

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

QPRIVACY USA LLC,

Plaintiff,

v.

CISCO SYSTEMS, INC.,

Defendant.

CASE NO. 2:24-cv-00855-JRG

DEFENDANT CISCO SYSTEMS, INC.'S
INVALIDITY AND SUBJECT MATTER ELIGIBILITY CONTENTIONS

I. INTRODUCTION

Pursuant to the Docket Control Order (ECF No. 29), Defendant Cisco Systems, Inc. (“Cisco”) provides these Preliminary Invalidity Contentions to Plaintiff QPrivacy USA LLC (“QPrivacy”) with respect to U.S. Patent Nos. 11,106,824 (the “’824 patent”) and 11,816,249 (the “’249 patent”) (collectively, the “Asserted Patents”). Plaintiff’s January 7, 2025 Infringement Contentions assert all claims of the Asserted Patents against Cisco (*i.e.*, claims 1–20 of the ’824 Patent and claims 1–30 of the ’249 Patent (collectively, the “Asserted Claims”)).

With respect to each Asserted Claim and based on their investigation to date, Cisco (a) identifies each item of prior art that anticipates each asserted claim or renders it obvious; (b) specifies whether each such item of prior art anticipates each Asserted Claim or renders it obvious, and, if it renders it obvious, explain why the prior art renders the asserted claim obvious and identify combinations of prior art showing obviousness; (c) submits charts specifically identifying where and how in each item of prior art each limitation of each Asserted Claim is found; (d) identifies any limitations that are indefinite, lack written description, or fail to satisfy the enablement requirement under 35 U.S.C. § 112; and (e) identifies any claims that are directed to ineligible subject matter under 35 U.S.C. § 101.

QPrivacy has failed to provide infringement contentions that comply with the patent local rules or that put Cisco on notice of QPrivacy’s infringement theories. P.L.R. 3-1 (requiring an identification of “specifically where each element of each asserted claim is found within each Accused Instrumentality.”); *see also Computer Acceleration Corp. v. Microsoft Corp.*, 503 F. Supp. 2d 819, 823 (E.D. Tex. 2007) (“The contentions must be specific enough to give a defendant notice of plaintiff’s infringement claims”). Given QPrivacy’s failure to identify the full scope of the accused instrumentalities and where QPrivacy contends that each element of the Asserted Claims is found within each instrumentality, Cisco lacks a complete understanding of QPrivacy’s alleged infringement and/or claim construction positions. Accordingly, Cisco reserves the right to amend, supplement, and/or otherwise modify these Preliminary Invalidity

Contentions if QPrivacy provides new infringement theories and/or claim construction theories inconsistent with its January 7, 2025 infringement contentions.

A. Claim Construction

The Court has not yet construed any of the terms in the Asserted Claims of the Asserted Patent. These Preliminary Invalidity Contentions are served in view of Cisco's current understanding of the Asserted Claims, without the benefit of claim construction proceedings in this action. Accordingly, Cisco does not take any position herein regarding the proper scope or construction of the Asserted Claims. To the extent that Cisco's contentions reflect, imply, or suggest a particular interpretation or construction of any claim element or term, Cisco does not adopt, advocate, or acquiesce to such an interpretation or construction. Cisco's contentions therefore should not be relied upon as a statement of Cisco's proposed claim constructions or as any admission regarding the proper scope of the claims. Nor do these Preliminary Invalidity Contentions constitute any admission by Cisco that any accused products or services, including any current or past versions of those products or services, are covered by any Asserted Claim.

These Preliminary Invalidity Contentions may consider QPrivacy's apparent interpretations of the Asserted Claims as reflected in QPrivacy's Infringement Contentions. Accordingly, any assertion herein that a particular limitation is disclosed by a prior art reference or references may be based in part on QPrivacy's apparent interpretation, but is not intended to be, and is not, an admission by Cisco that any such construction is supportable or correct, or that any claim terms of the Asserted Claims are not invalid under 35 U.S.C. § 112 for being indefinite, failing to satisfy the written description requirement, or failing to satisfy the enablement requirement. Moreover, nothing in these Preliminary Invalidity Contentions should be construed as an admission or a waiver by Cisco of any particular construction of any claim term. Further, Cisco specifically denies that QPrivacy's apparent claim constructions are supportable or correct.

B. Ongoing Discovery and Disclosures

These Preliminary Invalidity Contentions are based on Cisco's current knowledge and understanding of the Asserted Claims and review of prior art items as of the date of service, and are made without the benefit of discovery regarding the parties' claim construction contentions, any expert discovery, any third-party discovery, and any claim construction opinion or order by the Court. What's more, QPrivacy has failed to serve Infringement Contentions that comply with the Patent Local Rules, which prejudices Cisco's ability to adequately prepare its defenses. Accordingly, these Preliminary Invalidity Contentions are provided without prejudice to Cisco's right to revise, amend, correct, supplement, modify, or clarify the same. Cisco also reserves the right to complete their investigation and discovery of the facts, to produce subsequently discovered information, and to introduce such subsequently discovered information at the time of any hearing or trial in this action.

These Preliminary Invalidity Contentions are also based at least in part on Cisco's current understanding of the Asserted Claims in view of QPrivacy's Infringement Contentions, which fail to provide Cisco with requisite notice of QPrivacy's infringement theories under the Patent Local Rules. If QPrivacy amends its Infringement Contentions to address any deficiency therein, or for any other reason, Cisco reserves the right to amend or supplement these Preliminary Invalidity Contentions.

Cisco further reserves the right to supplement and amend these Preliminary Invalidity Contentions and its accompanying document production based on further investigation, analysis, and discovery, Cisco's consultation with experts and others, and contentions or court rulings on relevant issues such as claim construction and priority dates. For example, since fact discovery has not yet begun, deposing the alleged inventors may reveal information that affects the disclosures and contentions herein. In addition, Cisco has not completed discovery from third parties who have information concerning the prior art cited herein and possible additional art, including additional evidence regarding prior art system disclosed herein.

Because Cisco is continuing its search for and analysis of relevant prior art and seeking discovery from third parties with information concerning the prior art cited herein and possible additional art, Cisco reserves the right to revise, amend, and/or supplement the information provided herein, including identifying, charting, and/or relying upon additional prior art references, relevant disclosures, and bases for these Preliminary Invalidity Contentions. Additional prior art, disclosures, and invalidity grounds, whether or not cited in this disclosure and whether known or not known to Cisco, may become relevant as investigation, analysis, and discovery continue, and following claim construction proceedings in this case.

These Preliminary Invalidity Contentions also incorporate by reference all bases for invalidity identified in subsequent pleadings and discovery responses in this case, and any bases of invalidity identified during the prosecution of the Asserted Patents, as well as all related patents and/or patent applications. Cisco further incorporates by reference all admissions regarding the Asserted Patent including, but not limited to, admissions in the specification of the Asserted Patents and the prosecution of the Asserted Patents and related patents and/or patent applications.

These Preliminary Invalidity Contentions further incorporate by reference (1) any and all prior art identified in documents produced by QPrivacy to Cisco in this case; (2) any and all materials regarding invalidity that should have been produced to Cisco but have not been produced to date, to the extent that any exist; (3) any prior art of which a named inventor of the Asserted Patents is aware and/or on which he, she, and/or QPrivacy contends the alleged invention(s) of the Asserted Patents builds upon or improves; and (4) any and all admissions by QPrivacy and/or a named inventor regarding the Asserted Patents including, but not limited to, admissions in the specifications of the Asserted Patents and the prosecution of the Asserted Patents and related patents and/or patent applications. In addition, these Preliminary Invalidity Contentions incorporate all prior art identified and invalidity contentions served in any related litigation, including any petitions for *inter partes* review of the Asserted Patents.

II. PRIORITY DATE OF THE ASSERTED PATENT AND CLAIMS

QPrivacy asserts that the Asserted Patents “share a priority date based on foreign application IL251683 filed on April 9, 2017.” QPrivacy’s 2025-01-07 Infringement Contentions. QPrivacy has the burden to show entitlement to the asserted priority date that is earlier than the filing date of the Asserted Patent. QPrivacy has not met that burden and is not entitled to that alleged priority date. Cisco reserves the right to modify, amend, or supplement its Preliminary Invalidity Contentions with additional prior art references if any Asserted Claim is shown to not be entitled to the alleged priority date or if QPrivacy alleges any other priority date for any of the Asserted Claims.

III. PRIOR ART IDENTIFICATION AND INVALIDITY CLAIM CHARTS

The accompanying invalidity claim charts (identified in Section IV below) cite to particular teachings and disclosures of the prior art references as applied to elements of the Asserted Claims. Persons having ordinary skill in the art, however, may view an item of prior art generally in the context of other publications, literature, products, and understanding. Accordingly, the cited portions are only exemplary and are intended to put QPrivacy on notice of the basis for Cisco’s contentions. Cisco has endeavored to identify relevant portions of the references, but the references may contain additional support for particular claim limitations. Cisco reserves the right to rely on uncited portions of the prior art references, other documents, and/or operational systems, as well as fact and expert testimony, to provide context or to aid in understanding the cited portions of the references and interpreting the teachings of the prior art and to establish bases for combinations of certain cited references that render the Asserted Claims obvious. Cisco also reserves the right to rely on any prior art system referenced, embodied, or described in any of the prior art references identified herein, or which embodies any of the prior art references identified herein.

Moreover, Cisco reserves the right to rely on inventor admissions concerning the scope of the prior art relevant to the Asserted Patents found in, *inter alia*, the prosecution history of the Asserted Patents or related patents and/or patent applications, any testimony or declarations of

the named inventors concerning the Asserted Patents or related patents, and any papers or evidence submitted by QPrivacy in connection with this litigation, any other pending or future litigation brought by QPrivacy involving the Asserted Patents or related patents, any future *ex parte* reexamination proceedings involving the Asserted Patents or related patents, or any post grant proceedings (e.g., *inter partes* review) involving the Asserted Patents or related patents. Cisco also may establish what was known to a person having ordinary skill in the art through treatises, published industry standards, other publications, products, and/or testimony.

Where the invalidity claim charts (identified in Section IV below) cite to a particular figure in a reference, the citation should be understood to encompass the caption of the figure and other text relating to and/or describing the figure. Similarly, where the invalidity claim charts cite to particular text referring to a figure, the citation should be understood to include the figure and related figures as well.

