aff'd*, 784 F. App'x 785 (Fed. Cir. 2019).

<sup>4</sup> *Blix Inc. v. Apple, Inc.*, 2020 WL 7027494, at \*1-3 (D. Del. Nov. 30, 2020).

<sup>5</sup> *Simio, LLC v. FlexSim Software Prods., Inc.*, 983 F.3d 1353, 1358-59 (Fed. Cir. 2020).

I'm going to go through the cases in the order they were argued. So, first is *Content Square v. Quantum Metric*. The defendant, Quantum Metric, moves to dismiss all of the asserted claims, which are claims 1 and 15 of the '525 patent,<sup>[6]</sup> claims 1, 6, and 10 of the '081 patent,<sup>[7]</sup> claims 1, 12, and 13 of the '365 patent,<sup>[8]</sup> claims 1 and 16 of the '645 patent,<sup>[9]</sup> and claims 1 and 12 of the '737 patent.<sup>[10]</sup>

The Court agrees with the parties that claim 1 of each of these five patents is representative of all of the asserted claims of that particular patent. So the Court will address the patentability of just claim 1 of each of the five patents. But the decisions I'm announcing apply [only] to . . . the asserted claims for each of the patents I am discussing. I am not making any decisions about the patentability of any unasserted claim.

To simplify and shorten the discussion, I will group the patents into three categories, as the parties have.

I will first discuss what has been referred to as the "heat map patents." These are the '737 and '645 patents. Generally, these patents relate to visual displays known as "heat maps." With respect to these, the asserted claims of the heat map patents, Quantum Metric's motion is granted.

Let me go through the *Alice* Step 1 and Step 2 analysis to explain how I reached this conclusion.

At Step 1, the Court agrees with Quantum Metric that the '737 patent is directed to gathering, processing, and simultaneously displaying website browsing data. The Court further agrees with Quantum Metric that the '645 patent is directed to receiving and processing a user's webpage browsing data for display.

In other words, the Court also agrees with Quantum Metric that both of the heat map patents are directed to the collection, processing, and display of web browsing data. These are fair characterizations of the claims and do not improperly oversimplify them.

The Federal Circuit has repeatedly held that claims directed to the collection, analysis, and display of data are abstract.

---

<sup>6</sup> U.S. Patent No. 7,941,525.

<sup>7</sup> U.S. Patent No. 9,508,081.

<sup>8</sup> U.S. Patent No. 9,792,365.

<sup>9</sup> U.S. Patent No. 10,063,645.

<sup>10</sup> U.S. Patent No. 10,079,737.

*Trading Technologies II*<sup>[11]</sup> is instructive on these points. The heat maps in the '737 and '645 patents are similar to the graphical user interfaces in that case. Even if the heat maps process the displayed information, they are still abstract.

The *Electric Power* case<sup>[12]</sup> provides further support for the conclusion that the collection, analysis, and display of data is abstract.

These patents do not include specific details for how the visual displays are scaled. The claims are result-focused and functional, which . . . provides further support for the Court's conclusion that they are directed to an abstract idea.<sup>[13]</sup>

To the extent that the '645 patent discloses a simple algorithm for calculating the salience for the page view, such a calculation can also be performed mentally or by hand and is abstract.

Contrary to Plaintiffs' argument, these patents are not similar to the patents involved in *Core Wireless*,<sup>[14]</sup> in which the claims were directed to improved user interfaces. The '737 and '645 claims are not directed to interfaces.

Again, the Federal Circuit has stated that "the collection, organization, and display of two sets of information on a generic display device is abstract." That is from *Trading Techs. I*,<sup>[15]</sup> . . . [a]nd I believe that that fairly characterizes these claims at Step 1.

Because Defendant has met its burden at Step 1, the Court moves on to Step 2. At Step 2, the Court considers whether the claims as a whole contain an element, elements, or an ordered combination that ensures that the patent in practice amounts to significantly more than a patent upon the ineligible concept itself.

The representative claims of the '737 and '645 patents merely recite the abstract ideas themselves. And the case law is clear that an abstract idea itself cannot be the inventive concept required at Step 2.<sup>[16]</sup>

For example, Plaintiffs point to the "generating" steps, but those steps are abstract and cannot provide the inventive concept.

---

<sup>11</sup> *Trading Techs. Int'l, Inc. v. IBG LLC*, 921 F.3d 1378 (Fed. Cir. 2019).

<sup>12</sup> *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350 (Fed. Cir. 2016).

<sup>13</sup> See, e.g., *Affinity Labs of Tex., LLC v. DIRECTV, LLC*, 838 F.3d 1253 (Fed. Cir. 2016).

<sup>14</sup> *Core Wireless Licensing S.A.R.L. v. LG Elecs., Inc.*, 880 F.3d 1356 (Fed. Cir. 2018).

<sup>15</sup> *Trading Techs. Int'l, Inc. v. IBG LLC*, 921 F.3d 1084, 1093 (Fed. Cir. 2019) (quoting *Interval Licensing LLC v. AOL, Inc.*, 896 F.3d 1335, 1345 (Fed. Cir. 2018)).

<sup>16</sup> *Genetic Techs. Ltd. v. Merial L.L.C.*, 818 F.3d 1369 (Fed. Cir. 2016).



Nor does the ordered combination of the steps in the claimed method provide an inventive concept because that order is conventional. Data must be collected before it is analyzed, and it must be analyzed before it can be displayed in its processed form. That is the order in which the claims here are practiced. And among other cases, *Two-Way Media*<sup>17</sup> shows that this is conventional.

In reaching the conclusion that the asserted claims of the '645 patent are ineligible for patenting, the Court has determined that Plaintiffs' proposed claim construction for the '645 patent does not alter the analysis. I have assumed, for purposes of the motion, that the proposed construction that the plaintiffs identified is plausible and will be adopted. But even doing so, the claims fail at both Step 1 and 2.

Plaintiffs did not raise any potentially dispositive claim construction disputes for the '737 patent.

... Let me turn next to the "multivariate testing patent," the '365, which involves creating multiple versions of a website to determine users' preferences. With respect to the asserted claims of this patent, Quantum Metric's motion is denied.

There is at least a factual dispute at Step 2 as to whether the ordered combination of claim limitations in the representative claim is conventional, routine, and well understood.

At *Alice* Step 1, the Court does agree with Quantum Metric ... that the '365 patent is directed to gathering data, analyzing that data to recognize a subset of data, and storing that data. This is not, in my view, an oversimplification of the representative claim. The claim does not involve substantially more than the collection, analysis, and storage of data.

We know from cases like *Content Extraction*<sup>18</sup> that collecting data, recognizing a subset of the data, and storing the recognized data is an abstract idea.

Plaintiffs' analogy to *SRI International*<sup>19</sup> is unpersuasive. That case involved improvements to computer security, but it does not seem that this is what we have in the '365 patent.

Plaintiffs' allegation that this claim is directed to a technical improvement [and] solving [a] computer-specific problem is, in the context of Section 101, a legal conclusion which the Court need not take as true.

---

<sup>17</sup> *Two-Way Media Ltd. v. Comcast Cable Commc'ns, LLC*, 874 F.3d 1329 (Fed. Cir. 2017).

<sup>18</sup> *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat'l Ass'n*, 776 F.3d 1343 (Fed. Cir. 2014).

<sup>19</sup> *SRI Int'l, Inc. v. Cisco Sys., Inc.*, 930 F.3d 1295 (Fed. Cir. 2019).

It is here, as well, unpersuasive. The representative claim of the '365 patent does not appear to be directed to a specific technique for solving a computer-specific problem.

... At Step 2, the defendant has failed to meet its burden to show by clear and convincing evidence that claim 1 of the '365 patent does not capture an inventive concept.

The Court is not persuaded at this stage that the claim is nothing more than a claim to the abstract idea, or is merely a claim to practicing the abstract idea using ... conventional computer components and conventional computer techniques ...

While Defendant may ultimately prove that the web crawling limitation could be practiced using conventional web crawling techniques, which is at a minimum suggested in the specification, for instance, at column 4, lines 43 to 47, I am unable to find today, on the very limited record, that the claimed web crawling was conventional, well understood, and routine.

The Court does not view the web crawling technique in the '365 patent as analogous to the scanner in *Content Extraction*. There was a real-world comparison to the claims there, while no persuasive comparison has similarly been identified here as of yet.

Further, the representative claim of the '365 contains other limitations, including the "analyzing" limitation. Those other limitations may themselves be not conventional ... not well understood and not routine, and there is at minimum a factual question about that. And the same factual questions arise about the ordered combination of the claim limitations.

Plaintiffs propose a claim construction here as well, which, if adopted, would seem to raise the possibility of additional ... fact disputes.

So for all these reasons, Defendant's motion is denied with respect to the '365 patent.

The other Content Square patents that were argued are the "user tracking patents," that is the '081 and the '525 patents, which generally relate to methods for tracking users' web browsing activity, which Plaintiffs call "session replay." On these patents, Quantum Metric's motion is denied. ...

The Court believes it is fair to address both of these patents together, that is, the '081 and the '525, and I find for both of them that Defendant has failed at both Steps 1 and 2.

At Step 1, Quantum Metric argues that the '081 and '525 patents are directed to collecting data regarding a website and the user's activities and combining this data

to create user activity information that allows for compensating for display differences. That's the articulation from the brief.

This is not, in my view, a fair characterization of what the claims are directed to. The representative claims recite numerous steps, and Quantum Metric's proposal improperly oversimplifies them.

Quantum Metric compared this case to *Digitech*,<sup>[20]</sup> but there the claims were significantly more limited to the manipulation of data.

... The *McRO* decision,<sup>[21]</sup> . . . provides a better comparison. Like the claimed methods in *McRO*, which related to automatically animating lip synchronization and facial expressions for 3D characters, the methods here involve a process specifically designed to achieve an improved technological result in conventional industry practice.

While not dispositive, it is noteworthy that Defendant has also failed to persuade the Court that the methods of the user tracking patents were previously accomplished by humans.

I will move on to *Alice* Step 2, even though Defendant has failed at Step 1. Defendant has, in any event, failed at Step 2 as well, as it has not shown that the representative claims lack an inventive concept.

In particular, the '525 patent claims a non-linear transformation that involves converting each associated element of the portion of the webpage in a piece-wise linear fashion. Although claim 1 of the '081 patent is not as specific, it also requires compensating for differences in visual displays.

To me, that means there is at least a factual dispute as to whether the "transformation" and "compensating" steps were conventional, well understood, and routine at the pertinent date. There is also a factual dispute as to whether the ordered combination of the method steps might be inventive.

Further, to the extent claim construction is necessary, and as Content Square points to a couple of terms that it believes need to be construed prior to resolving the 101 issue, this would provide yet another reason that the motion should be denied with respect to the user tracking patents.

So in sum, the Quantum Metric motion to dismiss is granted in part and denied in part.

---

<sup>20</sup> *Digitech Image Techs., LLC v. Elecs. for Imaging, Inc.*, 758 F.3d 1344 (Fed. Cir. 2014).

<sup>21</sup> *McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299 (Fed. Cir. 2016).

It is granted to the extent that . . . the patent infringement claims based on the asserted claims of the heat map patents, the '737 and '645, . . . are dismissed because the patent claims are directed to non-patentable subject matter.

Now, I recognize that Plaintiffs have requested leave to amend with respect to any patents that the Court might find to be non-patentable.

It seems possible that, given my conclusions about the heat map patents, amendment might be futile, but there has been no briefing and no argument to date on that point.

Therefore, if Plaintiffs believe that amendment would not be futile and believe that amendment would not otherwise be unwarranted, Plaintiffs may, in a timely manner, file a motion for leave to amend, attaching the proposed amended complaint accompanied by a three-page letter brief. That is, if Plaintiffs choose to pursue amendment, we will follow the letter briefing procedure that I often use for motions to amend and motions to strike.

In all other respects, Defendant's motion is denied.

Defendant has not met its burden to show that the multivariate testing patent, that is, the '365, or the user tracking patents, the '525 and '081, are non-patentable.

. . . Quantum Metric's motion to dismiss Content Square SAS as a plaintiff for lack of standing is denied.

This denial is without prejudice to renew should Defendant develop evidence it believes would give the Court a basis to find that Content Square SAS lacks standing.

. . . Finally, in this case, there is the motion for a stay pending IPR. . . That motion is also denied, and that denial also is without prejudice.

. . . Defendant may renew its motion and submit briefing on it if any of the IPRs are actually instituted and if, after meeting and conferring with Plaintiffs, the parties do not agree on whether this case should be stayed.

I do further direct that the parties meet and confer and submit a joint status report a week from today.

. . . That's it on the first case.

Let me now move on to the second set of cases, the Moxchange cases.

Here, we have two different defendants, ALE and Avigilon, both of which filed their own 12(b)(6) motions to dismiss claims that they infringed the claims of three U.S. patents: The '254, the '664 and the '232.<sup>[22]</sup>

Generally, the '254 and '232 patents are directed to a method of generating new encryption keys from a data record and a previous encryption key.

The '664 patent generally discloses a method of authentication between wireless communication network nodes in which the nodes synchronously regenerate authentication keys based on an initial authentication key.

While the motions were briefed separately, they were efficiently argued together today. They present similar and pretty much identical arguments. Both involved Section 101 challenges to the patentability of the same claim[s] of the same three patents, so I will address both motions together.

Having conducted the necessary analysis, and for the reasons I will explain, I have decided that both ALE's motion to dismiss and Avigilon's motion to dismiss will be denied.

The Court limits its analysis to just claim 1 of each of the three patents just as the parties have. The motion was not directed to any other claims, no other claims have been briefed or argued, and my decision does not reach those claims.

One other preliminary point. I, of course, carefully considered the cases cited by the parties, and particularly those each identified as most applicable . . . . [F]or Plaintiff [that] is *TecSec*<sup>[23]</sup> and for Defendants it is *Digitech*.<sup>[24]</sup> But given my analysis of the motion, as you will see, I do not find it necessary to expressly address either of those cases. . . .

Because I find a fact dispute at Step 2 and find the defendants have not met their burden at Step 2, I am not making a decision today at Step 1 as to whether the claims at issue in this case are directed to an abstract idea.

As I will explain in a moment at Step 2, I also believe claim construction is necessary before the 101 decision can be made on these patents. That makes it prudent, at least in this case, not to make a determination at Step 1 until after claim construction.

I recognize that Plaintiff's operative complaint makes allegations about what the claims are directed to, and I recognize that Defendants agree that this is what the

<sup>22</sup> U.S. Patent Nos. 7,860,254; 7,376,232; and 7,233,664.

<sup>23</sup> *TecSec, Inc. v. Adobe Inc.*, 978 F.3d 1278 (Fed. Cir. 2020).

<sup>24</sup> *Digitech Image Techs., LLC v. Elecs. for Imaging, Inc.*, 758 F.3d 1344 (Fed. Cir. 2014).

claims are directed to, and, arguably, the Court could make a legal determination at this point whether the claims are directed to an abstract idea, but for the reasons I have just noted, I'm going to defer ruling on Step 1 and will only do so if, after claim construction, at some appropriate point, I am asked again to consider the 101 issue.

So I'll turn to Step 2. And here, I conclude . . . the defendants have failed to meet their burden for at least the reason that claim construction is necessary before the Court can complete the Step 2 analysis.

In the briefing, Plaintiff stated, though admittedly without any detail or sustained argument . . . that claim construction would be necessary before the 101 issues could be decided. In the recent checklist letter, Moxchange identified three claim terms it believed need to be construed before patentability could be determined.

Most importantly, Plaintiff proposes construing the term "regenerating" to mean "performing automated continuous key modification." The Court is unable to say at this stage that Plaintiff's . . . proposed claim construction[] is implausible or frivolous.

If the Court assumes without deciding that it will adopt Plaintiff's construction of "regenerating," then it appears to follow that there is at minimum a fact dispute as to whether what may be an inventive concept, the continuous nature of key regeneration, would be captured by the claim language.

There is, in the specification, extensive discussion of the purported benefits of practicing the claims of the Moxchange patents. But the real dispute in this case, as I see it, is whether those benefits, such as improved data security, quicker systems operation, encryption keys having very short lifetime . . . are captured in the claim. If I am persuaded in the claim construction process to adopt Plaintiff's proposed constructions, it may follow that those benefits are captured in the claim.

At this stage, drawing all reasonable factual inferences in favor of Plaintiff, and assuming without deciding that the Court will adopt Plaintiff's proposed construction of "regenerating," there is a factual dispute as to whether continuous regeneration of keys, which would seem to be on this construction, captured in the claim . . . would have been well understood, routine, or conventional at the time of the patent.

As to the conventionality of regenerating keys, Defendants point to what appears to be an impressive amount of evidence to support their position. But Plaintiff also point[s] to some evidence, including from the prosecution history, to support its contrary position. And Plaintiff is correct that just because what is now purported to be inventive may have been referenced in prior art, that does not prove that something was conventional, well understood, and routine. Although here, the Defendants cite more than just one place, including . . . the specification and file



history where the purported inventive concept may have been identified and described as non-inventive. . . .

[U]ltimately, this is a motion to dismiss. I am bound to draw all reasonable inferences in Plaintiff's favor, and the record also contains some evidence in the plaintiff's favor. So on the whole, I cannot find on this record clear and convincing evidence that the purported inventive concept[s] of these patents were all conventional, well understood, and routine. Therefore, the Court will deny Defendants' motions to dismiss.

