

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.

Petitioner

v.

BT AMERICAS INC.

Patent Owner.

Case IPR2023-00889
Patent 7,895,641

PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Level of Ordinary Skill in the Art.....	5
III.	DISCUSSION OF ASSERTED REFERENCES	5
IV.	Claim Construction	5
V.	The Prior Art Fails to Render the Challenged Claims Obvious	6
	A. Claims 1-25 are valid because Petitioner’s expert relies on stacked inferences to stitch Duvall and Chu together in a way that would never make sense to a POSA absent improper hindsight	6
	1. Petitioner’s expert first error is to assume that Duvall would be used for security.....	7
	2. Petitioner’s expert next errs by assuming Duvall would need “additional techniques” despite Duvall’s disclosure to the contrary.	9
	3. Petitioner’s expert assumes but never explains how Chu solves the problems he assumes exist with Duvall.....	10
	B. Duvall does not teach “analysis of the post-filtering residue” as claimed by Schneier because Duvall’s direct and deferred-actions are never applied to the same transmissions.	12
	1. Petitioner fundamentally misunderstands how Duvall’s filtering system operates.	12
	2. Petitioner reads Duvall without proper technical context and fails to recognize that Duvall operates on a sequence of transmissions, not the same transmissions.	15
	3. Petitioner ignores that Duvall’s direct-action filters, unlike its deferred-action filters, only operate on an open command.	17
	4. Petitioner fails to recognize that Duvall’s deferred-action filters cannot analyze the same transmissions filtered by direct-action filters because deferred-action filters only operate on transmission sent <i>through</i> an open TCP stream.....	19
	5. Petitioner’s expert’s imaginary version of Duvall is unsupported and technically wrong.	21

6. Duvall’s disclosure fails to disclose “analysis of post-filtering residue.”	24
C. Even under Petitioner’s Incorrect Interpretation of Duvall, Duvall fails to disclose “post-filtering residue.”	25
D. Petitioner never shows how Duvall-Chu selects, discards, or further analyzes “status data”	29
E. Petitioner never identifies an “analyst system,” as required by Claims 1-17	31
1. Under any reasonable construction, an “analyst system” must refer to a technological system used by analysts.....	31
2. Duvall-Chu does not include an “analyst system”.	33
F. Duvall-Chu is NOT “reasonably capable” of dynamic modification, as required by Claims 1-17.....	35
G. Petitioner fails to show how Duvall-Chu performs analysis in a SOC as part of the “ <i>identifying step</i> ” as required by Claim 6.....	38
H. Petitioner’s mapping of Claim 15 requires showing that the prior art performs the dynamic modification step of Limitation 1(e).....	40
I. Petitioner’s expert fails to consider the technical realities of Trcka’s implementation when examining Claims 7-16	41
1. Trcka does not teach the type of analysis techniques that Petitioner suggests a POSA would be motivated to incorporate..	41
2. Petitioner fails to explain <i>how</i> Trcka’s analysis could be technically incorporated into different parts of Duvall-Chu.	43
J. Petitioner’s Duvall-Chu-Trcka-Ziese combination requires an initial modification to Duvall-Chu-Trcka that Petitioner failed to consider.	50
1. Petitioner’s motivation to combine Ziese requires Duvall to be modified to use multiple servers contrary to Duvall’s own disclosure.	51
2. Petitioner never provides any motivation for modifying Duvall to use multiple servers.	53

K. Petitioner’s expert’s opinion regarding Duvall-Chu-Cogger in connection with Claims 18-25 is unsupported by evidence	54
1. Petitioner’s expert provides no evidence that a POSA could implement Cogger’s CSM.	55
2. Petitioner’s expert provides no evidence that the information in Cogger’s “problem tickets” could be generated.	58
VI. Secondary Considerations Indicate the Challenged Claims were Not Obvious	60
A. There is a nexus between the evidence of non-obviousness and Schneier’s claims.....	61
B. Counterpane MSM met a long-felt but unresolved need.	62
C. Industry Praise and Commercial Success of Counterpane MSM.....	63
VII. CONCLUSION.....	65
WORD COUNT CERTIFICATION	66
CERTIFICATE OF SERVICE	67

LIST OF EXHIBITS

Petitioner's Exhibits	
1001	U.S. Patent No. 7,895,641 to Schneier <i>et al.</i> (“’641 patent”)
1002	Prosecution History of U.S. Patent No. 7,895,641 (“Prosecution History”)
1003	Declaration of Dr. Kevin Jeffay in Support of Petition for <i>Inter Partes</i> Review of U.S. Patent No. 7,895,641 (“Jeffay Declaration”)
1004	U.S. Patent No. 5,884,033 to Duvall <i>et al.</i> (“Duvall”)
1005	Yang-hua Chu, “Trust Management for the World Wide Web, M.I.T. (June 13, 1997) (“Chu”)
1006	U.S. Patent No. 5,970,149 to Johnson (“Johnson”)
1007	U.S. Patent No. 6,088,804 to Hill <i>et al.</i> (“Hill”)
1008	Lane B. Warshaw <i>et al.</i> , “VenusIDS: An Active Database Component for Intrusion Detection,” Applied Research Laboratories / Department of Computer Sciences, The University of Texas at Austin, Annual Computer Security Application Conference (1999) (“Warshaw”)
1009	U.S. Patent No. 6,704,874 to Porras <i>et al.</i> (“Porras”)
1010	U.S. Patent No. 7,159,237 to Schneier <i>et al.</i> (“’237 patent”)
1011	<i>Fortinet Inc. v. BT Americas, Inc.</i> , IPR2019-01324, Paper 9 (Institution Decision) (P.T.A.B. Jan. 7, 2020)
1012	<i>British Telecommunications PLC v. Fortinet, Inc.</i> , Civil Action No. 18-1018, Memorandum Order re: Claim Construction (D. Del. Aug. 5, 2021)
1013	<i>British Telecommunications PLC v. Fortinet, Inc.</i> , Civil Action No. 18-1018, Claim Construction Order (Aug. 18, 2021 D. Del.)
1014	U.S. Patent Pub. No. 2001/0039579 to Trcka <i>et al.</i> (“Trcka”)
1015	U.S. Patent No. 6,484,315 to Ziese (“Ziese”)
1016	<i>British Telecommunications PLC v. Fortinet, Inc.</i> , Civil Action No. 18-1018, Dkt. No. 161 (D. Del. Dec. 31, 2021)
1017	Prosecution History of U.S. Patent No. 7,159,237 (“’237 Prosecution History”)
1018	Declaration of Dr. James L. Mullins regarding the authenticity and public accessibility of Chu
1019	Curriculum Vitae of Dr. James L. Mullins
1020	DSpace@MIT Listing for Chu, available at https://dspace.mit.edu/handle/1721.1/43534
1021	OPAC Listing for Chu showing availability at Barker Library

1022	MARC Record for Chu
1023	OPAC MIT Libraries search for “trust management”
1024	WorldCat Listing for Chu, available at https://www.worldcat.org/title/trust-management-for-the-world-wide-web/oclc/38271519&referer=brief_results
1025	WorldCat search for “trust management world wide web,” available at https://search.worldcat.org/search?q=k%3Atrust+management+world+wide+web&qt=results_page#%2528x0%253Abook%2Bx4%253Athisis%2529for%E2%80%A6
1026	Sinrod et al., “ <i>Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws</i> ,” Santa Clara High Technology Law Journal (January 2000)
1027	Guttman et al., “ <i>Implementing Internet Firewall Security Policy</i> ,” National Institute of Standards and Technology (April 13, 1998)
1028	Rothfuss et al., “ <i>Go Ahead, Visit Those Websites, You Can’t Get Hurt ... Can You?</i> ,” Lawrence Livermore National Laboratory (June 3, 1997)
1029	Capture of Merriam Webster definition of “empirical,” www.merriam-webster.com/dictionary/empirical
1030	Coates, et al., “ <i>Melissa Virus Exposes High-Tech Vulnerability</i> ,” Chicago Tribune (March 30, 1999)
1031	Abie, “ <i>An Overview of Firewall Technologies</i> ,” Norwegian Computing Center (January 2000)
1032	Curriculum Vitae of Kevin Jeffay, Ph.D.
1033	U.S. Patent No. 6,859,783 to Cogger <i>et al.</i> (“Cogger”)
1034	<i>British Telecommunications PLC v. Fortinet, Inc.</i> , Civil Action No. 18-1018, Claim Construction Report and Recommendation (Apr. 15, 2021 D. Del.)
1035	<i>British Telecommunications PLC & BT Americas, Inc. v. Palo Alto Networks, Inc.</i> , 14:22-cv-01538, Complaint (Nov. 28, 2022 D. Del.)
1036	U.S. Patent No. 6,775,657 to Baker (“Baker”)
1037	Escamilla, T., “ <i>Intrusion Detection: Network Security Beyond the Firewall</i> ,” Wiley Press, 263-281 (1998) (excerpt)
1038	U.S. Patent No. 5,261,044 to Dev <i>et al.</i> (“Dev”)
1039	U.S. Patent No. 5,768,501 to Lewis (“Lewis”)
Patent Owner’s Exhibits	
2001	Declaration of Wenke Lee
2002	Declaration of Bruce Schneier from IPR2019-01324
2003	Bruce Schneier’s Wikipedia

2004	John Callas' Wikipedia
2005	Jeffay, et al., " <i>What TCP/IP Protocol Headers Can Tell Us About the Web</i> ," Proceedings of ACM SIGMETRICS 2001/Performance 2001 (June 2001)
2006	Stipulated Protective Order Confidentiality Agreement from Fortinet
2007	Deposition Transcript of Dr. Jeffay
2008	Bassham, et al, " <i>Threat Assessment of Malicious Code and External Attacks</i> ," NISTIR 4939, NIST (October 1992).
2009	Schneier, " <i>Counterpane and Managed Security Monitoring</i> ," Counterpane (April 2002)
2010	Markoff, " <i>Beyond Computers in Computer Security</i> ," The New York Times (April 2000)
2011	" <i>Counterpane Internet Security Delivers Industry's Most Comprehensive Managed Security Services</i> ," Help Net Security (August 2003)
2012	Woodie, " <i>Counterpane Brings OS/400 Into its Managed Security Fold</i> ," IT Jungle (March 2005)
2013	Pescatore, et al., " <i>2H01 Managed Security Service Provider Magic Quadrant</i> ", Gartner (February 2002)
2014	Hunt, et al., " <i>Market Overview: Managed Security Services</i> ," Giga Information Group (April 2001)
2015	Gonsalves, " <i>Watchful Eyes – Outsourcing event-log monitoring saves health insurer money and provides early warnings on network intruders</i> ," United Business Media
2016	Declaration of Wenke Lee in Support of Patent Owner's Response
2017	Sturgeon, " <i>BT snaps up Counterpane Internet Security</i> ," CNET (October 2006)
2018	Excerpts of Deposition Transcript of Kevin Jeffay
2019	" <i>The Shrinking Cost of a Megabit</i> ," NCTA – The Internet & Television Association (March 2019)
2020	Curriculum Vitae of Wenke Lee, Ph.D.

I. INTRODUCTION

The Board should uphold the validity of Claims 1-25 of U.S. Patent No. 7,895,641 (“Schneier”) because Petitioner’s 35 U.S.C. § 103 challenge is not based on the language or teachings of the asserted prior art. Rather, it is a house of cards, founded on layer upon layer of inferences made by Petitioner’s expert, in a manner completely divorced from the record. As Petitioner’s expert’s deposition revealed, he uses the teachings of Schneier and 20-20 hindsight to blur the line between the teachings of the prior art and what *could* have been done. Petitioner’s expert ignores the implementation details disclosed by each prior art reference—instead, substituting them with his own unsupported assumptions. And when pushed at his deposition to identify specific support for his rationale, Petitioner’s expert almost always conceded that the prior art did not disclose, either expressly or implicitly, the implementations he claimed in his declaration to be express. Instead of pointing to the teachings of the cited art, he simply concluded, using 20-20 hindsight, that a POSA could modify the prior art to arrive at the invention of Schneier. Indeed, when Petitioner’s expert was asked to identify support for his opinion that something was *disclosed* by a particular reference, he was unable to do so—at least twenty times. *See, e.g.*, EX2007, 48:3-11; 57:2-9; 61:18-62:13; 90:20-91:7; 98:14-99:11; 99:12-100:4; 100:6-101:8; 104:21-105:15; 123:8-124:4;

136:6-137:1; 147:4-147:12; 148:8-149:11; 151:2-152:3; 152:9-153:4; 158:11-160:1; 160:22-161:15; 165:14-166:11; 179:8-180:5; 192:13-193:6; 203:10-204:18.

