

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

DECLARATION OF WENKE LEE

I. INTRODUCTION

1. My name is Wenke Lee. BT Americas Inc. (“BT”) has retained me as a technical expert witness in connection with this proceeding.

2. A curriculum vitae (“CV”), which I have recently reviewed and believe to be accurate, is attached as Exhibit A to this Declaration. My particular area of expertise is network security and attendant technologies, with an emphasis on the detection of malware and network intrusions, as well as remedial measures to be employed following detection.

3. I have been asked to provide insight into the state of the art during the relevant time frame. In this regard, the stated Field of Invention of the U.S. Patent 7,895,641 (“’641 Patent” or “Schneier”) (EX1001, 1:18-20) matches my own area of expertise and work, starting with my PhD Thesis, which was completed in 1999. My thesis is directed to a data mining framework for constructing features and models for network intrusion detection systems. It describes algorithms and procedures for processing network traffic data and extracting useful attributes and patterns (or signatures) for the purpose of detecting attacks to enterprise networks.

4. I will also address the technology described and inventions claimed in Schneier, the references cited by Petitioner, and the differences between the inventions claimed in Schneier and the disclosures of the cited references. I will

also address related technical points which may prove helpful to the Board in assessing factual assertions and opinions set forth in Petitioner's papers and exhibits, all of which I have read and will address as appropriate to the present context.

5. I am a named inventor in twenty one patents, eighteen of which are directed to detecting intrusions, malware, or responding to network attacks (as well as detecting them). I have also served as an expert and have provided testimony in multiple patent litigations. Consequently, I have a general familiarity with principles of patent law respecting validity and non-obviousness.

6. I understand that a patent is obvious if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art. BT's counsel has informed me that obviousness is a question of law based on underlying questions of fact.

7. I understand that the underlying factual inquiries in an obviousness analysis include: (1) determining the scope and content of the prior art; (2) resolving the level of ordinary skill in the prior art; (3) ascertaining the differences between the claimed invention and the prior art; and (4) considering objective evidence of nonobviousness.

8. I also understand that the Petitioner, Palo Alto Networks, Inc. (“PAN” or “Petitioner”), has the burden to show that a person of ordinary skill in the relevant field had a reason to combine the elements in the manner claimed when asserting obviousness in view of a combination of references. BT’s counsel has informed me that I should value “common sense” over “rigid preventative rules” in determining whether a motivation to combine references exists. I understand that any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed. However, I also understand that if a person of ordinary skill in the art would have had reason to attempt to make the composition or device, or carry out the claimed process, Petitioner must also demonstrate that such a person would have had a reasonable expectation of success in doing so.

9. I understand that the express, implicit, and inherent disclosures of a prior art reference may be relied upon in the rejection of claims for anticipation and obviousness.

10. Further, I understand that hindsight may not be used to determine obviousness. In other words, it is wrong to use the Schneier patent as a guide through the prior art references, to combine the right references in a particular way so as to achieve the result of the claims of the Schneier patent.

11. I further understand that a reference may be said to teach away from the subject matter claimed in the challenged patent when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the patent applicant. I also understand that a reference may teach away from a use when that use would render the result inoperable.

12. I understand that there is no suggestion or motivation to make a modification to a prior art reference if the proposed modification would render the prior art invention unsatisfactory for its intended purpose. I also understand that an obviousness allegation cannot be supported by a combination of references that would require a substantial reconstruction and redesign of the elements shown in the primary reference as well as a change in the basic principle under which the primary reference was designed to operate.

II. PERSON OF ORDINARY SKILL IN THE ART

13. For the purposes of this declaration, I have been asked to assume that a person of ordinary skill in the art (a “POSA”) pertaining to Schneier at the time it was invented has the education and/or experience that Petitioner’s expert has set out in his declaration. Specifically, Petitioner’s expert provides the following:

29. I understand that a POSA is presumed to be aware

of all pertinent art, thinks along conventional wisdom in the art, and is a person of ordinary creativity—not an automaton.

30. I have been asked to consider the level of ordinary skill in the field that someone would have had at the time the alleged invention was made. In deciding the level of ordinary skill, I considered the following: the levels of education and experience of persons working in the field; the types of problems encountered in the field; and the sophistication of the technology.

31. I understand that the relevant time for considering whether a claim would have been obvious to a POSA is at the time of the alleged invention, which I have assumed to be March 16, 2000.

EX1003 ¶¶29-31.

III. MY QUALIFICATIONS, COMPENSATION, AND EXPERIENCE

14. I am currently employed as a Professor at Georgia Institute of Technology, where I hold the John P. Imlay Chair in the College of Computing. I am receiving compensation from BT for my services in this proceeding at the rate of \$750/hr. My compensation is not dependent upon the outcome of this proceeding and has not affected the statements I am making in this Declaration in any way.

15. My main area of interest and the focus of my current research is malware analysis and detection. A fuller description of my current interests and areas of research can be found at the bottom of page 3 and top of page 4 of my CV (EX2020).

16. As reflected in the succeeding pages of my CV (pages 5-8 of EX2020), I have taught courses directed to Network and Information Security essentially continuously since 1999.

17. I have published more than two hundred academic papers in top journals and conference proceedings, published half a dozen books or parts of books, and participated in well over two hundred Conference Presentations and over a dozen Workshop Presentations, the vast preponderance of which relate to Network Security and most of which relate to Intrusion Detection in particular.

18. I have also performed and supervised a substantial amount of research in the field of Network Security. A list of the 54 Research Proposals and Grants in which I have participated can be found at pages 32-38 of my CV (EX2020).