I do believe that this case is ready for scheduling, and I direct the parties to meet and confer and to submit within two weeks their proposal for a schedule. Given my conclusions regarding Section 101, as well as concerns that have been raised about novelty and possibly even issues that might arise under Sections 102 and 103, I invite the parties as they are meeting and conferring and formulating their scheduling proposals to consider whether to propose a schedule that would get us to claim construction early, perhaps even before much or any discovery, and to further consider whether we might efficiently benefit from another round of motions practice after claim construction. I'm not agreeing that I will do any of these things, but I am willing to consider them, and I do invite the parties to consider whether they want to propose any of that and whether they think any of it logically follows from what I said today in denying the 101 motion.

That's all I had to say on the Moxchange cases, so let me finally turn to *Blix vs. Apple*.

Apple has moved to dismiss the remaining asserted claims of Blix's '284 patent.<sup>[25]</sup> For the reasons I will explain, Apple's motion is granted.

In this case, I have already ruled on a previous motion to dismiss the claim brought by Blix against Apple for infringement of the same '284 patent. I issued an opinion last November, in which I held that claim 17 is not representative. I also held that claim 17 was directed to non-patentable subject matter under Section 101 and, therefore, I granted Apple's motion to dismiss with respect to claim 17.<sup>[26]</sup>

In doing so, I held that claim 17 was directed to an abstract idea at Step 1, specifically, facilitating anonymous communication using a proxy. At Step 2, I found that claim 17 did not capture any inventive concept, explaining claim 17's method for controlling pre-interaction merely recites the conventional steps of gathering, categorizing, organizing, and comparing data . . . . [I] added that the ordered combination of limitations consists of performing conventional steps with conventional computer components.

<sup>25</sup> U.S. Patent No. 9,749,284.

<sup>26</sup> *Blix*, 2020 WL 7027494.

After some further consultation with the parties, I held that Blix could file an amended complaint if it wished to assert infringement of claims other than claim 17, and, of course, Apple would then have an opportunity to move to dismiss any additional asserted claims; and that is what has happened.

The operative complaint is now Blix's second amended complaint, and I view today's motion as directed to the second amended complaint. . . .

. . . The briefing on the motion cites 26 claims. [And] the parties agree today that the motion is directed to 26 claims. So my ruling goes to all 26 of them, so my finding is that all 26 of them are not patentable. To be precise, the claims that are ruled on today are 1 through 5, 7 through 11, 13 through 15, 18, 21 to 24, 28 to 30, and 33 to 37.

There is a somewhat tricky matter as to representative claims . . . . [I]n the November opinion[,] based on the briefing I had before me at that time[,] I found that claim 17 was not representative. I see no reason to reevaluate that decision today.

In the briefing for today, Apple briefed all 26 remaining asserted claims but Blix did not. Its brief is limited pretty much to claims 1 and 11. But Blix did not agree that these claims are representative of any other claims. Blix is correct that it's Defendant's burden to show by clear and convincing evidence that each of these 26 claims is not patentable. So, technically, I suppose Blix is correct that it does not have to respond to Apple's arguments on all of the claims. However, of course, it would have been helpful if Blix had responded on each of the claims it was still asserting and defending the validity of.

But more importantly, I do find, as I will further explain, that Apple has met its burden on all 26 claims. . . . I was persuaded by and agree with all of the arguments that Apple has made on all 26 claims with respect to Steps 1 and Step 2.

Turning to Step 1. In the November opinion I held, as I have already mentioned, that claim 17 was directed to the abstract idea of facilitating anonymous communication using a proxy. Blix has identified no material difference in any of the other 26 remaining asserted claims that would lead to a conclusion that any of them are directed to something other than that same abstract idea that I found claim 17 to be directed to.

Blix asserts that the remaining asserted claims are directed to a solution uniquely implementable in computers, such that it improves computer efficiency, relying on, for example, *TecSec*.<sup>27</sup> The Court already rejected this argument with respect to claim 17, and it fares no better in connection with the remaining asserted claims. In considering claim 17 as a whole, I found that it was directed to an abstract idea

---

<sup>27</sup> *TecSec*, 978 F.3d at 1278.



that invoked computers as a tool, claiming only desirable results rather than improving the performance of a computer. The Court's conclusion is the same with respect to the remaining asserted 26 claims.

Let me turn to those 26 claims. They can be categorized into three categories. . . .

[A]t Step 1, the first category I have considered are those claims that depend from claim 17. Those are claims 18, 21, 22, 23, and 24; the second category [are] those claims that depend from claim 27, that is, 28, 29, 30, 34, 35, 36 and 37. And the final category is claim 1, and those that depend from claim 1, that is, claims 2, 3, 4, 5, 7, 8, 9, 10, 11, 13, 14, and 15.

I see nothing in any of them, and I have considered them all, that changes the abstract idea analysis. And Plaintiff provides no persuasive argument to the contrary. So Apple has met its burden at Step 1 with respect to all of the remaining asserted claims.

Turning to Step 2, again, as mentioned, in November I found that claim 17 is not transformative and recites the merely conventional step[s] of gathering, categorizing, organizing, and comparing data. The Court reaches the same conclusion for all of the remaining 26 dependent claims.

Blix's efforts to persuade the Court that some or all of the remaining dependent claims are transformative under Step 2 fail. The purported inventive concepts are not in the claim[s]. The remaining asserted claims are not directed to anything more than the abstract idea and the conventional steps of communicating, that is, including gathering, categorizing, organizing, and comparing data. I'm going to now run through the limitations of the 26 claims, highlighting how they may differ from claim 17, but, again, I have found that none of these limitations make a difference in Step 2. The additional limitations are results-oriented and functional; they are not specific to computers.

None of these claims, taken as a whole and as an ordered combination, claim anything other than the conventional steps of communication and the abstract ideas I have identified.

The first category of those claims depending from claim 17 add only one of the following limitations:

- In claim 18, it's the method of claim 17 wherein that method is not followed by a communication.
- In claim 21, a predefined rule is performed, to include a predefined response, such as recording, converting, or forwarding a communication.

- Claim 22, a predefined rule is performed to include assignment to a private interaction address, a manageable public interaction address, or a reverse list.
- Claim 23 adds use of a communication preference with respect to the various interaction addresses.
- Claim 24 adds, where a different communication preference allows the display of the public interaction address.

None of these additional limitations make a difference, in my view, at Step 2.

The second category is claim 27 (which itself is not asserted) and the claims that depend from it. Claim 27 has the same limitations as claim 17, but it is in a system format. It uses generic computer components merely as a tool. And the claims depending from claim 27 add nothing to render them directed to anything other than the same abstract idea I have already identified.

- Claim 28 is the system of claim 27, wherein there is initiation of communication from a manageable public interaction address.
- Claim 29 adds to 27, wherein a networking terminal is configured to receive, identify, and associate the incoming communication with the public interaction address.
- Claim 30 adds to 27, wherein the system's use is not followed by a communication.
- Claim 33 adds to 27, a microprocessor that can execute a predefined rule, such as recording, converting, or forwarding a communication.
- Claim 34 adds to 27, a microprocessor that executes a predefined rule to include assignment to a private or manageable public interaction address or a reverse list.
- Claim 35 adds to 27, computer parts capable of enabling a default computer preference assigned to the various interaction addresses.
- Claim 36 adds to 27, use of a computer storage memory that presents content, such as text, data, audio, or video files, graphics, or links.
- Claim 37 adds to 27, computer storage memory configured to store a default communication preference which qualifies the means of pre-interaction.

Again, none of these, in my view, make a difference at Step 2.

And the same conclusion follows from the third and final category of remaining asserted claims, independent claim 1 and its dependent claims. These claims, too, are directed to the abstract idea of facilitating anonymous communication using a proxy, and they do not succeed at Step 2.

Claim 1 claims each of the same limitations as claim 17 with the addition that there be an incoming and outgoing communication, that these communications are initiated and received by various parties, and that those communications are identified and categorized. None of those additional limitations specify a problem uniquely related to computers and do not solve such a problem. Instead, they merely invoke the abstract idea of communication in which computers are used as a tool.

Blix asserts that claim 1 is directed to the ability to seamlessly communicate confidentially and transparently, which permits security and caller recognition for caller ID and screening. I conclude this is just another way of saying that the patent is directed to anonymous communication using the proxy.

Blix further argues that claim 1 claims a method that cannot be performed by humans without a computer, and that this is a significant clue that the claim is not directed to an abstract idea. Whether a human could perform the method is merely a clue and is not dispositive of any issue in a 101 analysis. But in any case, this clue detracts from Blix's position because, in my view, a human [can] perform the method of claim 1. For example, a human landlord can perform controlled reciprocal communications by putting an ad in a newspaper for a tenant. The tenant could perform the same by keeping himself or herself anonymous from the landlord by use of a reverse list, or a popular person could use telephone screening to remain anonymous while still remaining in communication with those they desire to communicate with. And these are examples for which you could find support in the '284 patent, for instance, at Columns 18 and 19.<sup>[28]</sup>

The claims depending from claim 1 add no limitations that change this analysis.

- Claim 2 is the method of claim 1 with the additional limitation that an identity of a communicator be identified and associated to that party.
- Claim 3 requires the additional limitation of associating an interaction address with the reverse list.
- Claim 4 requires the additional limitation that a communication be rejected, attempted, interrupted, incomplete, or abrupted.
- Claim 5 requires that an interaction address be associated with a telephone number, screen name, or other indicia of identity.

---

<sup>28</sup> See '284 Patent at 18:65-19:48.

- Claim 7 requires the forwarding of communications or information or presentation of communication or manageable public addresses.
- Claim 8 requires further the use of a reverse list to associate a name to addresses, identities, rules, or data.
- Claim 9 requires generation of a reverse list by specified entities.
- Claim 10 requires generation of a reverse list by further specified means, such as manual input.
- Claim 13 requires further performance of a predefined rule, such as rejection of, recording of, or converting a communication.
- Claim 14 further requires controlled reciprocating communication with the additional performance of a default communication preference or an alternative with respect to the interaction addresses.

I skipped claim 11. I'll come back to it just briefly. It is one of . . . only two of the remaining asserted claims that Blix really briefed. Claim 11 claims methods of controlled reciprocating communication or the interaction address and at least a portion of a reverse list entry are unavailable to a first party. Essentially, then, claim 11 claims methods of two-way communication where anonymity of a party is ensured. Claim 11, then, in my view is still directed to the abstract idea of anonymous communicating using a proxy.

And here, at Step 2, I find no basis in the record to conclude anything other than that claim 11 is using conventional methods to keep data confidential. Again, for all of the remaining asserted claims, each of the additional limitations relate to a result-oriented aspect of communication, not a computer-oriented solution or problem. I agree, then, with Apple, that the claims are not a computer-centric solution to a computer-centric problem. They are, instead, claims to the use of a generic computer as a tool, as a solution to a human problem. So Apple has met its burden at Step 2.

I'll just briefly address a few additional arguments that Blix has made. First, the cases relied on by Blix do not alter the outcome. All, or nearly all, of those cases are ones I already considered in connection with the decision on claim 17. They are all also distinguishable for at least the reasons Apple has given.

Second, Blix points out that during prosecution, the Examiner found the patent novel over the prior art. But novelty is not the same as 101, and the Court is not bound, of course, to agree with the Examiner. The appropriate deference is recognized by the clear and convincing burden of proof that rests on Defendant, and which here, for the reasons I have explained, Defendant has met.

Blix contends that its patent does not preempt all communication or even all anonymous communication. But even assuming that is true, it's not dispositive. If, as I have found, a patent claim fails both steps of the *Alice* test, that claim is not patent eligible and no separate preemption analysis is required.<sup>[29]</sup> . . .

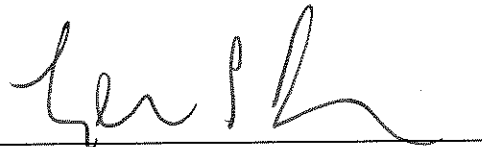
And, finally, Blix's allegations about statements Apple made about Apple's own products and Apple's problems do not plausibly support a finding that Blix's claims are patentable. So, again, the 101 motion from Apple is granted.

There is one other dispute between Blix and Apple that I want to take a moment to briefly address. . . . I'm going to now set out the schedule and page limits for Apple's forthcoming motion to dismiss the amended antitrust claim.

. . .

- Apple's opening brief will be due on April 15th and can be up to 30 pages.
- Blix's answering brief is due on May 15th, and also can be up to 30 pages.
- Apple's reply brief will be due on May 28th and can be up to 15 pages.

And I am scheduling oral argument for June 8th at 1:00 p.m. Each side will have up to one hour, and I am tentatively and optimistically and hopefully scheduling the June 8th hearing to be in court. That will be subject to further review by me and by the parties. If, as June 8th approaches, any party believes it would be a hardship or in any way wrong for us to meet together in court, just let me know that and we can, of course, easily convert it to a remote hearing.



HONORABLE LEONARD P. STARK  
UNITED STATES DISTRICT JUDGE

---

<sup>29</sup> *Athena Diagnostics, Inc. v. Mayo Collaborative Servs., LLC*, 915 F.3d 743, 752 (Fed. Cir. 2019) ("Preemption is sufficient to render a claim ineligible under § 101, but it is not necessary.").

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

---

BLIX INC.,	:	
	:	
Plaintiff,	:	
	:	
v.	:	C.A. No. 19-1869-LPS
	:	
APPLE, INC.,	:	
	:	
Defendant.	:	

---

John G. Day, Andrew C. Mayo, ASHBY & GEDDES, Wilmington, DE

Daniel J. Melman, Guy Yonay, Sarah Benowich, Shaoul Sussman, PEARL COHEN  
ZEDEK LATZER BARATZ LLP, New York, NY

Mark C. Rifkin, Thomas H. Burt, WOLF HALDENSTEIN ADLER FREEMAN & HERZ  
LLP, New York, NY

Attorneys for Plaintiff

David E. Moore, Bindu A. Palapura, POTTER ANDERSON & CORROON LLP, Wilmington,  
DE

Daniel G. Swanson, Jason C. Lo, Jennifer J. Rho, Raymond A. LaMagna, GIBSON, DUNN &  
CRUTCHER LLP, Los Angeles, CA

Cynthia E. Richman, Amalia Reiss, GIBSON, DUNN & CRUTCHER LLP, Washington, DC

H. Mark Lyon, GIBSON, DUNN & CRUTCHER LLP, Palo Alto, CA

Chris Whittaker, GIBSON, DUNN & CRUTCHER LLP, Irvine, CA

Attorneys for Defendant

**MEMORANDUM OPINION**

July 9, 2021  
Wilmington, Delaware



**STARK, U.S. District Judge:**

Pending before the Court is a renewed motion to dismiss Blix Inc.’s (“Blix” or “Plaintiff”) antitrust allegations against Defendant Apple, Inc. (“Apple” or “Defendant”). (D.I. 70) The operative complaint is Blix’s Second Amended Complaint. (D.I. 59) (hereinafter, “Complaint” or “Cmplt.”) Previous iterations alleged infringement of U.S. Patent No. 9,749,284 (the “’284 patent”) as well as certain antitrust claims (D.I. 13), which the Court dismissed in a November 30, 2020 memorandum opinion (D.I. 42), which also granted leave to file the new Complaint (D.I. 59). Following oral argument on March 12, 2021, the Court dismissed all of Blix’s patent infringement allegations due to the patent-in-suit being directed to patent-ineligible subject matter under 35 U.S.C. § 101. (D.I. 69)

As the parties note, the operative Complaint presents new and different antitrust allegations and theories of liability than appeared in the earlier complaints. (*See* D.I. 71 at 1-2; D.I. 74 at 1) On April 15, 2021, Apple filed a motion to dismiss these antitrust claims. (D.I. 70) The motion was fully briefed and then, on June 8, 2021, argued to the Court. (*See* D.I. 71, 74, 75; *see also* D.I. 78 (“Tr.”)) For the reasons stated below, the Court will grant Apple’s motion.

## **I. LEGAL STANDARDS**

### **A. Motion to Dismiss**

Evaluating a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) requires the Court to accept as true all material allegations of the complaint. *See Spruill v. Gillis*, 372 F.3d 218, 223 (3d Cir. 2004). “The issue is not whether a plaintiff will ultimately prevail but whether the claimant is entitled to offer evidence to support the claims.” *In re Burlington Coat Factory Sec. Litig.*, 114 F.3d 1410, 1420 (3d Cir. 1997) (internal quotation marks omitted). Thus, the Court may grant such a motion to dismiss only if, after “accepting all well-pleaded allegations in the



complaint as true, and viewing them in the light most favorable to plaintiff, plaintiff is not entitled to relief.” *Maio v. Aetna, Inc.*, 221 F.3d 472, 481-82 (3d Cir. 2000) (internal quotation marks omitted).

However, “[t]o survive a motion to dismiss, a civil plaintiff must allege facts that ‘raise a right to relief above the speculative level on the assumption that the allegations in the complaint are true (even if doubtful in fact).’” *Victaulic Co. v. Tieman*, 499 F.3d 227, 234 (3d Cir. 2007) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007)). A claim is facially plausible “when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). At bottom, “[t]he complaint must state enough facts to raise a reasonable expectation that discovery will reveal evidence of [each] necessary element” of a plaintiff’s claim. *Wilkerson v. New Media Tech. Charter Sch. Inc.*, 522 F.3d 315, 321 (3d Cir. 2008) (internal quotation marks omitted).