In fact, some of these logical leaps actually contradict the express disclosure of the cited art. For example, Petitioner suggests that the primary Duvall reference discloses a problem that would motivate a POSA to look for the Chu reference. But Petitioner's expert admitted during deposition that Duvall already disclosed a solution to that problem, and that a POSA would understand that no further techniques were needed. *Compare*, EX1003, 107 (suggesting the problem of “filtering too much or too little” would have “motivated [a POSA] to seek additional techniques for more accurately resolving the status of residue data transmissions”), *with*, EX2007, 133:17-22 (“I think that—Duvall does not disclose that anything more than that is needed. And given the operation of Duvall, a [POSA] would understand that nothing more is needed.”).

In other words, Duvall already solved the problem of filtering too much or too little and thus provides no motivation to look for Chu. Indeed, modifying Duvall in the manner Chu discloses would defeat the very purpose of Duvall. In short, there is no motivation to combine Duvall with Chu, without which Petitioner's entire obviousness argument falls apart.

Petitioner and its expert also fundamentally misread the primary Duvall reference. Schneier requires filtering followed by an “analysis of post-filtering

residue,” which requires a subset of the same status data previously filtered (post-filtering residue) to be further analyzed. But Duvall never discloses applying its direct and deferred action filters to the same transmissions, which means that no residue is ever analyzed. Petitioner fails to recognize that Duvall’s direct-action filters in Figure 3 applies to *different* transmissions than those later analyzed by Duvall’s deferred-action filters in Figure 4. In other words, the deferred-action filters of Figure 4 are not analyzing any residue from the direct filters shown in Figure 3. As a result, rather than relying on Duvall’s actual disclosure, Petitioner’s expert concocts his own imaginary filtering system that fundamentally changes the way Duvall operates. Petitioner’s expert concedes that Duvall does not disclose many aspects of this imaginary implementation but insists they would nevertheless be obvious. In other words, Petitioner’s expert modifies Duvall’s system to read on Schneier’s claims without any basis besides his own belief that it would have been obvious to do so. Petitioner’s expert thus assumes as obvious, without any factual underpinning, the very limitations the patent examiner originally found to be non-obvious. *See* EX1002, 238 (finding “prior art does not disclose or suggest data neither discarded by negative or positive [filtering] is the residue that is sent for further analysis”). In accordance with a proper understanding of Duvall, Duvall fails to actually *disclose* the limitations Petitioner argues are disclosed by Duvall.

In addition to Petitioner's problems in assessing the scope and content of the relied-upon references, Petitioner's Duvall-Chu combination also suffers from additional flaws.. For example, Patent Owner addresses independent reasons why (1) Claims 1-25 are valid in Section V.D (Petitioner never explains how Duvall-Chu selects, discards, or analyzes "status data"); (2) Claims 1-17 are valid in Section V.E (Petitioner never identifies an "analyst system"); (3) Claim 6 is valid in Section V.G (Petitioner misreads the claim altogether); and Claim 15 is valid in Section V.H (Petitioner's mapping requires the system to perform dynamic modification when the Board already ruled that this is not disclosed by the cited prior art).

Should the Board even get to the point of needing to consider Petitioner's combinations of additional references with Duvall-Chu, Patent Owner also explains why these arguments are also fatally flawed. For example, Petitioner's expert fails entirely to "explain how specific references could be combined, which combination(s) of elements in specific references would yield a predictable result, or how any specific combination would operate." *ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.*, 694 F.3d 1312, 1327 (Fed. Cir. 2012). Again, Petitioner's expert's deposition has revealed that much of what Petitioner purports is *disclosed* by a reference is not, and that Petitioner's expert opinions lack factual

support and credible analysis. Petitioner's further reliance on Trcka, Ziese, and Cogger is thus also unavailing. *See* §§V.I-K, *infra*.

At base, Petitioner has failed to establish that the cited references and combinations invalidate any of Schneier's claims. Moreover, objective evidence of secondary considerations of non-obviousness further underscore the validity of the challenged claims. *See* §VI, *infra*. The Board should confirm the patentability of Claims 1-25.

II. LEVEL OF ORDINARY SKILL IN THE ART

Patent Owner does not currently dispute Petitioner's characterization of the level of ordinary skill but reserves the right to do so in the future for this and/or other proceedings.

III. DISCUSSION OF ASSERTED REFERENCES

Petitioner does not separately provide a separate abstract discussion of each reference, but rather addresses relevant portions of each as part of the Argument sections.

IV. CLAIM CONSTRUCTION

In *inter partes* review proceedings, the words of the claim are given their ordinary and customary meaning as understood by persons of ordinary skill in the art at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-13 (Fed. Cir. 2005) (en banc); 37 C.F.R. 42.100(b); 83 Fed. Reg. 197 (Oct. 11, 2018).

As noted in the Petition, certain claim constructions from the *Fortinet* Litigation (terms previously construed or agreed upon constructions) are relevant to these proceedings. These terms include:

Claim Term	Construction
“post-filtering residue, wherein the postfiltering residue is data neither discarded nor selected by filtering”	“status data that undergoes negative and positive filtering, but is neither discarded by such negative filtering nor selected by such positive filtering”
“dynamically”	“during actual operation, rather than offline”

EX1013, 1-4. Petitioner misapplies Patent Owner’s constructions, including the prior *Fortinet* Court’s constructions, regarding “post-filtering residue” and “analyst system.”

Despite Petitioners’ misapplication of those constructions, the Board can resolve the controversy in favor of Patent Owner without ever addressing these constructions. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). Thus, Patent Owner only addresses these constructions where they are directly pertinent to certain of Patent Owner’s arguments or to otherwise preserve Patent Owner’s positions. *See V.C and V.E, infra.*

V. THE PRIOR ART FAILS TO RENDER THE CHALLENGED CLAIMS OBVIOUS

A. Claims 1-25 are valid because Petitioner’s expert relies on stacked inferences to stitch Duvall and Chu together in a way that would never make

sense to a POSA absent improper hindsight

Petitioner, through its expert, stacks inference upon inference to create its asserted Duvall-Chu combination. But neither Duvall nor Chu discloses (expressly or implicitly) any of the problems, solutions, or motivations that Petitioner suggests would drive a POSA to combine Duvall with Chu.

By way of background, Duvall discloses a filtering system that allows a user to “filter material received over the Internet that is personally objectionable ... depending on that user’s individual tastes and sensitivities.” EX1004, 2:12-16. Duvall’s filtering system is implemented with “patching code” that modifies an operating system’s libraries. *See generally id.*, 9:14-11:20. Duvall “monitors [] ports and maintains internal tables that indicate the state of each active TCP data stream.” *Id.*, 3:59-61. Duvall applies direct-action filters to transmissions that open a TCP connection as shown in Figure 3. *Id.*, 4:38-42; 6:14-18. And Duvall applies deferred-action filters to different transmissions sent through an “open TCP/IP connection” as shown in Figure 4. *Id.*, 5:19-29. Duvall’s filtering system also includes an editing manager that allows its filters to be edited. *Id.* 8:2-16.

1. Petitioner’s expert first error is to assume that Duvall would be used for security.

Petitioner’s expert first suggests a “POSA would have understood that such objectionable material [blocked by Duvall] often presented further security risks,”

and that by “securing the client computer against objectionable materials, Duvall’s system also secures the client computer against receiving viruses, worms, malware, etc. associated with the objectionable materials.” EX1004, ¶117. But Petitioner’s expert only observes a matter of coincidence that, in certain cases, objectionable material may also pose a security risk. See *id.*; EX2016, ¶35. Petitioner and its expert provide no evidence of any actual correlation between objectionable materials and security risks. See EX2007, 45:2-12. On the contrary, Petitioner ignores that non-objectionable material is equally (or even more likely) to raise security concerns. See EX2016, ¶37; see also EX2008, 7-8 (discussing malware spread through non-objectionable materials like digital Christmas cards). Indeed, Petitioner’s expert failed to identify any portion of Duvall that discusses computer security, and his testimony made clear that he has no expertise on this issue. EX2007, 61:18-62:5; 69:5-8 (responding he “[has not] seen any studies ...[and] that[] [it is] going to be a function of when you’re doing that study” when asked about “the detection of indecent content, as a statistical matter ... [in relation to] a security-related event”).

And although Petitioner mentions “illegal material,” Petitioner’s expert confirmed that Duvall’s discussion is about the Communications Decency Act—and not any bona fide *security* risk. EX2007, 42:12-17. Unless the word “potentially” in “potentially security-related events” is improperly interpreted so

broadly as to lack all meaning, this assumption cannot stand. See *Stumbo v. Eastman Outdoors, Inc.*, 508 F.3d 1358, 1362 (Fed. Cir. 2007) (denouncing constructions rendering phrases superfluous), *see also Bicon Inc. v. Straumann Co.*, 441 F.3d 945, 950 (Fed. Cir. 2006) (“claims are interpreted with an eye toward giving effect to all terms in the claim”). Petitioner’s suggested link between objectionable/illegal material and security thus fails, both in the context of Duvall and as a general, empirically-verifiable fact.

2. Petitioner’s expert next errs by assuming Duvall would need “additional techniques” despite Duvall’s disclosure to the contrary.

Petitioner’s expert also assumes that Duvall has an unresolved problem with “filtering too much or too little.” *See, e.g.*, EX1003, 107. According to Petitioner’s expert, this is why a POSA would be motivated to look for Chu. *See id.*, 107. But this assumption is undermined by the fact that Duvall explicitly discloses that a “user [can] make custom changes” using the editing manager to resolve that very problem. EX1004, 8:6-7. In fact, when pressed at his deposition, Petitioner’s expert admitted that “Duvall does not disclose that anything more than that is needed[] [a]nd given the operation of Duvall, a [POSA] would understand that nothing more is needed.” EX2007, 133:10-22 (responding to question asking whether “Duvall recognize[d] the need for any additional techniques to address the problem of filtering too much or too little beyond the disclosed editing manager”).

There is thus no motivation to look for Chu absent improper hindsight. Petitioner's expert's admission directly contradicts Petitioner's motivation for combination. *Compare*, EX1003, 107 (suggesting the problem of “filtering too much or too little” would have “motivated [a POSA] to seek additional techniques for more accurately resolving the status of residue data transmissions”), *with*, EX2007, 133:17-22 (“I think that—Duvall does not disclose that anything more than that is needed. And given the operation of Duvall, a [POSA] would understand that nothing more is needed.”).

3. Petitioner's expert assumes but never explains how Chu solves the problems he assumes exist with Duvall.

Chu discloses nothing to resolve the singular problem of “filtering too much or too little” that Petitioner surmised. After creating this fictional problem with Duval (which Petitioner's expert conceded at his deposition does not exist), Petitioner relies solely on Chu's mention of the words “human intervention” to infer something far more complex than what Chu discloses. Pet., 21, 38; EX1003, ¶¶83, 110, 142.

By way of background, Chu is a thesis that discloses a trust management system that runs on a client computer. EX1005, 34; EX2016, ¶27. Petitioner relies primarily on a single sample policy disclosed by Chu. Pet., 20-21. This sample policy uses a block list and allow list of URLs to determine whether an attempt to

download a file should be permitted. EX1005, 44. If the URL is on neither list, Chu's policy returns "unknown," which prompts the user that was trying to download the file. *Id.*; EX2016, ¶28.

But Petitioner's expert concludes that Chu teaches "providing information to a human for analysis." EX1003, ¶114. This characterization of Chu is wrong. EX2016, ¶46. Chu does not prompt "any human"—Chu only prompts the same user that was originally trying to download the file. *Id.* Importantly, Chu's prompted user likely has less expertise than whoever has the authority to edit Duvall's filters. EX2016, ¶48. Chu's user is just a generic person trying to download files from the Internet. *Id.* To the extent such a user would perform any analysis, it is not the same type of analysis Petitioner attempts to introduce into Duvall's system. EX2016, ¶47. Yet, Petitioner's expert suggests modifying Duvall with Chu to prompt a user with special expertise who can also edit Duvall's filters. EX1003, ¶¶110-114, 142-144. This modification is neither taught, nor suggested, by Chu. *See* EX2016, ¶46-54. Indeed, Petitioner's expert acknowledges in the context of Duvall that "allowing the user who is trying to access illicit content to edit the filters would defeat the purpose of the filtering system." EX1003, ¶143. Yet this is precisely what Chu teaches. EX2016, ¶50.