The prior art references listed herein and in the accompanying invalidity claim charts may disclose the elements of the Asserted Claims explicitly and/or inherently. The prior art references are also relevant for their showing of the state of the art and reasons and motivations for making improvements, additions, and combinations. The suggested obviousness combinations are provided in the alternative to Cisco's anticipation contentions and are not to be construed to suggest that any reference is not itself anticipatory.

Further, the combinations of prior art references contained herein demonstrating the obviousness of the Asserted Patents under 35 U.S.C. § 103 are merely exemplary and are not intended to be exhaustive. All such combinations are intended to include and be in view of the knowledge of a person of ordinary skill in the art. Additional obviousness combinations of the identified prior art references are possible, and Cisco reserves the right to use any such combination(s) in this litigation. In particular, Cisco is currently unaware of the extent to which QPrivacy may contend that limitations of any particular claim(s) are not disclosed in the art that Cisco has identified as anticipatory. To the extent that QPrivacy does so, Cisco reserves the right to identify other evidence or references that anticipate or render obvious the particular claim(s).

Nothing in these contentions should be treated as an admission that any of Cisco's accused instrumentalities meet any limitation of the Asserted Claims. Cisco denies infringement of the Asserted Claims. To the extent that any prior art references identified by QPrivacy contains a claim element that is the same as or similar to an element in an accused instrumentality, based on a claim construction inferred from QPrivacy's Infringement Contentions, inclusion of that reference in these Preliminary Invalidity Contentions is not a waiver by Cisco of any claim construction or non-infringement position, nor is it an admission or suggestion by Cisco that any accused instrumentality satisfies the limitations of the Asserted Claims under a proper construction of those claims.

IV. PRELIMINARY INVALIDITY CONTENTIONS FOR THE '824 AND '249 PATENTS

A. Prior Art References¹

1. Prior Art Patents and Publications

Cisco identifies the following prior art patents and printed publications, which anticipate the '824 and '249 asserted claims under 35 U.S.C. §§ 102(a), (b), (e), and/or (g), and/or render the '824 and '249 asserted claims obvious under 35 U.S.C. § 103, either alone or in combination.

Prior Art	Date of Issue / Publication	Effective Filing Date
US 2015/0040237 ("Vandervort")	February 5, 2015	August 5, 2013
US 9,946,895 ("Nagda")	December 15, 2015	December 15, 2015
US 10,311,446 ("Prehofer")	December 5, 2008	December 5, 2008
US 2017/0364794 ("Mahkonen")	June 20, 2016	June 20, 2016
US 11,108,627 ("Smith")	December 28, 2017	December 30, 2016
US 9,946,895 ("Kruse")	April 17, 2018	December 15, 2015

¹ To the extent one or more prior art patents, publications, or systems are identified in the claim charts attached hereto but are not included in the tables and lists below, those prior art patents, publications, or systems are also prior art to the '824 and '249 patents.

Prior Art	Date of Issue / Publication	Effective Filing Date
US 8,341,724 (“Burns”)	December 25, 2012	December 19, 2008
US 8,291,495 (“Yang”)	October 16, 2012	August 8, 2007
US 11,087,568 (“Deshmukh”)	February 3, 2020	March 31, 2017
US 8,209,756 (“Guruswamy”)	June 26, 2012	February 8, 2002
US 2005/0078668 (“Wittenberg”)	April 14, 2005	October 8, 2003
US 11,019,101 (“Narayanaswamy”)	December 2, 2016	March 11, 2016
US11277383 (“Devarajan”)	April 27, 2020	November 17, 2015
US 2018/0276401 (“Allen”)	September 27, 2018	March 23, 2017
US 2015/0163206 (“Wenzel”)	December 10, 2014	December 11, 2013
US 10,606,626 (“Feroz”)	July 30, 2015	December 29, 2014
US 11,558,398 (“Gvili”)	September 25, 2020	November 25, 2015
US 9,842,218 (“Johnstone”)	April 10, 2015	April 10, 2015
US 7,797,725 (“Lunt”)	September 14, 2010	December 2, 2004
US 2015/0324606 (“Grondin”)	November 12, 2015	May 6, 2015
US 2015/0186674 (“Vyas”)	July 2, 2015	January 2, 2014
US 9,552,272 (“Liang”)	January 24, 2017	July 29, 2011
US 2015/0199523 (“Hamilton”)	July 16, 2015	January 15, 2014
US 8,621,615 (“Zhao”)	December 13, 2013	April 3, 2009
US 9,088,508 (“Caputo”)	July 21, 2015	April 11, 2014
US 5,835,726 (“Shwed”)	Nov. 10, 1998	Dec. 15, 1993
US 6,725,378 (“Schuba”)	Apr. 20, 2004	Apr. 15, 1998
US 6,801,503 (“Wetherall”)	Oct. 5, 2004	Nov. 9, 2000
US 2011/0213869 (“Korsunsky”)	September 1, 2011	September 25, 2000

Prior Art	Date of Issue / Publication	Effective Filing Date
US 8,205,259 (“Stute”)	July 19, 2012	March 29, 2002
US 6,519,636 (“Engel”)	Feb. 11, 2003	Oct. 28, 1998
US 7,797,726 (“Ashley”)	September 14, 2010	December 16, 2004
US 2010/0250918 (“Tremblay”)	September 30, 2010	March 27, 2009
US 2014/0047551 (“Nagasundaram”)	February 13, 2014	August 10, 2012
Cryptographically Enforced Access Control for User Data in Untrusted Clouds (“Wang”)	February 1, 2016	N/A
Classifying Encrypted Traffic with TLS-aware Telemetry (“McGrew”)	January 14, 2016	N/A

2. Prior Art Systems and Products

Cisco also identifies the following prior art products or systems, which invalidate the ’824 and ’249 asserted claims under 35 U.S.C. §§ 102(a), (b), and/or (g), and/or render the ’824 and ’249 asserted claims obvious under 35 U.S.C. § 103, either alone or in combination.

Prior Art	Short Name	Date of Use, Sale, Offer for Sale, or Invention
ZyXEL ZyWall/USG Series Security Firewalls	“ZyXEL”	At least by April 2005
Blue Coat SSL Visibility Appliance	“Blue Coat System”	At least by July 2013
Ghostery privacy browser extension application	“Ghostery”	At least by February 2009
AVG PrivacyFix browser extension	“PrivacyFix”	At least by September 2013
Cliqz Privacy plug-in	“Cliqz”	At least by 2015
Disconnect.me browser extension	“Disconnect”	At least by June 2007
MyPermissions Privacy Cleaner	“MyPermissions”	At least by June 2013

Prior Art	Short Name	Date of Use, Sale, Offer for Sale, or Invention
Check Point Software Technologies Ltd. Firewall Systems, including FireWall-1, VPN-1, FloodGate-1 FireWall-1, FloodGate-1, VPN-1 (Gateway, Appliance, SecuRemote, SecureClient, SecureServer), Cyber Attack Defense System, Real Secure	“Check Point Systems”	At least by October 1996
Donottrackme browser extension	“Donottrackme”	At least by March 2011
Privacy Bird browser extension	“Privacy Bird”	At least by 2007
NETGEAR VPN Firewalls, including ProSafe VPN Firewall series.	“NETGEAR VPN Firewalls”	At least by May 2002
SourceFire SSL Appliance	“SourceFire”	At least by May 2010
uBlock browser extension	“uBlock”	At least by June 2014
Juniper Prior Art Systems, including M5, M10, M20, M40, and M160 Juniper M-series routers operating with or without the JUNOS OS	“Juniper Prior Art Systems”	At least by October 2000
Cisco NetRanger Prior Art System	“NetRanger”	At least by April 1998
Cisco SAFE Nimda Attack Mitigation System	“Cisco SAFE”	At least by October 2000
CYCON Labryinth Firewall	“Labryinth Firewall”	At least by Apr. 2000
Netguard Ltd Guardian Firewall	“Guardian Firewall”	At least by October 2000
CyberGuard Corp. CyberGuard Firewall	“CyberGuard Firewall”	At least by Mar. 2000
Raptor Systems Raptor Eagle Firewall	“Raptor Eagle Firewall”	At least by Nov. 1996
Milkyway Networks SecurIT FIREWALL	“SecurIT FIREWALL”	At least by Jan. 1997

Prior Art	Short Name	Date of Use, Sale, Offer for Sale, or Invention
WatchGuard Technologies WatchGuard Firebox	“WatchGuard Firebox”	At least by Jan. 1997
AltaVista Software The Active Firewall 97	“The Active Firewall 97”	At least by Jan. 1997
Global Technology Associates Inc. GNAT Box Firewall	“GNAT Box Firewall”	At least by Apr. 2000
Network-1 Software & Technology, Inc. Firewall/Plus	“Firewall/Plus”	At least by October 2000
Trusted Information Systems, Inc. Gauntlet Firewall	“Gauntlet Firewall”	At least by Jan. 1997
Sun Microsystems, Inc. SunScreen EFS Firewall Solstice Firewall-1	“Solstice Firewall-1”	At least by October 2000
Secure Computing Corp. Borderware Firewall	“Borderware Firewall”	At least by Jan. 1997

Discovery is not yet complete and Cisco continues to investigate these and other prior art products and systems and thus may uncover additional documentation and evidence regarding their operation and functionality.² Cisco may also rely on physical samples, executable software, or source code as evidence of the relevant functionality of these prior art products and systems. Cisco will make available for inspection any additional documentation and evidence and any physical samples of products, systems, or software listed above, and/or any source code therefor, that it has in its possession or that becomes available in the future during discovery.

3. The Accused Functionality

QPrivacy’s January 7, 2025 Infringement Contentions accuse “Cisco’s products/services involved with Encrypted Traffic Analytics (ETA) technology” of infringement. Cisco denies

² Cisco has served third party subpoenas with discovery requests related to these prior art products and systems and intends to amend or supplement these Preliminary Invalidity Contentions after it receives additional information and evidence related to these prior art products and systems.

that ETA or any other Cisco products, services, or functionalities infringe any valid or enforceable claim of the Asserted Patents. Further, Cisco's Encrypted Traffic Analytics functionality pre-dates the earliest priority date of the Asserted Patents. Cisco Encrypted Traffic Analytics functionality was also in commercial use at least a year before either the effective filing date of the alleged invention in the Asserted Patents or the date on which the alleged invention in the Asserted Patents was purportedly disclosed to the public. See 35 U.S.C. § 273.