The Court is not obligated to accept as true “bald assertions,” *Morse v. Lower Merion Sch. Dist.*, 132 F.3d 902, 906 (3d Cir. 1997) (internal quotation marks omitted), “unsupported conclusions and unwarranted inferences,” *Schuylkill Energy Res., Inc. v. Pa. Power & Light Co.*, 113 F.3d 405, 417 (3d Cir. 1997), or allegations that are “self-evidently false,” *Nami v. Fauver*, 82 F.3d 63, 69 (3d Cir. 1996).

## **B. Antitrust Standing**

As the Third Circuit explained in *Pace Electronics, Inc. v. Canon Computer Systems, Inc.*, 213 F.3d 118, 120 (3d Cir. 2000):

To state a claim for damages under section 4 of the Clayton Act, 15 U.S.C. § 15, a plaintiff must allege more than that it has suffered an injury causally linked to a violation of the antitrust laws. *See Brunswick Corp. v. Pueblo Bowl-O-Mat, Inc.*, 429 U.S. 477, 489, 97 S. Ct. 690, 50 L.Ed.2d 701 (1977). In addition, it must allege



antitrust injury, “which is to say injury of the type the antitrust laws were intended to prevent and that flows from that which makes defendants’ acts unlawful.” *Id.*

### C. Sherman Act Section 2

The Third Circuit’s opinion in *Broadcom Corp. v. Qualcomm Inc.* sets out the standards for analysis of a Sherman Act Section 2 claim:

Section 2 of the Sherman Act, in what we have called “sweeping language,” makes it unlawful to monopolize, attempt to monopolize, or conspire to monopolize, interstate or international commerce. It is, we have observed, “the provision of the antitrust laws designed to curb the excesses of monopolists and near-monopolists.” *LePage’s Inc. v. 3M*, 324 F.3d 141, 169 (3d Cir. 2003) (en banc). Liability under § 2 requires “(1) the possession of monopoly power in the relevant market and (2) the willful acquisition or maintenance of that power as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident.” *United States v. Grinnell Corp.*, 384 U.S. 563, 570-71, 86 S.Ct. 1698, 16 L.Ed.2d 778 (1966). . . .

The existence of monopoly power may be proven through direct evidence of supracompetitive prices and restricted output. *United States v. Microsoft Corp.*, 253 F.3d 34, 51 (D.C. Cir. 2001) (en banc); *Rebel Oil Co. v. Atl. Richfield Co.*, 51 F.3d 1421, 1434 (9th Cir. 1995). It may also be inferred from the structure and composition of the relevant market. *Harrison Aire*, 423 F.3d at 381; *Microsoft*, 253 F.3d at 51. . . .

The second element of a monopolization claim under § 2 requires the willful acquisition or maintenance of monopoly power. As this element makes clear, the acquisition or possession of monopoly power must be accompanied by some anticompetitive conduct on the part of the possessor. *Verizon Commcn’s Inc. v. Law Offices of Curtis V. Trinko, LLP*, 540 U.S. 398, 407, 124 S.Ct. 872, 157 L.Ed.2d 823 (2004). Anticompetitive conduct may take a variety of forms, but it is generally defined as conduct to obtain or maintain monopoly power as a result of competition on some basis other than the merits. *LePage’s*, 324 F.3d at 147. Conduct that impairs the opportunities of rivals and either does not further competition on the merits or does so in an unnecessarily restrictive way may be deemed anticompetitive. *Aspen Skiing Co. v. Aspen*

*Highlands Skiing Corp.*, 472 U.S. 585, 604-05 & n. 32, 105 S.Ct. 2847, 86 L.Ed.2d 467 (1985). Conduct that merely harms competitors, however, while not harming the competitive process itself, is not anticompetitive. *See Brooke Group Ltd. v. Brown & Williamson Tobacco Corp.*, 509 U.S. 209, 224, 113 S.Ct. 2578, 125 L.Ed.2d 168 (1993).

501 F.3d 297, 306-08 (3d Cir. 2007) (internal footnote omitted).

#### **D. Tying**

Tying involves conditioning the sale of one good on the purchase of another, separate good. *See Brokerage Concepts, Inc. v. U.S. Healthcare, Inc.*, 140 F.3d 494, 510 (3d Cir. 1998).

“The antitrust concern over tying arrangements arises when the seller can exploit its market power in the tying market to force buyers to purchase the tied product which they otherwise would not, thereby restraining competition in the tied product market.” *Id.* In proving a tying arrangement, a plaintiff must allege: “(1) a defendant seller ties two distinct products; (2) the seller possesses market power in the tying product market; and (3) a substantial amount of interstate commerce is affected.” *Town Sound & Custom Tops, Inc. v. Chrysler Motors Corp.*, 959 F.2d 468, 477 (3d Cir. 1992).

### **II. DISCUSSION**

#### **A. Monopoly Maintenance**

Blix’s amended antitrust allegations do not sufficiently plead the existence of an unlawful maintenance of monopoly in violation of Section 2 of the Sherman Act. Liability under Section 2 requires “(1) the possession of monopoly power in the relevant market and (2) the willful acquisition or maintenance of that power as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident.” *United States v. Grinnell Corp.*, 384 U.S. 563, 570-71 (1966). Apple assumes, only for purposes of this motion,

that Blix has sufficiently alleged monopoly power in the market for mobile operating systems (“OS”), satisfying the first requirement. (D.I. 71 at 8) But Apple challenges the sufficiency of Blix’s allegations relating to the second requirement. The Court agrees with Apple that Blix has failed with respect to this issue.

As an initial matter, the Court observes that a fundamental premise of Blix’s monopoly maintenance claim is that Apple infringes Blix’s patent. That is, Blix contends that Apple has stolen and copied Blix’s patented technology as part of Apple’s effort to maintain monopoly power. (*See, e.g.*, Cmplt. ¶¶ 16, 226, 350-51) Because the Court has dismissed the patent infringement claims, the patent infringement component of the monopoly maintenance claims cannot constitute improper conduct. Indeed, as Blix’s Complaint expressly recognizes: “Apple is free to offer its competing Consumer SSO solution, as long as that product does not infringe on the intellectual property of Blix.” (*Id.* ¶ 249) The dismissal of the patent infringement claim, therefore, eliminates at least a substantial portion of Blix’s monopoly maintenance allegations.<sup>1</sup>

The core of Blix’s allegation seems to be that Apple has constructed a “moat” around “its user base by a series of actions that, individually and especially together, make it difficult and expensive for Apple iOS users to leave the coordinated technological ecosystem;” this moat is allegedly “grounded and protected by [Apple’s] monopoly power in its OS.” (D.I. 74 at 13) Blix

---

<sup>1</sup> Blix also alleges what it calls “Sherlocking,” which it describes as Apple’s “require[ment] that every application made available to Apple end users has to be shown to [Apple] first,” so that Apple can review the application and “decide short of patent infringement, do they like an idea. If they like an idea that someone else had first, they don’t have to wait and roll that idea out after the application rolls it out” but can, instead, beat the innovative application developer to the market. (Tr. at 33-34) The Court agrees with Apple that Blix has not shown, in the context of the Complaint, how “Sherlocking” is different from patent infringement or how it provides a cognizable basis for alleging competitive harm. (*See id.* at 13-14, 59; *see also id.* at 49-50) More generally, Blix has failed to explain why the alleged “Sherlocking” – which, again, here does not constitute patent infringement – should be viewed as willful maintenance of monopoly power as opposed to the exercise of business acumen. *See generally Grinnell*, 384 U.S. at 570-71.

points to a variety of actions that Apple has purportedly taken to maintain its monopoly, including pricing its hardware at a high level, offering proprietary “family” applications, controlling iOS application development and application payment processing, and stealing others’ ideas. (*Id.* at 13-19) For example, Blix alleges that Apple took advantage of its structural advantages to steal from Blix’s BlueMail product the idea underlying Sign In With Apple, a consumer single-sign-on (“SSO”) option. (*Id.* at 21-24) In implementing Sign In With Apple, Apple then forced Blix (and other developers) to offer Sign In With Apple as an alternative to other SSOs, thereby “inject[ing] itself as an intermediary between the developer and the user of its app.” (*Id.* at 23)

As support for its contentions, Blix unpersuasively draws comparisons to the D.C. Circuit’s decision in *United States v. Microsoft*, 253 F.3d 34 (D.C. Cir. 2001). In *Microsoft*, the D.C. Circuit held that “[i]f a consumer could have access to the applications he desired – regardless of the operating system he uses – simply by installing a particular browser on his computer, then he would no longer feel compelled to select Windows in order to have access to those applications; he could select an operating system other than Windows based solely upon its quality and price. In other words, the market for operating systems would be competitive.” *Id.* at 60. There, in squashing the competitive threats posed by emerging middleware competitors in the *internet browser market*, Microsoft committed actionable anticompetitive conduct based on its existing monopoly in the *operating system market*, and the two markets were interrelated. *See id.*

Here, Blix suggests that Apple is doing something similar to Microsoft: “work[ing] to stuff Plaintiff’s technology before it gets a foothold, so as to prevent competition that would erode Apple’s monopoly.” (D.I. 74 at 9) Blix, however, has not alleged (nor explained) how Apple’s requirement to offer Sign In With Apple means that it is eliminating competition in any market. Blix does not explain how Apple’s requirement to offer Sign In With Apple restricts competition in

*the mobile operating system market*, and it appears to be undisputed that the requirement to offer Sign In With Apple actually expands consumer choice in the *SSO market*. While Blix views its offering as “a maverick middleware product that poses a fundamental threat to the iOS monopoly in ways that other Consumer SSOs do not” (D.I. 74 at 23), its Complaint fails to adequately and plausibly allege how any action Apple is allegedly taking is harming competition.

If Blix’s allegation is that Apple is maintaining its OS monopoly by squashing competitive threats (specifically, Blix) in the SSO market, then Blix has not adequately pled such a claim. Apple’s current policy of requiring Sign In With Apple whenever any SSO product is offered permits new competitors and competition (including Blix) because it does *not* foreclose the use of other SSOs. Allowing competition is the opposite of unlawfully constraining competition, so, again, Blix has failed to state a claim.

In making its arguments, Blix makes another unpersuasive analogy, to *Roxul USA, Inc. v. Armstrong World Industries, Inc.*, 2019 WL 1109868, at \*11 (D. Del. Mar. 8, 2019). In *Roxul*, the Court found anticompetitive effect from an exclusive dealing arrangement, which “prevent[ed] a ‘maverick’” from ever “achieving a footing in the market.” *Id.* Here, by contrast, there is no exclusive dealing arrangement. To the contrary, Apple makes implementation of Sign In With Apple voluntary: developers may choose to implement no SSO at all, to implement only Sign In With Apple, or to implement Sign In With Apple in conjunction with other SSOs, such as Google or Facebook. (D.I. 59 ¶ 244) The only thing a developer is not permitted to do is to offer one or more SSOs without also offering Apple’s SSO. Clearly, this is not an exclusive dealing arrangement.

Blix also attempts to plead its claim based on what it labels a “sand in the gears” theory. (*See, e.g.*, D.I. 74 at 19-21) These allegations do not survive the motion to dismiss, for the reasons

explained by Apple. (*See, e.g.*, Tr. at 15-17) Among other things, the Complaint fails to adequately and plausibly allege that Apple has thrown “sand in the gears” of competition as opposed to just in the gears of a single competitor. Furthermore, the alleged “sand” thrown by Apple at Blix relates to Blix’s BlueMail application, which was the focus of the first two complaints, and with respect to which the Court granted Apple’s earlier motion to dismiss. (*See generally* D.I. 42 at 14-15) Blix has provided no persuasive reason why the Court should view these allegations as any less deficient in connection with the operative Complaint.

Having found that Blix’s claim fails to adequately plead a Section 2 claim on the merits, the Court need not address the parties’ arguments as to whether the claim should also be dismissed for lack of antitrust standing.

#### **B. Tying<sup>2</sup>**

Blix’s tying allegations arise under both Sections 1 and 2 of the Sherman Act. (D.I. 59 at 91) For the reasons already given, Blix has failed to allege conduct making out a viable Section 2 monopoly maintenance claim, so any tying claim predicated on the deficient Section 2 claim must also fail. With respect to Section 1, the Court concludes that Blix has also failed to adequately allege the existence of an unlawful tying arrangement.

Noticeably absent from Blix’s allegations are facts that would suffice to establish the existence of a tying arrangement. “[A] tying arrangement may be defined as an agreement by a party to sell one product [or service] but only on the condition that the buyer also purchases a different (or tied) product [or service], or at least agrees that he will not purchase that product [or service] from any other supplier.” *Avaya Inc., RP v. Telecom Labs, Inc.*, 838 F.3d 354, 397 (3d

---

<sup>2</sup> The parties agree that the tying claim must be considered under the rule of reason. (*See* D.I. 74 at 25; Tr. at 6-7; *see also Microsoft*, 253 F.3d at 84)

Cir. 2016). No such arrangement is present here.

Blix points to the tying product as iOS, within the mobile OS market. (D.I. 59 ¶ 360) The tied product is Sign In With Apple, in the consumer SSO market. (*Id.*) There are no facts, however, from which it may be plausibly inferred that Apple ties purchases of Sign In With Apple to purchases of iOS. There is no requirement that purchasers of Apple devices running iOS implement Sign In With Apple. Nor is there any allegation that developers must purchase iOS as a condition of implementing Sign In With Apple. (*See* D.I. 71 at 21) If, as the Complaint seems to allege, Sign In With Apple is not always implemented in conjunction with purchase of iOS – because, among other reasons, developers do not purchase iOS – there is no tie.

As Apple has further explained, Blix’s allegations indicate that many applications do not require any sign in at all. (*See* Tr. at 8) Those applications that do require a sign in may require an application-specific sign in instead of an SSO. (*See id.* at 8-9) It is only when the application offers the **additional choice** of a single sign in that the application developer is required to **also offer** Sign In With Apple as a choice (a free choice). (*See id.* at 9) In none of this, again, is there an adequate and plausible allegation that Apple is coercing anyone to buy Sign In With Apple as a condition of buying mobile iOS. (*See generally* Tr. at 30) (Blix contending that coercion occurs not at consumer level, but “at the developer level”) There is no sufficient allegation of an improper tying arrangement.

Apple points to other deficiencies in Blix’s tying claim, such as the insufficiency of the allegations of any restraint of trade in the allegedly tied SSO market. (*See, e.g.,* Tr. at 7-8, 11-12) Given the Court’s conclusions as already explained, the Court need not determine if there are additional dispositive failings in the Complaint.



## V. CONCLUSION

For the foregoing reasons, the Court will grant Apple's Motion to Dismiss Plaintiff's Second Amended Complaint Pursuant to Fed. R. Civ. P. 12(b)(6). (D.I. 70) As the Court is now dismissing Blix's third complaint, and Blix has been provided multiple opportunities to try to plead its claims, today's dismissal is with prejudice. The Clerk of Court will be directed to close this case. An appropriate order follows.<sup>3</sup>

---

<sup>3</sup> Blix suggests that it should be given yet another attempt to amend its pleadings because of new information. (Tr. at 41-42) Even accepting this contention, Blix has had multiple opportunities to state an antitrust claim (or patent claim) and has repeatedly failed. Blix has provided the Court no basis to conclude that a fourth complaint would be any more likely to state a claim on which relief may be granted. The Court concludes, thus, that amendment would be futile.



**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

---

BLIX INC.,

Plaintiff,

v.

APPLE, INC.,

Defendant.

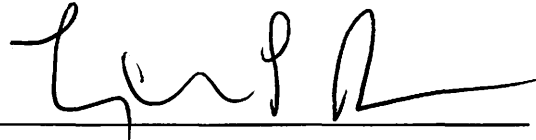
---

:  
:  
:  
:  
:  
:  
:  
:  
:  
:

C.A. No. 19-1869-LPS

**ORDER**

At Wilmington this **9th** day of **July, 2021**, consistent with and for the reasons stated in the Memorandum Opinion issued this same date, **IT IS HEREBY ORDERED** that Plaintiff Apple, Inc.'s Motion to Dismiss Plaintiff's Second Amended Complaint Pursuant to Fed. R. Civ. P. 12(b)(6) (D.I. 70) is **GRANTED**. The Clerk of Court is directed to **CLOSE** this case.



UNITED STATES DISTRICT JUDGE



US009749284B2

(12) **United States Patent**  
**Volach**

(10) **Patent No.:** **US 9,749,284 B2**  
(45) **Date of Patent:** **Aug. 29, 2017**

(54) **SYSTEMS AND METHODS OF  
CONTROLLED RECIPROCATING  
COMMUNICATION**

(71) Applicant: **PECAN TECHNOLOGIES INC.,**  
Tortola (VG)

(72) Inventor: **Ben Volach**, Haifa (IL)

(73) Assignee: **PECAN TECHNOLOGIES INC.,**  
Tortola (VG)

(\*) Notice: Subject to any disclaimer, the term of this  
patent is extended or adjusted under 35  
U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/890,986**

(22) PCT Filed: **May 12, 2014**

(86) PCT No.: **PCT/IB2014/061375**

§ 371 (c)(1),

(2) Date: **Nov. 13, 2015**

(87) PCT Pub. No.: **WO2014/184724**

PCT Pub. Date: **Nov. 20, 2014**

(65) **Prior Publication Data**

US 2016/0112368 A1 Apr. 21, 2016

#### **Related U.S. Application Data**

(60) Provisional application No. 61/822,716, filed on May  
13, 2013.