A POSA would never modify Duvall based on Chu’s disclosure as Petitioner’s expert suggests.

B. Duvall does not teach “analysis of the post-filtering residue” as claimed by Schneier because Duvall’s direct and deferred-actions are never applied to the same transmissions.

Both independent claims of Schneier require “filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is neither discarded nor selected by filtering.” Schneier requires further analysis of a subset of the *same* status data that was previously filtered (i.e., “post-filtering residue”). Petitioner mistakenly suggests that Duvall satisfies this limitation by sequentially applying direct and deferred actions to the *same* transmission when that is never disclosed by Duvall. *See* EX1003, ¶¶129-136; *see also id.*, ¶¶103-105; ¶¶76-77. A POSA would not read Duvall in this manner. EX2016, ¶55-57. Duvall’s direct and deferred actions filters look at different transmissions. EX2016, ¶58-77.

1. Petitioner fundamentally misunderstands how Duvall’s filtering system operates.

Duvall discloses applying direct-action filters to transmissions that open a TCP connection while using deferred-action filters to analyze *different*, subsequent transmissions—through the now-opened TCP connection. *See infra* V.B(3). In other words, Duvall does not teach any “analysis of post-filtering residue.” *Cf.* EX1001, cl. 1. This is true regardless of whether Petitioner is relying on the client-

side or server embodiment. *See* EX1004, 8:23-27 (explaining both “version[s] of the filtering system use[] the same type of filter database”). Indeed, the key difference between the embodiments is just the location of the database. *See id*; EX2016, ¶¶61.

Crucially, Petitioner fails to recognize that Figures 3 and 4 of Duvall are disclosed as applying to entirely different transmissions within a disclosed sequence of transmissions. In fact, Petitioner does not appreciate that Duvall actually discloses operating on a *sequence* of transmissions. EX1004, 6:10-28; EX2016, ¶¶58; *see also* EX2007, 102:5-18. Instead, Petitioner relies on general high-level statements to mistakenly suggest that the additional criteria in Duvall’s deferred action filters are used to analyze the *same* transmissions previously filtered by Duvall’s direct-action filters. *See* EX1003, ¶¶129-136; *see also id.*, ¶¶76-77. Indeed, Petitioner’s expert refers to “data transmissions” throughout his declaration, without ever specifying exactly which transmission he is talking about. *See e.g.*, EX1003, ¶¶103-106.

As a result, Petitioner incorrectly presents Figures 3 and 4 as if they were both applied to the same transmission. Pet., 16-19, 32-35. But even a cursory examination of Duvall’s written disclosure directly contradicts such a reading. Although the direct-action filters are disclosed as being applied first; they are *never* disclosed as being applied to the same transmission that the deferred-action

filters later analyze. *See* EX2016, ¶¶58-77. Nor does Duvall ever teach or disclose that a single transmission is analyzed according to both processes shown in Figures 3 (direct-action filters) and 4 (deferred-action filters). *See id.* Rather the process shown in Figure 3 applies to transmissions opening a TCP stream, *see infra* V.B(3), while the process shown in Figure 4 applies to different transmissions sent *through* the opened stream, *see infra* V.B(4). *See* EX2016, ¶¶83-94. Neither process is disclosed as being applied directly to the same transmission. *See id.* This is a critical distinction that Petitioner and its expert completely miss, or worse, deliberately ignore.

Petitioner's interpretation of Duvall is thus irreconcilable with Duvall's express disclosure of its operations. Petitioner cannot simply ignore the teachings of Duvall that do not favor Petitioner's argument to manufacture an invalidating reference, especially when a POSA would not understand Duvall in this way. Indeed, Petitioner's expert's deposition also revealed that he mistakenly treats Duvall's system as a packet inspection tool, even though Duvall never mentions packets. But as discussed, *infra* V.B(5), this imagined version of Duvall that performs packet inspection rather than analyzing application-level traffic is never disclosed and results in a system with superfluous and/or inoperable processing steps. EX2016, ¶¶95-105.

2. **Petitioner reads Duvall without proper technical context and fails to recognize that Duvall operates on a sequence of transmissions, not the same transmissions.**

To understand why the direct and deferred action filters operate on different transmissions, Duvall must be read with the technical context that a POSA would have when reading Duvall. Though Duvall itself provides this technical context, Petitioner and its expert ignore it entirely. Indeed, Petitioner's expert fails to recognize the interplay between the TCP/IP protocol and Duvall's filtering system, which is vital to properly understanding Duvall's disclosure and system.

Duvall itself recognizes the importance of understanding TCP/IP and repeatedly refers to aspects of this protocol throughout the specification. *See, e.g.*, EX1004, 2:42-3:19. For example, Duvall provides that “[m]essages [that] are transmitted over the Internet ... with a transport protocol known as ... TCP/IP,” and “higher level network protocols, including ... HTTP,” which sit on top of TCP/IP. EX1004, 2:42-48.¹ And Duvall's filtering system is always discussed in the context of TCP/IP or associated higher level protocols. *See, e.g.*, EX1004, 3:59-61 (explaining its “client monitors [] ports and maintains internal tables that

¹ The higher-level protocols Duvall discusses still rely on TCP/IP to transmit information. However, the data sent through a TCP connection may be formatted in accordance with higher-level protocols, such as HTTP.

indicate the state of each active *TCP data stream*” (emphasis added)); *see also* EX2016, ¶¶63, 73 (explaining a POSA would understand that the Winsock API disclosed by Duvall is used by the operating system to implement the TCP/IP protocol). Thus, Duvall’s disclosure can only be properly understood when read in the context of TCP/IP and these higher-level protocols.

Crucially, a POSA would know that the TCP/IP protocol is a connection-based protocol and would recognize that Duvall’s invention is designed to work specifically on connection-based protocols. EX2016, ¶70. Duvall’s system requires that the client must first open a TCP connection *before* any content can be transmitted or received over that connection. EX2016, ¶71. Indeed, this sequence of transmissions is expressly acknowledged by Duvall. *See* EX1004, 2:58-60 (recognizing “[t]o initiate communications with another computer ... a computer [must] open[] a port in its interface for a TCP data stream.”); *id.*, 3:18-19 (“client opens a TCP data stream and uses this IP address to communicate with the other computer”); *see generally id.*, 6:14-28.

And indeed, Duvall itself distinguishes between transmissions for opening a stream and transmitting messages through the stream. *See, e.g., id.*, 4:63-64 (separating “tr[ying] to open the stream [from] send[ing] the message”). The transmissions *opening* the TCP data stream (*i.e.*, the open command) must be sent before any subsequent transmissions can be sent or received *through* an established

TCP data stream (the GET command and associated response). EX2016, ¶74.

And Duvall's filtering system is specifically designed to block and allow transmissions with this context in mind. EX2016, ¶¶65-76.

As further explained below, the steps of Duvall's Figure 3 never apply to the same transmissions that are analyzed according to Figure 4. And yet, Petitioner's and its expert's assertions are both entirely premised and dependent upon that mistaken assumption—that the steps in Figures 3 and 4 apply to the same transmissions.

3. **Petitioner ignores that Duvall's direct-action filters, unlike its deferred-action filters, only operate on an open command.**

Petitioner ignores that Duvall's direct-action filters only operate on an open command, unlike Duvall's deferred-action filters, which only operate on subsequent transmissions after such an open command has been executed.

Petitioner's expert generally opines that Duvall's direct-action "BLOCK filter blocks data transmission from passing through." *See* EX1003, ¶103; *see also id.*, ¶72 (emphasis added). But this overbroad statement avoids specifying *what* transmissions are being blocked or allowed and *how*. Specifically, Duvall's direct-action filters block messages sent to *open* a TCP stream by "preventing execution of an open command," which is "preferably accomplished by simply not executing the open command." *Compare*, EX1004, 1:37-40 (listing blocking options), *with*,

EX1004, 4:57-58 (describing blocking with direct-action filters). Petitioner's expert glosses over this detail in his declaration.

Duvall's direct-action filters only operate on transmissions for opening a TCP stream. EX2016, ¶¶78-79. Indeed, there is no disclosure of Duvall's direct-action filters being applied to transmissions sent or received *through* an already opened TCP stream. EX2016, ¶82. Duvall explains with respect to Figure 3 that its direct-action filters are applied when “the filtering system detects [that] the client opens the data stream for a particular port and IP address.” EX1004, 4:40-42. And Duvall explicitly discloses using direct-action filters to prevent execution of an “open command.” *See, e.g.*, EX1004, 4:57-58 (“blocking is preferably accomplished by simply not executing the open command”). The steps of Figure 3 are thus clearly directed to determining whether a stream should be opened by either preventing or permitting the execution of the open command. *See* EX1004, 4:38-61.

And this understanding is fully consistent with the remainder of Duvall's entire disclosure and technical background. EX2016, ¶78. Indeed, Duvall's example of how its system operates explicitly discloses matching its direct-action filters when “[t]he client *tries to open* a TCP/IP connection.” *Id.*, 6:14-16 (emphasis added). Duvall explains that if the “IP address and port ... are together in a BLOCK filter, the system prevents the data stream from opening.” *Id.*, 6:16-

18. Indeed, opening a TCP stream also only requires an IP address and port—which is precisely the only criteria considered by Duvall’s direct-action filters. EX2016, ¶79. This confirms that the steps of Figure 3 only comes into play when a TCP stream might be opened. EX2016, ¶¶80-81.

Furthermore, given Duvall’s disclosure of its patching code, a POSA would also understand that Figure 3 occurs when Duvall’s patching code intercepts the operating system’s execution of an open command to open the TCP data stream. EX2016, ¶80. This is further consistent with Duvall’s explanation that its direct-action filters can block “by simply not executing the open command.” EX1004, 4:57-58. And a POSA would recognize that this requires Duvall’s direct-action filters to be applied (*i.e.*, the process in Fig. 3) *before* such a command has finished executing. EX2016, ¶¶80-81. Accordingly, a POSA would also understand that Duvall’s direct-action filters could not be operating on any transmissions sent *through* a TCP stream, because such a TCP stream has yet to be opened. EX2016, ¶¶81.

4. **Petitioner fails to recognize that Duvall’s deferred-action filters cannot analyze the same transmissions filtered by direct-action filters because deferred-action filters only operate on transmission sent *through* an open TCP stream.**

Petitioner incorrectly suggests that the “data transmission that do not match the immediate ALLOW or BLOCK filters in step 104 are *further analyzed* ... [as]

shown by the example in FIG. 4.” EX1003, ¶105 (emphasis added). But the transmissions analyzed by Figure 4 were sent through an open TCP stream whereas in Figure 3 those TCP streams had yet to even be open. Thus, Figures 3 and 4 cannot operate on the same transmissions. Consequently, Duvall does not teach “analysis of post-filtering residue”.

Indeed, with respect to Figure 4, Duvall explicitly discloses that deferred-action filters are applied when “data is transmitted over an *open* TCP/IP connection.” EX1004, 5:19-20 (emphasis); *see also* EX1003, 5:19-20; EX2007, 103:17-19 (agreeing a POSA would “understand this to mean data that[] is transmitted after a TCP connection has been established”). Despite Duvall’s explicit discussion, when asked whether “Figure 4 can also apply before the TCP connection is opened” Petitioner’s expert insisted that “Figure 4 [could] apply to all forms of traffic.” *See* EX2007, 104:8-9. This is technical nonsense and Petitioner’s expert provides no evidence besides his say so. EX2016, ¶¶75.

On the contrary, only after a stream is opened can content even be transmitted through the opened stream. EX2016, ¶74. Duvall’s example describes sending a transmission with a “GET command” to request content from a server, and separately receiving a transmission that “respond[s] with [the] data for that [requested] directory.” EX1004, 6:19-27. Duvall discloses applying its deferred-action filters to these latter transmissions, which confirms that by Step 130 of

Duvall's Figure 4, the TCP stream must have been opened. EX2016, ¶¶91. The steps of Figure 4 are thus clearly directed to filtering the content sent and received through an open stream. *See* EX1004, 5:19-39. Petitioner's understanding of Duvall is directly contradicted by Duvall. EX2016, ¶¶87-94.

