

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,

Petitioner

v.

QPRIVACY USA LLC,

Patent Owner

Case IPR2025-00837

Patent No. 11,106,824

PATENT OWNER'S PRELIMINARY RESPONSE ON THE MERITS

TABLE OF CONTENTS

I. INTRODUCTION.....1

II. THE ‘824 PATENT DISCLOSES SYSTEMS AND METHODS FOR PROTECTING PRIVATE USER DATA2

 A. Exemplary Claims.....4

 B. Level of Ordinary Skill in the Art.....5

 C. Claim Construction6

III. INTRODUCTION TO THE GROUNDS9

IV. GROUND 1 BASED ON BURNS + YANG FAILS10

 A. Summary of Burns (EX. 1005).....11

 B. Summary of Yang (EX. 1006)16

 C. Petitioner Fails to Establish that a POSITA Would Have Combined Burns and Yang as Proposed17

 D. Petitioner Fails to Establish that the Proposed Combination Discloses or Renders Obvious Claim Limitation [17.10]19

V. GROUND 2 BASED ON BURNS + YANG + WITTENBERG FAILS25

 A. Summary of Wittenberg (EX. 1007).....26

 B. Petitioner Fails to Establish that the Proposed Combination Discloses or Renders Obvious Claim Limitations [1.8] – [1.9].....27

1. Petitioner’s allegations regarding dropping the packets associated with the communication session are incorrect and/or insufficient.....	28
2. Petitioner’s allegations regarding automatically closing the communication session are incorrect and/or insufficient.....	30
3. Petitioner’s allegations regarding throttling down the communication session are incorrect and/or insufficient.....	34
VI. PATENT OWNER RESERVES ALL RIGHTS REGARDING SECONDARY CONSIDERATIONS OF NON-OBVIOUSNESS BASED ON THE PRACTICING PRODUCTS.....	38
VII. CONCLUSION.....	39

<u>PATENT OWNER'S LIST OF EXHIBITS</u>	
EX. 2001	Amended Docket Control Order, <i>QPrivacy USA LLC v. Cisco Systems Inc.</i> , No. 2:24-cv-00855, Dkt. 43 (E.D. Tex. May 23, 2025)
EX. 2002	Docket Navigator - Time to Trial Statistics for E.D. Tex., accessed on July 11, 2025
EX. 2003	Appeal Statistics, Patent Trial and Appeal Board dated May 31, 2025, accessed at https://www.uspto.gov/sites/default/files/documents/appeal_stats_may2025.pdf on July 2, 2025
EX. 2004	PTAB Trial Statistics, May 2025 IPR, PGR, Patent Trial and Appeal Board, accessed at https://www.uspto.gov/sites/default/files/documents/ptabaia20250531.pdf on July 2, 2025
EX. 2005	PTAB Trial Statistics, May 2024 IPR, PGR, Patent Trial and Appeal Board, accessed at https://www.uspto.gov/sites/default/files/documents/ptab_aia_20240531.pdf on July 2, 2025
EX. 2006	Defendant Cisco Systems, Inc.'s Invalidity and Subject Matter Eligibility Contentions dated March 31, 2025 – Cover Document
EX. 2007	Order of Recusal, <i>QPrivacy USA LLC v. Cisco Systems Inc.</i> , No. 2:24-cv-00855, Dkt. 39 (E.D. Tex. May 15, 2025)
EX. 2008	U.S. Patent No. 11,816,249
EX. 2009	Summons Returned Executed, <i>QPrivacy USA LLC v. Cisco Systems Inc.</i> , No. 2:24-cv-00855, Dkt. 14 (E.D. Tex. Oct. 29, 2024)
EX. 2010	Cisco Systems, Inc. – List of Subsidiaries as of February 12, 2025, accessed at https://www.cisco.com/c/dam/en_us/about/

	doing_business/trust-center/docs/list-of-cisco-global-entities.pdf on July 2, 2025
EX. 2011	U.S. Patent No. 10,505,970
EX. 2012	U.S. Patent No. 10,686,831
EX. 2013	U.S. Patent No. 10,320,823
EX. 2014	U.S. Patent No. 10,659,324
EX. 2015	Defendant Cisco Systems, Inc.'s Invalidation and Subject Matter Eligibility Contentions dated March 31, 2025 – Exhibit 6 for Burns
EX. 2016	Defendant Cisco Systems, Inc.'s Invalidation and Subject Matter Eligibility Contentions dated March 31, 2025 – Exhibit 7 for Yang
EX. 2017	U.S. Patent No. 9,077,692
EX. 2018	U.S. Patent No. 12,013,971
EX. 2019	Excerpt from prosecution history of U.S. Patent No. 12,013,971 – List of References cited by applicant and considered by examiner filed on March 11, 2024
EX. 2020	U.S. Patent No. 7,797,411
EX. 2021	U.S. Patent No. 8,266,267
EX. 2022	Excerpt from prosecution history of U.S. Patent No. 8,341,724 – Final Rejection dated June 18, 2012
EX. 2023	U.S. Pub. No. 2011/0041182
EX. 2024	RESERVED

EX. 2025	<i>Ex Parte</i> Reexamination Historical Statistics, updated March 2025, accessed at https://www.uspto.gov/learning-and-resources/statistics/reexamination-information on July 8, 2025
EX. 2026	Declaration of Dr. Tim A. Williams
EX. 2027	The Wayback Machine – Thoughts on Flash, accessed at https://web.archive.org/web/20100503010500/http://www.apple.com/hotnews/thoughts-on-flash/ on July 25, 2025
EX. 2028	Ars Technica – Google Talks Chrome OS, HTML5, and the future of software, accessed at https://arstechnica.com/information-technology/2010/01/chrome-os-interview-1/ on July 25, 2025
EX. 2029	Google Online Security Blog – HTTPS as a ranking signal, accessed at https://security.googleblog.com/2014/08/https-as-ranking-signal_6.html on July 25, 2025
EX. 2030	Chrome for Developers – Avoiding the not secure warning in chrome, accessed at https://developer.chrome.com/blog/avoid-not-secure-warn on July 25, 2025
EX. 2031	Google Online Security Blog – Moving towards a more secure web, accessed at https://security.googleblog.com/2016/09/moving-towards-more-secure-web.html on July 25, 2025
EX. 2032	WP Rocket – Google’s Enforcing HTTPS – Is your Website Ready for Chrome 68? accessed at https://wp-rocket.me/blog/googles-enforcing-https-website-ready-chrome-68/ on August 11, 2025

I. INTRODUCTION

Patent Owner previously submitted its discretionary denial brief explaining why the Director should discretionarily deny institution. Paper 8. Now, Patent Owner respectfully submits this preliminary response on the merits to explain why, if this IPR is referred to a panel, institution should be denied on the merits.¹

Petitioner does not allege anticipation, only obviousness. As further discussed herein, Petitioner fails to meet its burden to establish obviousness and institution should be denied on the merits for at least three reasons:

First, Petitioner fails to establish that a POSITA would have been motivated to combine Burns' IDS and Yang's static port mapping technique as proposed. Yang itself teaches away from doing so. Additionally, a POSITA in 2017 would have understood that there was not a 1-1 mapping of ports and applications at least because the use of port 443/HTTPS had become normalized.