(51) **Int. Cl.**

**H04L 29/12** (2006.01)

**H04W 4/08** (2009.01)

(Continued)

(52) **U.S. Cl.**

CPC ..... **H04L 61/10** (2013.01); **H04M 3/42008**  
(2013.01); **H04W 4/08** (2013.01); **H04W**  
**4/206** (2013.01); **H04L 61/1594** (2013.01)

(58) **Field of Classification Search**

CPC .... **H04L 51/043**; **H04L 67/24**; **G06Q 30/0243**  
See application file for complete search history.

(56) **References Cited**

#### **U.S. PATENT DOCUMENTS**

7,356,567 B2 \* 4/2008 Odell ..... G06Q 10/107  
709/206

7,706,371 B1 \* 4/2010 Wing ..... H04L 12/56  
370/392

(Continued)

*Primary Examiner* — Jimmy H Tran

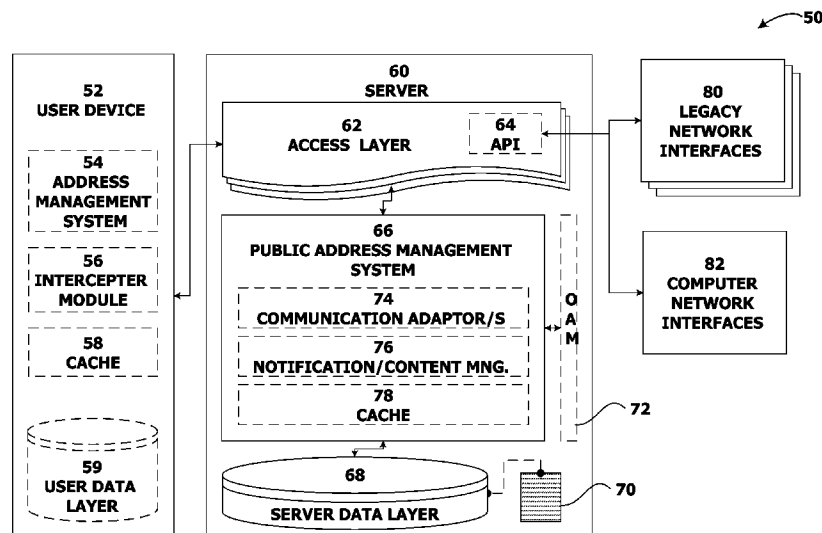
(74) *Attorney, Agent, or Firm* — Mark David Torche;  
Patwrit LLC

(57)

#### **ABSTRACT**

Systems and method for controlled pre-interaction are disclosed. The method of performing controlled pre-interaction includes: providing at least one private interaction address, defining at least one manageable public interaction address, forming a record of manageable public interaction address associated with the private interaction address. The method of performing controlled pre-interaction further includes: generating a reverse list, wherein an interaction address of a participant is associated at least with the manageable public interaction address, and performing at least one pre-interaction act. A pre-interaction act includes: accessing the reverse list, identifying the interaction address of the participant in the reverse list, and determining that the manageable public interaction address is associated, at the reverse list, with the interaction address of the participant.

**38 Claims, 4 Drawing Sheets**



## Page 2

- \* cited by examiner

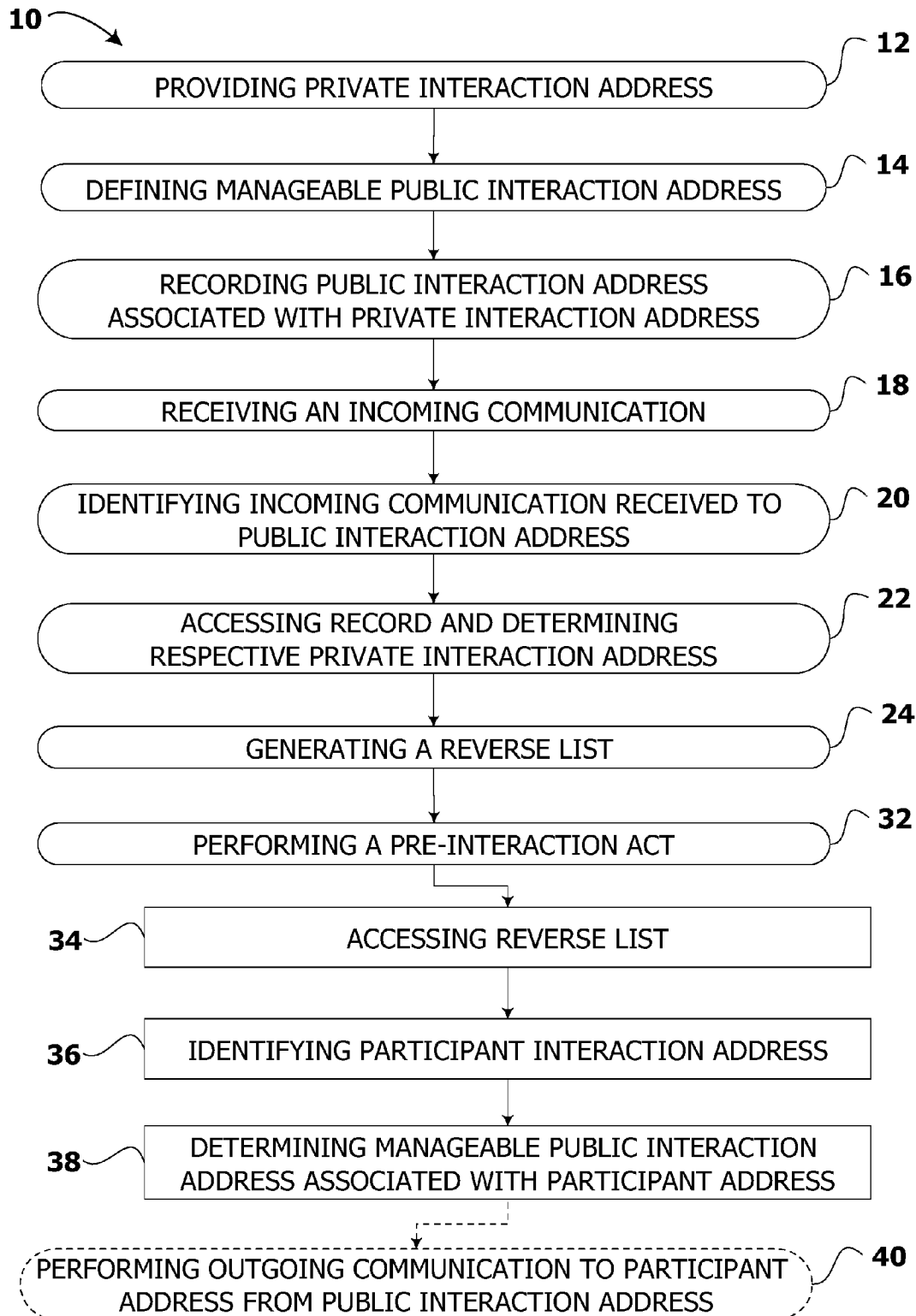
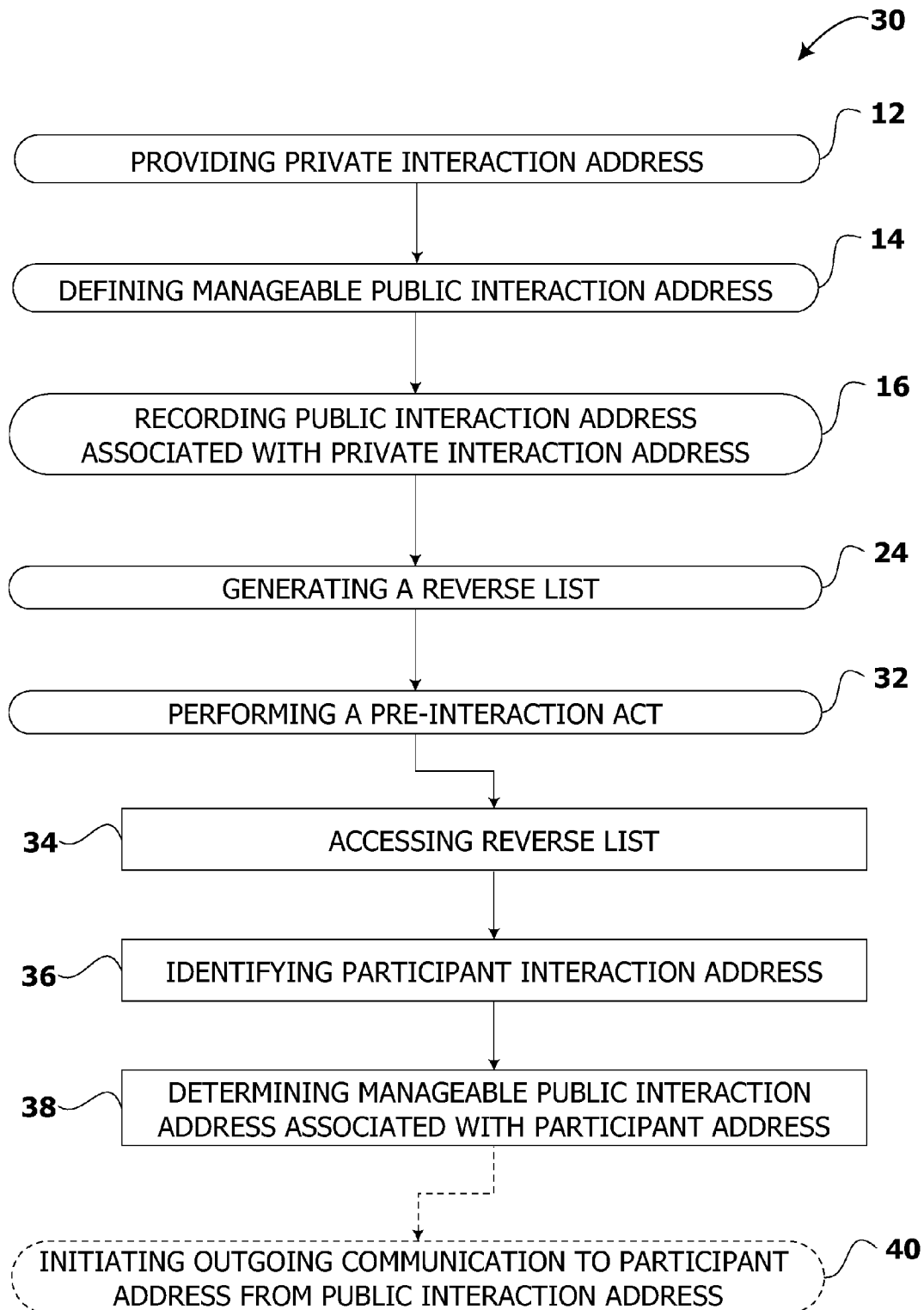


FIG 1



**FIG 2**

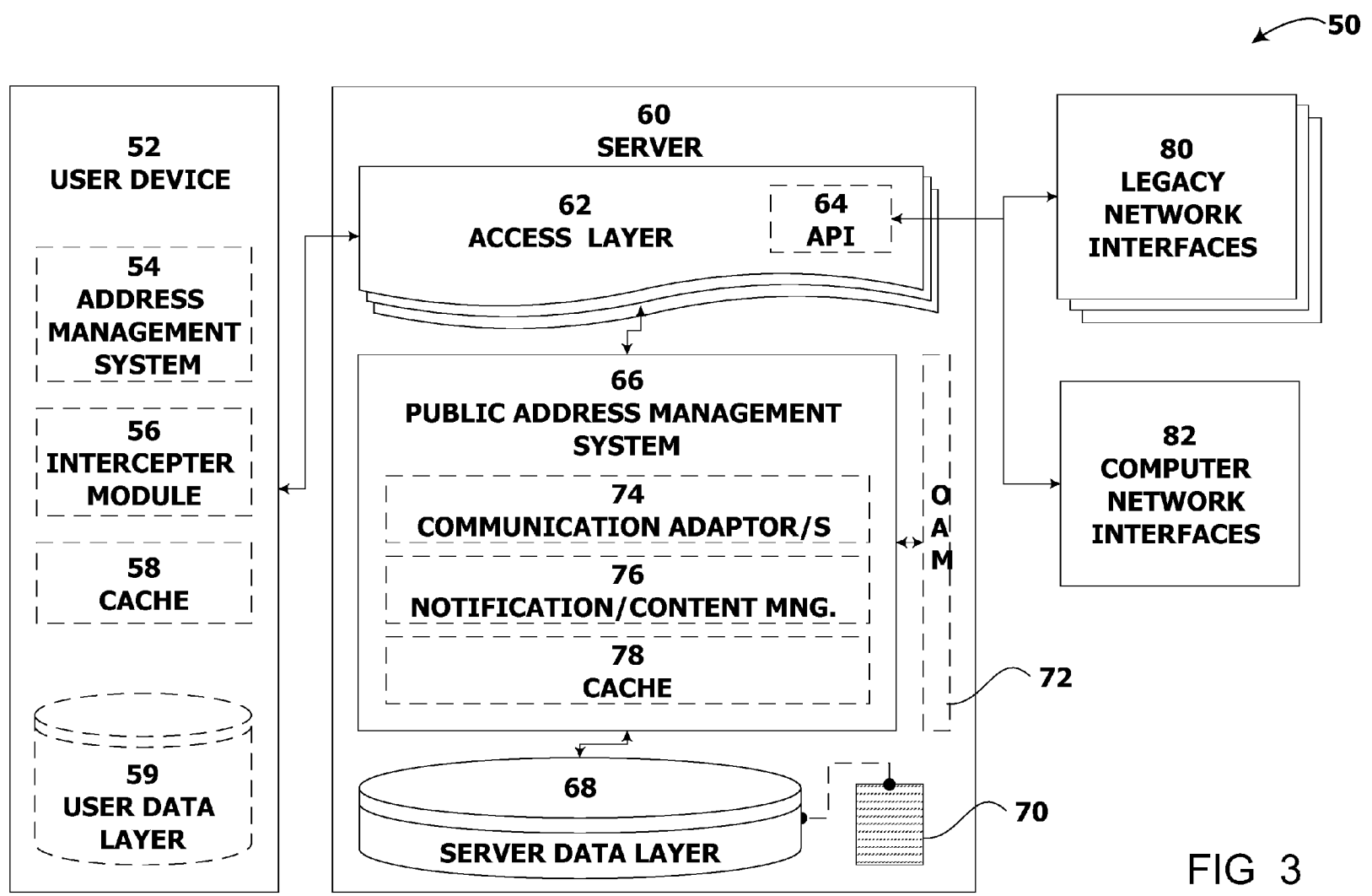
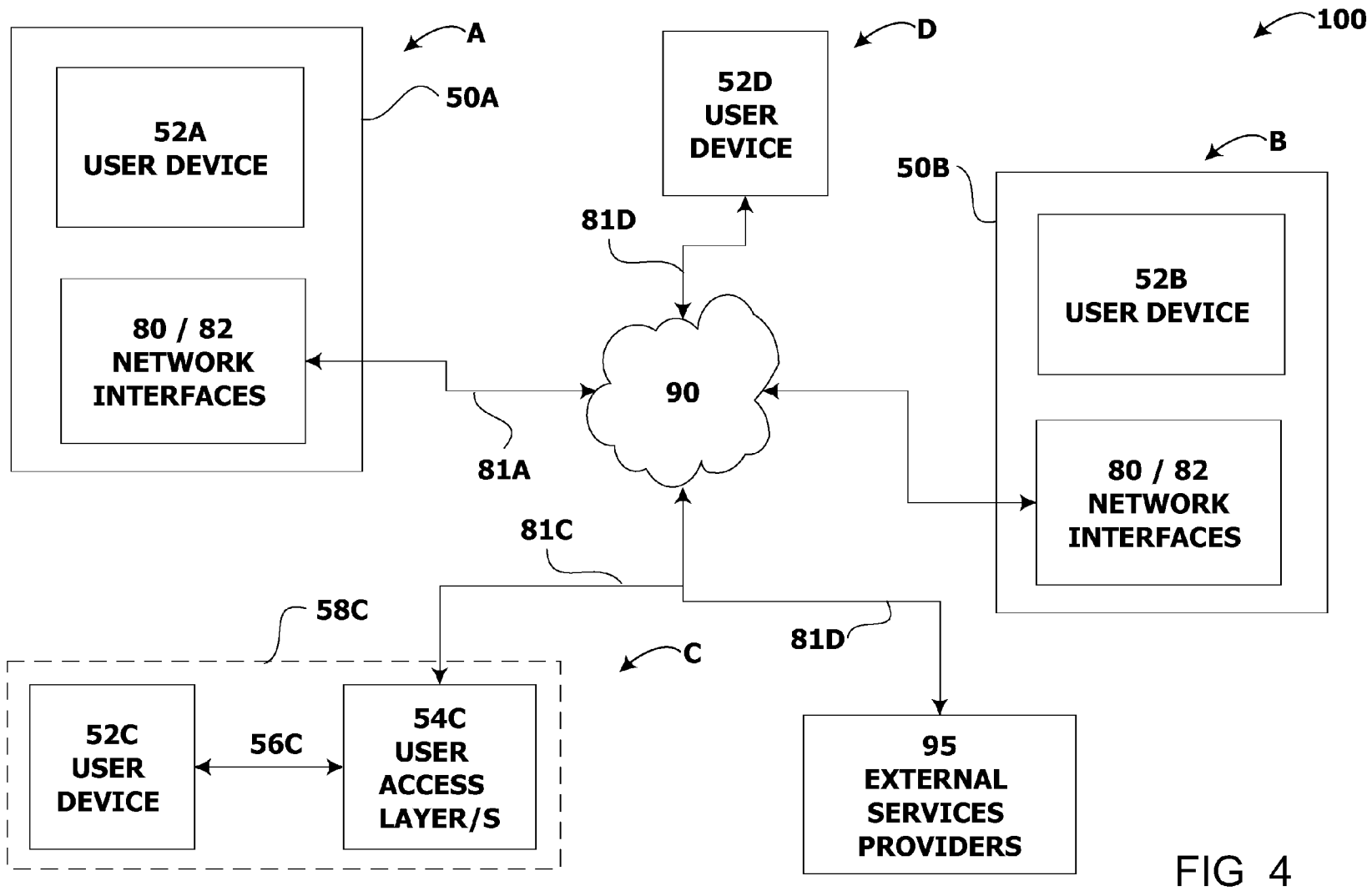


FIG 3



US 9,749,284 B2

1

# SYSTEMS AND METHODS OF CONTROLLED RECIPROCATING COMMUNICATION

## CROSS-REFERENCE TO RELATED APPLICATIONS

This application is national phase of international application PCT/1132014/061375, filed 12 May 2013. This application claims priority from U.S. provisional application 61/656,020 filed 13 May 2012, the contents of which are incorporated herein by reference.