For example, Cisco publicly disclosed and presented on Encrypted Traffic Analytics functionality and showed that it was in commercial use in early 2016, including at a FloCon Conference and in Cisco blog posts. See, e.g., *Hiding in Plain Sight: Malware's Use of TLS and Encryption*, Cisco Blogs (Jan 25, 2016), available at <https://blogs.cisco.com/security/malwares-use-of-tls-and-encryption>; *Classifying Encrypted Traffic with TLS-aware Telemetry*, Cisco (2016), available at https://insights.sei.cmu.edu/documents/3988/2016_017_001_449970.pdf, see also <https://flocon2016.sched.com/event/4ex7/classifying-encrypted-traffic-with-tls-aware-telemetry?iframe=no&w=i:100;&sidebar=no&bg=no>; *Understanding Network Traffic Through Intraflow Data*, Cisco (January 2016), available at <https://web.archive.org/web/20160610180551/http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=450405>; *Enhanced Telemetry for Encrypted Threat Analytics*, McGrew (November 2016).

Cisco has numerous other publications related to Encrypted Traffic Analytics functionality at least as early as 2016. See, e.g., *Identifying Encrypted Malware Traffic with Contextual Flow Data*, Anderson, McGrew (Oct. 28, 2016); *Automated Identification and Reverse Engineering of Malware*, Anderson (Oct. 20, 2016); *Classifying Encrypted Traffic with TLS-aware Telemetry*, McGrew (Jan. 14, 2016).

Cisco Encrypted Traffic Analysis functionality was offered and in use prior to the earliest priority date of the Asserted Patents. See, e.g., *SSL Security*, Conran (October 9, 2015), available at <https://network-insight.net/2015/10/09/ssl-security/>; *Configuring Cisco Encryption Technology* (March 26, 2008), available at

https://www.cisco.com/c/en/us/td/docs/ios/security/configuration/guide/sec_cfg_encrypt_tech.html; Cisco Cognitive Threat Analytics, Cisco (2016), *available at* <https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-a-glance-c45-736555.pdf>; *Cisco Stealthwatch with Web Security Appliance*, Cisco (2016), *available at* https://www.cisco.com/c/dam/global/en_au/assets/pdf/at-a-glance-c45-737228.pdf; Cisco Stealthwatch System Information Event Management Integration Service, Cisco (2016), *available at* https://www.cisco.com/c/dam/global/en_au/assets/pdf/at-a-glance-c45-736856.pdf; Introducing Cisco Cognitive Threat Analytics, Cisco (Fe. 28, 2014), *available at* <https://blogs.cisco.com/security/introducing-cisco-cognitive-threat-analytics>. Cisco also released its Joy software package, which “paved the way for Cisco’s Encrypted Traffic Analytics (ETA),” at least as early as 2016. *See* Cisco Joy software package, GitHub (2016), *available at* <https://github.com/cisco/joy>.

Cisco also has numerous patents and publications related to its Encrypted Traffic Analytics functionality that pre-date the earliest priority date of the Asserted Patents. Cisco identifies examples of these references in the chart below.

Reference	Date of Issue / Publication	Effective Filing Date
US Patent No. 10,305,928	May 28, 2019	May 26, 2015
US Patent No. 10,686,831	Jun 16, 2020	Nov 16, 2016
US Patent No. 10,362,373	Jul 23, 2019	Jan 7, 2016
US Patent No. 10,554,614	Feb 4, 2020	Jun 23, 2016
US Patent No. 10,375,090	Aug 6, 2019	Mar 27, 2017
US Patent No. 10,296,744	May 21, 2019	Sep 24, 2015
US Patent No. 9,237,168	Jan 12, 2016	May 17, 2012
US Patent No. 7,139,679	Nov 21, 2006	Jun 27, 2002
US Patent No. 9,288,186	Mar 15, 2016	Jun 4, 2013

Reference	Date of Issue / Publication	Effective Filing Date
US Patent No. 7,290,281	Oct 30, 2007	Jun 27, 2002
US Patent No. 8,806,572	Aug 12, 2014	May 30, 2009
US Pub No. 2014/0359277	Dec 4, 2014	Jun 4, 2013
US Pub No. 2016/0352761	Dec 1, 2016	May 26, 2015
US Pub No. 2017/0374016	Dec 28, 2017	Jun 23, 2016
US Pub No. 2018/0103056	Apr 12, 2018	Oct 6, 2016

A few weeks after QPrivacy filed suit against Cisco, Cisco put QPrivacy on notice that the Encrypted Traffic Analytics functionality that QPrivacy accuses of infringement pre-dates the earliest priority date of the Asserted Patents. *See* 2024-11-21 Rahebi Ltr to Harkins re *QPrivacy USA LLC v. Cisco Systems, Inc.*, Case No. 2:24-cv-00855-JRG (E.D. Tex). QPrivacy has since failed to provide any basis for maintaining that ETA infringes the Asserted Claims even though the Encrypted Traffic Analytics functionality pre-dates the earliest priority date of the Asserted Patents. Cisco denies that ETA or any other Cisco products, services, or functionalities infringe any valid or enforceable claim of the Asserted Patents. By maintaining that the Encrypted Traffic Analytics functionality infringes, QPrivacy is admitting that the same ETA functionality would render the Asserted Patents invalid as anticipated. *Upsher-Smith Labs., Inc. v. Pamlab, L.L.C.*, 412 F.3d 1319, 1322 (Fed. Cir. 2005) (“A century-old axiom of patent law holds that a product which would literally infringe if later in time anticipates if earlier.”) (citation omitted); accord *Peters v. Active Mfg. Co.*, 129 U.S. 530, 537 (1889) (“That which infringes, if later, would anticipate if earlier.”); *see also Vanmoor v. Wal-Mart Stores, Inc.*, 201 F.3d 1363, 1366 (Fed. Cir. 2000) (affirming invalidity of patent based on the patentee’s own infringement allegations because accused product was placed on-sale before critical date of the invention).

4. State of the Art and Admitted Prior Art

The Asserted Patents themselves acknowledge that many aspects of the alleged invention were already known in the art. The problems related to managing user data shared with external remote servers were already known, and the Asserted Patents note that solutions already existed for “the user to manage which data should be shared, with which parties, and at what time periods and/or under what circumstances such that private agreements cannot be fully enforced. *See, e.g.,* ’249 patent, 1:25-35; *see also* ’824 patent at 1:22-32. The Asserted Patents also acknowledge that “[s]ocial networking service providers usually collect user (private) data, for example user’s online habits.” *Id.*, 1:43-44. That data collection, according to the Asserted Patents, is done by “requesting to share user’s (private) information while the user’s device automatically shares the requested information.” *Id.* 46-47. The Asserted Patents explain that certain devices already exist for “blocking collection of certain private parameters, for example the location.” *Id.*, 54-55.

Accordingly, the Asserted Patents admit that a person of skill in the art would have been aware of problems associated with management of private data during communication between a remote serve and a user’s device, including those related to a remote server’s requests for user information. The Asserted Patents also admit that it was already known that a user’s device would automatically share the requested information, and that solutions already existed for determining the type and content of the data (e.g., cookie information, location information, online habits, etc.) and what to do with that private data (for example, blocking the collection of location information). All of this would have been known by at least persons of ordinary skill in the art—as well as the general public—before the Asserted Patents’ earliest priority date.

Indeed, many prior art systems were in existence well-before the priority date of the asserted patents that solves these same problems associated with management of private data during communication between a remote serve and a user’s device, including those related to a remote server’s requests for user information. For example, numerous firewall and visibility systems dating back to at least the 1990s addressed offered solutions to these problems related to

management of private data. See, e.g., ZyXEL, the Blue Coat System, the Check Point Systems, NETGEAR VPN Firewalls, SourceFire, Cisco SAFE, and Cisco NetRanger. Similarly, numerous privacy and security browser extensions for the management of private data during communication between a remote server and a user's device existed at least a decade before the priority date of the Asserted Patents. See, e.g., Ghostery, PrivacyFix, Cliqz, Disconnect, uBlock, and MyPermissions. These systems offered the same and many more solutions to the problems purportedly addressed by the Asserted Patents.

B. Identification of Anticipation and Obviousness Combinations

Pursuant to P. R. 3–3(b) and (c), Cisco provides the following exemplary charts identifying examples of prior art and prior art combinations that anticipate and/or render obvious each of the asserted claims of the Asserted Patents. Cisco's investigation, analysis, and review of these references is ongoing. Cisco will provide updated claim charts as necessary and as they are available.

Exhibit	Invalidity Chart Reference(s)
1	Vandervort
2	Mahkonen
3	Prehofer
4	Kruse
5	Wang
6	Burns
7	Yang
8	Blue Coat System
9	ZyXel
10	Ghostery
11	PrivacyFix

Exhibit	Invalidity Chart Reference(s)
12	Check Point Systems

In the Exhibits attached hereto, where Cisco cites to a particular figure in a prior art reference, the citation should be understood to encompass the caption and description of the figure and any text relating to the figure in addition to the figure itself. Conversely, where a cited portion of text refers to a figure, the citation should be understood to include the figure as well. Additional evidence regarding the features and elements of the prior art reference may be provided by witness testimony, or by additional documents that describe the prior art reference that are discovered through the course of ongoing discovery.