19. Research Honors and Awards I have received are listed on pages 39-40 of my CV (EX2020) and include a Test of Time award received in 2018 for co-authorship on a paper on malware analysis deemed to have had the greatest impact on security research and practice of the past decade. I have also received three Test of Time awards on papers on botnet taxonomy, virtual machine monitoring, and malware unpacking in 2022 and 2023 for the papers' "enduring significance and impact on the security community." I am a Fellow of the Association for Computing Machinery (ACM), which is the world's largest scientific and

educational computing society; only the top 1 percent of ACM members are recognized as Fellows. I am also a Fellow of the Institute of Electrical and Electronics Engineers (IEEE), the professional home for the engineering and technology community worldwide and the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

20. I am also active in Conference Committee Activities and Seminars, all as reflected towards the back end of my CV (EX2020).

21. I am named as an inventor in twenty-one patents (listed on pages 47-48 of my CV, EX2020), most of which relate to the Field of Invention at hand.

IV. THE PRIOR ART

A. Duvall Reference

22. Duval does not involve computer security. In fact, computer security is never mentioned once in Duvall. 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.

23. Duvall applies direct-action filters to transmissions that open a TCP connection as shown in Figure 3. *Id.*, 4:38-42; 6:14-18.

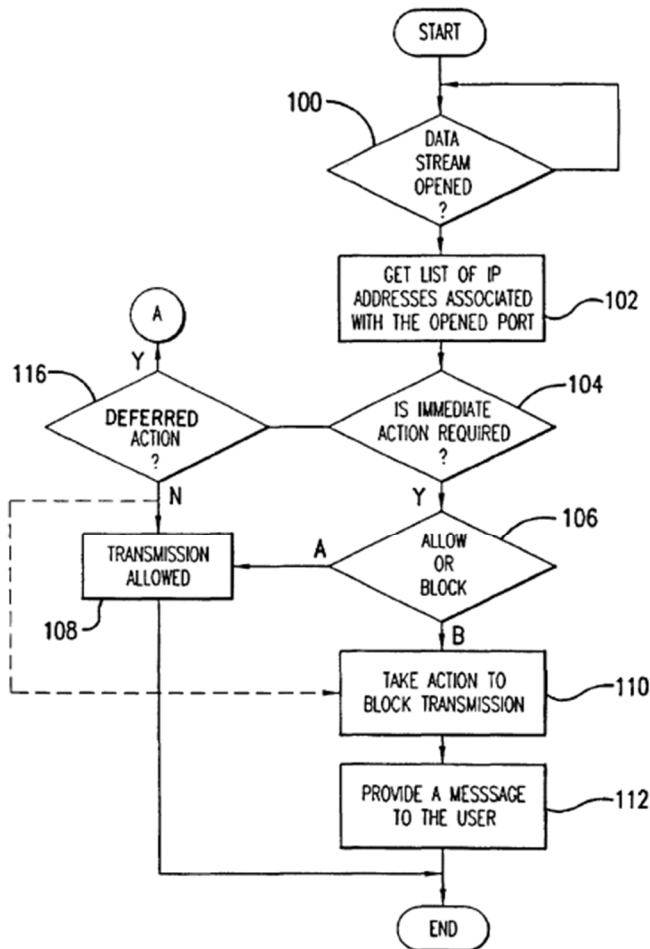


FIG.3

EX1004, Fig. 3.

24. And Duvall applies deferred-action filters to transmissions sent through an “open TCP/IP connection” as shown in Figure 4. *Id.*, 5:19-29.

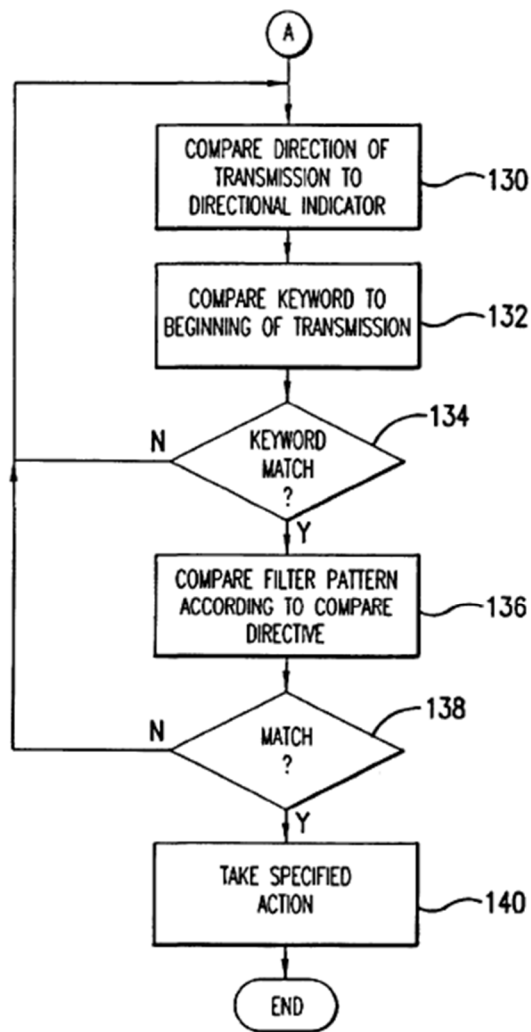


FIG.4

EX1004, Fig. 4.

25. Duvall discloses a client-based and server-based system. *Id.*, 8:18-27.

Both versions “use[] the same type of filter database ... but the filter database is located on [a] server” for the server-based system. *Id.*, 8:23-27.