## TECHNICAL FIELD

In general, the present invention pertains to the arts of telecommunications and/or computer networking. In particular, the invention relates to systems and methods of controlled reciprocating communication as well as systems and methods of controlled pre-interaction.

## BACKGROUND ART

It is believed that the pertinent state-of-the-art is represented by the following patent literature: U.S. Pat. No. 7,995,730, U.S. Pat. No. 7,436,943 and U.S. Pat. No. 7,602,894; US patent application Ser. No. US2010/054444 and US2012/328089; GB patent application Ser. No. GB2454886; European patent application Ser. No. EP2073521 and EP2448227 as well as by international patent applications having Publication No. WO2007/053768 and WO2010/135000.

It is believed that the pertinent state-of-the-art is represented by the following non-patent literature: Requests for Comments 3261 and 5627; Technical Specification of 3rd Generation Partnership Project—3GPP TS 23.228 V12.0.0 (2013-03); Session Initiation Protocol (SIP) and Session Initiation Protocol for Instant Messaging (SIMPLE) standards collection.

## DEFINITIONS

The term non-transitory computer readable media communication, as referred to herein, is to be construed to include all computer-readable media, with the sole exception being a transitory propagating signal per se.

The term communication, as referred to herein, is to be construed as any type of electronic communication, having an identifiable opponent and/or participant. Thus physical communications by couriers and types of electronic radio or television broadcasting, with unidentifiable watchers, are typically not within the scope of the term communication. Additionally, an attempted or incomplete communication, such as rejected telephone call or bounced email, is to be construed as communication. Instances of various types of communication inter alia include: a line telephone communication, line facsimile communication, cellular/mobile phone communication, short message service (SMS) communication, multimedia messaging service (MMS) communication, multimedia session, instant messaging (IM) communication, electronic mail (e-mail) communication, presence communication, personal message or private message (PM), voice over IP (VoIP) communication, video chatting communication, audio and/or video conferencing communication, file transfer and media sharing communication as well as any other communication by sharing.

2

The term interaction address, as referred to herein, is to be construed as any string of alphanumeric and/or other characters, which is uniquely associated to a party of communication. Instances of interaction address inter alia include: a line telephone number, line facsimile number, cellular/mobile phone number, IM contact or screen name, e-mail address, presence screen name or contact name, user service handle (e.g. Facebook or Twitter ID), Universal Resource Identifier (URI), Universal Resource Name (URN), Universal Resource Locator (URL), Extensive Resource Identifier (XRI), SIP URI, and any other type of user identifier for sharing or communication.

The term interaction address, as referred to herein, is to be construed as including a partial interaction address, namely any portion of the string of alphanumeric and/or other characters or a sub-string thereof. Particularly, an interaction address is optionally defined as including a sub-string of wildcards, typically representing a group of people having identical portions in their interaction addresses, such as coworkers in the same organization.

The term private interaction address, as referred to herein, is to be construed as an interaction address which the user wishes to controllably expose to participants; whereas public interaction address is to be construed as an interaction address which the user may distribute or publish, even uncontrollably.

The term controlled communication, as referred to herein, is to be construed as a communication performed from a particular selectable public interaction address, wherein the participant is exposed upon aforesaid communication merely to aforesaid selectable public interaction address.

The term controlled pre-interaction, as referred to herein, is to be construed as determining the particular selectable public interaction address associated with an interaction address of a participant. Controlled pre-interaction is optionally performed upon browsing, inspecting, accessing, searching, looking for friends, synchronizing contacts, viewing a profile and/or content on a presence network, such as a social or professional computer network (e.g. Facebook or LinkedIn).

A reverse list, as referred to herein, is to be construed as including at least one reverse list entry. The reverse list entry is defined as any entry in a database, row and/or column in a table or any other type of record for this matter, listing at least one interaction address of a participant alongside a public interaction address of the user, as well as association therebetween.

Whenever the terms: system, module, agent or server are used herein, they should be construed as a computer program, including any portion or alternative thereof, e.g. script, command, etc., and/or a hardware component's, including configurations or assemblies thereof, such computer storage medium, computer micro-processor, operative memory, graphical user interface (GUI), input devices and networking terminals, as well as any combination of the former with the latter.

The term integrated shall be inter alia construed as—operable on the same machine and/or executed by the same computer program. Depending on the actual deployment of the method, its implementation and topology, integration of agents and/or integration into modules as well as the terms “transfer”, “relaying”, “transmitting”, “forwarding”, “retrieving”, “accessing”, “pushed” or similar refer to any interaction between agents via methods inter alia including: function calling, API (Application Programming Interface), IPC (Inter-Process Communication), RPC (Remote procedure call) and/or communicating using of any standard or



US 9,749,284 B2

3

proprietary protocol, such as SMTP, IMAP, POP, MAPI, OMA, SIP/SIMPLE, XMPP, SMPP, IMS, SOAP/Rest, XML/RPC, web services.

Legacy and/or telephony network, as referred to herein, should be understood as any type of telephony system and particularly telephony systems compliant with standards know in the art as: POTS and PSTN.

SIP—Session Initiation Protocol as referred to herein includes: RFC 3261.

SIMPLE—Session Initiation Protocol for Instant Messaging and Presence standards collection as referred to herein includes: RFC 3428, RFC 3856, RFC 3857, RFC 3858 and RFC 4825.

It should be understood, however, that the particular definitions supra are not to limit the invention to the particular forms and examples, but on the contrary, is to cover all modifications, equivalents, and alternatives falling within the scope of the invention.

### DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more comprehensively from the following detailed description taken in conjunction with the appended drawings in which:

FIG. 1 is a high-level flowchart of an embodiment of the method of performing controlled reciprocating communication, in accordance with one aspect of the present invention;

FIG. 2 is a high-level flowchart of an embodiment of the method of performing controlled pre-interaction, in accordance with another aspect of the present invention;

FIG. 3 is a schematic diagram of an embodiment of the system for controlled pre-interaction, in accordance with the present invention;

FIG. 4 is a schematic diagram of an embodiment of the system for controlled pre-interaction, involving multiple and different parties.

While the invention is susceptible to various modifications and alternative forms, specific embodiments thereof have been shown merely by way of example in the drawings. The drawings are not necessarily complete, whereas emphasis instead was placed upon clearly illustrating the principles underlying the present invention.

### DETAILED DISCLOSURE OF EMBODIMENTS

Illustrative embodiments of the invention are described below. In the interest of clarity, not all features of actual implementation are described in this specification. It will of course be appreciated that in the development of any such actual embodiment, numerous implementation-specific decisions must be made to achieve the developers' specific goals, such as compliance with technology- or business-related constraints, which may vary from one implementation to another. Moreover, it will be appreciated that the effort of such a development might be complex and time-consuming, but would nevertheless be a routine undertaking for those of ordinary skill in the art having the benefit of this disclosure.

In accordance with some embodiments of the present invention, reference is now made to FIG. 1, showing a high-level flowchart of method 10 for controlled reciprocating communication. Method 10 of controlled reciprocating communication commences on step 12, with providing at least one private interaction address. It should be acknowledged that more than one private interaction address is optionally provided at step 12.

4

It should be further acknowledged that a plurality of private interaction addresses of different types is optionally provided at step 12; thus a telephone number and e-mail address can be concomitantly provided at step 12. Moreover updating, adding, replacing, altering or editing at least one additional or alternative private interaction address, of the same type and/or different types, any time thereafter, constitutes an iterative execution of step 12 and shall be considered as the providing of at least one private interaction address.

At step 14, at least one manageable public interaction address is defined in the system of the present invention. Aforesaid at least one manageable public interaction address is a non-limiting manner defined by: a user of the system of the present invention, an operator or administrator of the system of the present invention and/or a third party, such as external services providers.

It should be acknowledged that more than one manageable public interaction address, of the same type, is optionally defined at step 14; such as more than one e-mail address. It should be further acknowledged that a plurality of manageable public interaction addresses of different types is optionally defined at step 14; thus a public telephone number and public e-mail address can be concomitantly defined at step 14. Moreover updating, adding, replacing, altering and/or editing at least one additional or alternative manageable public interaction address, of the same type and/or different types, any time thereafter, constitutes an iterative execution of step 14 and shall be considered as the defining of at least one manageable public interaction address.

Subsequently, at step 16, at least one private interaction address, provided at step 12, is associated with at least one manageable public interaction address, defined at step 14. The association of the private interaction address with the manageable public interaction address is recorded at step 16. Aforesaid association of a private interaction address with a manageable public interaction address and recordal thereof, at step 16, is a non-limiting manner performed by: a user of the system of the present invention, an operator of the system of the present invention and/or a third party, such as external services providers.

It should be acknowledged that more than one manageable public interaction address is optionally associated, at step 16, with a single private interaction address and hence a plurality of associations of the same private interaction address with several different manageable public interaction addresses is optionally recorded at step 16. It should be further acknowledged that a plurality of manageable public interaction addresses of different types is optionally associated at step 16 with a single private interaction address. Thus for instance a public telephone number and public e-mail address can be concomitantly associated at step 16 to a single private telephone number and hence two respective associations, namely public telephone number with private telephone number and public e-mail address with private telephone number, are recorded at step 16. Furthermore updating, adding, replacing, altering and/or editing at least one additional or alternative association of a manageable public interaction address with a private interaction address, any time thereafter, constitutes an iterative execution of step 16 and shall be considered as the associating at least one manageable public interaction address to a private interaction address and recording such association. Moreover associating a manageable public interaction address to a plurality of private interaction address constitutes an iterative execution of step 16 and shall be considered as the associating at

US 9,749,284 B2

5

least one manageable public interaction address to a private interaction address and recording such association.

Each public interaction address is typically subjected to management. Management events of public interaction address in a non-exhaustive manner are selected from: 5 revoking public interaction address, renaming public interaction address, unrevoking public interaction address, suspending public interaction address for a predefined period of time, assigning public interaction address to a certain public profile, unassigning public interaction address off a certain public profile, renaming of or assigning/unassigning meta- 10 data to/off public interaction address, defining a rule for notification and/or content thereof, as well as arranging public interaction addresses for view or access, per private communication address, certain public profile or any other parameter for that matter, as elaborated hereunder.

The revoking of a given public interaction address, *inter alia*, comprises permanently deleting or temporally deactivating for indefinite period of time aforesaid given public interaction address from/at the record of public addresses, 20 formed at step 16; closing an account of aforesaid given public interaction address, defined at step 16, as well as permanently deleting or temporally deactivating for indefinite period of time an association of aforesaid given public interaction address to the respective private interaction address, recorded at step 16.

The unrevoking of a given public interaction address, *inter alia*, comprises reactivating aforesaid given public interaction address at the record of public addresses, formed at step 16; reopening an account of aforesaid given public interaction address, defined at step 16, as well as reactivating an association of aforesaid given public interaction address to the respective private interaction address, recorded at step 16.

The suspending of a given public interaction address comprises revoking aforesaid given public interaction address, as set forth hereinabove, followed by unrevoking aforesaid given public interaction address, after a predefined period of time and/or completion of predefined unrevoking event; suspending an account of aforesaid given public interaction address, as well as suspending an association of aforesaid given public communication to the respective private interaction address, recorded at step 16.

The renaming of a given public interaction address and/or editing metadata thereof, *inter alia*, comprises assigning a name and/or metadata to aforesaid given public interaction address at the record of public addresses, recorded at step 16, deleting, altering or editing a name and/or metadata assigned to aforesaid given public interaction address at the record of public addresses, recorded at step 16, as well as assigning a name and/or metadata to an association of aforesaid given public communication to a private interaction address, recorded at step 16.

The assigning public interaction address to a certain public profile, *inter alia*, comprises defining a public profile, associating at least one public interaction address the certain public profile and recording the association of aforesaid at least one public interaction address with the certain public profile. The public profiles and/or association thereof with public interaction address/addresses are optionally recorded at the record of public addresses, formed at step 16; however in some embodiments public profiles and/or association thereof with public interaction address/addresses are recorded in a dedicated record, other than the record of public addresses, formed at step 16. The assigning public interaction address to a certain public profile, optionally, further comprises unassigning/reassigning public interaction

6

address off/to the certain public profile, as well as deleting, altering or editing the definition of public profiles and/or association thereof with public interaction address/addresses at the record of public addresses, formed at step 16 and/or the aforesaid dedicated record, other than the record of public addresses, formed at step 16.

Defining a rule for notification and/or content of notification, as elaborated *infra*, comprises defining at least one rule for notification and/or content of notification, associating the aforementioned rule for notification and/or content thereof with a public interaction address and/or certain public profile and recording the association of aforesaid rule for notification and/or content thereof with a public interaction address or a certain public profile.

It should be acknowledged that aforementioned exemplary management events, for public interaction address/addresses, are optionally performed during step 16; however some or all of aforementioned exemplary management events are optionally performed at a dedicated step (not shown), of managing public interaction address/addresses.

At some time point, additionally to associating a manageable public interaction address with a private interaction address and recordal of the association thereof, performed at step 16, as well optionally to managing the public interaction address, as set forth *supra*, an incoming communication is typically received by the system of controlled reciprocating communication, at step 18. It is emphasized that despite the fact that step 18, of receiving an incoming communication is shown in flowchart 10 as following step 16, of associating a manageable public interaction address with a private interaction address and recordal of the association thereof, in various implementations of the method of performing controlled reciprocating communication, shown in flowchart 10, step 18 of receiving an incoming communication precedes step 16, of associating a manageable public interaction address and recordal of the association thereof. Moreover, it should be noted, that an attempted incoming communication, e.g. rejected telephone call or bounced email, constitutes receiving an incoming communication of step 18.

Upon receiving an incoming and/or attempted incoming communication, at step 18, the system of controlled reciprocating communication identifies that the incoming and/or attempted incoming communication was received to a given manageable public interaction address, at step 20.

Thereafter, upon identifying that the incoming and/or attempted incoming communication was received to a given manageable public interaction address, performed at step 20, the system of controlled reciprocating communication accesses the record of public addresses, formed at step 16, and determines the respective private interaction address/addresses, based on the association thereof with the manageable public interaction address, as recorded at step 16, to which the incoming and/or attempted incoming communication was received, during step 22.

Subsequently to determining the respective private interaction address/addresses, based on the association thereof with the manageable public interaction address, as recorded at step 16, to which the incoming and/or attempted incoming communication was received, during step 22, the system of controlled reciprocating communication, optionally, in a non-limiting manner performs at least one from the following (not shown).

The system of controlled reciprocating communication optionally forwards the incoming communication and/or information regarding an attempted incoming communication to the respective private interaction address/addresses associated with the manageable public interaction address,

US 9,749,284 B2

7

as recorded at step 16, to which the incoming and/or attempted incoming communication was received, during step 22.

Alternatively or additionally the system of controlled reciprocating communication retrieves/presents the manageable public interaction address to which the incoming and/or attempted incoming communication was received, during step 22 and/or retrieving/presenting name, metadata and/or certain public identity assigned the manageable public interaction address to which the incoming and/or attempted incoming communication was received, during step 22.

Alternatively or additionally the system of controlled reciprocating communication applies a notification rule to the incoming communication and/or information regarding an attempted incoming communication, as well as optionally selects the content of the aforementioned notification.

Then, upon completion of steps 12, 14 and 16 the system for controlled reciprocating communication, generates at least one reverse list entry, at step 24. A reverse list entry comprises at least one interaction address of a participant and at least one manageable public interaction address of the user of the system of the present invention. Alongside at least one interaction address of a participant and at least one manageable public interaction address of the user a reverse list entry, optionally, in a non-limiting comprises: a certain public identity assigned to the manageable public interaction address, name and/or metadata assigned to the manageable public interaction address, a rule relating to a notification and/or content thereof, a default communication preference and/or overruling alternative for the default communication preference, as well as personal information and/or contact information of participant. Updating, adding, replacing, altering and/or editing at least one additional or alternative constituent of a reverse list entry, any time thereafter, constitutes an iterative execution of step 24 and shall be considered as the generating at least one reverse list entry. Typically generating at least one reverse list entry includes accessing the reverse list and searching for similar/identical reverse list entry, prior to generating a new reverse list entry.