To the extent any of the prior art references in the attached exhibits are deemed not to disclose one or more limitations of the asserted claims, each of the prior art references in the attached exhibits can be used in combination with any one or more of the references identified in these contentions, including those disclosed in the attached exhibits, to render the asserted claims invalid under 35 U.S.C. §103. For example, Cisco identifies the following non-exhaustive combinations that render the Asserted Claims obvious under 35 U.S.C. § 103:

- Vandervort alone or in combination with at least one of Mahkonen, Prehofer, Kruse, Wang, Burns, Yang, Blue Coat System, ZyXEL, Ghostery, PrivacyFix, Check Point Systems, and/or the admitted prior art;
- Mahkonen alone or in combination with at least one of Vandervort, Prehofer, Kruse, Wang, Burns, Yang, Blue Coat System, ZyXEL, Ghostery, PrivacyFix, Check Point Systems, and/or the admitted prior art;
- Prehofer alone or in combination with at least one of Mahkonen, Vandervort, Kruse, Wang, Burns, Yang, Blue Coat System, ZyXEL, Ghostery, PrivacyFix, Check Point Systems, and/or the admitted prior art;

- Kruse alone or in combination with at least one of Mahkonen, Prehofer, Vandervort, Wang, Burns, Yang, Blue Coat System, ZyXEL, Ghostery, PrivacyFix, Check Point Systems, and/or the admitted prior art;
- Wang alone or in combination with at least one of Mahkonen, Prehofer, Kruse, Vandervort, Burns, Yang, Blue Coat System, ZyXEL, Ghostery, PrivacyFix, Check Point Systems, and/or the admitted prior art;
- Burns alone or in combination with at least one of Mahkonen, Prehofer, Kruse, Wang, Vandervort, Yang, Blue Coat System, ZyXEL, Ghostery, PrivacyFix, Check Point Systems, and/or the admitted prior art;
- Yang alone or in combination with at least one of Mahkonen, Prehofer, Kruse, Wang, Burns, Vandervort, Blue Coat System, ZyXEL, Ghostery, PrivacyFix, Check Point Systems, and/or the admitted prior art;
- Blue Coat System alone or in combination with at least one of Mahkonen, Prehofer, Kruse, Wang, Burns, Yang, Vandervort, ZyXEL, Ghostery, PrivacyFix, Check Point Systems, and/or the admitted prior art;
- ZyXEL alone or in combination with at least one of Mahkonen, Prehofer, Kruse, Wang, Burns, Yang, Blue Coat System, Vandervort, Ghostery, PrivacyFix, Check Point Systems, and/or the admitted prior art;
- Ghostery alone or in combination with at least one of Mahkonen, Prehofer, Kruse, Wang, Burns, Yang, Blue Coat System, ZyXEL, Vandervort, PrivacyFix, Check Point Systems, and/or the admitted prior art;
- PrivacyFix alone or in combination with at least one of Mahkonen, Prehofer, Kruse, Wang, Burns, Yang, Blue Coat System, ZyXEL, Ghostery, Vandervort, Check Point Systems, and/or the admitted prior art;
- Check Point Systems alone or in combination with at least one of Mahkonen, Prehofer, Kruse, Wang, Burns, Yang, Blue Coat System, ZyXEL, Ghostery, PrivacyFix, Vandervort, and/or the admitted prior art; and

These obviousness combinations are provided in the alternative to Cisco's anticipation and single-reference obviousness contentions and are not to be construed to suggest that any reference included in the combination is not itself anticipatory or would not render the Asserted Claims obvious in light of the knowledge of a person having ordinary skill in the art. Cisco also hereby incorporates by reference the prior art, invalidity grounds, and expert testimony submitted in connection with any related proceedings related to the Asserted Patents, including any future *ex parte* reexamination proceedings involving the Asserted Patents or related patents, or any post grant proceedings (e.g., *inter partes* review) involving the Asserted Patents or related patents.

1. Motivations to Combine, Reasonable Expectation of Success, and Obviousness

The ultimate determination of whether an invention is or is not obvious is a legal conclusion based on underlying factual inquiries including “(1) the scope and content of the prior art; (2) the level of ordinary skill in the art; (3) the differences between the claimed invention and the prior art; and (4) objective evidence of nonobviousness.” *Miles Labs., Inc. v. Shandon, Inc.*, 997 F.2d 870, 877 (Fed. Cir. 1993); *see also Graham v. John Deere Co. of Kan. City*, 383 U.S. 1, 17–18 (1966). The U.S. Supreme Court's decision in *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415–16 (2007), reaffirmed *Graham* and further held that a claimed invention can be obvious even if there is no teaching, suggestion, or motivation for combining the prior art to produce that invention. In summary, *KSR* holds that patents based on new combinations of elements or components already known in a technical field may be found to be obvious. *See generally KSR*, 550 U.S. 398. Specifically, the Court in *KSR* rejected a rigid application of the “teaching, suggestion, or motivation [to combine]” test. *Id.* at 418–19. “In determining whether the subject matter of a patent claim is obvious, neither the particular motivation or the avowed purpose of the patentee controls. What matters is the objective reach of the claim.” *Id.* at 419. “Under the correct analysis, any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.” *Id.* at 420. In particular, in *KSR*, the Supreme Court emphasized the principle that “[t]he

combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.” Id. at 416. A key inquiry is whether the “improvement is more than the predictable use of prior art elements according to their established functions.” Id. at 417.

Cisco generally contends that the Asserted Claims of the Asserted Patents would have been obvious because they, at most, only slightly modify a known solution to a common issue at the time or merely arrange old elements, with each performing the same function that had previously been known, to perform and yield no more than what one of ordinary skill would expect from such an arrangement. The Asserted Patents claim many generic elements of methods and/or systems for management of private and encrypted data. For example, as discussed above, the Asserted Patents admit that problems related to remote servers requesting a user’s private information was already known, and that methods already existed to determine whether to share that private data with the remote server based on a determination of the type and content of the data (e.g., cookie information, location information, online habits, etc.). It would have been obvious to, in order to maintain the privacy of the user’s data, determine the data type and content *without reading or decrypting* the content of underlying data, then determining, based on a comparison of the determined content, whether to share, modify, or block the data. It would also have been obvious to determine the data type and content *in real time* in order to maintain communication with the remote server.

All of the Asserted Claims of the Asserted Patents are also obvious based on one or more combinations of the prior art references above. The accompanying claim charts explain how different portions of each prior art reference discloses each limitation of the Asserted Claims. To the extent QPrivacy argues that any particular prior art reference lacks any feature, a person of ordinary skill in the art as of the Asserted Patents’ priority date would at a minimum have been motivated to modify the reference to include the allegedly missing feature(s), or to combine it with other references that include that feature. Cisco also hereby incorporates by reference any motivations to combine discussed in any related proceedings related to the Asserted Patents,

including any future *ex parte* reexamination proceedings involving the Asserted Patents or related patents, or any post grant proceedings (e.g., *inter partes* review) involving the Asserted Patents or related patents.

One of ordinary skill in the art, at the time of the purported inventions of the Asserted Claims, would have been motivated to combine the teachings of these references and would have had a reasonable expectation of success, as set forth in the combinations above, because these references relate to common objectives and subject matter, and for at least the reasons set forth herein, in the attached claim charts, in the prior art references themselves, and based on the knowledge of one of ordinary skill in the art. The references share commonalities in terms of their general subject matter as well as the types of equipment and/or approaches used. Further, some of the prior art references explicitly or implicitly reference each other, share common authors or inventors, and/or were developed at common companies, schools, or organizations, which would have motivated one of skill in the art to combine them. For example, these references are directed to the fields of network security, management of private or encrypted data during communication, and data privacy generally. These references also identify and address many of the same technical issues (*e.g.*, requests by a remote server to collect private or encrypted data and management of that data without decryption or reading the content) and suggest similar solutions to those issues (*e.g.*, determining content or data type based on header information or characteristics of the data packets; maintaining a list of preferences; sharing, modifying, or blocking communications based on those preferences). Moreover, all the references disclose determining content, data type, or data pattern, receiving or storing preferences, determining whether to block, forward, or modify data packets, blocking, forwarding, and modifying data packets, and maintaining communication with a remote server.

For example, from a motivation to combine perspective, one of ordinary skill in the art would have recognized that firewall and network visibility systems and browser-based privacy or security extensions serve overlapping and complementary functions in the domain of data protection. For example, firewalls traditionally operate at the network or system level to

monitor, filter, or block data packets based on security rules, while browser extensions offer more granular, user-facing privacy controls at the application level—such as blocking trackers, managing cookies, or obfuscating identifiers. In light of the shared goal of safeguarding user private and encrypted data and regulating information flows, it would have been natural for a person of ordinary skill to combine the packet inspection mechanisms of firewalls with the real-time control mechanisms provided by browser extensions. This combination would offer enhanced protection by leveraging multiple layers of visibility—both at the network perimeter and within the user’s browser environment—resulting in a more holistic approach to privacy enforcement. Additionally, industry trends have shown a convergence of endpoint and network security, with enterprise solutions increasingly offering threat intelligence feeds, traffic fingerprinting, and behavioral analytics, all of which span both browser-level and network-level insights, provides further incentive for integration.

A person of ordinary skill in the art would have also had a reasonable expectation of success in combining these technologies because they both operate within well-understood architectures and use interoperable data structures, such as HTTP headers, IP packets, and browser APIs. Developers and security professionals have long integrated multi-layered security tools—like intrusion detection systems with endpoint agents or VPN clients with browser plugins—demonstrating industry precedent for such combinations. Given the modular and flexible nature of browser extensions, and the evolving programmability of modern firewall and visibility platforms, a skilled artisan would have expected that combining elements of both would not only be feasible but also yield predictable improvements in security coverage without requiring undue experimentation. For example, browser APIs readily expose metadata that can be analyzed in conjunction with firewall data, enabling a straightforward technical path toward synthesizing these systems. The open-source nature of many browser extension frameworks and visibility tools would have also lowered implementation barriers, allowing for rapid prototyping and integration. In addition, many security platforms have begun to offer SDKs for third-party

extensions, making interoperability between endpoint (browser) and network layers both anticipated and technically achievable.

A person of ordinary skill in the art would have been motivated to make the foregoing combinations to provide management of private or encrypted data without decryption or reading the content of the data and to ensure real time communication with a remote server. Further, the prior art references explicitly or implicitly reference other prior art references, are within the field of the asserted patents and are directed to similar subject matter within the field. Additionally, the references, and any products, devices, or processes described in the references, existed and/or were invented in the same time period providing further motivation for combination.