Likewise, Duvall never discloses applying the steps of Figure 4 to an open command. EX2016, ¶¶83. And indeed, that would make no technical sense as the open command will lack content relevant to the fields considered in Figure 4. *Id.* Rather, Figure 4 only applies to transmissions that transmit content through an already open stream, such as HTTP transmissions. *See* EX1004, 6:10-29 (sending HTTP request with a "GET command" and receiving HTTP response with the requested data). Thus, Duvall's deferred-action filters cannot perform the claimed "analysis of post-filtering residue" by operating in accordance with Duvall's Figure 4, as Petitioner's expert mistakenly suggests.

5. Petitioner's expert's imaginary version of Duvall is unsupported and technically wrong.

As Petitioner's expert's deposition revealed, Petitioner is relying on an imaginary implementation of Duvall, which operates differently from what is disclosed. Petitioner's expert is relying on an un-disclosed system that performs deep packet inspection to filter *packets* rather than the application-level transmissions as actually disclosed. *See* EX2007, 98:14-99:11 (suggesting Duvall

“look[s] at every packet”), 101:11-19. Such an implementation fundamentally alters how Duvall operates and is inconsistent with Duvall’s explicit disclosures.

Despite Duvall’s thorough disclosure of operating at the application level, Petitioner’s expert insists that Duvall implicitly applies both its direct and deferred-action filters to the same individual packets. *See, e.g.*, EX2007, 98:14-99:11, 101:22-102:18. But Duvall never discloses applying its filters to any packets at all let alone applying direct and deferred action filters to the same transmission. EX2016, ¶¶97. Further, Duvall provides no guidance on *how* deep packet inspection could ever be implemented. As Petitioner’s expert conceded, “at the time this concept of deep packet inspection was ... a new thing.” EX2007, 71:11-12.

Indeed, packet inspection makes no technical sense given Duvall operates directly on application data. EX2016, ¶¶98-99. As Petitioner’s expert explained, “Duvall is writing its disclosures in the context of the way that an application developer would view the network communications.” EX2007, 93:1-4; *see also* EX2016, ¶99. A POSA would therefore understand that Duvall’s filtering system also discusses “transmissions” from the point of view of an “application developer” rather equating them to network packets. *Id.*

Petitioner’s expert acknowledges that Duvall’s disclosure contemplates “creating a structure called a ‘socket’” as part of the “TCP connection

establishment process.” EX2007, 93:5-19. As Petitioner’s expert recognized, a “socket is viewed as a file” by the operating system. EX2007, 93:12-14; *see also* EX2016, ¶100. And once opened, you can read and write to the socket like you would a file. *See id.*; *see also* EX2007, 93:12-14. A POSA would recognize that reading and writing to the created socket is how Duvall’s client receives and sends transmissions through an open TCP data stream. EX2016, ¶101. Indeed, Duvall teaches a POSA that the Winsock library can be patched to run its filtering code, which a POSA would recognize occurs when it reads and writes from the socket. EX2016, ¶102.

In contrast, Duvall does not teach a POSA how to match keywords or filter patterns to individual packets. As Petitioner’s expert recognized, the deferred-action filter’s keyword and filter pattern analysis would need to be conducted “over multiple packets” rather than just individual packets. EX2007, 107:17-19; *see also* EX1004, 6:10-27, 5:66-67. For example, a single HTTP transmission may require multiple packets to send the data over the network. EX2016, ¶103. Matching a keyword and filter pattern across multiple packets is not a trivial task and Duvall never discloses how this could be accomplished. EX2016, ¶103.

Moreover, using Duvall’s deferred-action filter’s additional criteria to match with the actual packets sent to establish a TCP connection would be entirely pointless. Duvall’s direct-action filters can already filter based on an IP address

and port and Petitioner's own expert admits that the "connection establishment packet does not have a payload." EX2007, 94:15-16; *see also* EX2016, ¶104.

Therefore, matching keywords (*cf.* Fig. 4, 134) and filter patterns (*cf.* Fig. 4, 136) would be entirely pointless because there is no payload to match against. EX2016, ¶104.

Likewise, it would not make technical sense to force Duvall's direct-action filters to apply to packets in an already opened stream. EX2016, ¶105.

Notwithstanding Duvall's explicit disclosure that it blocks by "prevent[ing] the data stream from opening," (EX1004, 1:6:18), there is still no action Duvall's direct-action filters could reasonably take when matched with the packets in an open stream. EX2016, ¶105. The fact that a stream is even opened, can only mean that Duvall's direct-action filter either previously ALLOWED the stream to open, or there was no applicable direct-action filter (only deferred-action filters). *Id.* But if the stream was already opened with an ALLOW filter, then reapplying the filter to each packet in the stream would be entirely redundant and pointless. *Id.*

6. Duvall's disclosure fails to disclose "analysis of post-filtering residue."

Because the direct-action filter is never applied to the same transmission analyzed by a deferred-action filter, Duvall's deferred-action filters cannot analyze "post filtering residue" as the claimed residue of Schneier is what is left over after

the filters have already been applied. Indeed, the transmissions in Duvall that are analyzed by the deferred-action filters were *never* previously filtered, so they could not have been discarded or selected by filtering. *See* EX1001, cl. 1(b). And the Duvall’s actually filtered transmissions (by direct-action filters) must have been allowed by Duvall, as a condition precedent to applying any deferred-action filters to subsequent transmissions. EX2016, ¶¶106-108. Duvall clearly does not *disclose* “filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is neither discarded nor selected by filtering.” Thus, all claims of Schneier remain valid.

C. Even under Petitioner’s Incorrect Interpretation of Duvall, Duvall fails to disclose “post-filtering residue.”

A proper construction of “post-filtering residue” requires the filtering that creates the “post-filtering residue” to be distinct from the “analysis of post-filtering residue.” Arbitrarily dividing a single filtering subsystem that selects and discards status data cannot satisfy the requirements of limitation 1(b) with respect to “post-filtering residue.”

“Post-filtering residue” is status data that was processed by a filtering subsystem and was “neither discarded by such negative filtering nor selected by such positive filtering.” EX1013, 4. Schneier claims require a filtering process that selects and discards known interesting or uninteresting information (more

specifically, status data). Schneier explains that status data is selected and discarded through a filtering process performed by positive and negative filtering subsystems. EX1001, 8:51-55. Any leftover status data which has not been selected or discarded after this filtering process concludes is the “post-filtering residue.” *Id.* The claims require this residue to be further analyzed as part of a separate process. EX1001, cls. 1, 18 (claiming the discarding and selecting process which yields post-filtering residue and a separate analysis of the post-filtering residue).

Petitioner applies a construction of “post-filtering residue” that effectively eliminates any distinction between the filtering step that creates the residue and the analysis of that post-filtering residue. In the Institution Decision, the Board correctly looked to the claim language and specification to determine the meaning of “post-filtering residue.” Paper 10 at 11-12. But the Board concluded that Schneier’s specification and claims “do not support Patent Owner” because limitation 1(b) “does not preclude further filtering of the residue” and the specification describes additional analysis that may include filtering. *Id.* Respectfully, Patent Owner’s “construction *does not preclude any filtering in the residue analysis.*” Paper 8 at 2 (emphasis added).

Any subsequent filtering, however, must be part of a distinct analysis done on the status data that was neither discarded nor selected. For example, merely

applying more filters from Schneier’s positive and negative filtering subsystems clearly would not amount to “analysis of post-filtering residue.” *See* EX1001, 8:55-59 (distinguishing the positive and negative filtering subsystems that “form the ‘residue’” from the anomaly engine that analyzes it). Accordingly, Patent Owner’s construction does not preclude use of filters by Schneier’s anomaly engine but precludes any suggestion that filtering by Schneier’s positive and negative filtering subsystems could satisfy the “analyzing post-filtering residue” limitation. In other words, a distinction must be drawn between the filtering to select and discard status data yielding “post-filtering residue” and analyzing whether the remaining residue status data is a potentially security-related event (even if that analysis also uses filters).

According to Petitioner’s misreading of Duvall (putting aside its inaccuracy, as discussed above), Duvall’s direct and deferred-action filters are supposedly all applied to the same transmission. *See* EX1003, ¶105. If Petitioner is right about this (it is not) then Duvall’s direct and deferred-action filters would thus be part of a single subsystem that either blocks or allows each transmission. EX2016, ¶113. Duvall’s single filtering subsystem cannot be arbitrarily divided such that “post-filtering residue” is created halfway through Duvall’s ongoing, incomplete filtering process. *Id.*

Indeed, Petitioner's expert concludes that blocking is discarding and allowing is selecting. EX1003, ¶133. Thus, there is no basis for artificially breaking Duvall's system in half to suggest that only certain block/allow filters in Duvall's filtering subsystem select and discard, while the other filters (which also block and allow) are performing a *distinct* analysis. Indeed, Petitioner's expert suggests that Duvall's deferred-action filters satisfy the discarding step required in Claim 1, which relates to the filtering limitation rather than the residue-analysis. *See* EX1003, ¶133 (relying on Duvall's disclosure of its deferred-action filters "block[ing] ... by discarding" to suggest that Duvall's system discards data when blocking).

Nowhere do Schneier claims suggest that the post-filtering residue analysis could be performed by the same initial filtering subsystem; such an approach improperly collapses the two-step process of the claims into a single step. Rather, the claims specifically require the analysis to "*follow[]*" filtering and defines the remainder as "*post-filtering residue.*" *See* EX1001, cls. 1, 18 (emphasis added); *see Intel Corp. v. Qualcomm Inc.*, 21 F.4th 801, 810 (Fed. Cir. 2021) ("It is highly disfavored to construe terms in a way that renders them void, meaningless, or superfluous."); *see also Canopy Growth Corp. v. GW Pharma Ltd.*, No. 2022-1603, 2023 WL 3048243, at *4 (Fed. Cir. Apr. 24, 2023) (*quoting* Scalia & Garner,

Reading Law § 26, at 174) (“If possible, every word and every provision is to be given effect.”) (internal quotation marks omitted).

Indeed, a POSA reading Schneier understands that the claimed analysis that follows the filtering process “reduce[s] the immense volume of raw data into core information worthy of further analysis.” EX1001, 3:17-26. As such, a POSA understands that the analysis of post-filtering residue is a *different* process than merely selecting or discarding with positive and negative filters. *See* [Lee Dec]. Any proper construction of “post-filtering residue” must therefore acknowledge that the filtering of status data (to select or discard status data) is first completed prior to any subsequent analysis, regardless of whether that separate analysis also includes filtering. Duvall therefore fails to disclose “post-filtering residue.”

D. Petitioner never shows how Duvall-Chu selects, discards, or further analyzes “status data”

Under any interpretation of Duvall, Petitioner fails to demonstrate that Duvall-Chu selects, discards, or further analyzes “status data.” Notably, Petitioner never suggests that the agreed-upon construction of “post-filtering residue...” is incorrect or that it differs meaningfully from that term’s plain and ordinary meaning. *See* Pet., 31-35. And that agreed-upon construction of “post-filtering residue...” clearly requires “status data” to be selected and discarded. *See* EX1013 at 4. Moreover, the claimed “analysis of post-filtering residue” must further

analyze that residual “status data.” *See id.* Thus, according to Petitioner’s Duvall-Chu combination, (1) Duvall’s direct-action filters must select and discard status data, while (2) Duvall’s deferred-action filters must analyze residual status data. Yet Petitioner’s expert, whose conclusions are incorporated by Petitioner, overlooks both requirements by focusing on the traffic itself rather than status data. Pet., 32-34; EX1003, ¶133.

Petitioner’s expert merely contends that “data that is blocked is discarded data,” while “[d]ata that is allowed is selected data.” EX1003, ¶133. But the only data Duvall blocks and allows are the transmissions (*i.e.*, traffic) and not the status data. EX2016, ¶117. Petitioner’s expert never explains how selecting and discarding traffic is the same as selecting or discarding the status data. *See* EX1003, ¶133; *see also* EX2007, 116:21-188:18 (conceding he was unable to identify where he discussed selecting/discarding status data rather than traffic, but suggesting it was “clear from the context”); EX2016, ¶118. Indeed, selecting and discarding traffic without more is different than selecting or discarding status data. *See id.*

Petitioner’s expert also never even attempts to identify any “status data” that is being further analyzed by Duvall’s deferred-action filters. *See id.* Petitioner’s expert only argues that Duvall’s deferred-action filter analyzes the same traffic that was analyzed by Duvall’s direct-action filters. *See* EX1003, ¶¶129-136; *but see*,

supra V.B(1)-(4) (explaining that Duvall’s deferred, and direct-action filters analyze different transmissions). But neither Petitioner nor its expert ever discusses “status data” in relation to Duvall’s deferred-action filter. *See generally*, Pet., 32-34; EX1003, ¶133. As such, Petitioner fails to show how Duvall selects, discards, or further analyzes “status data” as required by Schneier’s independent claims.