The generating of aforementioned constituents of a reverse list entry, at step 24, is a non-limiting manner performed by: a user of the system for controlled reciprocating communication, an operator of the system for controlled reciprocating communication and/or a third party, such as external services providers. A reverse list entry is preferably generated upon availability of the interaction address of a participant or some time subsequently to availability of the interaction address of a participant. However in some embodiments an incomplete reverse list entry is generated without the interaction address of a participant, pending the completion of the incomplete reverse list entry upon availability the interaction address of the participant. There are several preferable events and/or triggers for generating a reverse list entry, as detailed hereinafter.

Optionally a reverse list entry is generated, at step 24, manually by inputting the interaction address of the participant as well as optionally personal information and/or contact information of the participant, typically by the user, and optionally without any controlled reciprocating communication following thereafter.

Alternatively or additionally a reverse list entry is optionally generated upon receiving an incoming communication, at step 18. Upon receiving an incoming communication, at step 18, the system for controlled reciprocating communication identifies the interaction address of the participant and records the interaction address of the participant in a newly formed reverse list entry, alongside manageable public inter-

8

action address of the user and other optional constituents of reverse list entry. The process of generating a reverse list entry is typically performed either automatically by the system of the invention upon receiving an incoming communication and/or an attempted incoming communication or by prompting the user with proposed details of reverse list entry and upon confirmation of the user to form such an entry.

In some examples, such as with incoming telephone calls from undisclosed number, the interaction address of the participant, namely the telephone number of the calling person, is not available to the user but rather is known merely to the telephony switchboard facility. Therefore in such cases the interaction address of the participant, namely the telephone number of the calling person, is obtained from the telephony switchboard facility and inputted into the reverse list entry by the system for controlled pre-interaction, so that reverse list entry remains confidential to the user. The user in such case will still be able to perform an outgoing communication to the interaction address of the participant, namely the telephone number of the participant, without knowing the telephone number of the participant.

Alternatively or additionally a reverse list entry is optionally generated upon performing an outgoing communication and/or an attempted outgoing communication, at step 40. Upon performing an outgoing communication, at step 40, the system for controlled reciprocating communication identifies the interaction address of the participant and records the interaction address of the participant in a newly formed reverse list entry, alongside manageable public interaction address of the user and other optional constituents of reverse list entry. The process of generating a reverse list entry, upon outgoing communication, is typically performed either automatically by the system of the invention upon identifying the manageable public interaction address from which the participant was contacted or by prompting the user with proposed manageable public interaction address and/or certain public identity to be associated with interaction address of the participant in the proposed reverse list entry and upon confirmation of the user to form such an entry.

Alternatively or additionally a reverse list entry is optionally generated without performing any communication at all, by an operator or administrator of the system of the present invention and/or a third party, such as external services providers. The system for controlled reciprocating communication and/or a third party, such as external services providers, may identify that participant is connected or linked to a certain public profile of the user, for instance in a social or business network. The system for controlled reciprocating communication and/or a third party, such as external services providers, then obtains the interaction address of the participant, by retrieving from the exemplary social or business network data including the interaction address of the participant and by synchronizing these data with the reverse list. The user then may opt to use the interaction address of the participant at the reverse list, to contact the participant or perform a pre-interaction, some time thereafter or not to use the interaction address of the participant at the reverse list.

Subsequently to generating at least one reverse list entry, at step 24, the system for controlled reciprocating communication performs a pre-interaction act, at step 32. An exemplary pre-interaction act, performed at step 32, comprises sub-step 34 of accessing reverse list. Pre-interaction act, performed at step 32, further comprises sub-step 36 of identifying the interaction address of the participant in the reverse list. Ultimately pre-interaction act, performed at step

US 9,749,284 B2

9

32, includes sub-step 38 of determining the manageable public interaction address of the user, associated with the given interaction address of the participant in the reverse list. For the sake of clarity it is noted that a pre-interaction, performed at step 32, is not necessarily followed by a communication. Accordingly in some embodiments the system of the present invention performs merely a pre-interaction, as explained in a more detail infra.

Upon performing a pre-interaction act, at step 32 and consequently determining the manageable public interaction address of the user, associated with the given interaction address of the participant in the reverse list, the system for controlled reciprocating communication is capable of and optionally performs an outgoing communication, at step 40, from the manageable public interaction address of the user. Upon performing an outgoing communication, at step 40, the participant is exposed merely to manageable public interaction address of the user.

#### BEST MODE FOR CARRYING OUT THE METHOD OF THE INVENTION

In accordance with some preferred embodiments of the present invention, reference is now made to FIG. 2, showing a high-level flowchart of method 30 for controlled pre-interaction. Method 30 of controlled pre-interaction commences on step 12, with providing at least one private interaction address, essentially as described hereinabove.

Thereafter at least one manageable public interaction address is defined in the system for controlled pre-interaction, at step 14. Subsequently, at step 16, at least one private interaction address, provided at step 12, is associated with at least one manageable public interaction address, defined at step 14. The association of the private interaction address with the manageable public interaction address is recorded at step 16.

Additionally at least one complete or incomplete reverse list entry is generated, at step 24, in a non-limiting manner generated: (1) manually by inputting the interaction address of the participant; (2) upon receiving an incoming communication, at step 18, automatically or by prompting the user; (3) upon performing an outgoing communication, at step 40, automatically or by prompting the user; (4) upon synchronizing data from a third party, such as external services providers, with the reverse list.

Subsequently to generating at least one reverse list entry, at step 24, the system for controlled pre-interaction performs at least one pre-interaction act, at step 32. An exemplary pre-interaction act, performed at step 32, comprises sub-step 34 of accessing reverse list. Pre-interaction act, performed at step 32, further comprises sub-step 36 of identifying the interaction address of the participant in the reverse list. Ultimately pre-interaction act, performed at step 32, includes sub-step 38 of determining the manageable public interaction address of the user, associated with the given interaction address of the participant in the reverse list.

In accordance with the preferred embodiment of method 30, shown in FIG. 2, the pre-interaction, performed at step 32, is in a non-limiting manner: not followed by a communication, followed by communication indefinite time thereafter, followed by communication of a different type, followed by communication over different network. During the pre-interaction, performed at step 32, the system for controlled pre-interaction determining the manageable public interaction address of the user, associated with the given interaction address of the participant, as recorded in the respective reverse list entry. Optionally sometime thereafter

10

an outgoing communication may be initiated, at step 40, occasionally by a different operator and/or over a different network. For instance an e-mail address or presence address recorded in a reverse list entry is optionally followed by a communication of sharing type, indefinite time thereafter. Another instance of a reverse list entry formed upon incoming/outgoing call, followed by a communication of SMS type.

In some embodiments the system for controlled pre-interaction synchronizes contact details of a participant or simultaneously of a plurality of participants, including several interaction addresses of different types for the same participant. In such cases the pre-interaction, performed at step 32, is optionally followed by initiating an outgoing communication, at step 40, to a different interaction address and occasionally over a different network.

For example contact information of participant, including e-mail address and telephone number, can be synchronized over computer network, at step 24, due to an association of the participant to instant messaging address of the user, generating two reverse list entries for the participant, first with a manageable public e-mail address and second with manageable public telephone number of the user. These reverse list entries are optionally merely stored and/or accessed during the pre-interaction, performed at step 32, without performing outgoing or incoming communication. Rules, Notifications and Communication Preferences

In some embodiments the system for controlled pre-interaction employs predefined rules. Rules are optionally assigned to at least one of: a private interaction address of the user (e.g. contained in the record formed at step 16), manageable public interaction address of the user (e.g. contained in the record formed at step 16 and/or in a reverse list entry generated at step 24), and interaction address of the participant (e.g. contained in a reverse list entry generated at step 24).

Rules assigned to a manageable public interaction address of the user comprise an instruction or set of instructions for a predefined response, in a situation meeting particular criteria, relating to the manageable public interaction address. Rules assigned to a manageable public interaction address of the user may for example dictate that if the manageable public interaction address is suspended or revoked, any incoming communication is in a non-limiting manner: to be rejected, to be recorded, to be converted to another format and/or forwarded to a private interaction address of the user. It should be noted that the type of communication as well as private interaction address may independently vary according to different rules. Thus if a manageable public telephone number of the user has been suspended or revoked, a rule may dictate that upon receiving an incoming phone call to the suspended or revoked manageable public telephone number, (1) the incoming phone call is to be rejected and (2) a notification about the attempted incoming phone call (e.g. time and participant number) is to be sent by SMS to the private telephone number of the user. Alternatively or additionally if a manageable public telephone number of the user has been suspended or revoked, another rule may dictate that upon receiving an incoming phone call to the suspended or revoked manageable public telephone number, (1) the incoming phone call is to be rejected and (2) a notification about the attempted incoming phone call (e.g. time and participant number) is to be sent by e-mail to the private e-mail address of the user.

Rules assigned to an interaction address of the participant comprise an instruction or set of instructions for a predefined



US 9,749,284 B2

11

response, in a situation meeting particular criteria, relating to the interaction address of the participant. Rules assigned to an interaction address of the participant may for example dictate that any incoming communication from the address of the participant is in a non-limiting manner: to be rejected, to be recorded, to be converted to another format and/or forwarded to a private interaction address of the user. It should be noted that the type of communication as well as private interaction address of the user may independently vary according to different rules. Thus a rule may dictate that upon receiving an incoming phone call from an interaction address of the participant, (1) the incoming phone call is to be rejected and (2) a notification about the attempted incoming phone call (e.g. time and participant number) is to be sent by SMS to the private telephone number of the user. Alternatively or additionally a rule may dictate that upon receiving an incoming phone call from an interaction address of the participant, (1) the incoming phone call is to be recorded or transcribed to text and (2) a notification including the audio file of the recording of incoming phone call or transcript of the transcribing thereof is to be sent by e-mail to the private e-mail address of the user.

Notifications are any type of media or electronic data and/or files sent or pushed by the system for controlled pre-interaction, to the user and/or participant, other than the communication itself. Notifications are typically either triggered by a communication event, e.g. assigned rules, or initiated by the system for controlled pre-interaction, for example as a part of a maintenance procedure. Notifications triggered by a communication event are typically initiated by rules assigned to at least one of: a private interaction address of the user, manageable public interaction address of the user, and interaction address of the participant.

Notifications to the user triggered by an event of incoming communication, which are optionally initiated by rules assigned to a manageable public interaction address of the user and/or interaction address of the participant, typically include at least one of: extract or synopsis with information about incoming communication (e.g. time and participant number), recording of communication (e.g. audio file) and transcript of communication (e.g. text). Notifications to the participant triggered by an event of incoming communication, which are optionally initiated by rules assigned to a manageable public interaction address of the user and/or interaction address of the participant, typically include at least one of: a notification sent in reply (namely to the same interaction address of the participant) with a preset content, by a communication of the same or different type, a pre-recorded message (e.g. audio or video file) played to the participant upon receiving an incoming communication.

Notifications initiated by the system for controlled pre-interaction are typically sent to the user and/or participant in the event the system opts to inform the user and/or participant. Notifications initiated by the system for controlled pre-interaction further include notifications provisioned by the user. Notifications initiated by the system for controlled pre-interaction in a non-limiting manner include: messages about maintenance/unavailability of the system for controlled pre-interaction, changes of tariffs charged for the service, greetings for holidays or birthdays. Notifications provisioned by the user in a non-limiting manner include a notification to all interaction addresses of participants associated in reverse list with a given manageable public address of the user, for instance that aforesaid manageable public address was revoked or suspended.

User or administrator of the system for controlled pre-interaction may define a preset content for a notification. A

12

preset content for a notification inter alia includes: text, alphanumeric data, audio files, video files, graphics and hyperlinks. The preset content for a notification optionally defines a template with several empty fields, which are filled-in with details becoming available some time thereafter.

The system for controlled pre-interaction is preferably prescribed with default communication preferences and overruling alternative therefor. Communication preferences and overruling alternative therefor are optionally prescribed to at least one of: a private interaction address of the user (e.g. contained in the record formed at step 16), manageable public interaction address of the user (e.g. contained in the record formed at step 16 and/or in a reverse list entry generated at step 24), and interaction address of the participant (e.g. contained in a reverse list entry generated at step 24). As the method of performing controlled pre-interaction is primary aimed at safeguarding the privacy of the user, a default communication preference typically prescribes indicating for communication the manageable public address of the user as determined in sub-step 38 of a pre-interaction act, performed at step 32.

However in some preferred embodiments communication preferences are prescribed with overruling alternative/s therefor. Thus for instance if the network associated with the manageable public address of the user as determined in sub-step 38 of a pre-interaction act, performed at step 32, an overruling alternative of the default communication preference may indicate an alternative manageable public interaction address of the user or even the private interaction address of the user for a communication session. Alternatively or additionally if the communication costs associated with the manageable public address of the user as determined in sub-step 38 of a pre-interaction act, performed at step 32, exceed a predefined threshold, an overruling alternative of the default communication preference may indicate an alternative manageable public interaction address of the user or even the private interaction address of the user for a communication session, wherein the costs precede the predefined threshold. Therefore in order to implement an overruling alternative of the default communication preference, the system of controlled pre-interaction optionally accesses to and/or retrieves data from at least of the following: the record formed at step 16, a reverse list entry generated at step 24 and an external reference or source of information (e.g. tariffs table); in order to determine the alternative for manageable public address of the user as determined in sub-step 38 of a pre-interaction act, performed at step 32. The System for Controlled Pre-Interaction

In accordance with some preferred embodiments of the present invention, reference is now made to FIG. 3, showing a block diagram of system 50 for controlled pre-interaction. System 50 for controlled pre-interaction comprises user device 52. User device 52 is an electronic device, comprising a user interface (not shown) assessable by the user. In some embodiments the user interface of user device 52 in a non-limiting manner includes: a GUI (e.g. screen), sound reproducing device (e.g. speakers or headphones), sound collecting device (e.g. microphone), an imaging device (e.g. video camera), inputting device (e.g. keyboard or dialing pad), etc.

It would be appreciated that depending on various implementations of system 50 for controlled pre-interaction optionally embodies a plurality of different electronic devices which are operable as user device 52 is system 50. In instances of e-mail communication, instant messaging (IM) communication, voice over IP (VoIP) communication

US 9,749,284 B2

13

or presence communication it is rather common that the same account is accessed from different devices.

It would be further appreciated that depending on various implementations of system 50 for controlled pre-interaction the very same electronic device embodies a plurality of user devices 52 of different systems 50 of communications of different types. In instances of versatile devices (e.g. personal computers), the same device is frequently operable for providing the user/communication interface of several communications of different types (e.g. e-mail, IM and presence communications).

Moreover it would be appreciated that depending on various implementations of system 50 for controlled pre-interaction the very same electronic device embodies a plurality of user devices 52 of different systems 50 of communication of the same type. For instance a single dual-SIM mobile phone is optionally operable as two different user devices 52 or the same computer is used to access a plurality of different communication accounts.

Device 52 of system 50 optionally comprises address management system 54, which is capable of performing some or all steps of method 10 for controlled reciprocating communication and/or method 30 for controlled pre-interaction, as described in FIGS. 1 and 2. Typically, additionally to address management non-limiting manner system 54, device 52 of system 50 comprises user data layer 59, in a non-limiting manner storing: the record of public interaction addresses and association thereof to private interaction addresses formed at step 16, the entries of reverse list generated at step 24, as well as optionally: list of public identities assigned to manageable public interaction address, name and/or metadata assigned to manageable public interaction address, name and/or metadata assigned to interaction addresses of participants, rules relating to notification, predefined content for notifications, a default communication preference for interaction addresses of participants and/or overruling alternative for the default communication preference for interaction address of participants, personal information and/or contact information of participant.

Device 52 of system 50 optionally further comprises interceptor module 56. Interceptor module 56 is capable of monitoring the activity of device 52 and detecting initiation or occurrence of communication. Upon detecting initiation or occurrence of communication on device 52, interceptor module 56 optionally disables a communication from the outset, halts or otherwise prevents further progression of communication on device 52. Alternatively or additionally upon detecting initiation or occurrence of communication on device 52, interceptor module 56 optionally redirects the communication, according to the default communication preference, to the manageable public interaction address of the user associated in a reverse list entry with a given interaction address of participant or according to the overruling alternative for the default communication preference, to a private interaction address or manageable public interaction address other than manageable public interaction address associated in a reverse list entry with a given interaction address of participant.

Alternatively or additionally upon detecting initiation or occurrence of communication on device 52, interceptor module 56 inter alia performs: presenting to the user details/data/name/metadata of the record of public interaction addresses formed at step 16, presenting to the user details/data/name/metadata of entries in reverse list generated at step 24, prompting the user for further progression of communication on device 52 or prompting the user for further progression of communication and providing preset

14

options for further progression of communication on device 52. Alternatively or additionally during an occurrence or upon completion of communication on device 52, interceptor module 56 presents and/or prompts to the user proposed details/data/name/metadata for a newly suggested reverse list entry to be generated at step 24.