For instance, a person of ordinary skill in the art would have found it obvious, been motivated to combine, and would have had a reasonable expectation of success in combining the teachings of either Kruse or Prehofer and either the Blue Coat System or Check Point Systems because, for example, analyzing “one or more portions, subsets, or fields of data that are sensitive . . . and thus should be obfuscated before being provided in response to the request” (Kruse at 9:33-44) or analyzing “context information” that is “obfuscated . . . based on a privacy policy associated with [a] user” (Prehofer, 4:33-56) would have motivated a person of ordinary skill in the art to look to either the Blue Coat System or Check Point Systems for additional disclosure of a list of preferences as part of determining to obfuscate (modify) data. Specifically, the Blue Coat System explicitly discloses storing policy enforcement lists (*see* Blue Coat System’s disclosure of “policy enforcement” lists and “establish[ing] and implement[ing] whitelist (allow) and blacklist (reject) policies by providing a host categorization list”) and Check Point Systems disclose maintaining similar security and privacy policies and rules (*see* Check Point Systems’ disclosure of “Define and implement security policies that are applied to the network and Users” and “rules govern the communications flowing into and out of the module . . . [providing] a means to control the types of traffic permitted to flow through the module”). Moreover, all references “are directed to the same field and address the same set of

problems” related to management of private data, network security, and traffic management. *Tech Pharm. Servs., LLC v. Alixa Rx LLC*, No. 4:15-cv-766, 2017 WL 3318247, at *3 (E.D. Tex. Aug. 3, 2017). This aligns with the *KSR* rationale of combining prior art elements according to known methods to yield predictable results. The Graham factors also support such combination: the scope and content of the prior art all relate to these same fields; the differences between the prior art and the claimed invention are minimal for this specific element; and the level of ordinary skill in the art would likely find the combination obvious. A person of ordinary skill in the art would have had a reasonable expectation of success for such combination for the same reasons discussed above.

Similarly, a person of ordinary skill in the art would have found it obvious, been motivated to combine, and would have had a reasonable expectation of success in combining the teachings of Burns and Yang (incorporated by Burns by reference) with either the Blue Coat System, Check Point Systems, or ZyXEL for these reasons. Burns and Yang, like the Blue Coat System, Check Point Systems, and ZyXEL, are related to the same field of dynamic management of network communications and are directed to addressing the same problems related to controlling the transmission of a user’s private data. *See, e.g.*, Burns at 2:47-59 (describing techniques “for discovering and preventing network access or network utilization by software applications that employ encrypted communication” and “identifyi[ing] the application in use for the communication session or . . . determine[ing] whether the communication session is following a known network protocol”; *see also* Yang at 1:6-42. Burns’ intrusion detection system that “attempts to identify applications and protocols for each communication session.” Burns, 4:36-39. Burns specifically refers to Yang’s “techniques for identifying specific applications and protocols.” Burns, 4:39-40. A person of ordinary skill in the art would have found the Blue Coat System’s “policies that detect SSL communications with reputable consumer websites” and methods of detecting “approved SSL traffic” instructive for additional methods of identifying such applications and protocols for each communication session. A person of ordinary skill in the art would also have found the ZyXEL’s Intrusion Detection and

Prevention Packet Inspection disclosures—including its disclosures related to “encrypted traffic inspection” for “detect[ing] malicious or suspicious packets and respond[ing] instantaneously” instructive, as it discloses additional techniques for identifying specific applications, protocols, data types, and content of encrypted data and responding “instantaneously.” A person of ordinary skill in the art would have found it obvious and been motivated to combine the teachings of the identified references and systems in the combinations claimed in the Asserted Patents because of the shared desire and incentives in the marketplace discussed above for intrusion detection and prevention, including for performing such detection and prevention on encrypted data and doing so instantaneously. A person of ordinary skill in the art would have had a reasonable expectation of success for such combination for the same reasons discussed above.

As another example, a person of ordinary skill in the art would have found it obvious, been motivated to combine, and would have had a reasonable expectation of success in combining the teachings of Burns with Yang. A person of ordinary skill in the art would have combined Burns and Yang because Burns refers to and incorporates Yang by reference. Burns, 4:39-45. Burns therefore encourages the combination of its disclosure with Yang and states that Yang provides “exemplary techniques for identifying specific applications and protocols.” Burns, 4:39-45. Burns describes an intrusion detection system that is responsible for “monitor[ing] traffic into and out of an enterprise network.” Burns, 2:52-54. Yang’s disclosure is directed to “techniques for detecting and preventing network attacks ... network viruses or other malicious activity.” Yang, 1:45-49. Yang adds implementation details to Burns’ system. For example, implementing Burns by itself would result in an intrusion detection system that can identify a threat, but does not have capability alone to address it. A person of ordinary skill in the art would have seen this to be a shortcoming and would have looked to a reference like Yang to provide Burns’ system with the functionality to respond to a threat, not just identify it. To ensure that an intrusion detection system would detect and prevent attacks or other malicious

activity, it would have been obvious to incorporate the disclosure of Yang into the disclosure of Burns.

As another example a person of ordinary skill in the art would have found it obvious, been motivated to combine, and would have had a reasonable expectation of success in combining the teachings of Burns and/or Yang with ZyXEL, Blue Coat System, or Check Point Systems. Burns and Yang both disclose an intrusion detection system receiving packets from a firewall. Burns, Fig. 1, 5:1-53; Yang, Fig. 1, 4:27-45. Burns further discloses receiving encrypted packets from a firewall. Burns, Fig. 1, 5:1-53. However, neither Burns nor Yang discloses a specific firewall for communicating decrypted and encrypted packets to an intrusion detection system. A person of ordinary skill in the art would have looked to ZyXEL, Blue Coat System, or Check Point Systems for adding a specific firewall to Burns and Yang's networks. ZyXEL can handle both decrypted and encrypted packets securely, consistent with Burns and Yang's goals. ZyXEL User's Guide, 504, 509. ZyXEL comprises a firewall and an intrusion detection system for an enterprise network. ZyXEL User's Guide, 20-21. Blue Coat System dynamically manages private and encrypted data between network devices according to policies. Managing Encrypted Traffic with Blue Coat Solutions. Check Point Systems inspect encrypted packets using security policies. VPN-1 Firewall-1 Reference Guide, 68; VPN-1 User Guide, 245, 246, 314-358. Similarly, Burns and Yang both disclose an enterprise network comprising a firewall and an intrusion detection system. Burns, Fig. 1, 4:20-45; Yang, Fig. 1, 4:13-45. Burns, Yang, ZyXEL, Blue Coat System, and Check Point Systems are all directed to network security devices for defending against network attacks. Burns, Abstract; Yang, Abstract; ZyXEL User's Guide, 339; Managing Encrypted Traffic With Blue Coat Solutions; VPN-1 User Guide, 314-358. It would have been obvious to incorporate ZyXEL's firewall into Burns and Yang's networks to communicate packets to Burns and Yang's intrusion detection systems. A person of ordinary skill in the art would have had a reasonable expectation of success for such combination for the same reasons discussed above.

As another example, a person of ordinary skill in the art would have found it obvious, been motivated to combine, and would have had a reasonable expectation of success in combining the teachings of ZyXEL, Blue Coat System, or Check Point Systems with Mahkonen. ZyXEL meets legal and privacy requirements by not inspecting a user's encrypted session. ZyXEL User's Guide, 509. Blue Coat System bypasses decryption to maintain user privacy. Encrypted Traffic Management for Dummies, Blue Coat, Special Edition, 16. Check Point Systems allow traffic matching certain rules to pass without decryption. VPN-1 User Guide, 161, 378, 388. A person of ordinary skill in the art would have recognized that without inspecting the session, a device may not efficiently manage the session's traffic, degrading performance. To address this drawback while meeting the legal and privacy requirements, a person of ordinary skill in the art would have consulted Mahkonen, which teaches classifying encrypted traffic more accurately and securely without decrypting. Mahkonen, [0039]-[0040]. Thus, ZyXEL, Blue Coat System, Check Point Systems, and Mahkonen are concerned with handling encrypted traffic securely. ZyXEL User's Guide, 509; Encrypted Traffic Management for Dummies, Blue Coat, Special Edition, 16; VPN-1 User Guide, 297, 610; Mahkonen, [0039]-[0040]. Mahkonen's encrypted traffic classification is performed by a networking device connected to the internet and managing internet communications for a user device. Mahkonen, Fig. 1, [0047]-[0048]. ZyXEL, Blue Coat System, and Check Point Systems are also networking devices connected to the internet and managing internet communications for a user device. ZyXEL User's Guide, 20-23; Blue Coat SSL Visibility Appliances Datasheet; VPN-1 FIPS 140-1 Non-Proprietary Security Policy, Fig. 1. To meet the legal and privacy requirements and effectively manage encrypted traffic, it would have been obvious to combine ZyXEL, Blue Coat System, or Check Point Systems with Mahkonen. A person of ordinary skill in the art would have had a reasonable expectation of success for such combination for the same reasons discussed above.

As another example, a person of ordinary skill in the art would have found it obvious, been motivated to combine, and would have had a reasonable expectation of success in

combining the teachings of Vandervort with ZyXEL, Blue Coat System, or Check Point Systems, for example, to add encryption. Vandervort is directed to masking and encoding private information in documents, preventing sensitive data from being identified. Vandervort, Abstract, [0028]. Vandervort is silent on encrypting the private information. A person of ordinary skill in the art would have recognized the benefits of encryption to further protect the sensitive data. Thus, a person of ordinary skill in the art would have reviewed encryption schemes, such as ones disclosed by ZyXEL, Blue Coat System, or Check Point Systems, to encrypt the sensitive data and provide further protection. ZyXEL User's Guide, 65, 75; Encrypted Traffic Management For Dummies, Blue Coat, Special Edition, 3-6; VPN-1 User Guide, 245, 246. ZyXEL, Blue Coat System, and Check Point Systems disclose example networks similar to Vandervort's network. ZyXEL User's Guide, 20-23; Blue Coat SSL Visibility Appliances Datasheet; VPN-1 FIPS 140-1 Non-Proprietary Security Policy, Fig. 1; Vandervort, Figs. 1, 2. It would have been obvious to add ZyXEL, Blue Coat System, or Check Point Systems into Vandervort's network to provide encryption and better secure Vandervort's private data.