E. Petitioner never identifies an “analyst system,” as required by Claims 1-17

1. Under any reasonable construction, an “analyst system” must refer to a technological system used by analysts.

Petitioner ignores the language of Claims 1-17 requiring an “analyst system.” The plain and ordinary meaning of an “analyst system” to POSA reading Schneier claims and specification requires a system usable by security analysts. An “analyst system”—within the confines of Schneier—cannot just be a group of analysts or the end-user. *Cf.* Pet., 39 (suggesting a “group of trained professionals ... is ‘an analyst system’”); *see also* EX1003, ¶143 (same). Rather, an “analyst system” denotes a technological system that is used by analysts.

Schneier Claim 1(c) recites: “a communications system coupled to transmit information about the identified events to an analyst system associated with the security monitoring system.” EX1001, cl. 1. The use of the term “analyst system” in this claim refers to a technological system capable of assisting an analyst in his

role. *See* EX1001, cl. 1; *see also id.* 2:43-46 (explaining an “analyst system” is used by “security analysts”).

When the claim terms are properly read within the context of Schneier specification, the confines of the term “analyst system” are made clear. Schneier specification explains how the security analyst, trained in network security, utilizes an analyst system, such as the disclosed SOCRATES system, to resolve potential incidents that are identified in claim limitation 1(b). *See* EX1001, 3:41-50, 4:4-5 (explaining “SOCRATES” stands for “Secure Operation Center Responsive Analyst Technical Expertise System”) (emphasis added). Schneier’s specification further describes how security analysts use SOCRATES “to categorize, prioritize, investigate and respond to customer incidents or ‘problems.’” *Id.*, 3:42-45, 7:24-30; *see also* 3:47-49 (SOCRATES’ use of “problem tickets”). Moreover, SOCRATES “provides security analysts at a SOC a single, integrated system with which to track information concerning, for example, problems, companies, people, contacts, tools, and installed network components and known vulnerabilities.” *Id.*, 9:56-62, 10:60-65.

While SOCRATES, including its specific functions and capabilities, is just a preferred embodiment, its description is still highly instructive. *See Phillips*, 415 F.3d at 1325 (looking to the specification to determine the “purposes served” by the disputed claim term).

2. Duvall-Chu does not include an “analyst system”.

Petitioner argues that the Duvall-Chu combination discloses an “analyst system.” Petitioner is wrong. As explained above, limitation 1(c) of Schneier requires “transmitting ... to an analyst system.” EX1001, cl. 1. Petitioner’s expert suggests that Duvall-Chu’s “human intervention would be performed by an analyst system.” EX1003, ¶142. But rather than explain where such a *system* comes from what it is, Petitioner’s expert only explains why Duvall-Chu would include an *analyst*. *See id.* (concluding “information about the unresolved residue data would be sent to a trained network analyst”); *see also, e.g.*, 143:18-144-20 (explaining the series of inferences required to reach an analyst system). But reference to an analyst does not itself teach or suggest an “analyst system.”

Moreover, Petitioner’s expert’s rationale for including an analyst is not even based on the references that form Petitioner’s statutory grounds, but instead on other references, which do not even form part of Petitioner’s grounds of unpatentability. *See id.*, ¶¶142-143 (citing EX1037-1039). Indeed, during his deposition, Petitioner’s expert was unable to identify which reference actually taught an analyst—let alone an analyst system—instead just concluding it would exist when Chu was combined with Duvall. *See* EX2007, 148:8-149:11; *see also* EX2007, 152:9-153:4 (conceding no “express disclosure” in Duvall, but suggesting it would be *obvious*). Regardless, none of those other references show that

transmitting to an analyst *system* would be *inherent* to Duvall-Chu. Nor does Petitioner's expert explain why it would be *obvious* to add an analyst *system* to Duvall-Chu, or how it could even be accomplished. Indeed, Petitioner relies on EX1037 as evidence that the state of the art included outsourcing. *See* EX1003, ¶143. But EX1037 provides no actual disclosure of *how* such outsourcing was accomplished, nor any disclosure of the systems used by the third parties. *See* EX1037, 224. The mere fact that outsourcing is possible does not mean that it would be either obvious or inherent to incorporate such undisclosed systems (presumably used by third-party analysts) into Duvall-Chu.

Even if Petitioner could show that Duvall-Chu included a group of analysts, there is still no disclosure of any analyst *system* used by those analysts. Absent any disclosure, it would not have been obvious to POSA what the "analyst system" is or how to implement it. EX2016, ¶127. Indeed, neither Duvall nor Chu even discloses a system that could receive transmissions (*i.e.*, prompt) sent from Duvall's probe. EX2016, ¶129; *but see* EX2007, 149:13-22 (suggesting the editing manager in Duvall-Chu is an analyst system). Petitioner cannot rely "on the combined teachings of Chu and Duvall to teach or suggest an analyst system," when neither reference teaches the necessary components of such a system. *Cf.*, Paper 10 at 31. During his deposition, Petitioner's expert appeared to argue that Duvall's editing manager would be an analyst system when combined with Chu.

EX2007, 149:13-22. But Duvall's editing manager is only capable of editing filters using known database techniques. EX1004, 8:11-12. And there is no disclosure of how such an editing manager could be modified into an analyst system capable of receiving any transmissions from a probe (as the claims require) or responding to any prompts (as required to satisfy Petitioner's motivation). EX2016, ¶130. Likewise, Chu merely displays a prompt on the device of the same user attempting to download the file. EX1005, 44. That end-user's device is not an "analyst system" under any proper construction of the term. *But see* Paper 10 at 32 (equating "end user/analyst system" (emphasis added)). Nor would Chu's prompted device be equivalent to Duvall's editing manager. EX2016, ¶¶130-133. Petitioner never identifies any analyst systems in the prior art capable of receiving whatever was transmitted by its probe. *See* EX1001, cl. 1(c).

F. Duvall-Chu is NOT "reasonably capable" of dynamic modification, as required by Claims 1-17

Petitioner does not sufficiently demonstrate that Duvall-Chu is "reasonably capable" of dynamic modification. Limitation 1(e) recites "a modification control system for dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback." EX1001, cl. 1. As noted by the Board, the term "for" is important as it implies the system need only be "reasonably capable" of doing so. Paper 10 at 38-40 (citing *ParkerVision, Inc. v.*

Qualcomm Inc., 903 F.3d 1354, 1361 (Fed. Cir. 2018)). In such situations, however, an invalidating reference must still contain some kind of disclosure to indicate that the claimed functionality would be carried out by the prior art at least some of the time. *See INVT SPE LLC v. ITC*, 46 F.4th 1361, 1375-76 (Fed. Cir. 2022); *see also Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F.3d 1201, 1217 (Fed. Cir. 2014) (finding reasonable capability where “the accused devices in fact identified the type of information ... only some of the time”); *Versata Software, Inc. v. SAP Am., Inc.*, 717 F.3d 1255, 1263 (Fed. Cir. 2013) (holding customers were expected to perform the claimed functionality); *Finjan, Inc. v. Secure Computing Corp.*, 626 F.3d 1354, 1366 (Fed. Cir. 2010) (concluding software was disclosed and existed, but not enabled, was “reasonably capable” of being enabled to meet the claimed invention).

Claim language that recites capabilities—such as “system for dynamically modifying”—cannot be stretched to include potential capabilities that are not disclosed and/or would require “significant alterations.” *See ParkerVision*, 903 F.3d at 1362. Moreover, “[i]n contexts involving software functionality,” the Federal Circuit “ha[s] never suggested that reasonable capability can be established without any evidence or undisputed knowledge of an instance that the accused product performs the claimed function when placed in operation.” *INVT SPE*, 46 F.4th at 1376 (emphasis in original). As such, any prior art reference

purporting to invalidate Claims 1-17 must have some indication in its disclosure that it actually does or would perform the claimed functionality.

Limitation 1(e) of Schneier requires a modification control system to either dynamically modify or be reasonably capable of dynamically modifying an analysis capability of the probe. EX1001, cl. 1. As the Board recognized, “Duvall does not explicitly disclose such a capability.” Paper 10, 42. Petitioner’s expert suggests “dynamic modification” would be inherent to Duvall’s system. *See* Pet., 42. But Duvall’s mere use of a database does not make its system inherently capable of dynamic modification. EX2016, ¶134. Indeed, nowhere does Duvall or Chu suggest this capability would occur even some of the time or in certain modes of operation. EX2016, ¶¶134-141. Rather, the Duvall-Chu system must be significantly altered to perform this claimed functionality. EX2016, ¶141.

Petitioner does not “sufficiently demonstrate that the prior art provided such a solution.” Paper 10, 42. Nor does Petitioner’s expert provide any evidence that a POSA would have known *how* to modify Duvall’s system for such functionality. EX2016, ¶141; *see, e.g.*, EX2007, 157:12-17 (suggesting it would be “obvious ... to try,” but providing no explanation how it would be accomplished), 164:20-165:13 (recognizing dynamic modification could create problems with cache consistency but providing no evidence of prior art solutions available at the time).

Rather, Petitioner's expert only speculates that dynamic modification would not be theoretically impossible if properly implemented during specific windows of time. *See, e.g.*, Paper 10, 40-42. But that is insufficient to satisfy the Federal Circuit's "reasonable capability" test. *See INVT SPE*, 46 F.4t at 1376 (citing *Fantasy Sports Props., Inc. v. Sportsline.com*, 287 F.3d 1108, 1119 (Fed. Cir. 2002)). Petitioner must still show that it would actually have been obvious to implement such functionality, even if it only occurred during those windows of time. Thus, Petitioner has failed to identify any evidence from the prior art that the Duvall-Chu system was reasonably capable of dynamic modification.

G. Petitioner fails to show how Duvall-Chu performs analysis in a SOC as part of the "identifying step" as required by Claim 6

Petitioner misreads Claim 6 of Schneier. As a result, Petitioner fails entirely to meet its burden of proof because it completely ignores the actual analysis that Claim 6 requires. More specifically, Claim 6 requires analysis at a SOC as part of the identifying step of Claim 1(b). *See* EX1001, cls. 1, 2, 6; *see also* EX2007, 168:15-17 ("I believe that Claim 6 narrows ... the limitations of B of Claim 1"). Claim 2, from which Claim 6 depends, requires potentially security-related events to be identified through a "multi-stage analysis." *See* EX1001, cl. 2 (requiring "the identifying step [to] include[] performing a multi-stage analysis"); EX1001, cl. 1(b) (reciting the identifying step of "analyz[ing] status data to identify potentially

security-related events”). And per Claim 6, that “multi-stage analysis [of Claim 2] includes analysis at the probe and analysis at a secure operations center.” EX1001, cl. 6.

Petitioner only suggests that some analysis could be performed in a secure operations center (“SOC”) by Duvall-Chu’s purported analyst system. *See* Pet. 44-46. But the claimed analyst system is not part of Claim 1(b)—it is part of a later step in the claims. The analyst system of Claim 1(c) receives information “about the identified events” previously identified by the identifying step 1(b). *See* Claim 1(c). The only analysis Petitioner suggests would be performed by Duvall-Chu’s analyst system occurs *after* both the identifying step and after information about those identified events have been sent to the analyst system. *See, e.g.,* Pet., 38-40; 44-46. In other words, it comes too late.

Rather than explaining how the analyst system also performs a separate analysis as part of the “identifying step,” Petitioner just relies on its previous mapping of Claim 1. *See* Pet., 44-45 (citing to Pet. §§VI.A.2(c)-(d) to show “analysis at a probe followed by analysis at an analyst system”). Petitioner thus fails to show how any analysis at a SOC is incorporated *into* the identifying step (as required by Claim 6) rather than *after* the analyst system receives information about previously identified events (as Claim 1 would suggest). *Cf.* EX2007, 167:17-168:2 (acknowledging that identifying step occurs before step 1(c)).

And indeed, this is neither taught nor disclosed by Petitioner's cited prior art. Petitioner's challenge to Claim 6 therefore fails.