Device 52 of system 50 optionally further comprises cache module 58, typically for sustaining fluent data exchange, between user device 52 and server 60 of system 50, even during interruptive communication therebetween. Cache module 58 typically employs RAM, SDRAM and/or Flash memory on device 52.

FIG. 3 shows an embodiment of system 50 which employs a client-server configuration, of user device 52 and server 60. It would be appreciated, however, that depending on various configurations, system 50 employs thin-server or no-server configuration, wherein some or all components of server 60 are optionally present on and operable by user device 52. Moreover depending on various configurations, such as feature phone or line phone device with legacy telephony, system 50 optionally employs a thin-client or no-client configurations, where user device 52 comprises merely a minimal user interface, whereas the steps of the method for controlled pre-interaction are performed by server 60. Server 60 may act as full server for some user device 52, and as a partial or thin-server for a different user device 52, concurrently.

Server 60 of system 50 typically includes access layer 62. Access layer 62 typically comprises a plurality of communication protocols, adapted to sustain communication between user device 52 and server 60. Access layer 62 of server 60 is connected to and is capable of sustaining communication with user device 52 of system 50. Access layer 62 of server 60 is connected to and is capable of sustaining communication with at least one network interface of system 50, as explained below. Access layer 62 preferably includes an application programming interface 64 (API) to communicate with other software components.

Server 60 of system 50 comprises public address management system 66. Public address management system 66 of server 60 is capable of performing some or all steps of method 10 for controlled reciprocating communication and/or method 30 for controlled pre-interaction, as described in FIGS. 1 and 2. Typically, additionally to public address management system 66, server 60 comprises server data layer 68, in a non-limiting manner storing: the record of public interaction addresses and association thereof to private interaction addresses formed at step 16, the entries of reverse list 70 generated at step 24, as well as optionally: list of public identities assigned to manageable public interaction address, name and/or metadata assigned to manageable public interaction address, name and/or metadata assigned to interaction addresses of participants, rules relating to notification, predefined content for notifications, a default communication preference for interaction addresses of participants and/or overruling alternative for the default communication preference for interaction address of participants, personal information and/or contact information of participant.

Preferably server 60 comprises operations, administration and management (OA&M) module 72. OA&M module 72 is inter alia employed for: provisioning, auditing, log recording, billing and alike of various operations performed by public address management system 66 and/or in server data layer 68.

Public address management system 66 of server 60 optionally further comprises at least one communication

US 9,749,284 B2

15

adaptor 74. Communication adaptor 74 of server 60 functions essentially similarly to interceptor module 56 of device 52 but in specific types of communication and certain networks, such as telephony/legacy networks, communication adaptor 74 of server 60 optionally employs solely a monitoring and notification scheme and does not actually halt or prevent further progression of a communication. Communication adaptor 74 of server 60 is capable of monitoring the activity on device 52 and/or and detecting initiation or occurrence of communication on device 52 and/or server 60. Upon detecting initiation or occurrence of communication on device 52 and/or server 60, communication adaptor 74 optionally halts or otherwise prevents further progression of communication on device 52 and/or server 60. Alternatively or additionally upon detecting initiation or occurrence of communication on device 52 and/or server 60, communication adaptor 74 optionally redirects the communication, according to the default communication preference, to the manageable public interaction address of the user associated in a reverse list entry with a given interaction address of participant or according to the overruling alternative for the default communication preference, to a private interaction address or manageable public interaction address other than manageable public interaction address associated in a reverse list entry with a given interaction address of participant.

Alternatively or additionally upon detecting initiation or occurrence of communication on device 52 and/or server 60, communication adaptor 74 inter alia: presents to the user details/data/name/metadata of the record of public interaction addresses formed at step 16, presents to the user details/data/name/metadata of entries in reverse list generated at step 24, prompts the user for further progression of communication on device 52 and/or server 60, or prompts the user for further progression of communication and provides preset options for further progression of communication on device 52 and/or server 60. Alternatively or additionally during an occurrence or upon completion of communication device 52 and/or server 60, communication adaptor 74 presents and/or prompts to the user proposed details/data/name/metadata for a newly suggested reverse list entry to be generated at step 24.

Server 60 of system 50 optionally further comprises cache and/or in-memory database (IMDB) module 78, typically for sustaining fluent data exchange, between user device 52 and server 60 of system 50, even during interruptive communication therebetween. Cache module and/or in-memory database 78 typically employs RAM, SDRAM, Flash memory or fast disks on server 60.

System 50 further comprises at least one network interface selected from: legacy network interface/s 80 and computer interface/s 82. Legacy network interface 80 and/or computer interface 82 are connected to access layer 62 of server 60. Legacy network interface 80 and/or computer interface 82 are preferably commendable with access layer 62 via application programming interface 64 (API) of the latter.

Legacy network interface 80 and/or computer interface 82 of system 50 are characterized by the capability to perform an incoming and/or outgoing communication from at least one manageable public address, as listed in an entry of reverse list 70, in server data layer 68 and/or user data layer 59. System 50 typically performs an outgoing communication of step 40 from a manageable public address, as in an entry of reverse list 70, on server data layer 68 and/or user

16

data layer 59, in either of the three of the following modes: (1) a proxy mode; (2) forwarding mode, and (3) redirecting to another system 50 mode.

In proxy mode, which is typically applicable in situations where system 50 is operable by the communication provider itself, the participant is merely presented with a manageable public address of the user, whereas the communication de facto is performed from a private interaction address of the user. The aforementioned merely presenting to the participant a manageable public address of the user may be referred as “disguising” the actual private interaction address of the user. The disguising the actual private interaction address of the user is typically applicable in various types of computer networks communication such as: e-mail communication, VoIP communication, presence communication and IM communication.

In forwarding mode, system 50 forwards the communication from a private interaction address of the user to a manageable public address of the user, listed in an entry of reverse list 70, on server data layer 68 and/or user data layer 59. The communication forwarded from a private interaction address of the user to a manageable public address of the user is then addressed to the interaction address of the participant. In forwarding mode, performing an outgoing communication of step 40, entails sustaining two communication sessions, namely first from a private interaction address of the user to a manageable public address of the user and second from aforesaid manageable public address to the interaction address of the participant. It is noted that forwarding mode is particularly applicable for legacy/telephony networks.

In redirecting mode the communication is redirected from system 50, having a network interface of private interaction address of the user, to another system 50, having a network interface of the manageable public address of the user, listed in an entry of reverse list 70, on server data layer 68 and/or user data layer 59. The redirecting mode is particularly applicable in implementations where a plurality of systems 50, of communications of the same type, is operable on a singular user device 52.

In instances of a multi-SIM phone, namely wherein the same device embodies user device 52A, associated with a private interaction address of the user, as well as user device 52B, associated with a manageable public interaction address of the user, the performing an incoming and/or outgoing communication from at least one manageable public address, as listed in an entry of reverse list 70, in server data layer 68 and/or user data layer 59, at step 40, is typically performed in either of the three of the above-listed modes: (1) a proxy mode; (2) forwarding mode, and (3) redirecting to another system 50 mode. In proxy mode, the communication is performed while merely presenting a manageable public address of the user to the participant, whereas the communication de facto is performed from a private interaction address of the user, optionally by employing interceptor module 56 of user device 52A and/or communication adaptor of server 60. In forwarding mode the communication is typically forwarded from the SIM associated with a private interaction address of the user to the telephone number of the SIM associated with a manageable public address of the user. In redirecting to another system 50 mode, system 50A of the SIM associated with a private interaction address of the user redirects the communication, such as phone call or SMS, to another system 50B of the SIM associated with a manageable public interaction address of the user.

US 9,749,284 B2

17

In accordance with some preferred embodiments of the present invention, reference is now made to FIG. 4, showing block diagram of system 100, including system 50A for controlled pre-interaction and optionally controlled reciprocating communication of user party A system 50A with system 50B of participant party B, as well as user devices 52C and 52D of participant parties C and D respectively. Parties A to D in system 100 are connected to and communicable over network 90 via connections 81A to 81D, respectively. It should be acknowledged that for the sake of simplicity network 90 is shown in FIG. 4 as an exemplary singular network; whereas depending on various types of communication, network 90 embodies a plurality of networks of different types, such as legacy/telephony networks and computer networks. Moreover it should be acknowledged that particular branch connections 81A to 81D, of parties A to D, on network 90 shown in FIG. 4, are optionally different networks of the same type, such as GSM, CDMA and 3GPP mobile networks.

System 100 preferably comprises at least one third party, such as external services providers 95, capable for controlled pre-interaction for user party A. External services providers 95 as referred to herein are to be construed inter alia as a source of personal and/or contact information about participant party B to D, including at least one interaction address of participant party B to D. For example external services providers 95, which is/are exemplarily presence server/s for at least one party A to D, may contain a telephone numbers of parties B to D, which are also connected to presence server 95 of user party A. System 100, as a part of controlled pre-interaction for user party A, may initially determine that the presence address of participant party B to D is associated in a reverse list entry of system for controlled pre-interaction 50A with a manageable public presence address of user party A and/or certain public profile of user party A. System for controlled pre-interaction 50A is then optionally synchronizes the telephone numbers of participant party B to D, for example from external services providers 95, such as servers presence of participant party B to D, with at least manageable public telephone number of user party A, based on the appurtenance thereof to a manageable public presence address of user party A and/or certain public profile of user party A.

System for controlled pre-interaction 50A is then typically either automatically generates a plurality of reverse list entries, wherein manageable public telephone number of user party A is associated with telephone numbers of participant party B to D, or prompts the user with details of newly suggested reverse list entries prior to generating the same. System for controlled pre-interaction 50A is then capable of determining the manageable public telephone number of user party A associated with telephone numbers of participant party B to D, by accessing the reverse list, an optionally merely stores such determined manageable public telephone number of user party A for a possible later communication by phone, even despite the fact that party A has never been in touch by telephone with participant party B to D and never personally obtained the telephone numbers of participant party B to D.

It should be acknowledged however that despite the exemplary division of system 100, shown in FIG. 4, participant party B to D user devices 52B to 52D respectively, network 90 and/or external services providers 95 are optionally, partially or entirely, integrated in system for controlled pre-interaction 50A.

According to FIG. 4 participants of various types are concomitantly served to system 100. Thus participant parties

18

B to D user devices 52B to 52D are optionally of different types, namely having different functional capabilities/limitations. Thus participant party B optionally has system for controlled pre-interaction 50B of his/her own. Party B in such a case is capable of controlled pre-interaction with party A, from a manageable public address of party B to a manageable public address of party A.

Participant party C may have a user device 52C or integrated user module 58C, which are optionally a mobile phone built on a mobile operating system (e.g. Smartphone) with relatively more advanced computing capability and connectivity; whereas party D may have a user device 52D, which is a line telephone or mobile feature phone with relatively more limited computing capability and connectivity. Typically with user device 52D having limited computing capability and connectivity, such as DECT phone and feature phone, system 50 optionally employs a thin-client or no-client configurations, where user device 52D comprises merely a minimal user interface, whereas the steps of the method for controlled pre-interaction are performed by system 50. Therefore systems for controlled pre-interaction 50A and 50B are capable to sustain a controlled pre-interaction among parties A to D and optionally a controlled reciprocating communication of parties A through D.

#### Multiple Parties Pre-Interaction

In accordance with some preferred embodiments, systems 50A and 50B are adapted to sustain a controlled pre-interaction capable among multiple parties, such as parties A to D. A participant in a multi-party communication and/or conferencing is referred to herein as participant.

For instance party C is added to or creates a VoIP chatting conferencing communication performed between parties A to D, while the VoIP chat of party A with party C is performed from a different manageable public VoIP screen name than the VoIP screen name of the chat of party A with party B.

Alternatively or additionally, multiple parties' pre-interaction is initiated upon proposing a contact, friend or connection of party C for user party A by participant party B; for a presence communication, IM communication, VoIP communication, audio and/or video conferencing communication etc. For instance a presence address of party C may be suggested by participant party B to user party A or a connection request (e.g. handshake) may be sent by participant party B to user party A on behalf of party C, while the manageable public presence address of user party A provided to party C is different than the manageable public or private presence address of party A available to party B.

Alternatively or additionally, multiple parties pre-interaction is initiated upon sharing, posting, publishing or notifying electronic files or data (e.g. content), with/to participant party C by user party A previously shared, posted, published or notified with/to party B. For instance electronic files or data (e.g. content) may be shared, posted, published or notified by user party A with/to participant party C using a manageable public interaction address (e.g. sharing address, presence address or IM address) that is different than the manageable public or private interaction address (e.g. sharing address, presence address or IM address) from/at which party A has previously shared, posted, published or notified aforesaid electronic files and/or data with/to party B.

#### Examples

According to first example, party A is a landlord renting a house. Landlord party A hence defines a manageable public telephone number, for the purposes of communicat-



US 9,749,284 B2

19

ing with potential tenants, such as parties B to D. Landlord party A then publishes the manageable public telephone number, for instance in a local newspaper. Potential tenants, such as parties B to D, then optionally call the manageable public telephone number, to contact landlord party A. Landlord party A generates reverse list entries for tenants parties B to D and then in turn can contact tenants parties B to D from the manageable public telephone number, whilst keeping the private telephone number of landlord party A discreet from tenants parties B to D.

According to second example, party A has a dual-SIM mobile phone, wherein the telephone number of one SIM is defined as the private interaction address of party A, whereas the telephone number of another SIM is defined as the manageable public interaction address of party A. The dual-SIM mobile phone in such example embodies the user device, associated with a private interaction address of party A, as well as the user device, associated with a manageable public interaction address of party A. The dual-SIM mobile phone optionally further includes the public interaction address management system and reverse list registry of party A. Party A thence is able to perform an incoming and/or outgoing communication in a controlled manner—namely from the telephone number of another SIM which is defined as the manageable public address of party A and listed in an entry of reverse list as associated with telephone numbers of participant parties, such as parties B to D.

According to third example, party A is a landlord renting a house. Landlord party A hence defines a manageable public telephone number, for the purposes of communicating with potential tenants, such as party B. Potential tenant party B may also implement a system for controlled pre-interaction. Potential tenant party B generates a reverse list entry for landlord for party A and then contacts landlord for party A from the manageable public telephone number of tenant party B and to the manageable public telephone number of landlord party A, whilst keeping the private telephone number of tenant party B discreet from landlord party A.

According to fourth example, party A is a popular person, defining a manageable public telephone number, for supporters or followers parties B to D expiring after several hours or days. Popular person party A then defines a rule that upon expiration any incoming communications to manageable public telephone number, listed in the public addresses record, is replied to with SMS having predefined content, such as party A that is currently unavailable and/or when one should try again to reach party A.

According to fifth example, party A is a member of a professional or social computer network, such as LinkedIn. Party A is then optionally inspects a profile of member party B on aforesaid network. Upon such inspecting of the profile of member party B, party A is optionally advised on the profiles of other members who had inspected or connected with member party B. Thereafter the system optionally indicates which of the profiles of party B were inspected and accordingly may be advised for party A profile. A reverse list is then optionally generated, preferably automatically, in the public address management system, listing the public profile of party B and optionally associating the profile of the inspecting party A, typically either automatically or in according with predefined preference. Later communications via the professional network or via other interaction means, from party A to party B, will expose particular profile details of party B.

According to sixth example, party A is a member of a social computer network, such as Facebook, identified by a

20

public Facebook interaction address. Party A is then optionally inspects, accesses, searches, views, befriends, pokes or otherwise connects or attempts a connection with party B, who is another member of the same social network, which may be collectively referred to as an interaction or inspection. The system will consider such an interaction or inspection as a form of interaction as defined herein and will ensure that information of party B exposed to A, matches party B privacy requirements, as well as any other communication for that matter.

In the instance of social network, party B may have multiple profiles that may include multiple profile information elements (e.g. different contact fields, languages spoken, address location or any other profile information). When party A inspects party B, he may be exposed to a specific profile or subset of profiles of party B, based on various criteria. This criteria may include a pre-determined rules or grouping (such as party B putting party A in a specific group of friends), based on the actual profile information of party A (e.g. gender, city or country, age or age-group, workplace, education or other), the actual inspection or interaction details (such as country inferred from IP address of party A inspection, time or date of inspection, type of device used by party A for the inspection, computer network type used for the inspection, etc.) or any other criteria for that matter.

Consequently, a reverse list is optionally generated, preferably automatically, in the public address management system of party B, identifying which of the public profiles of party B is to be exposed to party A denoted by party A social network interaction address. The details of party B that A was exposed to based on this criteria will be associated for future interactions or communications.

Note that in this case no specific communication between A and B was yet performed. Future such inspections, or communications within the Social Network, or outside of it using any other means of communication, will use the reverse list and associated profile information as described in this invention, an accordingly maintain B privacy.

According to seventh example, party A is an employee or contractor in an organization. Parties B to D are optionally coworkers or clientele of party A. An administrator of the system for controlled pre-interaction is then can import, synchronize or provision a plurality of reverse list entries for party A, wherein the interaction addresses of parties B to D are associated with a manageable public interaction address of party A dedicated for work purposes.