As another example a person of ordinary skill in the art would have found it obvious, been motivated to combine, and would have had a reasonable expectation of success in combining the teachings of Ghostery or PrivacyFix with a networking device such as the Blue Coat System, Check Point Systems, or ZyXEL. A person of ordinary skill in the art would have understood that Ghostery and PrivacyFix only protect one user device from sharing private data to web servers. Thus, to improve efficiency, a person of ordinary skill in the art would have been motivated to protect more user devices, without installing the software on each device. Therefore, a person of ordinary skill in the art would have looked for a device that manages webpage communications for a plurality of user devices, where Ghostery and PrivacyFix's tracker blocking features can protect more user devices at one time. The Blue Coat System, Check Point Systems, and ZyXEL are examples of such devices. *See, e.g.*, Blue Coat System (providing "threat analysis," stressing importance of maintaining "user privacy," and noting that

“administrators can configure policies that block SSL traffic that doesn’t adhere to the company’s policies regarding minimum key length and approved cipher suites.”); VPN-1 FIPS 140-1 Non-Proprietary Security Policy, Fig. 1; ZyXEL User’s Guide, 20-23. A person of ordinary skill in the art would have understood that the Blue Coat System, Check Point Systems, or ZyXEL, as modified by Ghostery or PrivacyFix, would block requests for user private data the same way. It would have been obvious to incorporate Ghostery or PrivacyFix into the Blue Coat System, Check Point Systems, or ZyXEL to protect more user devices from sharing private data to web servers. A person of ordinary skill in the art would have had a reasonable expectation of success for such combination for the same reasons discussed above.

As another example, a person of ordinary skill in the art would have found it obvious, been motivated to combine, and would have had a reasonable expectation of success in combining the teachings of Ghostery or PrivacyFix with a networking device disclosed in Vandervort, Mahkonen, Burns, or Yang. A person of ordinary skill in the art would have understood that Ghostery and PrivacyFix only protect one user device from sharing private data to web servers. Thus, to improve efficiency, a person of ordinary skill in the art would have been motivated to protect more user devices, without installing the software on each device. Therefore, a person of ordinary skill in the art would have looked for a device that manages webpage communications for a plurality of user devices, where Ghostery and PrivacyFix’s tracker blocking features can protect more user devices at one time. Vandervort, Mahkonen, Burns, and Yang disclose examples of such devices. *See, e.g.*, Vandervort, Fig. 1, [0030]; Mahkonen, Fig. 1, [0045]-[0048], Burns, Fig. 1, 4:20-45; Yang, Fig. 1, 4:12-58. A person of ordinary skill in the art would have understood that the Vandervort, Mahkonen, Burns, or Yang, as modified by Ghostery or PrivacyFix, would block requests for user private data the same way. It would have been obvious to incorporate Ghostery or PrivacyFix into Vandervort, Mahkonen, Burns, or Yang’s networking device to protect more user devices from sharing private data to web servers. A person of ordinary skill in the art would have had a reasonable expectation of success for such combination for the same reasons discussed above.

As another example, a person of ordinary skill in the art would have found it obvious, been motivated to combine, and would have had a reasonable expectation of success in combining the teachings of Burns and/or Yang with Mahkonen. Burns and Yang are directed to

managing encrypted and private communication sessions. Burns, Abstract; Yang, 4:12-58. A person of ordinary skill in the art would have recognized that without inspecting the session, a device may not efficiently manage the session's traffic, degrading performance. To address this drawback while meeting the security and privacy requirements, a person of ordinary skill in the art would have consulted Mahkonen, which teaches classifying encrypted traffic more accurately and securely without decrypting. Mahkonen, [0039]-[0040]. Thus, Burns, Yang, and Mahkonen are concerned with handling encrypted and private traffic securely. Burns, Abstract; Yang, 1:46-65; Mahkonen, [0039]-[0040]. Mahkonen's encrypted traffic classification is performed by a networking device connected to the internet and managing internet communications for a user device. Mahkonen, Fig. 1, [0047]-[0048]. Burns and Yang also disclose networking devices connected to the internet and managing internet communications for a user device. Burns, Fig. 1, 4:20-45; Yang, Fig. 1, 4:12-58. To meet the security and privacy requirements and effectively manage traffic comprising sensitive data, it would have been obvious to combine Burns and/or Yang with Mahkonen. A person of ordinary skill in the art would have had a reasonable expectation of success for such combination for the same reasons discussed above.

As another example, a person of ordinary skill in the art would have found it obvious, been motivated to combine, and would have had a reasonable expectation of success in combining the teachings of Vandervort with Burns or Yang. Vandervort is directed to storing private information in documents and keys for decoding the private information. Vandervort, [0028]. Vandervort is silent on securing the private information and the keys. A person of ordinary skill in the art would have recognized that Vandervort's private information and key storage would be vulnerable to attacks. Thus, a person of ordinary skill in the art would have reviewed network security systems, such as an intrusion detection system (IDS) disclosed by Burns or Yang, to protect the sensitive data. Burns, Abstract, 4:20-45; Yang, 1:46-65. Burns and Yang disclose example networks similar to Vandervort's network. Burns, Fig. 1, 4:20-45; Yang, Fig. 1, 4:12-58; Vandervort, Figs. 1, 2. It would have been obvious to add Burns or Yang's IDS into Vandervort's network to better secure Vandervort's private data.

V. GROUNDS OF INVALIDITY OTHER THAN ANTICIPATION OR OBVIOUSNESS

The Asserted Claims are also invalid for failure to meet one or more of the requirements of 35 U.S.C. § 112.

Cisco reserves the right to amend, supplement, and/or otherwise modify these Preliminary Invalidity Contentions with respect to grounds of invalidity other than anticipation or obviousness. Due in part to QPrivacy's failure to sufficiently identify (a) the full scope of the accused instrumentalities and (b) where QPrivacy contends that each element of the Asserted Claims is found within each instrumentality, Cisco lacks a complete understanding of QPrivacy's alleged infringement and/or claim construction positions. If and when QPrivacy develops an infringement and/or claim construction theory that implicates infringement by Cisco, Cisco reserves the right to argue that the specification does not enable and/or provide a written description for such an interpretation or that such an interpretation renders the claim indefinite. The Court has not yet construed any terms, phrases, or clauses of the Asserted Claims, and QPrivacy has not yet provided any validity contentions in response to Cisco's Preliminary Invalidity Contentions. In particular, QPrivacy has not identified any way in which it disputes that the Asserted Claims are invalid under 35 U.S.C. § 112. Moreover, Cisco's discovery and investigation in connection with this lawsuit is ongoing, and these grounds are based on information obtained to date. Accordingly, Cisco reserves the right to amend, supplement, and/or otherwise modify these Preliminary Invalidity Contentions. Cisco further reserves the right to rely on expert reports or testimony and any third-party discovery.

Cisco lists below exemplary grounds upon which Cisco presently contends the Asserted Claims of the Asserted Patents are invalid for failure to meet one or more of the requirements of 35 U.S.C. § 112. Cisco identifies at least the following grounds of invalidity based on inadequate written description under 35 U.S.C. § 112(a), lack of enablement under 35 U.S.C. § 112(a), and indefiniteness under 35 U.S.C. § 112(b) for the Asserted Claims. These grounds are identified based on knowledge currently in Cisco's possession. A more detailed basis for Cisco's written description, enablement, and/or indefiniteness defenses will be set forth in Cisco's claim construction briefs and expert reports on invalidity, to be served in accordance with the Docket Control Order. Further investigation may uncover additional grounds for invalidity, and Cisco reserves the right to supplement these disclosures to include all additional

grounds.

A. Lack of Written Description and Lack of Enablement Under 35 U.S.C. § 112

Pursuant to 35 U.S.C. § 112(a), a patent specification:

shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make, and use the same[.]

The Federal Circuit has held that this language creates two closely related, yet separate requirements for a specification: (i) a written description of the invention (“written description”) and (ii) a written description of the manner and process of making and using the invention (“enablement”). *See Ariad Pharm., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1344 (Fed. Cir. 2010) (*en banc*).

To satisfy the written description requirement, the description must “clearly allow persons of ordinary skill in the art to recognize that [the inventor] invented what is claimed.” *Ariad Pharm., Inc. v. Eli Lilly and Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (internal citation omitted). The test for sufficiency is whether the disclosure of the application relied upon reasonably conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date. *Id.*

The test requires an objective inquiry into the four corners of the specification from the perspective of a person of ordinary skill in the art. Based on that inquiry, the specification must describe an invention understandable to that skilled artisan and show that the inventor actually invented the invention claimed. “Whether the written description requirement is satisfied is a fact-based inquiry that will depend on the nature of the claimed invention, and the knowledge of one skilled in the art at the time an invention is made and a patent application is filed.” *Carnegie Mellon Univ. v. Hoffmann La Roche Inc.*, 541 F.3d 1115, 1122 (Fed. Cir. 2008) (internal citation omitted). Actual “possession” or reduction to practice outside of the specification is not enough. Instead, the specification itself must demonstrate possession.

While the written description requirement does not demand any particular form of disclosure, a description that merely renders the invention obvious does not satisfy the requirement. *Lockwood v. Am. Airlines*, 107 F.3d 1565, 1571-72 (Fed. Cir. 1997).

To satisfy the enablement requirement of 35 U.S.C § 112, the disclosure “must teach those skilled in the art how to make and use the full scope of the claimed invention without ‘undue experimentation.’” *Genentech, Inc. v. Novo Nordisk, A/S*, 108 F.3d 1361, 1365 (Fed. Cir. 1997) (citations omitted). Moreover, “[i]t is the specification, not the knowledge of one skilled in the art, that must supply the novel aspects of [the] invention in order to constitute adequate enablement.” *Id.* at 1366. The Federal Circuit has enumerated several factors to consider in determining whether a disclosure would require “undue experimentation”: “(1) the quantity of experimentation necessary, (2) the amount of direction or guidance presented, (3) the presence or absence of working examples, (4) the nature of the invention, (5) the state of the prior art, (6) the relative skill of those in the art, (7) the predictability or unpredictability of the art, and (8) the breadth of the claims.” *In re Wands*, 858 F.2d 731, 737 (Fed. Cir. 1988).