H. Petitioner's mapping of Claim 15 requires showing that the prior art performs the dynamic modification step of Limitation 1(e)

Petitioner fails to show how any combination of prior art references teaches or discloses Claim 15. Claim 15 relates to the dynamic modification step in Claim 1(e). And as further discussed below, Petitioner relies on performance of the dynamic modification step by Duvall-Chu to show that it also teaches Claims 15. But the Board already determined that the dynamic modification step was "neither taught or even suggested by the combined teachings of Duvall and Chu." *See* IPR2023-0888, Paper 9, 35.² Therefore, Claim 15 is also not taught by Duvall-Chu.

Notably, the Board previously construed Claim 1(e) of *Schneier* to only require "mere 'capability.'" Paper 9, 39. Under this broader construction, the Board determined that Petitioner had sufficiently shown—for purposes of institution—that Duvall-Chu had satisfied this limitation in *Schneier*. *But see, supra* §V.F. In contrast, Claim 1(e) of the '237 Patent required the dynamic modification step to actually be performed. *See* '237 Patent, Claim 1(e). And

² Petitioner's "dynamic modification" arguments were identical in both proceedings and those arguments were decided by this same panel.

there, the Board determined the limitation was “neither taught or even suggested by the combined teachings of Duvall and Chu.” *See* IPR2023-0888, Paper 9, 35.

Here, Petitioner’s Duvall-Chu combination requires the dynamic modification step Claim 1(e) to be performed to read on Claim 15. Petitioner relies on its discussion regarding the “modification control system” of Claim 1(e) to argue that “when filters are updated in Duvall’s system, the analysis is instantaneously self-tuned.” Pet., 47 (quotations and alterations omitted). Indeed, Petitioner’s expert admitted that he did not consider other ways Duvall-Chu could perform instantaneous self-tuning besides performing dynamic modification. *See* EX2007, 170:18-22 (“I think dynamic modification is certainly a way in which instantaneous self-tuning can occur. But are there other ways in which it can occur? I haven’t considered that question.”). Therefore, Petitioner’s mapping of Claim 15 assumes the dynamic modification limitation is actually performed, which Duvall-Chu fails to teach or suggest. *See* EX1001, cl. 1(e); *see also, supra* §V.F. Accordingly, Petitioner’s challenge to Claim 15 fails.

I. Petitioner’s expert fails to consider the technical realities of Trcka’s implementation when examining Claims 7-16

1. Trcka does not teach the type of analysis techniques that Petitioner suggests a POSA would be motivated to incorporate.

Claims 7-16 are valid in view of Duvall-Chu-Trcka because Petitioner’s motivation to combine Trcka with Duvall-Chu is flawed. Trcka’s techniques

cannot be used to satisfy the motivation Petitioner proffers. Petitioner suggests a “POSA would have been motivated to incorporate Trcka’s techniques ... to enable the user to analyze whether ‘the filtering system is filtering too much or too little.’” Pet., 51. But Trcka’s disclosed techniques are incapable of determining whether Duvall-Chu is filtering too much or too little. EX2016, ¶¶158-159.

Trcka’s analysis techniques only analyze the data recorded in its archive. *See* EX1014, ¶¶35-67, 108-109; EX2016, ¶157. But Trcka’s archive will not reflect Duvall’s decisions to either block or allow data because Trcka only records what ends up being sent over the network. *See* EX2016, ¶¶157-159. For example, outgoing data blocked by Duvall is never sent over the network and thus will never be recorded in Trcka’s archive. *Id.*, ¶158. Likewise, Trcka will never know whether Duvall blocks or allows incoming data after Duvall’s system receives the data because it will be recorded in the archive either way. *Id.* Worse yet, if Duvall was incorporated into a firewall, Trcka’s techniques would also be unable to distinguish between the firewall and Duvall’s filtering system. EX2016, ¶159. There is thus no disclosure of how a POSA could “incorporate Trcka’s techniques ... to enable the user to analyze whether ‘the filtering system is filtering too much or too little.’” EX1003, ¶186. Because of these issues, a POSA would have lacked a reasonable expectation of success in combining Trcka with Duvall-Chu for this specifically-alleged purpose. EX2016, ¶159.

2. Petitioner fails to explain *how* Trcka’s analysis could be technically incorporated into different parts of Duvall-Chu.

Petitioner’s combination of Duvall-Chu-Trcka is unsupported because its “expert failed to explain how specific references could be combined, which combination(s) of elements in specific references would yield a predictable result, or how any specific combination would operate.” *See ActiveVideo*, 694 F.3d, 1327. Notably, Petitioner’s expert appears to rely on a single combination of Duvall-Chu-Trcka to teach all of Claims 7-13 and 16. But, Claims 7-9 and 12-13 all relate to the “identifying step” of Claim 1(b) at the probe, while Claims 10-11 relates to a different computerized analysis that occurs (in a SOC) *after* the “identifying step.” *See* EX1001, cls. 7-13. Petitioner’s expert suggests combining Trcka’s techniques into different parts of Duvall-Chu’s system without considering any of the material differences between the various components of Duvall-Chu. *See generally*, EX1003, ¶¶184-206; *see also* EX2016, ¶¶160-164. Petitioner’s expert never even acknowledges that Trcka’s analysis techniques would have to be implemented in more than one part of Duvall-Chu’s system. *See generally, id.* In fact, Petitioner’s expert provides no discussion of *how* Trcka could be combined into Duvall-Chu at all, whether into the portions of Duvall-Chu’s system that perform the “identifying step,” the “SOC” in Duvall-Chu’s system, or anywhere else. *See generally, id.* Petitioner’s challenge to Claims 7-16 fails because

Petitioner has entirely failed its burden to explain *how* Trcka is being combined into Duvall-Chu. *See ActiveVideo*, 694 F.3d, 1327.

- a. Petitioner’s expert fails to consider the differences between Trcka’s analysis and Duvall-Chu’s “Identifying Step,” which makes them incompatible with each other.

For Claims 7-9 and 12-13, Petitioner’s expert also fails to consider various differences between Trcka’s techniques and the portions of Duvall-Chu’s system that purportedly performs the “identifying step,” which make them unsuitable for combining as one works on live traffic and the other only on offline archived historic data. *See generally*, EX1003, ¶¶184-195. Trcka’s analysis applications only “allow[] an authorized user to analyze the archived traffic data in an ‘off-line’ mode.” EX1014, ¶15. Petitioner’s expert’s opinion that a “POSA would have been motivated to incorporate Trcka’s techniques ... to enable the user to analyze whether ‘the filtering system is filtering too much or too little’” fails to consider the differences between Duvall’s system that operates using patching code to inspect live traffic and Trcka’s system that operates entirely on archived historical data. EX2016, ¶¶165-166; *Cf.* EX1003, ¶186.

First, Trcka’s analysis applications only operate on the archived traffic data “in an ‘off-line’ mode.” EX1014, ¶15. Indeed, unlike existing firewalls, Trcka’s “data capture step takes place *passively* and without regard to packet content.” EX1014, ¶50 (emphasis added). In other words, Trcka cannot analyze live

traffic—only a copy of the traffic after-the-fact. *Id.* But Duvall’s “identifying step” operates – and needs to operate - on live data, as it is intercepted by the operating system so that certain commands or transmissions can be blocked or altered. *See, e.g.*, EX1004, 6:10-29. Trcka’s *offline* analysis of data in an archive is facially incompatible with analyzing transmissions intercepted by Duvall’s system. EX2016, ¶167. Indeed, Petitioner’s own expert admitted that there were “analyses that you can do o[n] archived traffic that you fundamentally can’t do on live traffic.” EX2007, 181:14-16.

Second, Trcka’s analysis applications only operate on “archived traffic data.” EX1014, ¶15. Without such an archive, Trcka’s analysis techniques do not work. *See* EX2016, ¶¶168-169. And Trcka also explains that “the selection of the network connection point can play an important role in determining the types of network events that are captured within the archival recording.” EX1014, ¶51. Yet Petitioner’s expert never considers *how* the archive could be created or even where the monitoring point could be in Duvall-Chu. Given that Duvall-Chu never captures, records, or processes any data at the packet-level (*supra*, §V.B(5)) and Trcka cannot determine what is blocked or allowed by Duvall-Chu’s filters (*supra*, §V.I(1)), a different archive would be needed for Duvall-Chu’s system than what is taught or disclosed by Trcka. Neither Duvall, Chu, nor Trcka teaches or discloses *how* such a different archive could be created.

Third, Trcka’s analysis applications are “interactive analysis applications.” EX1014, ¶109. And these applications are only designed to be used by “authorized user[s].” EX1014, ¶15. In other words, “interactive” in this context requires human and not automatic operation. In contrast, the operating system of Duvall’s client devices performs the “identifying step” *automatically* by applying filters. *See, e.g.*, EX1004, 6:10-29; 9:14-11:19. Petitioner’s expert never considers how an “authorized user” could be incorporated into Duvall’s “identifying step” or how Trcka’s *interactive* analysis tool could be used to perform the type of *automatic* analysis needed by Duvall. EX2016, ¶¶170-171. Indeed, Trcka’s interactive analysis tool is unsuitable for Duvall’s “identifying step” because manual analysis is facially incompatible with Duvall’s need for automatic analysis. *Id.*

Despite these technical hurdles, Petitioner concludes—without any support—that a “POSA would encounter no technical hurdles.” Pet., 52; *see also* EX1003, ¶187. Ignoring apparent technical issues does not obviate the need to consider them. Therefore, Petitioner has failed its burden to show *how* Trcka could be combined into Duvall-Chu’s “identifying step” for Claims 7-9 and 12-13.

- b. Petitioner’s expert fails to consider glaring privacy and security concerns inherent to combining Trcka’s techniques into a remote SOC.

Likewise, for Claims 10-11, Petitioner’s expert provides no discussion of *how* Trcka is being combined into what is alleged to be Duvall-Chu’s remote SOC.

See EX1003, ¶¶196-202. Neither Petitioner nor its expert even acknowledges that Duvall-Chu would need to be modified by Trcka in a different manner than it was modified for Claims 7-9 and 12-13. *Id.* Claims 10-11 require further computer-based analysis at a SOC, rather than as part of the “identifying step.” *Compare*, EX1001, cls. 10-11, *with*, cls. 7-9, 12-13. And Petitioner relies on its previous discussion of Claim 6, to suggest that Duvall-Chu utilizes third-party network administrators located in a “secure remote site, i.e., ‘a secure operations center.’” *See* Pet., 45 (discussing Claim 6); Pet., 54 (“As discussed for claim 6, a POSA would have understood that Duvall’s ‘corporate network’ provides a ‘secure operations center’....”). But as discussed, *supra* V.I(2)(a), Trcka’s analysis can only “analyze [] archived traffic data.” EX1014, ¶15. And Petitioner’s expert never considers *how* such an archive could be made available to a remote SOC such that Trcka’s analysis could be used to analyze whether Duvall’s system was “filtering too much or too little.” *See* EX1003, ¶186, ¶¶196-202.

Notably, Petitioner’s failure to discuss *how* Trcka would be combined with Duvall-Chu also conceals the security and privacy concerns inherent to providing a remote SOC with access to such an archive. Petitioner’s expert fails to consider these issues altogether. *See* EX1003, ¶¶196-202. Rather than being obvious, a POSA would have resisted such a modification due to the security and privacy concerns implicated by allowing a remote third party at a SOC full access to a

network's raw packet data. EX2016, ¶177. At the time of invention, there were (and still are) privacy and security concerns related to providing third parties with access to raw traffic. *See id.* Yet for Trcka's analysis to work in a SOC, not only does the SOC need access to the raw traffic, but every single packet sent or received on the network must also be accessible from the SOC. *See* EX1014, ¶12; EX2016, ¶177. Petitioner's expert fails to even acknowledge these concerns related to making such a modification.

First, providing remote access to Trcka's archival unit greatly increases the risk that sensitive information would be exposed. EX2016, ¶178. A POSA would have recognized that the attack surface to obtain such sensitive information would effectively become tripled. *Id.* Attackers could not only target the corporate network, but would now also be able to target the remotely accessible archival unit, or the SOC. *Id.* And because the archival unit contains raw packet data, rather than, *e.g.*, status data, an attacker would have full visibility into the corporate network. *See* EX1004, 12; EX2016, ¶179. Not only is the risk that sensitive information would be exposed heightened, but such visibility into the network could also be used to find further weaknesses in the corporate network. EX2016, ¶179. Petitioner's expert never considers and provides no explanation of how such risks could be addressed. A POSA would not have made such a modification to

Duvall-Chu without addressing this security risk, but there is no disclosure in the prior art about how this could be done. EX2016, ¶179.