Second, Petitioner fails to establish that the proposed combination operates "in real-time" as claimed. The prior art itself directly contradicts Petitioner's

¹ Patent Owner additionally reiterates its request for the Director to consider the weakness of the merits of the petition in deciding whether to discretionarily deny institution. Paper 8 at 30.

allegations. Additionally, Petitioner relies on conclusory expert testimony that is insufficient to meet its burden or otherwise justify conducting a full trial.

Third, Petitioner fails to establish that the proposed combination performs the “modifying” and “sharing” steps as claimed. Petitioner again relies on conclusory expert testimony that is incorrect and/or insufficient.

Additionally, Petitioner fails to address secondary considerations of non-obviousness based on the practicing products. At least since the filing of the complaint in the parallel litigation, Petitioner has been on notice that the identified products practice the claims of the ‘824 Patent.

Overall, because Petitioner fails to show, in the petition, that there is a reasonable likelihood that any independent claim would have been obvious, conducting this IPR is not a good use of the PTAB’s resources. Institution should be denied.

II. THE ‘824 PATENT DISCLOSES SYSTEMS AND METHODS FOR PROTECTING PRIVATE USER DATA

The ‘824 Patent explains that web servers may seek to collect various information (data packets) about a user, e.g., time zone, type of operating system, location, web browsing history, etc. *See, e.g.*, EX. 1001 at 1:22-25, 12:56-62. The ‘824 Patent discloses systems and methods that protect private user data from being

collected from the user's device, e.g., by Facebook, while the user is browsing the website. *See, e.g.*, EX. 1001 at 1:40-59.

During a communication session between the user's device and the web server, the user's device may receive a request from the web server, wherein the web server is requesting retrieval of at least one data packet from the user's device. *See, e.g.*, EX. 1001 at FIG. 6A, FIG. 6B. The user's device may provide a corresponding response, wherein the response comprises encrypted data packets. *Id.*; *see also, e.g.*, EX. 1001 at 12:38-43.

Sometimes the user's device may provide a response automatically without knowledge and/or authorization of the user. *See, e.g.*, EX. 1001 at 12:63-13:1. Therefore, the '824 Patent teaches that an intermediary device may serve as a "gatekeeper" monitoring communications between the user's device and the web server. *See, e.g.*, EX. 1001 at 13:1-11, 16:25-36. The intermediary device may store a privacy preference for the user's device that lists certain static data types and/or dynamic data patterns. *See, e.g.*, EX. 1001 at 8:21-43, 9:38-42.

The intermediary device may analyze the response provided by the user's device to determine whether to modify at least one data packet in the response based on a comparison with the privacy preference. For example, the privacy preference may dictate changing the location of the user's device from USA to a random country in one data packet before sharing, while allowing the other data packets to

remain unchanged. *See, e.g.*, EX. 1001 at 8:38-43, 13:66-14:5. The modified response may then be shared with the web server in order to maintain the communication session between the user’s device and the web server. *See id.*

A. Exemplary Claims

The ‘824 Patent includes claims 1-20. Claims 1, 9, and 17 are independent.

Exemplary independent claim 1 is reproduced below with annotations.²

1.0	A method of dynamic management of private data during communication between a remote server and a user's device, the method comprising:
1.1	receiving, by the user's device, a request for retrieval of at least one data packet from the user's device,
1.2	wherein the user's device is configured to provide a response corresponding to the received request;
1.3	determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request,
1.4	wherein the at least one communication data type is determined in accordance with characteristics of the communication data packet, and
1.5	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;
1.6	receiving, by the user's device, a privacy preference for the user's device,
1.7	wherein the privacy preference comprises a list of allowed data packet communication types for sharing during communication;
1.8	modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference; and
1.9	maintaining communication between the remote server and the user's device, with sharing of the modified data packets.

² Patent Owner uses the same annotations as Petitioner for ease of review.

As shown above, independent claim 1 recites a method including determining a “communication data type” in accordance with “characteristics of the communication data packet”. Independent claim 9 recites a method including determining a “communication data pattern” in accordance with a “behavior range of the communication data packet”. Independent claim 17 recites a system including a communication data type database, a privacy preference database, and a processor that is configured to instruct the remote server to perform steps similar to those in claim 1.

B. Level of Ordinary Skill in the Art

Petitioner proposes a person of ordinary skill in the art (“POSITA”) would, as of April 9, 2017, have had “a bachelor’s degree in computer science, computer engineering, or an equivalent, and three years of professional experience relating to packet-based network communications.” Paper 2 at 11. Petitioner additionally proposes that a POSITA “would have had a working knowledge of the data communications art... including packet-based computer networking” and “would be familiar with a variety of computer and internet networking topics such as the World Wide Web and TCP/IP.” *Id.*

Patent Owner does not dispute Petitioner’s proposed POSITA definition for purposes of determining whether to deny institution in this IPR.³ However, as discussed herein, Patent Owner disputes Petitioner’s attempts to gap-fill the prior art by relying on the proposed POSITA definition and/or conclusory expert testimony. *See, e.g., Virtek Vision Int'l ULC v. Assembly Guidance Sys.*, 97 F.4th 882, 888 (Fed. Cir. 2024) (finding no motivation to combine because “[i]t does not suffice to simply be known.”).

C. Claim Construction

Patent Owner submits that the panel need not expressly construe any claim terms/phrases to determine whether to deny institution in this IPR at least because the technical distinctions discussed herein do not turn on whether the implicit constructions relied on by Petitioner are correct.⁴ Nonetheless, Patent Owner submits that Petitioner has violated the statutory requirements for IPR petitions for the reasons discussed below. *See also* Paper 8 at 26-28.

Despite Petitioner alleging indefiniteness of at least 11 terms/phrases in the ‘824 Patent in its district court invalidity contentions (EX. 2006 at 41,) neither

³ Patent Owner reserves all rights regarding the correct POSITA definition.

⁴ Patent Owner reserves all rights regarding the correct construction of claim terms/phrases in the ‘824 Patent.

Petitioner nor its expert identified any claim terms/phrases for construction in this IPR. Paper 2 at 12; EX. 1003 at ¶53. However, Petitioner is relying on its expert's implicit claim constructions in this IPR instead of proposing express constructions and providing supporting evidence.

Petitioner's expert is implicitly construing claims without expressly opining on the correct construction in the context of the '824 Patent with supporting evidence. Implicit claim constructions violate 37 C.F.R. § 42.104(b)(3) which requires a petitioner to "[p]rovide a statement of the precise relief requested for each claim challenged," which must include "[h]ow the challenged claim is to be construed."

Below are exemplary terms/phrases identified as allegedly indefinite in Petitioner's invalidity contentions and corresponding testimony from Petitioner's expert in this IPR.

For the claimed step of "determining, by the remote server, at least one communication data type...", Petitioner's expert opines that "Burns's IDS (*remote server*) identifies an application or protocol (*data type*) based on mapping port numbers from TCP packet headers (*characteristics*)." EX. 1003 at ¶176 (italics original). Thus, Petitioner's expert implicitly construes the claimed "data type" as an application or protocol and the claimed "characteristics" as a port number. *Id.*

Petitioner’s expert does not opine on the correct constructions in the context of the ‘824 Patent with supporting evidence.⁵

For the claimed “privacy preference,” Petitioner’s expert opines that (a) “Burns allows a system administrator to ‘configure IDS 10 to explicitly allow all identifiable applications, allow all applications except for a specified list of identifiable applications, or prevent all communications’” (EX. 1003 at ¶180 (citing EX. 1005 at 5:30-34)); and (b) “[a] POSITA would have appreciated that, because the configuration information allows administrator to tailor the IDS to their preferences, the configuration information specified by the administrator corresponds to a ‘*preference list.*’” (EX. 1003 at ¶181) (*italics original*). Thus, Petitioner’s expert implicitly construes the claimed “privacy preference” as configuration information. *Id.* Petitioner’s expert does not opine on the correct construction in the context of the ‘824 Patent with supporting evidence.