Cisco provides below an exemplary list of claim elements for which there is inadequate written description and/or lack of enablement under U.S.C. § 112(a). For example, certain claim limitations fail to describe an invention understandable to a skilled artisan at the time of the invention and/or fail to show that the inventor actually possessed the invention claimed. *See Ariad*, 598 F.3d at 1351. As a further example, certain claims are invalid because the specification fails to teach those skilled in the art at the time of the alleged invention how to make and use the full scope of the claimed invention without undue experimentation. *See ALZA Corp. v. Andrx Pharms., LLC*, 603 F.3d 935, 940 (Fed. Cir. 2010). As an additional example, certain claim limitations encompass any and all structures or acts for performing a recited function, including those beyond what their applicant(s) invented, such that the specification fails to provide a scope of enablement commensurate with the scope of the claim as asserted. *See Halliburton Oil Well Cementing Co. v. Walker*, 329 U.S. 1, 12–13 (1946). As yet another example, certain claims are invalid for failing to enable the full scope of the invention as defined

by the claims. *See Amgen Inc. v. Sanofi*, 143 S. Ct. 1243, 1254 (2023) (“If a patent claims an entire class of processes, machines, manufactures, or compositions of matter, the patent’s specification must enable a person skilled in the art to make and use the entire class.”).

In addition, and without limitation, the Asserted Claims taken as a whole (rather than only as the sum of its individual limitations) are invalid for lack of written description and enablement. *See, e.g., Novozymes A/S v. DuPont Nutrition Biosciences APS*, 723 F.3d 1336, 1346–51 (Fed. Cir. 2013). As described below, by way of example, a person of ordinary skill in the art at the time of the alleged invention would not understand that the named inventors of the ’958 patent were in possession of the claimed subject matter as of the effective filing date, nor would the patent’s disclosure have enabled one skilled in the art at the time of the alleged invention to practice the Asserted Claims without undue experimentation.

Any deficiencies that render claims invalid for written description and/or enablement under 35 U.S.C. § 112 also infect and thereby invalidate any and all claims depending therefrom.

In addition to the claim as a whole, at least the following claim elements, or portions thereof, of the claims in the Asserted Patents are not supported by the written description and/or are not enabled under 35 U.S.C. § 112(a):

- **’824 patent:**

- Claims 1 and 9 of the ’824 patent and any claims dependent therefrom are invalid for failure to satisfy the requirements of 35 U.S.C. § 112 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “the user’s device is configured to provide a response corresponding to the received request.” The specification discloses a method wherein the user’s device receives a “request for retrieval of at least one data packet from the user’s device” and the user’s device “is configured to provide a response corresponding to the received request” without any further definition or explanation as to how one would configure the user’s device without undue experimentation. ’824 patent at 2:3–19, 2:54–3:13. Accordingly, the specification fails to reasonably convey to one of ordinary skill in the art that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claims 1 and 9 of the ’824 patent and any claims dependent therefrom are invalid for failure to satisfy the requirements of 35 U.S.C. § 112 because

the specification as filed does not contain an adequate written description and/or enabling disclosure of “determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request” and “determining, by the remote server, at least one communication data pattern corresponding to the received request.” The specification acknowledges that terms like “determining” may “refer to operation(s) and/or process(es) of a computer, a computing platform, a computing system, or other electronic computing that manipulates and/or transforms data represented as physical (e.g., electronic) quantities within the computer’s registers and/or memories into other data similarly represented as physical quantities within the computer’s registers and/or memories or other information non-transitory storage medium that may store instructions to perform operations and/or processes.” ’824 patent at 5:23–35. But the ’824 patent does not disclose anywhere what those operations or processes are, let alone how they would work. Accordingly, the specification fails to reasonably convey to one of ordinary skill in the art that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- o Claims 1, 9, and 17 of the ’824 patent and any claims dependent therefrom are invalid for failure to satisfy the requirements of 35 U.S.C. § 112 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “wherein the content of the at least one data packet is not read by the remote server for continued operation by the user’s device in real time.” The specification acknowledges that the remote server or data management system may determine the data type of at least one data packet without “read[ing] the actual content of the data packets.” ’824 patent at 12:38–48. *See also id.* at 13:11–15. But as discussed above, the patent does not disclose how a remote server would determine the data type or data pattern of a data packet, let alone how a remote server would determine such information without reading the actual content of the packets. Accordingly, the specification fails to reasonably convey to one of ordinary skill in the art that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- o Claims 1, 9, and 18 of the ’824 patent and any claims dependent therefrom are invalid for failure to satisfy the requirements of 35 U.S.C. § 112 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference.” The specification conclusorily discloses “modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference,” ’824 patent at 2:15–19, 2:25–18, 3:9–11, 3:19–22, 4:20–23. The

specification also states that the modification may be done by a “predetermined algorithm” or a “modification algorithm.” ’824 patent at 8:39-41, 12:8-10. But the patent does not disclose how one of ordinary skill would know what algorithm to use. Accordingly, the specification fails to reasonably convey to one of ordinary skill in the art that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- o Claim 6 of the ’824 patent and any claims dependent therefrom are invalid for failure to satisfy the requirements of 35 U.S.C. § 112 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “linking at least one response from the user's device to a type of data packet from the user's device.” The specification does not disclose any process or method of “linking” the response from the user’s device to a “type of data packet from the user’s device, wherein the linking is based on the communication data type and communication data pattern of the at least one response.” Accordingly, the specification fails to reasonably convey to one of ordinary skill in the art that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- o Claim 18 of the ’824 patent and any claims dependent therefrom are invalid for failure to satisfy the requirements of 35 U.S.C. § 112 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “wherein the processor is configured to modify data packets corresponding to requests for retrieval of data packets and communication data types that are not compatible with communication data patterns from a communication data pattern database.” The specification notes that “[i]n some embodiments, the system further includes a data pattern database, coupled to the processor, wherein the processor is configured to modify data packets corresponding to requests for retrieval of data packets and data types that are not compatible with data patterns from a data pattern database.” ’824 patent at 4:20-23. The specification, however, does not disclose what specific configurations are made to enable the processor to modify the data packets. Accordingly, the specification fails to reasonably convey to one of ordinary skill in the art that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- o Claim 17 of the ’824 patent and any claims dependent therefrom are invalid for failure to satisfy the requirements of 35 U.S.C. § 112 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “a processor, coupled to a response database and to the privacy preference database.” Although the specification

discloses that a processor that, in some cases, is coupled with “a privacy preference database” and a “response database,” the patent does not explain how this coupling occurs. ’824 patent at 4:8–11. Accordingly, the specification fails to reasonably convey to one of ordinary skill in the art that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- o Claim 17 of the ’824 patent and any claims dependent therefrom are invalid for failure to satisfy the requirements of 35 U.S.C. § 112 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “wherein the processor is configured to instruct the remote server to determine at least one data type for sharing of data packet that is compatible with the list of allowed patterns of data packets for sharing.” The specification does not disclose anywhere that the processor is configured to instruct the remote server to determine at least one data type for sharing of data packet that is compatible, let alone how. Accordingly, the specification fails to reasonably convey to one of ordinary skill in the art that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- **’249 patent:**
 - o Claims 1 and 19 of the ’249 patent and any claims dependent therefrom are invalid for failure to satisfy the requirements of 35 U.S.C. § 112 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “determining, by the remote server, a content of at least one data packet of the communication in accordance with characteristics of the at least one data packet” or “determine a content of at least one data packet of the communication in accordance with characteristics of the at least one data packet.” The specification acknowledges that terms like “determining” may “refer to operation(s) and/or process(es) of a computer, a computing platform, a computing system, or other electronic computing that manipulates and/or transforms data represented as physical (e.g., electronic) quantities within the computer’s registers and/or memories into other data similarly represented as physical quantities within the computer’s registers and/or memories or other information non-transitory storage medium that may store instructions to perform operations and/or processes.” ’249 patent at 5:25–38. But the ’249 patent does not disclose anywhere what those operations or processes are, let alone how they would work. Accordingly, the specification fails to reasonably convey to one of ordinary skill in the art that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- o Claim 2 of the '249 patent and any claims dependent therefrom are invalid for failure to satisfy the requirements of 35 U.S.C. § 112 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “determining at least one data type of the at least one data packet of the communication in accordance with characteristics of the at least one data packet.” The specification acknowledges that terms like “determining” may “refer to operation(s) and/or process(es) of a computer, a computing platform, a computing system, or other electronic computing that manipulates and/or transforms data represented as physical (e.g., electronic) quantities within the computer’s registers and/or memories into other data similarly represented as physical quantities within the computer’s registers and/or memories or other information non-transitory storage medium that may store instructions to perform operations and/or processes.” ’249 patent at 5:25–38. But the ’249 patent does not disclose anywhere what those operations or processes are, let alone how they would work. Accordingly, the specification fails to reasonably convey to one of ordinary skill in the art that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- o Claims 1, 12, and 19 of the ’249 patent and any claims dependent therefrom are invalid for failure to satisfy the requirements of 35 U.S.C. § 112 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “wherein the content of the at least one data packet is not decrypted by the remote server.” From the outset, the specification does not disclose the remote server determining a content of the data packet wherein the content of at least one data packet “is not decrypted by the remote server.” The specification does disclose that the remote server determining the data type of at least one data packet without “read[ing] the actual content of the data packets.” ’824 patent at 12:42–53. *See also id.* at 13:11–15. But as discussed above, the patent does not disclose how a remote server would determine the data type or data pattern of a data packet, let alone how a remote server would determine such information without reading the actual content of the packets. Accordingly, the specification fails to reasonably convey to one of ordinary skill in the art that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- o Claim 12 of the ’249 patent and any claims dependent therefrom are invalid for failure to satisfy the requirements of 35 U.S.C. § 112 because the specification as filed does not contain an adequate written description and/or enabling disclosure of “determination of the content is performed by the remote server in real time during a communication session between the remote server and the user’s device” (claims 1 and 19) / “determination of the at least one data pattern is performed by the remote

server in real time during a communication session between the remote server and the user's device." The specification discloses that "executable code may carry out operations described herein [the patent] in real-time." '249 patent at 6:18–19. But as discussed above, the patent does not disclose how a remote server would determine the data type or data pattern of a data packet, let alone how a remote server would determine such information in real time. Accordingly, the specification fails to reasonably convey to one of ordinary skill in the art that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- o Claims 5 and 14 of the '249 patent and any claims dependent therefrom are invalid for failure to satisfy the requirements of 35 U.S.C. § 112 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "wherein the modification of the communication is selected from the group consisting of: blocking the at least one data packet that is not compatible with the preference list, data nullification, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet, and encryption." The specification baldly discloses modifying data packets by utilizing "data nullification, change of encoding and/or file template, change of header and/or footer, blocking, data randomization, content modification, addition of a predetermined data packet, encryption or the like." '249 patent at 15:15–19. *See also id.* at 2:49–54, 3:46–52. The specification does not, however, specify how these methods are used or implemented without undue experimentation. Accordingly, the specification fails to reasonably convey to one of ordinary skill in the art that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- o Claim 30 of the '249 patent and any claims dependent therefrom are invalid for failure to satisfy the requirements of 35 U.S.C. § 112 because the specification as filed does not contain an adequate written description and/or enabling disclosure of "the processor is configured to determine whether to modify the at least one data packet based on the determined data type and the preference list without performing a comparison of a determined data pattern and the preference list." The specification does not disclose anywhere how a processor could determine whether to modify a data packet based on (1) the determined data type and (2) the preference list, without performing a comparison or analysis on said items. Accordingly, the specification fails to reasonably convey to one of ordinary skill in the art that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