Second, providing third parties with access to a corporate networks' raw traffic would also have raised privacy concerns, beyond these security concerns. *See* EX2016, ¶180. Indeed, providing *all* of a network's raw traffic to a third-party was unheard of at the time and even today. *Id.* Even the managed security monitoring systems today will not grant a managed security service provider full access to a networks' raw traffic—not to mention access to raw traffic in the form of the raw packet data. *Id.* Rather, managed security monitoring systems only have access to limited information relevant to a potential incident rather than unfettered access to all the traffic in a network (not to mention at the packet level). *Id.* Although Petitioner's expert suggests there were "very obvious" techniques to mitigate privacy concerns, the only proposed solution he mentions is from his 2001 paper, which teaches directly against providing full access to raw network traffic. *See* EX2007, 195:17-196:1; *see also* EX2005, 1, 3, 11 (avoiding privacy concerns by omitting HTTP header data altogether); EX2016, ¶181-182. But an archive of raw packet data necessarily provides access to HTTP headers, along with everything else. EX2016, ¶181-182. Without addressing such privacy concerns, a POSA would not have found it obvious to make such a modification.

Third, providing the SOC with access to the archival recording of raw packet data essentially requires retransmitting every packet sent or received from the corporate network to the SOC. *See* EX2016, ¶183. A POSA would not have found it obvious because it would essentially require the corporate network to double its bandwidth. *Id.* Indeed, at the time of invention the cost of bandwidth was many times what it is today. *Id.* A POSA would thus not have found it obvious to double its network bandwidth at the time just to incorporate Trcka's analysis in a SOC, especially given the additional security and privacy concerns. *Id.* Petitioner never discloses any alternatives, and the cited prior art does not teach a POSA how to address such a problem.

Petitioner's expert fails to acknowledge these concerns and his opinions therefore cannot be credited. The challenge to Claims 10-11 is flawed for these further reasons.

J. Petitioner's Duvall-Chu-Trcka-Ziese combination requires an initial modification to Duvall-Chu-Trcka that Petitioner failed to consider.

Petitioner's challenge to Claims 14 and 15 is based on improper hindsight, relying on a separate series of initial modifications to Duvall's system as a condition precedent. Petitioner first modifies Duvall for a distributed corporate network and then assumes if Duvall was used in a distributed corporate network Duvall would also be modified to use multiple servers, which Petitioner's expert

finally concludes is the reason why Duvall needs Ziese's techniques. *See* EX1003, ¶¶207-212; *see also* EX2007, 200:22-201:5.

Petitioner's expert therefore suggests a POSA would be motivated to search for Ziese's techniques only because Duvall was first modified in at least two different ways to need those techniques. *See* EX1003, ¶¶207-212. But Petitioner's expert never provides any motivation or prior art supporting Petitioner's initial series of modifications to Duvall-Chu-Trcka in the first place. *See* Pet., 58-63. As discussed below, not only is Petitioner's motivation driven by improper hindsight, but the cited art also fails to support Petitioner's initial modification of Duvall to require Ziese's techniques.

1. Petitioner's motivation to combine Ziese requires Duvall to be modified to use multiple servers contrary to Duvall's own disclosure.

Ziese discloses techniques to *distribute* updates to *multiple devices*. *See, e.g.,* EX1015, 1:7-9 ("method and system for dynamically distributing updates in a network"), 2:34-36 ("systems with a common program separately running at several sites may update each site with no or minimal operator interaction"); *see also* Pet. 58-60. But there is no need for Ziese if there are not already multiple servers that need updates. EX2016, ¶188. Therefore, Petitioner's motivation to combine Ziese assumes Duvall already has *multiple servers* needing filter updates. *See* Pet. 60-61; EX1003, ¶¶207-208. Yet Petitioner has admitted that "Duvall

expressly discloses only a single ‘server 30’ on which the filtering system is running in a ‘corporate network.’” Pet, 59-60; *see also* EX1003, ¶209. And indeed, Petitioner’s own combination of Duvall-Chu-Trcka also contains only a single server. *See* Pet., 27-28; *see also* Pet., 50-58. Thus, by Petitioner’s expert’s own acknowledgment, there is no logical reason to look for Ziese, because there is only one server. *See* Pet., 59-60; EX1004, 8:18-26.

Indeed, Duvall actually teaches away from using multiple servers. In Petitioner’s expert’s own words, “[i]mplementing Duvall’s ‘editing manager’ on each local server, [] would require common filter updates ... to be made on each individual server.” EX1003, 211. As Petitioner’s expert recognizes, Duvall would require additional “techniques [to] resolve this problem,” which are not contemplated by Duvall. *Id.* Petitioner’s expert also acknowledges that “Duvall already suggests the use of centralized updates.” EX1003, ¶212. Duvall thus teaches away from using multiple servers because such a configuration would just create an unnecessary problem for Duvall, while also working against the goal of centralizing updates. EX2016, ¶¶190-191. In short, Petitioner’s expert fails to explain why a POSA would ever look for Ziese, when Ziese is only pertinent to resolving Petitioner’s self-manufactured problem.

2. Petitioner never provides any motivation for modifying Duvall to use multiple servers.

As explained above, Duvall must have multiple servers as a condition precedent to Petitioner's motivation to look for and combine Ziese into Duvall-Chu-Trcka. But Petitioner's expert provides no motivation to initially add multiple servers to Duvall-Chu-Trcka. *See generally*, EX1003, ¶¶207-212. And none of Petitioner's cited art provides any such motivation either. EX2016, ¶192. Petitioner's expert presumes there would be multiple servers when Duvall-Chu-Trcka is used in a distributed corporate environment. EX1003, ¶210 (suggesting that in "a distributed corporate network, a POSA would have understood that Duvall's 'filtering system' would employ multiple 'server[s] 30'"). But Petitioner's expert also never provides any motivation to modify Duvall-Chu-Trcka into a distributed corporate environment. *See* EX2016, ¶¶192-194. Rather, Petitioner's expert opines that "both Duvall and Ziese explain that clients may be distributed widely outside of a traditional [LAN]". EX1003, ¶209 (citing EX1004, 2:35-39 (discussing a broad-based commercial service as an alternative to LAN)). But Duvall's identification of a "broad-based commercial service" as an alternative to LAN neither teaches nor suggests a distributed corporate network. *See* EX1004, 2:38-39; EX2016, ¶193; *see also* EX2007, 200:1-3 (distinguishing among LAN, broadband, and distributed networks). And likewise, Ziese's disclosure of how to

distribute updates to multiple devices contains no motivation to modify a system like Duvall-Chu into a distributed corporate network. EX2016, ¶194.

Moreover, even if there could be a valid motivation to modify Duvall-Chu-Trcka into a distributed corporate network, Petitioner's expert never explains how that would necessitate adding multiple servers. Rather, Petitioner's expert's proffered motivation "for a distributed corporate network to *centrally* analyze and update filters" suggests a POSA would be motivated to do the opposite—keep using a single server rather than adding multiple servers. *See* EX1003, ¶211 (emphasis added). This is especially true given that Petitioner's expert recognizes that a POSA could not add multiple servers to Duvall without relying on another reference like Ziese. *See* EX1003, ¶211 (explaining that Ziese resolves a problem created by forcing Duvall to use multiple servers). Petitioner's expert thus fails to explain why a POSA would ever modify Duvall-Chu-Trcka to use multiple servers.³

K. Petitioner's expert's opinion regarding Duvall-Chu-Cogger in connection with Claims 18-25 is unsupported by evidence

³ Petitioner also fails to consider how to combine Ziese with Trcka's techniques as they never even mention Trcka in the Duvall-Chu-Trcka-Ziese combination.

1. Petitioner's expert provides no evidence that a POSA could implement Cogger's CSM.

Petitioner's combination of Duvall-Chu-Cogger is unsupported because the key component that Petitioner's expert suggests would need to be incorporated into Duvall-Chu from Cogger is not disclosed in sufficient detail for a POSA to understand how to actually incorporate it. Petitioner relies on its expert's conclusory suggestion that in Duvall-Chu-Cogger, "a POSA would have implemented Cogger's CSM." EX1003, ¶230. But Petitioner's expert provides no factual support for this statement. Indeed, neither Petitioner nor its expert cites to any of the components, systems, or processes that form Cogger's CSM. *See generally* EX1003, ¶¶228-224. Though Petitioner's expert purports to describe Cogger's CSM, as explained below, those cited portions of Cogger do not actually describe the CSM itself.

For example, Petitioner's expert suggests that Cogger's "CSM is 'secure' because it provides 'secure web servers and back end services to provide applications that establish user sessions ... and communicate with adaptor programs to simplify the interchange of data across the network.'" *See* Pet., 67 (citing EX1033, 5:46-50; 7:55-60). But these cited portions of Cogger only describe a "second or middle tier" connection to legacy back-end services. *See* EX1033, 5:46-52. Indeed, Figure 2 clearly shows that the web servers (Fig. 2, 24)

and DMZ (Fig. 2, 17) are all part of the *interface* connecting a customer's browser (Fig. 2, 20) to the legacy back-end CSM (Fig.2, 40(a)). *See also* EX1033, 13:22-24 ("FIG. 2 illustrates the service inquiry 'SI' application server 36 interfacing with a backend Customer Service Management[] ('CSM') legacy host system 40(a).").

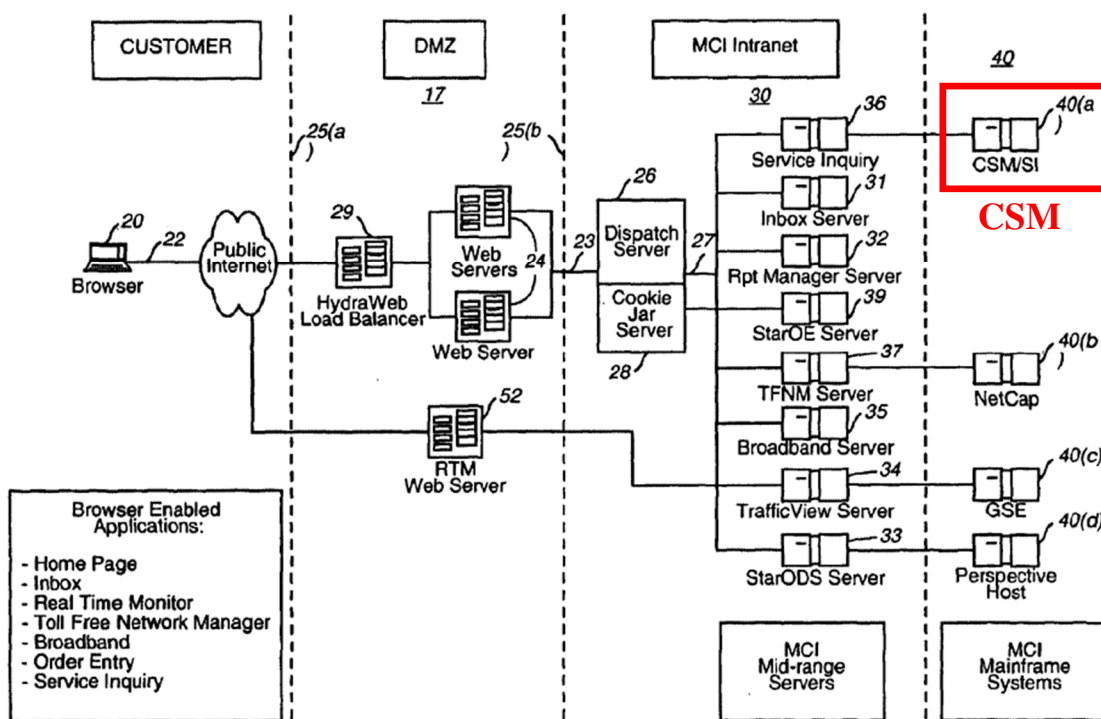


FIG. 2

Not CSM

EX1033, Fig. 2 (annotations added).

Likewise, Petitioner's expert's reliance on Cogger's front-end user interface also fails to teach a POSA how to implement the CSM itself. *See, e.g.,* EX1033, Fig. 8(a)-(k). Rather, Figures 8(a)-(k) only depict a "service inquiry main screen." *Id.*, 17:50-51. This front-end GUI is not the CSM. *See* EX1033, 13:22-24

(explaining “service inquiry” application interfaces with CSM); *see also id.*, 15:51-22 (explaining “[c]ommunication between the SI application server 36 and CSM 40(a) is via Registry middleware”); 16:5-9 (explaining “request data that comes from the Front-End/Client application..., builds the CSM/SI request transactions ... and ships off the requests to CSM”).