For at least these reasons, Petitioner fails to meet its burden under § 42.104(b)(3) and institution should be denied.

⁵ The ‘824 Patent shows exemplary data types (content) in FIG. 3C including audio, location (country), contact name, password. EX. 1001 at FIG. 3C.

III. INTRODUCTION TO THE GROUNDS

Petitioner challenges the '824 Patent based only on obviousness grounds and therefore, concedes that no single reference discloses all claim limitations.

Nonetheless, Petitioner fails to establish that the claimed invention **as a whole** would have been obvious to a POSITA.

As discussed below, the prior art relied on in the grounds and the '824 Patent are directed at different problems in networking – security versus privacy - and because they are directed at different problems, they disclose different solutions. While security solutions protect data from being accessed by illegitimate applications, privacy solutions protect how data is accessed, collected, used, stored, and/or shared. Even if there is no security risk, privacy solutions are needed to ensure proper data handling.

For example, Burns is focused on network security and as a result, Burns will prevent an illegitimate application from accessing the internal nodes on the private network, e.g., by terminating the connection. However, Burns might determine an application is legitimate and allow the application to access the internal nodes on the private network, thereby allowing the legitimate application to collect private user data on the internal nodes. Unlike the '824 Patent, Burns is not trying to protect private user data in accordance with a privacy preference for

the internal node(s). Burns is only trying to identify and prevent unwanted/malicious applications from accessing the private network.

In contrast to Burns, the ‘824 Patent discloses protecting private user data and ensuring proper data handling during a communication session by evaluating compatibility with a privacy preference and modifying the data packet(s) as appropriate. The ‘824 Patent makes clear that there may be, e.g., 10 packets, and only one of those 10 packets may be modified to prevent the collection of private user data such as location. Because the ‘824 Patent is focused on protecting private user data, the ‘824 Patent does not teach, e.g., terminating the connection anytime a web server requests private user data – the Internet would be unusable. Instead, the ‘824 Patent discloses methods that maintain the connection so that the user can continue web browsing.

IV. GROUND 1 BASED ON BURNS + YANG FAILS

Ground 1	Claims 17-20	§103 Burns + Yang
----------	--------------	-------------------

Burns and Yang are both directed at improving network security by detecting and preventing network attacks. As discussed below, Burns and Yang both teach methods for an intrusion detection system (IDS) to identify and prevent unwanted/malicious applications from accessing the private enterprise network.

Burns and Yang seek to solve a different problem than the '824 Patent which is directed at protecting private user data while maintaining a communication session.

A. Summary of Burns (EX. 1005)

FIG. 1 of Burns (reproduced below) shows public network 6 and private enterprise network 5. *See, e.g.*, EX. 1005 at 4:27-29. IDS 10 intercepts packets sent from client computing devices on the public network 6 to internal nodes 8 on the private enterprise network 5 to filter unwanted/malicious packets. *See, e.g.*, EX. 1005 at 4:20-32.

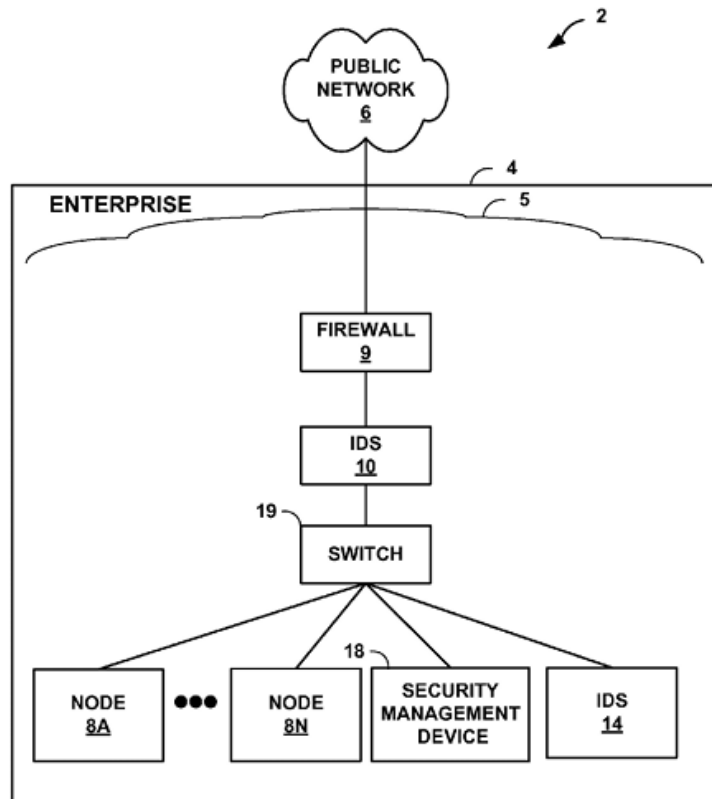


FIG. 1

EX. 1005 at FIG. 1.

In particular, IDS 10 attempts to identify a packet that is fully encrypted and if identified, IDS 10 determines that packet likely originated from an unwanted/malicious application. *See, e.g.*, EX. 1005 at 5:20-26. In the context of Burns, “fully encrypted” means that both the application-layer header and the application-layer payload are encrypted. EX. 1005 at 5:17-20, 9:9-12. Burns explains that legitimate applications following a well-known encryption protocol will encrypt the application-layer payload, but not the application-layer header. EX. 1005 at 5:7-13. However, malicious applications attempting to avoid detection will encrypt the application-layer header and the application-layer payload. EX. 1005 at 5:13-16.

FIG. 2 of Burns (reproduced below) shows additional components of the IDS, including security management module 44 which presents a user interface for administrator 42 to (a) specify attack definitions 33, which are sent to stateful inspection engine 28 and (b) configure the IDS to take particular actions when a fully encrypted packet is identified. *See, e.g.*, EX. 1005 at 6:36-59.