26. Duvall's filtering system also includes an editing manager that allows its filters to be edited. *Id.* 8:2-16.

B. Chu Reference

27. Chu is a master's thesis that discloses a trust management system that runs on a client computer. EX1005, 34. Petitioner relies primarily on a single sample policy disclosed by Chu. Pet., 20-21.

Policy in English

```
Do not download the code if the URL is served from Harvard or CalTech
Web servers. Download it automatically if served from MIT. Prompt me
for my attention otherwise.
```

Profiles-0.92

```
(threshold-and
  2
  (not (url-match URL ("http://www.harvard.edu"
                      "http://www.caltech.edu")))
  (url-match URL ("http://web.mit.edu"))
  unknown)
```

EX1005, 44.

28. This sample Chu 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.*

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

C. In my opinion Petitioner's expert stacks inferences to stitch Duvall and Chu together in a way that would never make sense to a POSA

29. In my opinion, Petitioner's motivation to combine relies on multiple

unsupported inferences about both Duvall and Chu. But none of these inferences are actually supported by either reference.

30. I initially note that in my opinion, Petitioner's expert's opinions in his declaration are generally unsupported by the reference's actual disclosures. And in my opinion, his deposition has confirmed that his positions are not actually supported by the cited art. Attached as Exhibit EX2018, I provide some examples where Petitioner's expert suggested a reference disclosed something but was unable to identify where or how the reference disclosed it when pressed.

1. Petitioner's expert's assumption that Duvall would be used for security is not an assumption a POSA would make

31. Duvall is unequivocally focused on censorship of objectionable material. EX1004, 2:12-16 ("With the present invention, a user can filter received over the internet that is personally objectionable...depending on that user's individual tastes and sensitivities."). In my opinion, it is important to recognize that Duvall itself does not contemplate or consider any computer security-related concerns. Indeed, computer security is never even mentioned once in Duvall.

32. At minimum, a POSA would recognize that there are necessarily going to be differences between what a system used for censorship needs and what a system used for computer security would need. For example, a censorship tool is

primarily focused on content, whereas a security system is concerned about security threats. Therefore, while a censorship tool can focus primarily on TCP/IP related transmissions, that would likely be inadequate for a security system. Indeed, security systems typically require analyzing all the traffic and at a lower level (*e.g.*, packet-level). *See, e.g.*, EX1014, ¶¶9-12. But a censorship tool will generally not need to analyze the traffic at such a level of detail. Rather, censorship tools will only be concerned with whether the *content* of the traffic contains anything objectionable. *See generally*, EX1004.

33. Whereas censorship tools are generally less concerned with external attempts to bypass its censorship, security devices are very concerned with external threats to security. *See, e.g.*, EX1014, ¶4 (discussing break-ins and downloading viruses). Moreover, the negative implications of accidentally allowing objectionable material are comparatively less for a censorship tool as compared to a security device. If objectionable material is accidentally allowed, it can simply be blocked the next time with little to no consequence. But if a security threat is accidentally allowed, it could result in “devastating consequences.” *See* EX1014, ¶4. In other words, security systems need to be far more stringent and accurate than censorship devices.

34. Thus, a POSA would not be motivated to use Duvall’s disclosed

system for security. For example, Duvall's system operates on TCP traffic by patching, *e.g.*, a Winsock library. *See, e.g.*, EX1004, 1:34-3:12, 9:13-11:16.

While this solution is very effective at monitoring content, at the same cannot be said for detecting anomalous network activity, which may require looking at individual packets. *See, e.g.*, EX1014, ¶5 (discussing firewalls that filter traffic at packet level).

35. Petitioner's expert also assumes that 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. In my opinion, Petitioner's expert's logic is flawed because—at most—he is only observing that there may be coincidental circumstances where objectionable material might also pose security risks. Again, Duvall makes no mention of security risks.

36. Although objectionable material may sometimes also pose a risk to security, a POSA would recognize that the same is obviously true for non-objectionable material as well. Petitioner's expert has not provided any evidence of any actual correlation between objectionable materials and security risks.

Indeed, just as a matter of common sense, a POSA would recognize that simply because a curse word is used in a website, does not mean that website is more or less likely to have a virus.

37. Petitioner ignores that a POSA would recognize that non-objectionable material is equally (or even more likely) to raise security concerns. A POSA would understand that security threats are commonly accompanied with benign material because users are likely to be more receptive to such material.

38. For example, a POSA would have been aware of a number of notorious malware attacks that were spread through non-objectionable material at the time. *See, e.g.,* EX2008, 7-8. For example, EX2008 discusses how malware was spread through digital Christmas cards or Christmas-related emails, which matches my recollection. *See id.* Thus, a POSA would recognize that potentially security-related events are often spread through such non-objectionable material. Thus, the issue of whether content is objectionable is an entirely separate issue from whether than content also poses security concerns and Petitioner's expert is wrong to conflate the two issues in the manner he does. Duvall's discussion of objectionable material simply has no bearing on computer-security whatsoever. Duvall itself cannot be properly characterized as contemplating security when it clearly only discusses objectionable material.

39. As a separate note, Petitioner's expert also suggests that it would be obvious to use Duvall for computer security. EX1003, 117-118. However, a POSA would recognize that computer security has nothing to do with a "user's individual tastes and sensitivities." EX1004, 2:15-16. By way of example, whether content is objectionable to a specific user might depend—at least in part—on that user's cultural background. For example, one user may find certain words objectionable, while another user may not. There is no objective right or wrong answer in this case. But whether something is a threat to a network does not vary based on a user's cultural background. Either it will harm the network, or it will not. There is thus an objectively right or wrong answer to the determination that something is or is not potentially security related.