Petitioner’s expert cannot maintain that “a POSA would have implemented Cogger’s CSM” without—at minimum—citing to the portions of Cogger describing the actual CSM. *Cf.*, EX1003, 230. But Cogger’s CSM is just a black box. *See* EX2016, ¶¶198-206. Indeed, Petitioner’s expert admits as much. *See* EX2007, 206:11-15 (“I think what Cogger discloses are the functions of the CSM, and some of the data flows of the CSM. And like most patents, it leaves the implementation details up to a [POSA].”). At best, Cogger only discloses how a customer can access the CSM remotely through its disclosed interface. *See, e.g.*, EX0133, 2:38-43 (explaining “what is needed is a system and method for *allowing a customer to remotely access* a service provider’s trouble ticketing system” (emphasis added)); *see also id.*, Fig. 2 (depicting interface between customer browser, 20, and CSM, 40(a)), Fig. 5 (depicting interface between customer browser, 14, and CSM, 20(a)), Fig. 6 (depicting relationship between service inquiry server and CSM, 40(a)), Fig. 7(b) (depicting how service inquiry application interfaces with CSM, 40(a)).

Cogger fails to teach a POSA how to implement the actual CSM system. EX2016, ¶¶198-206. Cogger does not disclose any systems or processes used to create, store, or manage the trouble tickets in the CSM. *Id.* Cogger does not disclose any systems or processes allowing a customer service representative to access or use the CSM. *Id.* Cogger does not disclose any systems and processes related to securing the CSM itself, rather than the customer's connection to it. *Id.* Petitioner's expert's suggestion that "a POSA would have implemented Cogger's CSM" is therefore unsupported by evidence. EX1003, ¶230.

2. Petitioner's expert provides no evidence that the information in Cogger's "problem tickets" could be generated.

Petitioner relies on its Duvall-Chu combination as discussed for Limitations 1(b) and 1(c) to teach the "event record" that is created in accordance with Claim 18. *See* EX1003, ¶232. Petitioner's expert also suggests this "event record" would be placed into a problem ticket along with various other information. *Id.* Indeed, Petitioner's expert suggests that Duvall-Chu-Cogger teaches "consolidating the event record, correlated customer information and symptom record, and linked problem resolution assistance information into a problem ticket" because Cogger discloses such information in its problem tickets. EX1003, ¶242. But though Cogger's problem tickets contain such information, Petitioner's expert fails to

show *how* Duvall-Chu could be modified to populate such information in the problem tickets.

Petitioner's Duvall-Chu combination automatically prompts the network administrator whenever a transmission does not match any of Duvall's existing filters. *See* Pet., 17-23. Duvall-Chu's filtering system thus provides no opportunity for a customer to manually populate new trouble tickets related to each "event record." EX2016, ¶¶208-210. But Cogger discloses exactly that—customers must manually populate majority of the information in its problem tickets. *See, e.g.*, EX1033, 21:27-41.

Indeed, Petitioner's expert relies on Cogger's disclosure of a customer manually populating the trouble ticket as evidence that Cogger teaches a "symptom record." *See* EX1003, ¶¶235-236; *see also* EX1033, 21:27-41. The "questions that need to be asked to open a ticket vary by product and problem type." EX1033, 22:58-59. And Petitioner suggests that these answers from the customer are what "relate to '*symptom[s]*' of a particular problem." Pet., 236 (alterations in original).

Petitioner's expert therefore fails to explain "which combination(s) of elements in [the] specific references would yield a predictable result, or how any specific combination would operate." *See ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.*, 694 F.3d 1312, 1327 (Fed. Cir. 2012). Rather, Petitioner's expert only concludes that a "POSA would have implemented Cogger's CSM," with no

explanation of how any elements would relate to Duvall-Chu's existing elements. EX1003, ¶230. Petitioner's expert's "testimony is generic and bears no relation to any specific combination of prior art elements." *ActiveVideo Networks*, 694 F.3d at 1328.

VI. SECONDARY CONSIDERATIONS INDICATE THE CHALLENGED CLAIMS WERE NOT OBVIOUS

Petitioner fails to account for any secondary considerations or indicia of non-obviousness regarding Schneier's invention. "Evidence of objective indicia of nonobviousness, if present, must always be considered before reaching a determination on the issue of obviousness." *Quanergy Sys., Inc. v. Velodyne Lidar USA, Inc.*, 24 F.4th 1406, 1417 (Fed. Cir. 2022); *see also Robert Bosch Tool Corp. v. SD3, LLC*, IPR2016-01753, Paper 15 at 28 (PTAB Mar. 22, 2017) ("known evidence of secondary considerations should be addressed in the Petition").

Counterpane's Managed Security Monitoring ("Counterpane MSM") service was a service created by Bruce Schneier and offered by Counterpane Internet Security, Inc. in 2000. *See* [NY Times Article]. Counterpane MSM is an embodiment of the Schneier Patent and is captured by the claims. [Expert dec]. The Board should consider evidence of a long-felt but unresolved need in the network security market, industry praise, and commercial success of Counterpane MSM as objective evidence of non-obviousness.

A. There is a nexus between the evidence of non-obviousness and Schneier's claims

Counterpane MSM is a “system for operating a probe as part of a security monitoring system for a computer network.” EX1001, cl. 1; *see also id.*, cl. 18 (Counterpane MSM carries out the claimed method). A nexus between evidence of non-obviousness and the claimed invention is presumed when the product is coextensive with the claimed features. *See Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1072 (Fed. Cir. 2018). “The coextensive requirement does not require a patentee to prove perfect correspondence between the product and a patent claim.... Rather, it requires the patentee to demonstrate that the product is essentially the claimed invention.” *Quanergy Sys.*, 24 F.4th at 1417-18 (internal citations and quotation marks omitted).

Here, Counterpane MSM is “essentially the claimed invention.” *Quanergy Sys.*, 24 F.4th at 1418. Like the claimed invention, Counterpane MSM utilizes a probe (*i.e.*, Sentry) and an analyst system (*i.e.*, Socrates). *See, e.g.*, EX2009, 6, 12; *see also* EX2011, 2 (“At the core of Counterpane’s Managed Security Monitoring are Sentry and Socrates, patented technologies developed by Counterpane.”). Counterpane MSM’s probes collect data from network devices, filters potential security threats, further analyzes post-filtering residue, and sends identified events to analyst systems. EX2009, 6, 12; EX2016, ¶214. Trained security analysts then

“filter[] out the chaff” and refine the potential security threat information that is presented to customers. EX2012, 2.

B. Counterpane MSM met a long-felt but unresolved need.

Counterpane MSM, which embodies the challenged claims, filled a gap missing in the industry at the time of invention. The challenged claims provide a novel approach to discovering more threats than were possible with previous techniques and provided an architecture enabling reactive and proactive responses to potential threats. The long-felt need recognized by the Schneier patents and solved by Counterpane’s MSM were unresolved in the network security industry before 2000. *See* EX2016, ¶¶ 215-222. This missing need “would not have persisted had the solution been obvious.” *Apple Inc. v. Samsung Elecs., Co.*, 839 F.3d 1034, 1054-56 (Fed. Cir. 2016). And that is where the Schneier Patent and Counterpane MSM stepped in.

As the inventors recognized, “[t]he present state of computer security just [wasn’t] working” and there were “just too many attacks.” EX2010, 3. Prior to Counterpane MSM, internet security was “static: install a firewall, configure a PKI, add access-control measures, and you’re done.” EX2009, 9. But the Schneier inventors noted that “[r]eal security is dynamic,” and a proper “defense has to be able to respond to attacks effectively.” EX2009, 9. Indeed, the increased use of the Internet over the years “created the need for such monitoring and alarm

services for e-commerce companies of all sizes,” and these needs were not met by traditional network security approaches. EX2010, 3; EX2009, 9; *see also* EX2012, 3 (describing how Counterpane MSM also took at the lead in the OS/400 server market and was the “only managed security provider” to do so).

Moreover, there was a long felt need for the ability to detect the threats that these static systems could not detect. EX2016, ¶¶ 217-219. Indeed, when Counterpane MSM entered this space with its new approach to managed security monitoring, its competitors were mainly Intrusion Detection System monitoring companies that performed discrete filtering functions and did not have the level of detection, monitoring, and response that were provided by Counterpane MSM. EX2010. The claimed solution therefore provided a novel architecture to solve these long-felt needs. EX2016, ¶¶ 220-222.

Accordingly, Counterpane’s release of its MSM meet a long-felt need that existed for internet security.

C. Industry Praise and Commercial Success of Counterpane MSM

“[I]ndustry praise ... provides probative and cogent evidence that one of ordinary skill in the art would not have reasonably expected [the claimed invention].” *Institut Pasteur & Universite Pierre Et Marie Curie v. Focarino*, 738 F.3d 1337, 1347 (Fed. Cir. 2013). Like industry praise, commercial success

provides further evidence of non-obviousness. *See, e.g., Polaris Indus.*, 882 F.3d at 1073.

Counterpane, through its MSM service, was repeatedly recognized as an industry leader and visionary within the network security field. *See, e.g.,* EX2013, 2 (listing Counterpane Internet Security as a “visionary”); EX2014, 7 (describing Counterpane as a “leading vendor” in “managed security monitoring”); EX2011, 1, 3 (describing “Counterpane’s industry leading Security Monitoring Service” and quoting a security analyst who also recognized “Counterpane has been an industry leading security services provider since the market’s inception”).

The industry acclaim awarded to Counterpane and its Counterpane MSM service, specifically, is complemented by Counterpane’s commercial success in the industry. *See* EX2010, 3 (noting that “International Data Corp., a research house, estimates that the national market for computer security management services was \$703 million last year and will reach \$2.2 billion a year by 2003.”). Counterpane’s MSM service was very successful:

And it has been successful. Counterpane claims that, in 2003, it processed 523 billion messages, detected more than 70,000 attacks, and directly notified customers 21,000 times. In 2004, Counterpane successfully defended over 400,000 attacks without one of its customers suffering a financial loss, according to Counterpane CEO, Paul Stitch.

EX2012, 3. One of its client's The Regence Group, credits Counterpane's MSM service for successfully defending its network from cyberattacks and spent \$450,000 on Counterpane every year. *See* EX2015. Counterpane was so successful, that by 2006 it was acquired "for a sum of more than \$20 million." EX2017.

The objective evidence shows that Schneier's patented invention was not obvious because Counterpane MSM met a long-felt but unresolved need, was given industry praise, and was commercially successful. Thus, secondary considerations support the validity of the challenged claims.

VII. CONCLUSION

For the foregoing reasons, the Board should issue a Final Written Decision finding all claims patentable.

Respectfully submitted,

Dated: February 21, 2024

/Nolan M. Goldberg/

Nolan M. Goldberg (Reg. No. 54,126)
PROSKAUER ROSE LLP
Eleven Time Square
New York, NY 10036-8299
Baldassare Vinti (Reg. No. 43,970)

*Counsel for Patent Owner
BT Americas Inc.*

WORD COUNT CERTIFICATION

Under the provisions of 37 C.F.R. § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Patent Owner's Response totals 13,949 words, which is less than the 14,000 allowed under 37 C.F.R. § 42.24. Counsel has relied upon the word count feature provided by Microsoft Word™.

Dated: 2/21/2024

/Nolan M. Goldberg/

Nolan M. Goldberg (Reg. No. 54,126)
PROSKAUER ROSE LLP
Eleven Time Square
New York, NY 10036-8299

*Counsel for Patent Owner
BT Americas Inc.*

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true copy of the foregoing Patent Owner's Response and all exhibits filed therewith, was served on Petitioner on 2/21/24, by emailing a copy to counsel at the email addresses listed below:

Jonathan Tuminaro
Daniel S. Block
Michael D. Specht
Steven M. Pappas
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 New York Avenue, N.W.
Washington, D.C. 20005
Tel. (202) 371-2600
Fax. (202) 371-2540

jtuminar-PTAB@sternekessler.com
mspecht-PTAB@sternekessler.com
dblock-PTAB@sternekessler.com
spappasPTAB@sternekessler.com
PTAB@sternekessler.com.

Dated: 2/21/2024

/Nolan M. Goldberg/

Nolan M. Goldberg
PROSKAUER ROSE LLP
Eleven Time Square
New York, NY 10036-8299
Registration No. 54,126

*Counsel for Patent Owner
BT Americas Inc.*