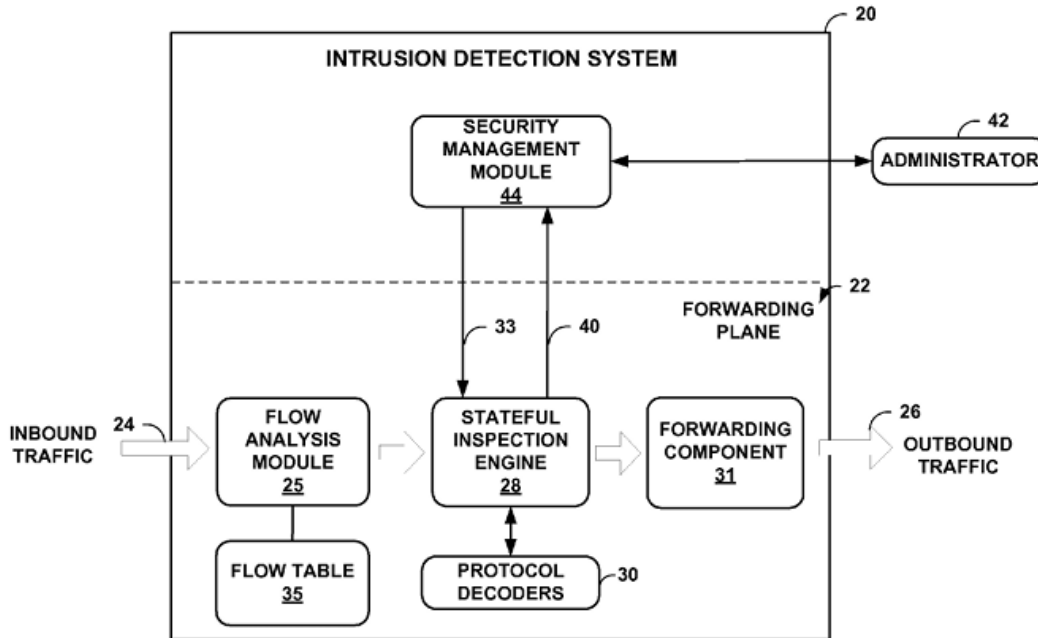


FIG. 2

EX. 1005 at FIG. 2

As shown in FIG. 2 of Burns, flow analysis module 25 receives inbound traffic 24 and maintains data in flow table 35 for each active packet flow, where flow table 35 specifies network elements associated with each active packet flow in order to identify pairs of packet flows that form a single communication session. EX. 1005 at 6:60-7:15.

To determine whether the packet flow is associated with an identifiable application, stateful inspection engine 28 buffers a copy of the packet flow and reassembles the buffered packet flow to form application-layer communications. EX. 1005 at 7:17-20. FIG. 3 of Burns (reproduced below) shows that stateful inspection engine 28 includes application identification module 51, which attempts

to identify the application associated with the reassembled/reconstructed application-layer data from reassembly module 50. EX. 1005 at 8:11-23. If an application is identified, the data is sent to a specific protocol decoder 30. EX. 1005 at 8:25-29. If an application is not identified, the data is sent to the default protocol decoder 30. EX. 1005 at 8:29-34.

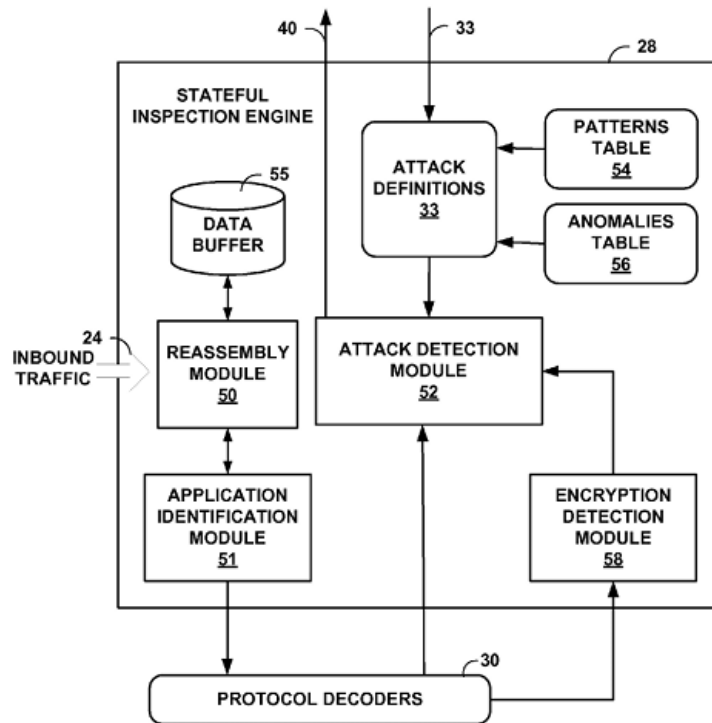


FIG. 3

EX. 1005 at FIG. 3

To determine whether the packet flow is associated with an identifiable protocol, protocol decoders 30 inspect the application-layer header or other elements of the communication session. EX. 1005 at 8:35-41, 8:56-57. Protocol decoders 30 may analyze the bi-directional communications for the communication

session to identify a key exchange and log the fact that a non-hidden (detectable) key exchange occurred. EX. 1005 at 8:59-62, 13:33-41.

Ultimately, if the protocol is identified, the data is sent from the protocol decoder 30 to attack detection module 52. EX. 1005 at 9:1-4. If the protocol is not identified, the data is sent from the protocol decoder 30 to encryption detection module 58. EX. 1005 at 9:5-8.

To determine whether a packet is fully encrypted, encryption detection module 58 analyzes the TCP/IP payload, including the application-layer header and the application-layer payload, to determine a randomness value. EX. 1005 at 9:9-44. If the randomness value exceeds a randomness threshold defined by the administrator 42, encryption detection module 58 determines that the packet is fully encrypted. *Id.*⁶ Encryption detection module 58 then sends a message to attack detection module 52 that the communication session is being conducted by an

⁶ FIG. 4 shows an embodiment in which encryption detection module 58 determines if the packet is fully encrypted. However, the administrator may select “detect fully encrypted packets” and/or “detect key exchange”. FIG. 5 shows an alternative embodiment in which encryption detection module 58 determines if the packet is fully encrypted and if so, determines if a key exchange was identified by protocol decoders 30. EX. 1005 at 13:22-24, 13:33-41, 13:53-57.

unwanted/malicious application. *Id.* Attack detection module 52 will then perform one or more actions defined by the administrator 42. *Id.*

B. Summary of Yang (EX. 1006)

Yang discloses a similar system architecture to Burns. Yang seeks to improve the accuracy of attack identifications by the IDS. EX. 1006 at Abstract.

Yang analyzes a first inbound packet flow from a client on public network 6 to a sever-node on private enterprise network 5 and performs an initial assessment of the type of application and protocol. *See, e.g.,* EX. 1006 at 1:55-65, 6:18-21. Based on this initial assessment, the IDS applies a first set of attack definitions. *Id.*

Yang then analyzes a second outbound packet flow from the server-node to the client and the IDS attempts to confirm the initial assessment. *See, e.g.,* EX. 1006 at 6:22-44. If the initial assessment was incorrect, then the IDS reclassifies the type of application and protocol and applies a second set of attack definitions. *Id.* The IDS will also apply the second set of attack definitions to the first packet flow. *Id.*

Like Burns, Yang attempts to determine whether the packet flow is associated with an identifiable application. Yang explains that, as of 2007, conventional IDS would “associate applications with a static port assignment and use[] these static port assignments to determine the type of application and protocol associated with a given data stream.” EX. 1006 at 1:33-36. Yang further explains that it was well

known for an IDS to use a static port bindings list (e.g., Table 1 reproduced below) to determine an application/protocol. EX. 1006 at 9:61-66.

5

TABLE I

PORT	APPLICATION
20	FTP
22	SSH
23	Telnet
25	SMTP
43	WHOIS
53	DNS
67	BOOTP or DHCP
70	Gopher
79	Finger
80	HTTP
109	POP
110	POP3
113	ident/IRC
118	SQL
119	NNTP
194	IRC
443	HTTPS
445	SMB
564	RTSP

EX. 1006 at 10:5-24.

C. Petitioner Fails to Establish that a POSITA Would Have Combined Burns and Yang as Proposed

Petitioner alleges that it would have been obvious for a POSITA reading Burns to use Yang’s static port mapping technique to identify an application/protocol associated with the packet flow. *See, e.g.*, Paper 2 at 21-23. Patent Owner disputes this allegation for at least two reasons.