40. Further, while expertise might be needed to ascertain whether or not something poses a threat to security, no similar expertise is needed to determine whether something is objectionable. Indeed, Duvall discloses that its filtering system can be edited by any parent that wants to restrict the material that their child can access. EX1004, 1:14-16. Therefore, the motivation to use Duvall for security cannot come from Duvall itself.

41. Petitioner and its expert also do not provide sufficient motivation to use Duvall's system for security from anywhere else. Petitioner's expert only

suggests that based on Chu a POSA would recognize that “data transmission from unknown or questionable sources can carry viruses or malware.” EX1003, 118.

But that recognition does not mean a POSA would automatically be motivated to transform any censorship tool into a tool for blocking viruses. Duvall states that its filtering system could be located in “a firewall, gateway, or proxy server,” but never suggests its system is designed to replace the firewall or supplement its security-related functions. *See* EX1004, 1:63-64. Indeed, Petitioner’s expert highlights that “firewalls are commonly used for protecting networks,” but provides no justification for substituting the firewall’s role with Duvall’s system. EX1003, 118.

2. Petitioner’s expert motivation to look for Chu is contradicted by Duvall’s express disclosure

42. In my opinion, Petitioner’s motivation to look for and combine Chu with Duvall is directly contradicted by Duvall’s express disclosure. Petitioner’s expert suggests that Duvall has an unresolved problem with “filtering too much or too little.” *See, e.g.*, EX1003, 107. But the only instance where Duvall discusses such a “problem” is in the context of explaining how a “user [can] make custom changes” using the editing manager to resolve that very problem. EX1004, 8:6-7. Indeed, Duvall clearly contemplates its users simply accessing websites to

determine whether they should be blocked or allowed and then using the editing manager to make the change. *See* EX1004, 8:13-16 (“during a session over the Internet, a user can copy URLs for later editing.... [and] can then copy those URLs for inclusion in the database, or can edit the entry, e.g., to change the action from allow to block or vice versa.”). And this is clearly possible for Duvall’s system because the determination of whether something should be blocked or allowed is subjective. *See*, EX1004, 2:12-16.

43. Given Duvall’s express disclosure of a solution to this problem, a POSA would not be motivated to look for Chu. Petitioner’s expert never clearly articulates what sort of “problem” with Duvall’s system would still remain given Duvall’s explicit disclosure. *See generally* EX1003, 110-112. Indeed, Petitioner’s expert does not explain what problem that is not already resolved through Duvall’s editing manager would motivate a POSA to look for Chu. *Id.*

44. Importantly, I note that Petitioner’s expert actually conceded during his deposition that a POSA would understand that nothing more is needed to solve this supposed “problem.” An excerpt of the transcript is as follows:

Q Okay. Does Duvall recognize the need for any additional techniques to address the problem of filtering too much or too little beyond the disclosed editing manager?

A I -- I think a person of skill would understand that

what Duvall is disclosing is a mechanism for updating filter database. And it's a very general purpose and generic mechanism. And I think that -- Duvall does not disclose that anything more than that is needed. And given the operation of Duvall, a person of ordinary skill in the art would understand that nothing more is needed.

EX2007, 133:10-22.

45. I agree with Petitioner's expert that a POSA would understand based on Duvall's disclosure that nothing more is needed. And because a POSA reading Duvall would not find that anything more is needed, in my opinion, a POSA would not be motivated to look for Chu when given Duvall.

3. Petitioner's expert's modification to Duvall is not supported by how a POSA would understand the Chu reference

46. I also note that Petitioner's proposed modification to Duvall is not actually supported by Chu's disclosure. *See, e.g.*, EX1003, 109-115. Petitioner's expert relies solely on Chu's mention of the words "human intervention" to suggest that it teaches "providing information to a human for analysis." EX1003, ¶114. In my opinion, this characterization of Chu is overbroad and allows Petitioner to suggest making a modification to Duvall that is not actually consistent with what Chu discloses. What Chu actually discloses is much more specific than "providing information to a human." *Cf.*, EX1003, ¶114. Chu teaches prompting the same user that was originally trying to download a file. And although

Petitioner suggest that Chu teaches the general idea of sending information to a human, Petitioner does not actually modify Duvall to send generally send information to a human but modifies Duvall to send information specifically to an analyst. EX1003, 109-115. But Chu never teaches sending a prompt to anyone with special expertise. Rather, the human that Chu prompts is just a lay person—*i.e.*, anyone that might use the device to try and download a file. *See* EX1005, 44.

47. More importantly, Chu does not even explicitly disclose that any analysis is being performed by the human that it prompts. *See id.* And to the extent any analysis by that human is arguably implied, it is not the same type of analysis that Petitioner is trying to introduce into Duvall's system (*i.e.*, not an analysis by an analyst). *Compare, id., with*, EX1003, 109-115. Rather, the extent of any implied analysis would be limited to the analysis a generic user could be expected to perform when they received such a prompt. Chu does not suggest to a POSA that the prompted user can or will take any further steps to verify the source. Rather, a POSA would recognize that Chu's prompt merely allows the user to decide whether they want to accept the risk that whatever they are downloading has an unverified source. To the extent that can be considered "analysis" Chu is still not disclosing (expressly or impliedly) any sort of analysis that would require special expertise. Indeed, a lay user would have no special expertise at all.

48. Instead, a POSA would certainly recognize that Chu’s prompted user is not in the position to perform that type of further analysis needed by Duvall’s system. *See* EX1003, ¶142. Chu’s prompted user has less expertise than whoever ultimately has authority to edit Duvall’s filters because Chu’s prompted user is just a lay person using a computer. A lay user cannot be expected to have the special expertise of “a highly-skilled network administrator” that Petitioner’s expert suggests would be needed to tune Duvall’s filters. *See, e.g.*, EX1003, ¶142.