#### Patent Literature References

US patent Ser. No. U.S. Pat. No. 7,995,730, U.S. Pat. No. 7,436,943, U.S. Pat. No. 7,602,894  
US patent application Ser. No. US2010/054444, US2012/328089  
GB patent application Ser. No. GB2454886  
European patent application Ser. No. EP2073521, EP2448227  
PCT applications Pub. No. WO2007/053768, WO2010/135000

#### Non Patent Literature References

Request for Comments: 3261—Session Initiation Protocol Available at: <http://www.ietf.org/rfc/rfc3261.txt>  
Request for Comments: 5627—Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP) Available at: <http://tools.ietf.org/html/rfc5627>

US 9,749,284 B2

21

3GPP TS 23.228 V5.13.0—3rd Generation Partnership Project (2004-12) Available at: <http://www.ipi.etsi.org/ipilib/ipilib/BaseDocs/3GPP23.228.htm>

Instant Messaging draft-saintandre SIP-XMPP-IM-01 (Mar. 8, 2009) Available at: <http://tools.ietf.org/html/draft-saintandre-sip-xmpp-im-01>

One-to-one text chat draft-saintandre SIP-XMPP-CHAT-03 (Mar. 8, 2009) Available at: <http://tools.ietf.org/html/draft-saintandre-sip-xmpp-chat-03>

Presence Draft-Saintandre XMPP-PRESENCE-02 (Mar. 8, 2009) Available at: <http://tools.ietf.org/html/draft-saintandre-sip-xmpp-precense-02>

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described herein above. Rather the scope of the invention is defined by the claims which follow:

The invention claimed is:

1. A method of performing controlled reciprocating communication, wherein said controlled reciprocating communication comprises an incoming and outgoing communications, between a first party and at least one second party, said method comprises:

- (a) providing at least one private interaction address of said first party;
- (b) defining at least one manageable public interaction address for said first party;
- (c) forming a record, wherein said manageable public interaction address is associated with said private interaction address for said first party;
- (d) receiving an incoming communication, said incoming communication comprises a communication from said second party to said first party; wherein said incoming communication is initiated by said second party to said manageable public interaction address of said first party;
- (e) identifying that said incoming communication was received to said manageable public interaction address;
- (f) accessing said record and performing at least one step selected from the group consisting of:
  - (I) determining said respective identity associated with said manageable public interaction address identified in said incoming communication, and
  - (II) determining said private interaction address of said first party associated at said record with said manageable public interaction address identified in said incoming communication;

said method is characterized by:

- (g) generating at least one reverse list entry, wherein an interaction address of said second party is associated at least with said manageable public interaction address of said first party;
- (h) performing a pre-interaction act, said pre-interaction act comprises:
  - (I) accessing said reverse list;
  - (II) identifying said interaction address of said second party in said reverse list;
  - (III) determining that said manageable public interaction address of said first party is associated, at said reverse list, with said interaction address of said second party;
- (i) performing an outgoing communication, said outgoing communication comprises a communication from said first party to said second party, said outgoing communication is initiated by said first party;
- (j) said outgoing communication is characterized by that said outgoing communication, to said interaction

22

address of said second party, is performed from said manageable public interaction address of said first party;

wherein upon performing said outgoing communication, said second party is exposed merely to said manageable public interaction address of said first party;

wherein said interaction address of said second party is obtainable from a third party or external services provider, wherein said at least one reverse list entry is formed by synchronizing said interaction address of said second party with said manageable public interaction address.

2. The method of performing controlled reciprocating communication as set forth in claim 1, wherein said steps of defining and forming further comprise:

- (a) defining a respective identity of said first party, for said manageable public interaction address of said first party, and
- (b) forming a record associating said respective identity of said first party with said manageable public interaction address of said first party.

3. The method of performing controlled reciprocating communication as set forth in claim 2, wherein said step of determining further comprises determining that said interaction address of said second party is associated, at said reverse list, with said respective identity of said first party.

4. The method of performing controlled reciprocating communication as set forth in claim 1, wherein said communication comprises a communication selected from the group consisting of: an attempted communication, incomplete communication, rejected communication, interrupted communication and abrupt communication.

5. The method of performing controlled reciprocating communication, as set forth in claim 1, wherein said interaction address selected from the group consisting of: a line telephone number, line facsimile number, cellular/mobile phone number, instant messaging (IM) name, e-mail address, presence screen name, service handle, universal resource identifier (URI), universal resource name (URN), universal resource locator (URL), extensive resource identifier (XRI), SIP identifier, any type of user identifier for sharing or and any type of user identifier communication.

6. The method of performing controlled reciprocating communication as set forth in claim 1, wherein said interaction address is a partial interaction address, comprising a portion of said string of characters or a sub-string thereof or wherein said string is defined as including at least one wildcard, representing more than one participant having identical portions in their interaction addresses.

7. The method of performing controlled reciprocating communication, as set forth in claim 1, wherein said step of determining said private interaction address, during said step of accessing said record, further comprises performing at least one step selected from the group consisting of:

- (a) forwarding said incoming communication to said at least one private interaction address associated with said manageable public interaction address at said record;
- (b) forwarding information regarding said incoming communication to said at least one private interaction address associated with said manageable public interaction address at said record;
- (c) presenting said manageable public interaction address to which said incoming communication was received;
- (d) presenting at least one information item selected from the group consisting of:
  - (I) a name assigned to said manageable public interaction address;

US 9,749,284 B2

23

- (II) metadata assigned to said manageable public interaction address;
- (III) public identity assigned to said manageable public interaction address;
- (e) applying a notification rule to said incoming communication;
- (f) selecting contents for said notification.

8. The method of performing controlled reciprocating communication, as set forth in claim 1, wherein said reverse list further comprises at least one constituent selected from the group consisting of: a name assigned to said manageable public interaction address; metadata assigned to said manageable public interaction address; a public identity assigned to said manageable public interaction address; a rule relating to a notification; a content for said notification; a default communication preference; an overruling alternative for said default communication preference; personal information of said second party; contact information of said second party.

9. The method of performing controlled reciprocating communication, as set forth in claim 1, wherein generating said reverse list is performed by at least one selected from the group consisting of: said first party; a user of a system for controlled reciprocating communication; an operator of said system for controlled reciprocating communication; a third party related to said system for sustaining a controlled reciprocating communication, and external services providers for said system for sustaining a controlled reciprocating communication.

10. The method of performing controlled reciprocating communication, as set forth in claim 1, wherein said reverse list entry is generated in at least one manner selected from the group consisting of: manually by inputting said interaction address of said second party; upon receiving said incoming communication; upon performing said outgoing communication; by external services providers for a system for sustaining a controlled reciprocating communication.

11. The method of performing controlled reciprocating communication, as set forth in claim 1, wherein said interaction address of said second party is unavailable to said first party, wherein at least a portion of said reverse list entry is confidential to said first party.

12. The method of performing controlled reciprocating communication, as set forth in claim 1, wherein said reverse list entry is generated upon said outgoing communication, is performed in at least one manner selected from the group consisting of:

- (a) automatically upon identifying said manageable public interaction address from which said second party is contacted
- (b) by prompting said first party with a proposed reverse list entry and completed upon confirmation of said first party to form said entry.

13. The method of performing controlled reciprocating communication, as set forth in claim 1, further comprises performing at least one predefined rule, said rule comprises at least one instruction for a predefined response, wherein said response selected from the group consisting of: rejecting a communication; recording a communication; converting a communication to another format; forwarding a communication to said private interaction address of said first party.

14. The method of performing controlled reciprocating communication, as set forth in claim 1, further comprises prescribing at least one communication preference selected from the group consisting of: a default communication preference and overruling alternative for said default com-

24

munication preference, said communication preference is assigned to at least one selected from the group consisting of:

- (a) said private interaction address of said first party, contained in said record
- (b) said manageable public interaction address of said first party, contained in said record or said reverse list, and
- (c) said interaction address of said second party, contained in said reverse list.

15. The method of performing controlled reciprocating communication, as set forth in claim 1, further comprises prescribing at least one default communication preference, wherein said default communication preference indicates said manageable public interaction address of said first party, determined at said step of determining during said pre-interaction act.

16. The method of performing controlled reciprocating communication, as set forth in claim 1, further comprises prescribing at least one default communication preference, wherein said default communication preference indicates said manageable public interaction address of said first party, determined at said step of determining during said pre-interaction act, and further comprises an overruling alternative for said default communication preference, wherein said overruling alternative indicates an alternative manageable public interaction address of said first party or said private interaction address of said first party for a particular communication session, if a predefined condition is met.

17. A method of performing controlled pre-interaction, between a first party and at least one second party, said method comprises:

- (a) providing at least one private interaction address of said first party;
- (b) defining at least one manageable public interaction address for said first party;
- (c) forming a record, wherein said manageable public interaction address is associated with said private interaction address for said first party;
- (d) generating a reverse list, wherein an interaction address of said second party is associated at least with said manageable public interaction address of said first party;
- (e) performing at least one pre-interaction act, said pre-interaction act comprises:
  - (I) accessing said reverse list;
  - (II) identifying said interaction address of said second party in said reverse list;
- (f) determining that said manageable public interaction address of said first party is associated, at said reverse list, with said interaction address of said second party; wherein said interaction address of said second party is obtainable from a third party or external services provider, wherein said at least one reverse list entry is formed by synchronizing said interaction address of said second party with said manageable public interaction address.

18. The method of performing controlled pre-interaction, as set forth in claim 17, wherein said method is not followed by a communication.

19. The method of performing controlled pre-interaction, as set forth in claim 17, wherein said method is followed by a communication to another interaction address of said second party, wherein said another interaction address of said second party is of a different type than said interaction address of said second party.

US 9,749,284 B2

25

20. The method of performing controlled pre-interaction, as set forth in claim 17, wherein said interaction address of said second party is obtainable from a third party comprises several interaction addresses of different types of said second party.

21. The method of performing controlled pre-interaction, as set forth in claim 17, further comprises performing at least one predefined rule, said rule comprises at least one instruction for a predefined response, wherein said response selected from the group consisting of: recording a communication; converting a communication to another format; forwarding a communication to said private interaction address of said first party.

22. The method of performing controlled pre-interaction, as set forth in claim 17, further comprises performing at least one predefined rule, said rule is assigned to at least one selected from the group consisting of: said private interaction address of said first party, contained in said record; said manageable public interaction address of said first party, contained in said record or said reverse list, and said interaction address of said second party, contained in said reverse list.

23. The method of performing controlled pre-interaction, as set forth in claim 17, further comprises prescribing at least one communication preference selected from the group consisting of: a default communication preference and overruling alternative for said default communication preference, said communication preference is assigned to at least one selected from the group consisting of: said private interaction address of said first party, contained in said record, said manageable public interaction address of said first party, contained in said record or said reverse list, and said interaction address of said second party, contained in said reverse list.

24. The method of performing controlled pre-interaction, as set forth in claim 17, further comprises prescribing at least one default communication preference, wherein said default communication preference indicates said manageable public interaction address of said first party, determined at said step of determining during said pre-interaction act.

25. The method of performing controlled pre-interaction, as set forth in claim 17, further comprises prescribing at least one default communication preference, wherein said default communication preference indicates said manageable public interaction address of said first party, determined at said step of determining during said pre-interaction act, and further comprises an overruling alternative for said default communication preference, wherein said overruling alternative indicates an alternative manageable public interaction address of said first party or said private interaction address of said first party for a particular communication session, if a predefined condition is met.

26. Non-transitory computer readable media having computer-executable instructions embodied thereon, that when executed by a computing system, perform a method of controlled reciprocating communication, the non-transitory computer readable media comprising instructions as set forth in claim 17.

27. A system for performing a controlled pre-interaction, between a first party and at least one second party, said system comprises:

- (a) at least one member selected from the group consisting of: a graphical user interface, input device and computer networking terminal, configured for providing at least one private interaction address of said first party;
- (b) at least one member selected from the group consisting of: a graphical user interface, input device and

26

computer networking terminal, configured for defining at least one manageable public interaction address for said first party;

- (c) at least one non-transitory computer storage memory configured for forming and storing a record, wherein said manageable public interaction address is associated with said private interaction address for said first party;
- (d) at least one computer non-transitory storage memory configured for forming and storing at least one reverse list entry, wherein an interaction address of said second party is associated at least with said manageable public interaction address of said first party;
- (e) at least one microprocessor configured for accessing said reverse list;
- (f) at least one microprocessor configured for identifying said interaction address of said second party in said reverse list; and
- (g) at least one microprocessor configured for determining whether said manageable public interaction address of said first party is associated, at said reverse list, with said interaction address of said second party;

wherein said interaction address of said second party is obtainable from a third party or external services provider, wherein said at least one reverse list entry is formed by synchronizing said interaction address of said second party with said manageable public interaction address.

28. The system for performing a controlled pre-interaction, as set forth in claim 27, further comprises a networking terminal configured for performing a controlled outgoing communication, said controlled outgoing communication comprises a communication from said first party to said second party, said controlled outgoing communication is initiated by said first party, wherein initiating of said controlled outgoing communication, to said interaction address of said second party, is performed from said manageable public interaction address of said first party.

29. The system for performing a controlled pre-interaction, as set forth in claim 27, further comprises a networking terminal configured to receive said incoming communication, wherein said receiving of said incoming communication is performed by at least one networking terminal selected from the group consisting of:

- (a) a networking terminal configured for receiving said incoming communication from said second party to said first party; wherein said incoming communication is initiated by said second party to said manageable public interaction address of said first party;
- (b) a networking terminal configured identifying that said incoming communication was received to said manageable public interaction address;
- (c) a networking terminal configured accessing said record and determining said respective identity associated with said manageable public interaction address identified with said means of identifying.

30. The system for performing a controlled pre-interaction, as set forth in claim 27, wherein said controlled pre-interaction is not followed by a communication.

31. The system for performing a controlled pre-interaction, as set forth in claim 27, wherein said pre-interaction is followed by a communication to another interaction address of said second party, wherein said another interaction address of said second party is of a different type than said interaction address of said second party.

32. The system for performing a controlled pre-interaction, as set forth in claim 27, wherein said interaction



US 9,749,284 B2

27

address of said second party is obtainable from a third party comprises several interaction addresses of different types of said second party.

33. The system for performing a controlled pre-interaction, as set forth in claim 27, further comprises at least one microprocessor configured for executing at least one predefined rule selected from the group consisting of: recording a communication, converting a communication to another format, forwarding a communication to said private interaction address of said first party.

34. The system for performing a controlled pre-interaction, as set forth in claim 27, further comprises at least one microprocessor configured for executing at least one predefined rule, said rule is assigned to at least one member selected from the group consisting of: said private interaction address of said first party, contained in said record; said manageable public interaction address of said first party, contained in said record or said reverse list, and said interaction address of said second party, contained in said reverse list.

35. The system for performing a controlled pre-interaction, as set forth in claim 27, further comprises at least one non-transitory computer storage memory configured to store therein at least one communication preference selected from the group consisting of: a default communication preference and overruling alternative for said default communication preference, said communication preference is assigned by said means of prescribing to at least one selected from the group consisting of: said private interaction address of said first party, contained in said record; said manageable public interaction address of said first party, contained in said

28

record or said reverse list, and said interaction address of said second party, contained in said reverse list.

36. The system for performing a controlled pre-interaction, as set forth in claim 27, further comprises at least one non-transitory computer storage memory configured to store therein a preset content for a notification, said preset content for said notification selected from the group consisting of: text, alphanumeric data, audio files, video files, graphics, hyperlinks and a template comprising at least one empty field, which is filled-in with content thereafter.

37. The system for performing a controlled pre-interaction, as set forth in claim 27, further comprises at least one non-transitory computer storage memory configured to store therein at least one default communication preference, wherein said default communication preference indicates said manageable public interaction address of said first party, determined by said means of determining during said pre-interaction act.

38. The system for performing a controlled pre-interaction, as set forth in claim 27, further comprises at least one non-transitory computer storage memory configured to store therein at least one default communication preference, wherein said default communication preference indicates said manageable public interaction address of said first party, determined by said means of determining during said pre-interaction act, and further comprises an overruling alternative for said default communication preference, wherein said overruling alternative indicates an alternative manageable public interaction address of said first party or said private interaction address of said first party for a particular communication session, if a predefined condition is met.

\* \* \* \* \*

### **CERTIFICATE OF SERVICE**

I hereby certify that, on this 3rd day of November, 2021, I filed the foregoing Brief for Plaintiff-Appellant with the Clerk of the United States Court of Appeals for the Federal Circuit via the CM/ECF system, which will send notice of such filing to all registered CM/ECF users.

/s/ Thomas H. Burt  
THOMAS H. BURT

**WOLF HALDENSTEIN ADLER  
FREEMAN & HERZ LLP**  
270 Madison Avenue, 9<sup>th</sup> Floor  
New York, New York 10016  
Tel: (212) 545-4600

### **CERTIFICATE OF COMPLIANCE**

Pursuant to Fed. R. App. P. 32(a)(7)(C), the undersigned hereby certifies that this brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) and Circuit Rule 32(b).

1. Exclusive of the exempted portions of the brief, as provided in Fed. R. App. P. 32(a)(7)(B), the brief contains 13,404 words.

2. The brief has been prepared in proportionally spaced typeface using Microsoft Word 2010 in 14-point Times New Roman font. As permitted by Fed. R. App. P. 32(a)(7)(C), the undersigned has relied upon the word count feature of Word software in preparing this certificate.

Dated: November 3, 2021

/s/ Thomas H. Burt  
THOMAS H. BURT

**WOLF HALDENSTEIN ADLER  
FREEMAN & HERZ LLP**  
270 Madison Avenue, 9<sup>th</sup> Floor  
New York, New York 10016  
Tel: (212) 545-4600