These elements fail to meet the written description requirement and/or are not enabled. The Asserted Patents would not convey to one of skill in the art that, as of the filing date, the inventor had possession of the claimed subject matter. Nor would the Asserted Patents teach one of ordinary skill in the art how to practice these claim elements without undue experimentation. To the contrary, the Asserted Patents recite only generic components in the embodiments disclosed. Additionally, the claims containing these limitations are invalid for failing to enable the full scope of the invention as defined by the claim.

B. Indefiniteness Under 35 U.S.C. § 112

Below is an exemplary list of claim elements³ that are indefinite and/or render claims that include such elements indefinite under 35 U.S.C. § 112(b). “[A] patent is invalid for indefiniteness if its claims, read in light of the specification delineating the patent, and the prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention.” *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014); *see also Allen Eng’g Corp. v. Bartell Indus., Inc.*, 299 F.3d 1336, 1348 (Fed. Cir. 2002) (quoting *Solomon v. Kimberly-Clark Corp.*, 216 F.3d 1372, 1377 (Fed. Cir. 2000) (“[F]irst, [the claim] must set forth what ‘the applicant regards as his invention’ and second, it must do so with sufficient particularity and distinctness, i.e., the claim must be sufficiently, ‘definite.’”) (second alteration in original)).

Because Cisco’s investigation, prior art search, analysis, discovery, and trial preparation are still ongoing, Cisco expressly reserves the right to amend, supplement, and/or otherwise modify these Preliminary Invalidity Contentions, including by identifying and providing additional evidence and arguments that the Asserted Claims are indefinite under 35 U.S.C. § 112(b) following any constructions QPrivacy proposes or the Court adopts.

³ Any discrepancy between the language included in the bullets of this paragraph and the language of the corresponding claim element is inadvertent, and it is Cisco’s contention that the claim element is not adequately described and/or enabled under 35 U.S.C. § 112(a) and/or is indefinite under 35 U.S.C. § 112(b).

Any deficiencies that render claims invalid for indefiniteness under 35 U.S.C. § 112(b) also infect and thereby invalidate any and all claims depending therefrom.

At least the following claim elements, or portions thereof, used in the Asserted Patents are indefinite under 35 U.S.C. § 112(b) for failure to inform, with reasonable certainty, those skilled in the art about the scope of the invention:

- **'824 patent:**

- o “receiving, by the user’s device, a request for retrieval of at least one data packet from the user’s device” (claims 1, 9)
- o “wherein the user’s device is configured to provide a response corresponding to the received request” (claims 1, 9)
- o “privacy preference” / “privacy preference database” (claims 1, 9, and 17)
- o “determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request” (claims 1, 9)
- o “in accordance with a behavior range” (claim 9)
- o “at least one data type” (claim 17)
- o “determining, by the remote server, at least one communication data type . . . wherein the content of the at least one data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device” (all claims)
- o “data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference” (all claims)
- o “by the user’s device” / “by the remote server” (all claims)

- **'249 patent:**

- o “a content of at least one data packet of the communication” (claims 1, 19)
- o “a preference list” (claims 1, 3–5, 11–14, 18–19, 21–22, 25, 29–30)
- o “preference list database” (claim 19)
- o “communication session” (claims 1, 12, 19, and 22)
- o “the processor is configured to determine whether to modify the at least one data packet based on the determined data type and the preference list without performing a comparison of a determined data pattern and the preference list.” (claim 30)
- o “in accordance with a behavior range of the data packet” / “based on communication behavior” (claims 4, 7, 12, 15, 22, 24)
- o “gatekeeper server” (claims 10, 17, 28)
- o “list of forbidden and/or allowed data packet types” (claims 3, 4, 13, 21, 30)
- o “at least one data type of the at least one data packet” (claims 20, 30)
- o “determining, by the remote server, a content of at least one data packet . . . wherein the content of the at least one data packet is not decrypted by the remote server, and the determination of the content is performed by the remote server in real time during a communication session between the remote server and the user's device” (all claims)
- o “determining, by the remote server, based on a comparison of the determined content, whether to modify the at least one data packet” (all claims)
- o “by the remote server” / “by the user’s device” (all claims)

As used in the context of the claim language, these claim elements are indefinite for failure to inform, with reasonable certainty, those skilled in the art about the scope of the

invention as claimed. Based on Cisco's present understanding of QPrivacy's Infringement Contentions, at least one or more of these claim terms, phrases, and limitations are indefinite because they are inconsistent with and/or broader than the alleged invention disclosed in the specification and during prosecution, and given QPrivacy's apparent construction of the claims, any person of ordinary skill in the art at the time of the invention would not understand what is claimed with reasonable certainty, even when the claims are read in light of the specification and prosecution history.

VI. SUBJECT MATTER INELIGIBILITY CONTENTIONS – INELIGIBLE SUBJECT MATTER UNDER 35 U.S.C. § 101

Pursuant to this Court's Standing Order Regarding Subject-Matter Eligibility Contentions ("Standing Order") and the Court's Docket Control Order (ECF No. 29), Cisco serves Preliminary Subject Matter Ineligibility Contentions ("Ineligibility Contentions") attached hereto as Appendix A addressing how the Asserted Claims of the Asserted Patents are invalid.

Pursuant to paragraph (c) of the Standing Order, Cisco reserves the right to amend or supplement these Preliminary Ineligibility Contentions if: (1) QPrivacy amends its infringement contentions; or (2) the Court's Claim construction ruling so requires.

The information provided should not be deemed an admission regarding the scope of any claims or the proper construction of those claims or any terms contained therein. Cisco's claim construction disclosures will be provided under P.R. 4 as required by the Court's Docket Control Order. Nothing contained in these Ineligibility Contentions should be understood or deemed to be an express or implied admission or contention with respect to the absence of factual disputes relating patent ineligibility, the absence of a need for construction of any terms in an asserted claim, any proper construction of any terms in an asserted claim, or alleged infringement of that claim. There is no claim construction issue or factual issue that precludes the Court finding that the claims of the asserted patents are patent-ineligible. Nothing in these disclosures should be treated as an admission that Cisco is obligated to produce documentation not under its custody or control, or that can be obtained from some other source that is more convenient, less burdensome

and/or less expensive, or for which the burden or expense outweighs its likely benefit. Cisco expressly reserves the right to revise, amend, and/or supplement their disclosures and document production should additional documentation become available.

Cisco's Ineligibility Contentions address only the Asserted Claims. Cisco reserves the right to supplement these contentions if QPrivacy asserts infringement of any claim other than the Asserted Claims.

Cisco's discovery and investigations in this lawsuit are ongoing, and therefore, Cisco reserves the right to revise, amend, and/or supplement these Ineligibility Contentions as discovery progresses and as they discovers additional information. Discovery is ongoing, and Cisco's prior art investigation and third-party discovery are in the initial stages. Cisco reserves the right to revise, amend, and/or supplement the information provided herein, including identifying, and relying on additional references, should Cisco further search and analysis yield additional information or references, consistent with the Local Rules, Judge Gilstrap's Standing Order, and the Federal Rules of Civil Procedure. In particular, Cisco reserves the right to rely on, and Cisco incorporates by reference into its Ineligibility Contentions, all prior art identified by Cisco in conjunction with its Invalidity Contentions. Cisco also reserves the right to amend, modify, or supplement these Ineligibility Contentions to include prior art under 35 U.S.C. §§ 102 and 103 identified in its Invalidity Contentions. Cisco reserves the right to rely on all documents produced by Cisco, as well as QPrivacy, any predecessors in interest, the named inventors, and any other third parties, as discovery is ongoing.

Dated: March 31, 2025

Respectfully submitted,

By: /s/ Nima Kiaei

Melissa R. Smith
State Bar No. 24001351

GILLAM & SMITH, LLP
303 South Washington Avenue
Marshall, Texas 75670
Telephone: (903) 934-8450
Facsimile: (903) 934-9257
Email: Melissa@gillamsmithlaw.com

Bitra Rahebi
Nima Kiaei (*pro hac vice*)
MORRISON & FOERSTER LLP
707 Wilshire Boulevard
Los Angeles, California 90017-3543
Telephone: (213) 892-5200
Facsimile: (213) 892-5454
Email: BRahebi@mofo.com
Email: NKiaei@mofo.com

Brian C. Nash
Catherine J. Canby
MORRISON & FOERSTER LLP
300 Colorado Street, Suite 1800
Austin, TX 78701
Telephone: (512) 617-0650
Facsimile: (737) 910-0730
Email: BNash@mofo.com
Email: CCanby@mofo.com

Hannah T. Jiam
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, California 94105-2482
Telephone: (415) 268-7000
Facsimile: (415) 268-7522
Email: HJiam@mofo.com

Attorneys for Defendant Cisco Systems, Inc.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that all counsel of record who have appeared in this case are being served with a copy of this document via email per Local Rule CV-5(d) on March 31, 2025.

/s/ Silvia Specht
Silvia Specht