49. Notably, Chu’s prompt is also nearly identical to the existing prompts already disclosed by Duvall. Duvall discloses displaying a prompt on the screen of the user attempting to access a blocked website. *See* EX1004, 4:61-64 (“system also provides a screen on the user’s display indicating that the transmission was blocked, and advising the user on how to get back to the state before the user tried to open the stream and send the message”). At best, a POSA would understand that Chu teaches the equivalent of displaying another prompt on this same screen every time a transmission hits Duvall’s default filter. *Compare*, EX1005, 44, *with*, EX1004, 4:61-64. But this would be redundant and unhelpful to Duvall.

50. Petitioner’s expert apparently recognizes that modifying Duvall as Chu actually discloses would be entirely unhelpful to Duvall’s system. Petitioner’s expert even explains 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 exactly what Chu teaches. Petitioner’s expert is relying on Chu’s teaching of sending a prompt to the same user that would be accessing illicit content in Duvall. Indeed, a POSA would recognize that Chu is unhelpful to Duvall for this very same reason.

51. Thus, rather than try to make the modifications to Duvall that Petitioner’s expert suggests, as POSA would simply not be motivated to combine Chu with Duvall. Indeed, as I have explained, Chu is simply unhelpful to Duvall’s system.

52. I also note that during his deposition, Petitioner’s expert appeared to indicate Chu somehow taught “that the prompt is being sent to the person that has generated Chu’s filtering rules.” EX2007, 136:1-5. But this cannot be how a POSA would understand Chu because Chu never discloses any system that could receive or respond to such a prompt. *See generally*, EX1005.

53. Instead, a POSA would recognize that Chu is disclosed in the context of establishing trust policies for a single device, such as a personal computer. *See, e.g.*, EX1005, 23-25 (describing solutions to trust management solutions for individual devices). Thus, a POSA would understand that the prompt Chu discloses would be displayed on that same computer. EX1005, 44. Indeed,

whoever is trying to download the file at that time will be the one that sees and responds to the prompt.

54. In contrast, a POSA would not conclude that Chu contemplates some undisclosed system that allows the user that configured the filtering rules to receive the prompt. A POSA would also not conclude that its prompt would only be accessible by an individual with special expertise rather than the user trying to download the file. Therefore, a POSA reading Chu would not conclude that it teaches or suggests any sort of analysis being done by the user receiving the prompt. Indeed, such a reading of Chu is entirely unsupported by the reference. In my opinion, this cannot be how a POSA would understand Chu.

D. Claims 1-25 are valid because Duvall's direct and deferred-actions are never applied to the same transmissions

55. In my opinion, both Petitioner and its expert fundamentally misunderstand Duvall's disclosure. *See generally*, EX1003, ¶¶68-79, 99-107, 117-138. Petitioner and its expert also misunderstand how Duvall's direct-action and deferred-action filters operate on a technical level. *See generally, id.* This mistake is evident in Petitioner and its expert's characterizations of Duvall and became even more evident based on Petitioner's expert's deposition.

56. Petitioner's expert suggests that Duvall discloses the limitation of

“filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is neither discarded nor selected by filtering,” which is required by both independent claims of the ’641 Patent. EX1003, ¶¶125-138. Petitioner’s expert suggests that Duvall’s filtering system satisfies this limitation by applying both direct and deferred actions to the same transmission. *See* EX1003, ¶¶129-136; *see also id.*, ¶¶103-105; ¶¶76-77.

57. Petitioner’s expert first suggests that the direct-action filters are applied to some *unspecified* “transmission,” which can either be blocked or allowed by such direct-action filter. EX1003, ¶134. Petitioner’s expert then suggest that this *same* “transmission” might not be blocked or allowed by a direct-action filter, which makes it “post-filtering residue.” *Id.* Petitioner’s expert then mistakenly concludes that those *same unspecified* “transmissions” that were neither blocked nor allowed by any direct-action filters would then be further analyzed using deferred-action filters. *Id.*, ¶135. Petitioner’s expert’s suggestion that direct-action and deferred-action filters would apply to the same “transmission” is fundamentally wrong. A POSA would not read Duvall in this manner.

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

58. In my opinion, Petitioner’s expert has failed to appreciate that Duvall

discloses multiple types of transmissions, each of which is part of a sequence of different transmissions. *See, e.g.*, EX1004, 6:10-27. The different transmissions within this sequence of transmissions are processed differently by either direct or deferred-action filters. *See, e.g.*, EX1004, 6:10-27. Petitioner's expert's characterization of Duvall contributes to this mistake because he does not specify exactly which transmission he is talking about when discussing how Duvall's filters apply to "transmissions." *See, e.g.*, EX1003, ¶134. As a result, Petitioner's expert interprets Duvall differently than a POSA would.

59. Petitioner's expert appears to be reading certain portions of Duvall's disclosures, completely out of context, imagining an embodiment that operates completely differently than how Duvall describes itself. *See* EX1003, ¶¶68-79, 99-107, 117-138. The result is that Petitioner's expert mistakenly suggests that the additional criteria in Duvall's deferred action filters are being used to analyze the *same* transmissions previously filtered by Duvall's direct-action filters. *See* EX1003, ¶¶129-136; *see also id.*, ¶¶76-77.