First, a POSITA in 2017 would not have been motivated to use Yang’s static port mapping technique in Burns’ IDS at least because Yang itself teaches away

from doing so. Yang warns that “many hackers or other malicious individuals utilize software application that employ dynamic or randomized port assignments rather than conform to the static port assignments in order to evade detection and containment” and that “[s]uch techniques render it difficult for IDSs to correctly identify the type of application and protocol.” EX. 1006 at 1:36-42. Because unwanted/malicious applications do not conform to static port assignments, a POSITA would not be motivated to use the static port mapping technique to identify and filter unwanted/malicious packets. EX. 2026 at ¶38.

Second, Petitioner ignores the advances in technology between 2007, when the underlying application of Yang was filed, and 2017. By 2017, the use of port 443/HTTPS had become normalized. EX. 2026 at ¶¶39-43. As such, a POSITA would not have been motivated to use Yang’s static port mapping technique in Burns’ IDS as proposed. *Id.* By 2017, there was no longer a 1-1 mapping of ports and applications so a POSITA would have understood that using a port to identify an application was no longer useful. *Id.*

As Patent Owner’s expert, Dr. Williams, explains, web-based activity had significantly increased by 2010 due to the modern HTML 5 standard and the development of mobile devices and web-based applications. EX. 2026 at ¶40 (discussing for example Google Chrome OS supporting Gmail, Google Drive, etc.); EX. 2027; EX. 2028. In 2014, Google campaigned for “HTTPS Everywhere”

encouraging the use of HTTPS by default. EX. 2026 at ¶42; EX. 2029. In 2016, Google announced it would start displaying warning messages for websites using HTTP instead of HTTPS. EX. 2026 at ¶42; EX. 2030; EX. 2031. By 2016, the majority of web traffic was using HTTPS. EX. 2026 at ¶42; EX. 2032.

Because identifying the use of port 443 would not help the POSITA identify a legitimate versus illegitimate application, a POSITA would not have been motivated to use Yang's static port mapping technique as proposed.

For at least these reasons, a POSITA would not have been motivated to use Yang's static port mapping technique in Burns' IDS as proposed. As such, all grounds fail and institution should be denied.

D. Petitioner Fails to Establish that the Proposed Combination Discloses or Renders Obvious Claim Limitation [17.10]

17.10	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.
-------	--

Petitioner alleges that it would have been obvious for Burns' IDS to perform the determination "in real time". Paper 2 at 38-40. Patent Owner disputes this allegation for at least four reasons.

First, Petitioner quotes Yang, but this quote is taken out of context and refers to a different embodiment for a line-rate buffering approach disclosed in Yang. Paper 2 at 39 (citing EX. 1006 at 11:63-12:3); EX. 2026 at ¶46. Petitioner relies on

Burns' use of the mirrored approach, not the line-rate buffering approach, in its analysis of claim 1. Yang actually teaches that its mirrored approach does **not** analyze the network traffic in "real-time" as that term is used in Yang. Therefore, Yang directly contradicts Petitioner's allegations regarding claim limitation [17.10]

In context, the full cited quote from Yang reads as follows:

"Once configured, IDS 20 monitors network traffic 24 (72). In some configurations, stateful inspection engine 28 of forwarding plane 22 may receive network traffic and mirror the network traffic for purposes of analysis. Forwarding component 31 seamlessly forwards the original network traffic. In other embodiments, traffic is not mirrored, rather a line-rate buffering approach is used to analyze the traffic in real-time prior to forwarding."

EX. 1006 at 11:63-12:3. Thus, Yang distinguishes its mirrored approach from its line-rate buffering approach where the line-rate buffering approach analyzes network traffic in "real-time" as that term is used in Yang. EX. 2026 at ¶46.

Because Yang distinguishes these two approaches, Yang actually informs a POSITA that its mirrored approach does not analyze network traffic in "real-time."

*Id.*⁷

⁷ Petitioner does not allege that "mirrored approach" has a different meaning in the context of Yang versus Burns.

Burns repeatedly refers to the mirrored approach.⁸ EX. 1005 at 10:18-22 (“...stateful inspection engine 28 of forwarding plane 22 may receive network traffic and mirror the network traffic for purposes of analysis...”) and 11:63-67 (same). Burns’ IDS performs its analysis on mirrored packets (e.g., reconstructed, reassembled, copied data). *See, e.g.*, EX. 1005 at 7:65-8:02 (discussing reassembly module 50) and 8:11-34 (same); *see also, e.g.*, EX. 1006 at 8:27-32 (discussing reassembled application-layer communications 32) and 8:49-51 (same) and 9:14-18 (same). A POSITA would have understood that the disclosed mirrored approach analyzes the mirrored packets instead of analyzing the original packets. EX. 2026 at ¶48. Because Yang teaches that the disclosed mirrored approach does not analyze network traffic in “real-time” as that term is used in Yang, the cited quote from Yang directly contradicts Petitioner’s allegations for claim limitation [17.10]. EX. 2026 at ¶47.

For at least these reasons, the cited quote from Yang does not show that the proposed combination of Burns + Yang renders obvious claim limitation [17.10] as alleged.

Second, Petitioner quotes Burns and argues that because Burns discloses the IDS “transparently monitors inbound network traffic 24 and forwards the network

⁸ Burns never refers to a line-rate buffering approach. *See generally* EX. 1005.

traffic as outbound network traffic 26,” then the IDS necessarily performs the determination in “real-time.” Paper 2 at 38-39 (citing EX. 1005 at 6:30-36, 8:11-23). However, Petitioner misplaces reliance on the adverb “transparently” and its expert’s testimony. *See, e.g.*, Paper 2 at 39.⁹

In computer networking, “transparently” means invisibly or unknowingly. EX. 2026 at ¶49. For example, the IDS’ monitoring might be described as transparent because the user is not actively involved and/or because the user does not know the specific details of the monitoring. *Id.* As another example, the IDS’ monitoring might be described as transparent because the IDS is in-line with the destination device and the IDS intercepts network traffic without requiring changes to the destination IP address. *Id.*

Ultimately, Burns’ reference to the IDS “transparently” monitoring inbound network traffic does not inform a POSITA that the IDS satisfies the “determining” step of claim 1 in real time. EX. 2026 at ¶49.

For at least these reasons, the cited quote from Burns does not show that the proposed combination of Burns + Yang renders obvious claim limitation [17.10] as alleged.

⁹ Petitioner’s expert repeats the statements in the petition verbatim. *Compare* EX. 1003 at ¶¶119-121 *with* Paper 2 at 14, 39-40.

Third, Petitioner quotes Proctor’s textbook to allege that “[m]ost commercial network intrusion detection systems run in real-time.” Paper 2 at 40 (citing EX. 1036 at 38).¹⁰ Petitioner fails to establish that this cited quote is applicable to Burns’ IDS specifically. EX. 2026 at ¶50. As such, Petitioner fails to establish that Burns’ IDS performs the determination in real time as claimed.

For example, Petitioner fails to distinguish an intrusion detection system from an intrusion prevention system as understood by a POSITA. EX. 2026 at ¶50; EX. 1017 at 238. Typically, an intrusion detection system monitors and detects any suspicious activity on a network. *Id.* An intrusion detection system does not take any action by itself to protect the system or network. *Id.* In contrast, an intrusion prevention system detects suspicious activity and also prevents the intrusions by taking proactive steps. *Id.* Petitioner does not explain whether Proctor’s textbook distinguishes an intrusion detection system versus an intrusion prevention system. *Id.* Petitioner also does not explain how Proctor’s textbook relates to Burns’ system as either an intrusion detection system or an intrusion prevention system. *Id.*

¹⁰ It is noted that EX. 1036 is only an excerpt from Proctor’s textbook and therefore incomplete. It is also noted that EX. 1036 does not discuss encrypted communications.