60. For example, Petitioner's expert often relies on Duvall's server embodiment to suggest that Duvall's disclosure does not apply to his suggested implementation of Duvall. *See, e.g.*, EX2007, 160:12-18; 200:4-7; 148:12-18. However, Duvall is express that the filtering database used in the server

embodiment is the same filtering database as the one used in the client embodiment. EX1004, 8:24-27 (explaining the server-based system “of the filtering system uses the same type of filter database as a client-based filtering system, but the filter database is located on server 30”).

61. Indeed, with respect to Duvall’s server-based system, Duvall thoroughly discloses the only differences between the server-based embodiment and the client-based embodiment. *See*, EX1004, 8:18-9:11. These differences are 1) the location of the database, EX1004, 8:26-27 (“located on server 30”), a 2) local domain name table, EX1004, 8:28-38, and 3) a different “algorithm for pattern matching,” EX1004, 8:39-67. Given this clear disclosure from Duvall, a POSA would not assume that Duvall’s disclosures regarding the client-based embodiment are inapplicable to its server-based embodiment. Rather, a POSA would understand that the client-based embodiment would be identical except for those changes Duvall has identified. *See* EX1004, 8:18-9:11. There is no legitimate basis for Petitioner’s expert’s suggestion that the server embodiment would operate in a fundamentally different way than the client-based embodiment. In my opinion, Petitioner’s expert has “invented” an entirely new system purely to map to Schneier’s claims.

62. As shown above and below, A POSA would understand that Duvall’s

written disclosure directly contradicts Petitioner's expert's mistaken interpretation.

See, e.g., EX1004, 3:50-63, 4:56-58, 5:19-20, 5:30-40, 6:10-27, 9:14-11:20.

Petitioner's expert's reading of Duvall is irreconcilable with Duvall's express disclosure of its implementation and operation throughout the reference.

63. As I will explain further below, Petitioner's expert's fundamental misunderstanding of Duvall seems to stem from his failure to recognize that Duvall's system is designed to operate on a sequence of different transmissions. This mistake is most evident in Petitioner's expert's discussion of Duvall in the context of Figures 3 and 4. *See, e.g.*, EX1003, ¶¶125-138

64. More specifically, I note that Petitioner's expert correctly recognizes that Duvall's direct-action filters are applied according to Figure 3 (*see* EX1003, ¶130 (explaining the direct-action filters "are shown in Duvall's Figure 3"); *see also id.*, ¶¶131-133), while Duvall's deferred-action figures are applied according to Figure 4 (*see* EX1003, ¶135 (explaining Duvall's deferred-action filters are applied "as depicted in Figure 4")). Petitioner's expert also correctly recognizes that Duvall's filters are implemented in sequence, such that the processing shown in Figure 3 occurs before the processing shown in Figure 4. *See, e.g.*, EX1003, ¶¶104-105. However, what Petitioner's expert fails to recognize is that Figures 3 and 4 are actually processing different transmissions in a sequence of

transmissions. *See generally* EX1003, ¶¶125-138. Indeed, Figures 3 and 4 are not processing the same data. Petitioner's expert never acknowledges that Duvall's system operates on a sequence of transmissions at all. *Id.* Rather, Petitioner's expert mistakenly presents Figures 3 and 4 as if they were both applied to the same transmission. *Id.* But a POSA would understand that they are not.

65. A POSA with a proper understanding of Duvall would recognize that, although the direct-action filters are applied first (compared to deferred-action filters), they are *never* applied to the same transmission that the deferred-action filters later analyze. *See, e.g.,* EX1004, 4:38-57, 5:19-20, 6:10-27. Instead, the direct-action filter is applied to transmissions that must occur earlier in the sequence of transmissions, because they are needed to open a TCP stream. *See* EX1004, 6:10-18. On the other hand, the deferred-action filter is applied later in the sequence of transmissions, because those transmissions analyzed by the deferred-action filter can only be sent after the TCP stream has been opened. *See* EX1004, 6:19-27.

66. In my opinion, Duvall must be read in the context of the technical background that it provides. For example, Petitioner's expert does not consider the interplay between the TCP/IP protocol and Duvall's filtering system, which is vital to properly understanding Duvall's 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.

67. 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. A POSA would recognize that these higher-level protocols Duvall discusses relate to the data that would be sent through TCP streams and analyzed by its deferred-action filters. In my opinion it is telling that Duvall never discusses any lower-level protocols or any messages transmitted using a protocol other than TCP/IP.¹ Instead, Duvall’s filtering system is always discussed in the context of TCP/IP or associated higher level protocols.

68. For example, Duvall explicitly discloses how the client monitors TCP data streams. *See, e.g.*, EX1004, 3:59-61 (explaining its “client monitors [] ports and maintains internal tables that indicate the state of each active *TCP data*

¹ Indeed, a POSA would recognize that TCP/IP is (and was at the time) the most commonly used way to transmit content over the Internet, hence why Duvall was focused specifically on TCP/IP for its content censorship system.

stream” (emphasis added)). A POSA would therefore understand that Duvall’s filtering system operates in the context of these TCP data streams.

69. Moreover, when read in conjunction with the rest of Duvall’s disclosure, a POSA would understand that Duvall’s filtering system actually operates directly on these monitored TCP data streams. *See, e.g.*, EX1004, 3:50-63. Duvall itself discloses that “[t]he filtering system provides patching code for the client computer’s operating system.” EX1004, 9:14-15. A POSA would understand that based on Duvall’s disclosure of the patching code, Duvall’s system operates by patching the existing libraries in the operating system of a client device, which are used to process TCP/IP related data. *See* EX1004, 9:14-11:19. For example, Duvall discusses how to patch the Winsock API, which a POSA would understand is a library used by the Windows operating system to process transmissions according to the TCP/IP protocol. *See* EX1004, 10:34-41. A POSA would understand that Duvall’s filtering system thus operates by inserting patching code into an operating system’s pre-existing routines for processing TCP/IP-related transmissions. *See generally, id.* Thus, Duvall’s disclosure can only be properly understood when read in the context of TCP/IP and the higher-level network protocols.

70. Critically, a POSA would know that the TCP/IP protocol is a

connection-based protocol. Indeed, even to the extent one could argue that Duvall could be applied more broadly, it would still be limited to at least connection-based protocols. A POSA would understand that a TCP client must first open a TCP connection *before* any data can be transmitted or received over that connection. Indeed, this sequence of transmissions are 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.

71. A POSA would also understand that the transmissions *opening* the TCP data stream must actually be sent before any subsequent transmissions can be sent or received *through* an established TCP data stream. *See, e.g.*, EX1004, 2:58-60 (“To initiate communications with another computer over the Internet, a computer opens a port in its interface for a TCP data stream.”). Indeed, if the transmission to open the TCP data stream were not actually sent, then there would be no TCP data stream for the subsequent transmissions to be transmitted through.

72. In my opinion, Duvall is clear that the steps of Figure 3 are directed to determining whether or not a stream should be opened by either preventing or permitting the execution of the open command. *See* EX1004, 4:38-61. Given that

Duvall's filtering system operates by patching the operating system's libraries, a POSA would understand that Duvall's discussion of an "open command" refers to a command used by the operating system to open a TCP data stream. *See* EX1004, 1:39-40, 4:56-61. Duvall explains with respect to Figure 3, that Duvall's 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 the use of 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").

73. A POSA would therefore understand that Duvall's patching code shown in Figure 3 runs when the operating system would call the "open command" to open a TCP data stream. *See* EX1004, 4:37-57. Rather than immediately execute the "open command," Duvall's filtering system is patched to execute its patching code, which applies the process shown in Figure 3. *See* EX1004, 10:34-36 (explaining that patching "replace[s] Winsock calls with filtering system calls"); *see also, e.g.*, Fig. 5(d), 202. Duvall applies its filters and determines whether to execute the "open command." *See, e.g.*, Fig. 5(d), 204. If the "open command" should be executed, Duvall's system can simply call the original Winsock routine, *i.e.*, the open command. *See, e.g.*, Fig. 5(d), 210; EX1004,

10:38-39 (“a call 206 points to entry 208 of the original Winsock routine 210”).

74. In my opinion, POSA would recognize that the steps of Figure 4 are clearly directed to determining whether the content sent and received through the open stream should be discarded or replaced. *See* EX1004, 5:19-39. With respect to Figure 4, Duvall explicitly states that deferred-action filters are applied to “data [] transmitted over an open TCP/IP connection.” EX1003, 5:19-20. A POSA would therefore recognize that the processing of Figure 4 must occur *after* the stream is opened, rather than before (like Figure 3). Only after a stream is opened, can content then be transmitted through that opened stream. For example, Duvall 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.” *See* EX1004, 6:19-27. Duvall’s deferred-action filters are applied to these subsequent transmissions, and “can block the incoming data by discarding it or replacing it.” *Id.*

75. Notably, during his deposition Petitioner’s expert insisted that Figure 4 was “just talking about one particular example” and that it could actually “apply to all forms of traffic.” EX2007, 103:22-104:4. In my opinion, that understanding is directly contradicted by Duvall’s explicit disclosure that Fig. 4 applies “when data is transmitted over an open TCP/IP connection.” EX1004, 5:19-20. Duvall’s

disclosure of Fig. 4 does not use any language that would suggest to a POSA that the requirement that the TCP/IP connection be open was just exemplary. *see generally*, 5:7-40. And indeed, given the technical context of how the deferred-action filter operates, a POSA would recognize that Duvall is acknowledging that the TCP/IP connection must necessarily be open. *See* EX1004, 5:7-40. I note that Petitioner's expert provides no further evidence besides his say so.

76. Therefore, a POSA would also recognize that the steps of Figure 3 never apply to the same transmissions that are analyzed according to Figure 4. In my opinion, this is not only evident based on Duvall's explicit disclosure in relation to Figures 3 and 4, but also fully consistent with Duvall's disclosure of its patching code. *See* EX1004, 4:38-57, 5:8-29, 6:10-27, 9:14-11:16. Indeed, in the context of Duvall's patching code, the process shown in Figure 3 would be executed when the system calls an "open command," but the process in Figure 4 would not. *See* EX1004, 4:38-57, 5:8-29. Rather, the process shown in Figure 4 would only apply when Duvall's system attempts to send or receive a transmission through an opened stream—which would not involve any processing in accordance with Figure 3. *See* EX1004, 5:8-29.

77. Therefore, the suggestion that Figures 3 and 4 apply to the same transmission is unsupported by Duvall and contrary to how a POSA would

understand Duvall. Petitioner's expert has misunderstood Duvall.

2. Duvall's direct-action filters only operate on transmissions sent to open a TCP stream, which Petitioner's expert ignores

78. As I have already explained, Duvall's direct-action filters are applied when the system *opens* a TCP stream, rather than when transmissions are sent or received *through* an already opened TCP stream. *Compare*, EX1004, 4:38-57, *with, id.*, 5:8-29. To the extent Duvall's direct-action filters match with any transmissions, it is only the transmission that would be sent to open the TCP stream. *See, e.g.*, EX1004, 6:10-19. This understanding of Duvall is fully consistent with Duvall's entire disclosure and technical background.