As another example, Petitioner fails to distinguish network-based systems and host-based systems, as discussed in Proctor's textbook, and how they relate to Burns' system. *See, e.g.*, EX. 1036 at 38. As yet another example, Petitioner fails to discuss the number of passive sensors, as discussed in Proctor's textbook, and how they relate to Burns' system. *Id.*

For at least these reasons, Petitioner fails to establish that the cited quote from Proctor's textbook applies to Burns. As such, the cited quote from Proctor's textbook does not show that the proposed combination of Burns + Yang renders obvious claim limitation [17.10] as alleged.

Fourth, Burns is directed at a different problem where if a security risk is detected, the IDS will prevent network access. This is inapposite to the "real-time" nature of the claimed invention which allows for the data management system to "operate in the background" while a user continues browsing the web. *See, e.g.*, EX. 1001 at 12:31-38. As discussed above, the '824 Patent maintains network access while preventing the collection of private user data. *See supra*, section III.

For at least these reasons, Petitioner fails to establish that Burns' IDS performs the determination in "real-time" as alleged. As such, all grounds fail and institution should be denied.

V. GROUND 2 BASED ON BURNS + YANG + WITTENBERG FAILS

Ground 2	Claims 1-16	§103 Burns + Yang + Wittenberg
----------	-------------	--------------------------------

Wittenberg is not related to improving network security as discussed in Burns and Yang. Wittenberg is instead directed at improving redirect services for Internet Service Providers (ISPs) and/or Content Providers, specifically by using a built-in redirect server rather than an external redirect server. *See, e.g.*, EX. 1007 at [0004].

For the same reasons discussed above with respect to Ground 1, Ground 2 also fails. Petitioner fails to establish that a POSITA would have been motivated to combine Burns and Yang, let alone to combine Burns, Yang, and Wittenberg. *See supra*, section IV.C. Additionally, Petitioner fails to establish that Burns and Yang disclose performing the determination in real time as recited in each of the independent claims. *See supra*, section IV.D.¹¹ Petitioner does not allege that Wittenberg cures any of the deficiencies discussed above with respect to Burns and Yang.

¹¹ Petitioner relies on its analysis of independent claim 17 for independent claims 1 and 9. Paper 2 at 53-54 (analyzing claim 1) and 67-68 (analyzing claim 9).

A. Summary of Wittenberg (EX. 1007)

Wittenberg discloses an intermediary, service selection network element that includes a built-in redirect server. EX. 1007 at [0016]. As shown in FIG. 2A of Wittenberg (reproduced below), element 201 receives a request, e.g., from computing device 204 to access service 209 provided by ISP 208 or service 211 provided by Content Provider 210. Wittenberg explains that ISPs and Content Providers increasingly seek to redirect certain requests to other sites, such as a Web portal, for some other purpose, such as billing. EX. 1007 at [0002], [0003].

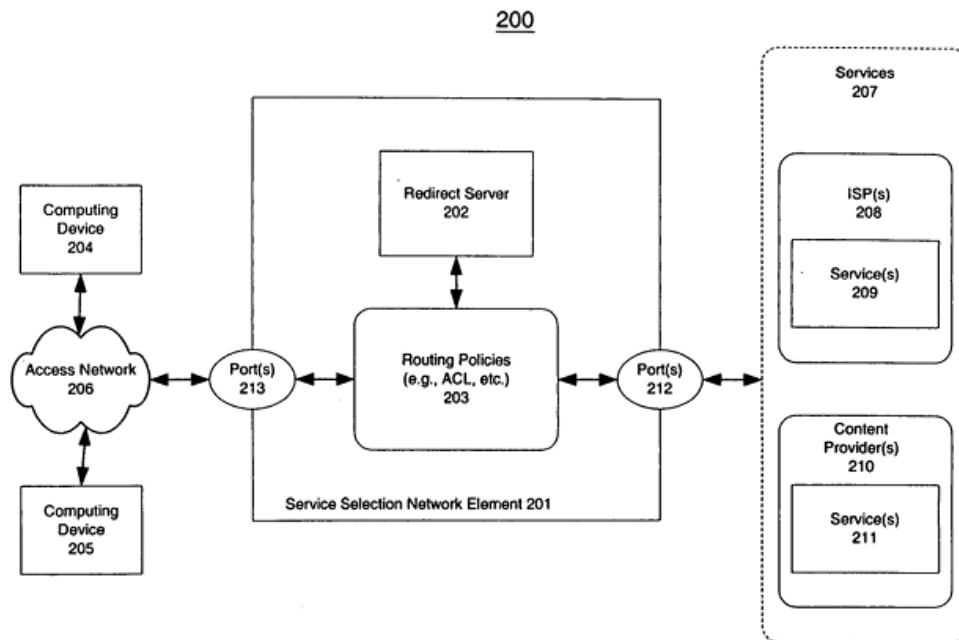


Fig. 2A

EX. 1007 at FIG. 2A.

Element 201 accesses one or more routing policies 203 to determine whether the request should be redirected to another destination. EX. 1007 at [0029], [0030].

If it is determined that the request should be redirected, the redirect server 202 may determine the redirect URL and return the redirect URL to the browser of the computing device. *Id.* The browser of the computing device may then use the redirect URL to access the redirect destination via element 201. *Id.*

B. Petitioner Fails to Establish that the Proposed Combination Discloses or Renders Obvious Claim Limitations [1.8] – [1.9]

1.8	modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference; and
1.9	maintaining communication between the remote server and the user's device, with sharing of the modified data packets.

Burns discloses that if a security risk is detected, the IDS will perform one or more actions defined by the administrator including (1) dropping the packets associated with the communication session, (2) automatically closing the communication session, and/or (3) throttling down the communication session. EX. 1005 at 7:47-51, 10:6-9. Petitioner alleges that each of these actions discloses or renders obvious claim limitations [1.8] – [1.9]. Paper 2 at 55; *see also* Paper 2 at 44-46 (analyzing claim 18 in Ground 1).¹² Patent Owner disagrees and submits that none of these actions satisfies the claim limitations as discussed below.

¹² Petitioner relies on its analysis of independent claim 1 for independent claim 9. Paper 2 at 67-68 (analyzing claim 9).

1. Petitioner’s allegations regarding dropping the packets associated with the communication session are incorrect and/or insufficient

Burns discloses: “In addition, stateful inspection engine 28 may take additional actions, such as dropping the packets associated with the communication session...” Paper 2 at 44 (citing EX. 1005 at 7:47-51). Petitioner alleges that Burns’ disclosure regarding “dropping” packets satisfies the “modifying” step of claim 1. Paper 2 at 45, 55. Petitioner does not address the “sharing” step of claim 1 in the petition itself. Paper 2 at 55. Petitioner cites only to the expert declaration.¹³ Overall, Petitioner’s allegations regarding “dropping the packets associated with the communication session” fail for at least three reasons.

First, Petitioner alleges that “dropping” packets in Burns discloses “blocking” packets as claimed¹⁴, however, Petitioner fails to establish that “dropping” is synonymous with “blocking” in the context of the ‘824 Patent. A POSITA would have understood “dropping” and “blocking” to have different meanings including for example whether the sender is notified. EX. 2026 at ¶56. At least because

¹³ Petitioner engaged in improper incorporation by reference for at least claim limitation [1.9]. Paper 2 at 55.

¹⁴ Petitioner points to the language of claim 8 of the ‘824 Patent to argue that “blocking” is a form of “modifying.” Paper 2 at 45.

Petitioner fails to address a POSITA's understanding of "dropping" versus "blocking," Petitioner fails to establish that the proposed combination satisfies the "modifying" step of claim 1.

Second, Burns discloses dropping **all** packets associated with a communication session if a security risk is detected. *See, e.g.*, EX. 1005 at 7:45-50. Thus, there is no "sharing" of the dropped packets. EX. 2026 at ¶57. Petitioner never even identifies the "modified data packets" that are allegedly shared. Paper 2 at 55.

Third, Petitioner incorporates by reference its expert's testimony, which alleges that logging information about the communication session satisfies the "sharing" step of claim 1. Paper 2 at 55; EX. 1003 at ¶ 193. This allegation fails for multiple reasons.

Burns discloses that "logging" means "security management module 44 records the source port, destination port, source IP address, destination IP address, time of discovery, packet size, a copy of the packet, other actions taken in response to the detection, or any other information that administrator 42 may find useful." EX. 1005 at 20:60-65. Logging this information, even including a copy of the packet, does not satisfy sharing the modified communication as claimed. EX. 2026 at ¶59. The logged copy of the packet would not be "modified" in any way. *Id.*

Additionally, the logging is performed by security management module 44 which is part of IDS 20. *See, e.g.*, EX. 1005 at FIG. 2. Therefore, there is no sharing by IDS 20, the alleged remote server. EX. 2026 at ¶60.

As discussed above, Burns and the ‘824 Patent are directed at different problems and therefore have different solutions. *See supra*, section III. While Burns is focused on preventing network access, the ‘824 Patent is focused on maintaining network access while protecting private user data. For example, the ‘824 Patent makes clear that the communication may comprise, e.g., 10 packets, and only one of those 10 packets may be modified to change the location. The modified communication may then be shared with the web server.

For at least these reasons, Petitioner fails to establish that Burns’ IDS “dropping the packets associated with the communication session” renders obvious claim 1. As such, Ground 2 fails and institution should be denied.

2. Petitioner’s allegations regarding automatically closing the communication session are incorrect and/or insufficient

Burns discloses: “In addition, stateful inspection engine 28 may take additional actions, such as ... automatically closing the communication session...” Paper 2 at 44 (citing EX. 1005 at 7:47-51). Petitioner alleges that Burns discloses automatically closing the communication session and that it would have been obvious to set a FIN flag value in the TCP Header in order to do so. Paper 2 at 45,

55. Petitioner’s allegations regarding “automatically closing the communication session” fail for at least four reasons.

First, Petitioner is using hindsight bias in its analysis of claim 1. It is impermissible to use the claim language as a road map. A POSITA reading Burns would not be motivated to set a FIN flag value in the TCP Header in order to close the communication session in response to a detected security risk. EX. 2026 at ¶63. The use of a FIN flag is for mutually terminating a connection when there is no more data to transmit. *Id.* A POSITA would not use a FIN flag to close a connection with an attacker. *Id.*

As explained by Tanenbaum:

“To release a connection, either party can send a TCP segment with the *FIN* bit set, which means that it has no more data to transmit. When the *FIN* is acknowledged, that direction is shut down. Data may continue to flow indefinitely in the other direction, however. When both directions have been shut down, the connection is released. Normally, four TCP segments are needed to release a connection, one *FIN* and one *ACK* for each direction. However, it is possible for the first *ACK* and the second *FIN* to be contained in the same segment, reducing the total count to three.”

EX. 1012 at 530.

In the context of Burns, an attacker would never acknowledge the first FIN and an attacker would never send a second FIN. EX. 2026 at ¶64. Even if an attacker received the first FIN, the attacker may continue to send unwanted/malicious packets. *Id.*

Second, sending a first FIN does not “automatically” close the communication session because there is a handshaking process that must be completed. EX. 2026 at ¶64. As discussed above, four or at minimum three TCP segments must be exchanged to close a connection. EX. 1012 at 530.

Third, Petitioner makes no argument that modifying the TCP Header to accomplish automatically closing the communication session is inherently disclosed in Burns. The Federal Circuit has made clear that inherency “may not be established by probabilities or possibilities.” *Par Pharm. v. TWI Pharm., Inc.*, 773 F.3d 1186, 1195 (Fed. Cir. 2014). Patent Owner submits that modifying the TCP Header, let alone setting a FIN flag value in the TCP Header, to accomplish automatically closing the communication session is **not** inherently disclosed in Burns, Yang, or Wittenberg.

Fourth, Petitioner makes no argument as to why a POSITA would have been motivated to set a FIN flag value in the TCP Header, specifically, to accomplish automatically closing the communication session. *See Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) (“[O]bviousness concerns whether a skilled artisan not only *could have made* but *would have been motivated to make* the combinations or modifications of prior art to arrive at the claimed invention.”). Petitioner is using hindsight bias. Patent Owner submits that a POSITA would **not** have been motivated to set a FIN flag value in the TCP Header to accomplish

automatically closing the communication session. Regardless, Petitioner fails to meet its burden to establish otherwise.

Patent Owner does not dispute that “[a] POSITA would have been familiar with techniques for closing a communication session.” Paper 2 at 45. However, there are many techniques to accomplish this goal. For example, a POSITA may close the socket thereby terminating the associated connection. EX. 2026 at ¶65. As another example, a POSITA may drop all packets associated with the connection which would eventually cause the connection to time out and close. *Id.*

Petitioner fails to explain why a POSITA would have been motivated to modify the FIN flag value in a TCP Header, specifically, and Petitioner fails to explain “any advantages that would flow from doing so”. *Virtek Vision Int’l ULC v. Assembly Guidance Sys.*, 97 F.4th 882, 887 (Fed. Cir. 2024). “It does not suffice to simply be known.” *Id.* at 888.

Unlike in *KSR*, there is no argument about the mere application of common sense, there is not a finite number of identified, predictable solutions, and there is no evidence of a design need or market pressure that suggests a POSITA would accomplish automatically closing the communication session as proposed by Petitioner. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 421 (2007).

For at least these reasons, Petitioner fails to establish that Burns' IDS "automatically closing the communication session" renders obvious claim 1. As such, Ground 2 fails and institution should be denied.

3. Petitioner's allegations regarding throttling down the communication session are incorrect and/or insufficient

Burns discloses: "Administrator 42 may also configure IDS 20 to throttle down (i.e., bandwidth limit) the communication session associated with the packets to minimize the bandwidth used by the communication session." Paper 2 at 45 (citing EX. 1005 at 10:6-9). Petitioner alleges that Burns discloses throttling down the communication session and that it would have been obvious to modify the "TCP congestion window size" in a TCP Header in order to do so. Paper 2 at 46, 55. Petitioner's allegations regarding "throttling down the communication session" fail for at least three reasons.

First, Petitioner confuses "TCP reception window size" and "TCP congestion window size".¹⁵ As discussed below, the "TCP congestion window size" is not advertised or otherwise included in a TCP Header.

¹⁵ Petitioner refers to "TCP congestion window size" in analyzing claim limitation [18.3] in Ground 1. Paper 2 at 46. Petitioner also refers to "TCP congestion window size" in Material Fact #4. Paper 2 at 15.

When Petitioner uses the phrase “TCP reception window size,” Petitioner appears to be referring to the window size specified by the receiver and advertised to the sender. EX. 2026 at ¶66; EX. 1012, Tanenbaum, at 536-537. The “TCP reception window size” is advertised by the receiver to the sender in a TCP Header. EX. 1011, RFC 793, at 15 (Figure 3 showing TCP Header Format). This advertisement prevents buffer overflow at the receiver. EX. 1011 at 42; EX. 1012 at 536-537. As further explained by Tanenbaum, there may still be problems due to internal network congestion that need to be addressed by TCP congestion control algorithms. *Id.* To avoid problems related to receiver capacity and network capacity, the sender maintains two windows: (1) the window the receiver has advertised (rwnd) and (2) the congestion window (cwnd). *Id.*

In contrast to the “TCP reception window size”, Tanenbaum explains the slow start algorithm for the congestion window size (cwnd) as follows:

“When a connection is established, the sender initializes the congestion window to the size of the maximum segment in use on the connection. It then sends one maximum segment. If this segment is acknowledged before the timer goes off, it adds one segment's worth of bytes to the congestion window to make it two maximum size segments and sends two segments. As each of these segments is acknowledged, the congestion window is increased by one maximum segment size. When the congestion window is n segments, if all n are acknowledged on time, the congestion window is increased by the byte count corresponding to n segments. In effect, each burst successfully acknowledged doubles the congestion window. The congestion window keeps growing exponentially until either a timeout occurs or the receiver's window is reached.”

EX. 1012 at 538. The slow start algorithm is supported by all TCP implementations. *Id.* Tanenbaum also explains the use of a threshold parameter in the Internet congestion control algorithm, which stops exponential growth once the threshold is hit. *Id.*

Thus, the “TCP congestion window size” is maintained independently by the sender. EX. 2026 at ¶69. The “TCP congestion window size” is not advertised by the sender to the receiver in a TCP Header. *Id.* Petitioner fails to establish that a POSITA could have, or would have, modified the “TCP congestion window size” in a TCP Header to accomplish throttling down the communication session. As such, Petitioner fails to establish that the proposed combination renders obvious claim 1.

Second, Petitioner makes no argument that modifying the TCP Header to accomplish throttling down the communication session is inherently disclosed in Burns. The Federal Circuit has made clear that inherency “may not be established by probabilities or possibilities.” *Par Pharm. v. TWI Pharm., Inc.*, 773 F.3d 1186, 1195 (Fed. Cir. 2014). Patent Owner submits that modifying the TCP Header to accomplish throttling down the communication session is **not** inherently disclosed in Burns, Yang, or Wittenberg.

Third, assuming *arguendo* that Petitioner is suggesting a POSITA would have changed the “TCP reception window size;” Petitioner makes no argument as to why a POSITA would have been motivated to modify the “TCP reception window

size” in a TCP Header, specifically, to accomplish throttling down the communication session. *See Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) (“[O]bviousness concerns whether a skilled artisan not only *could have made* but *would have been motivated to make* the combinations or modifications of prior art to arrive at the claimed invention.”). Petitioner is using hindsight bias. Patent Owner submits that a POSITA would **not** have been motivated to change the “TCP reception window size” in the TCP Header to accomplish throttling down the communication session. Regardless, Petitioner fails to meet its burden to establish otherwise.

Patent Owner does not dispute that “[a] POSITA would have been familiar with techniques for throttling a communication session” Paper 2 at 46. However, there are many techniques to accomplish this goal. For example, a POSITA may impose a limit on the number of packets accepted in a certain timeframe. EX. 2026 at ¶70. This limit is enforced by not accepting the excess data. *Id.* As another example, a POSITA may slow down acknowledgements or send back false acknowledgements so that the sender must retransmit. *Id.* As yet another example, a POSITA may impose a limit on the number of packets sent/forwarded in a certain time frame. *Id.*

Petitioner fails to explain why a POSITA would have been motivated to modify the “TCP reception window size” specifically and Petitioner fails to explain

“any advantages that would flow from doing so”. *Virtek Vision Int’l ULC v. Assembly Guidance Sys.*, 97 F.4th 882, 887 (Fed. Cir. 2024). “It does not suffice to simply be known.” *Id.* at 888.

Unlike in *KSR*, there is no argument about the mere application of common sense, there is not a finite number of identified, predictable solutions, and there is no evidence of a design need or market pressure that suggests a POSITA would accomplish throttling down the communication session as proposed by Petitioner. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 421 (2007).

For at least these reasons, Petitioner fails to establish that Burns’ IDS “throttling down the communication session” renders obvious claim 1. As such, Ground 2 fails and institution should be denied.

VI. PATENT OWNER RESERVES ALL RIGHTS REGARDING SECONDARY CONSIDERATIONS OF NON-OBVIOUSNESS BASED ON THE PRACTICING PRODUCTS

At least as of the filing of the complaint in October 2024 in the parallel litigation, Petitioner was on notice of relevant practicing products. *See, e.g.*, EX. 1008 at ¶8 (“QPrivacy’s parent company and predecessor in interest in the [‘824 Patent and related ‘249 Patent] Privacy Rating Ltd. has launched multiple products including QPaudit, QPrules, and QPtrust, with customers across different markets and lines of business.”). The related website (qprivacy.com) is cited in the complaint and details the functionality of these products as well as provides patent marking.

Patent Owner has also made the source code available for inspection in the parallel litigation. Even so, Petitioner did not address secondary considerations of non-obviousness based on the practicing products in the petition.

Patent Owner reserves all rights regarding secondary considerations of non-obviousness based on the practicing products.

VII. CONCLUSION

For at least the reasons discussed herein, Patent Owner respectfully requests that institution be denied on the merits.

Respectfully submitted,

Date: August 12, 2025

By: /s/ Thomas M. Dunham
Thomas M. Dunham
Reg. No. 39,965

Cherian LLP
2001 L Street NW, Suite 650
Washington, D.C. 20036
(202) 838-1567

ATTORNEY FOR PATENT OWNER,
BRIGHT DATA LTD.

CERTIFICATE OF COMPLIANCE

Consistent with 37 C.F.R. § 42.24, this paper consists of no more than 14,000 words. In preparing this certificate, counsel has relied on the word count of the word-processing system used to prepare the paper (Microsoft Word).

Respectfully submitted,

Date: August 12, 2025

By: /s/ Thomas M. Dunham
Thomas M. Dunham
Reg. No. 39,965

Cherian LLP
2001 L Street NW, Suite 650
Washington, D.C. 20036
(202) 838-1567

ATTORNEY FOR PATENT OWNER,
BRIGHT DATA LTD.

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), the undersigned hereby certifies this paper and all exhibits thereto were served on the undersigned date via email, as authorized by Petitioner, at the following email addresses:

ipr.theo.foster@haynesboone.com

david.mcombs.ipr@haynesboone.com

calmann.clements.ipr@haynesboone.com

al.malecha.ipr@haynesboone.com

Respectfully submitted,

Date: August 12, 2025

By: /s/ Thomas M. Dunham
Thomas M. Dunham
Reg. No. 39,965

Cherian LLP
2001 L Street NW, Suite 650
Washington, D.C. 20036
(202) 838-1567

ATTORNEY FOR PATENT OWNER,
BRIGHT DATA LTD.