79. For example, when describing direct-action filters in reference to Fig. 3, Duvall explicitly discloses that its "filtering system detects when the client opens the data stream for a particular port and IP address ... and searches the filter database for matching filters." EX1004, 4:39-42. Unsurprisingly, 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. 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. Indeed, 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.

80. And that is further consistent with Duvall's disclosure of its patching code. As I have discussed, a POSA would 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. *Compare* EX1004, 4:57-58, *with*, EX1004, 9:14-11:16. This allows Duvall's system to execute the process of Fig. 3 *before* the "open command," and also provides Duvall's system with access to the IP address and port used to execute the open command. *Compare* EX1004, 4:57-58, *with*, EX1004, 9:14-11:16.

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 at that point of Duvall's processing. *See, e.g.*, EX1004, 6:10-20. Indeed, when Duvall is operating in accordance with Figure 3, Duvall's direct-action filters would not even have access to any of the additional fields that Duvall's deferred-action filters need to consider. *See* EX1004, 5:8-15, 5:66-67. This is because the "open command" only uses an IP address and port to open a TCP stream and there are no other transmissions being considered at that point in time.

82. In my opinion, Petitioner's expert glosses over all of these details with

its general claim that Duvall’s direct-action “BLOCK filter blocks data transmission from passing through.” *See* EX1003, ¶103; *see also id.*, ¶72 (emphasis added). Petitioner’s broad statement avoids specifying *what* transmissions are being blocked or allowed and *how*. *Id.* But a POSA would recognize that 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). Indeed, there is no disclosure of Duvall’s direct-action filters being applied to transmissions sent or received through an already open TCP stream.

3. **Duvall’s deferred-action filters operate on transmission sent through an open TCP stream, and therefore cannot analyze the same transmissions filtered by direct-action filters**

83. As I have also explained, Duvall’s disclosure is also clear that the additional criteria in its deferred-action filters analyze transmissions sent through an already open TCP stream in accordance with Figure 4. EX1004, 5:8-29. Indeed, Duvall explicitly discloses that the additional criteria in Figure 4 is matched “when data is transmitted over an *open* TCP/IP connection.” EX1004, 5:19-20 (emphasis added). Duvall never discloses applying the steps of Figure 4 to

an open command, nor could it. *See generally* EX1004, 5:19-6:9. Indeed, that would make no technical sense as the open command only utilizes an IP address and port. The open command will never have any content that can match the additional fields being considered in Figure 4.

84. A POSA would recognize that Figure 4 only applies to transmissions that communicate content through an already open stream, such as HTTP transmissions. *See, e.g.*, EX1004, 6:10-27. Indeed, a POSA would understand that the transmissions sent through the open TCP stream relate to higher-level protocols, such as HTTP. Duvall itself recognizes as much. *See, e.g.*, EX1004, 2:46-47 (explaining TCP/IP “sits underneath and works in conjunction with higher level network protocols”); *id.*, 3:51-54 (explaining “certain default ports are associated with certain [higher-level] protocols” and that “HTTP communications are typically transmitted through a port numbered 80” (emphasis added)). Likewise, Duvall’s own example of its deferred-action filters in operation are also in the context of higher level protocols such as HTTP transmissions. *See* EX1004, 6:10-29 (sending HTTP request with a “GET command” and receiving HTTP response with the requested data).

85. In my opinion, a POSA would also recognize that this is why Duvall mentions the higher level protocols in its technical background. *See, e.g.*, EX1004,

2:45-50. For example, Duvall itself explains that the “locations, names, and meanings” of the additional fields in a deferred-action filter depend on the higher-level protocols used to transmit the content through the TCP stream. See EX1004, 5:66-67 (“locations, names, and meanings of keywords and filter patterns in the URL vary with the particular protocol”). A POSA would therefore recognize that Duvall’s deferred-action filters depend on the higher level protocols. In contrast, Duvall’s direct-action filters relate only to TCP/IP. Thus a POSA would recognize that Duvall’s direct and deferred-action filters clearly operate on different transmissions.

86. In my opinion, Petitioner’s expert completely ignores these technical differences when discussing how Duvall’s system moves from Fig. 3 to Fig. 4. See EX1003, ¶¶77, ¶¶103-105. Petitioner’s expert’s suggestion 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,” is factually incorrect. EX1003, ¶105 (emphasis added). Those transmissions analyzed by Fig. 4 are detected after a TCP stream is opened, whereas in Fig. 3 Duvall’s system is still deciding whether to open such a TCP stream. By the time Duvall’s system applies the process shown in Figure 4, Duvall must already have been allowed the transmissions related to opening the TCP stream (or else the TCP stream could not

be opened). Therefore, Figures 3 and 4 do not operate on the same transmissions.

4. Petitioner's expert's understanding of Duvall is directly contradicted by Duvall's own example of how its system operates

87. Duvall's own "example of blocking an HTTP transmission" with its filtering system is further confirmation that Petitioner's expert has misunderstood Duvall. *See* EX1004, 6:10-27. Duvall's example directly contradicts Petitioner's expert's understanding of Duvall while being entirely consistent with how I present Duvall.

88. Notably, Duvall's example also discloses that its direct-action filters are matched when "[t]he client *tries to open* a TCP/IP connection." *Id.*, 6:14-16 (emphasis added). Again, this is consistent with Duvall's Fig. 3, Step 100, which explicitly discloses that it detects "when the client opens the data stream." *See* EX1004, 4:40-42. And this is also consistent with how I have explained Duvall's system would work with its patching code.

89. Duvall goes on to explain 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. This further confirms what I have said about the steps of Fig. 3 occurring *before* the TCP stream opens.

90. Duvall then explains that "[r]ather than specifying blocking *at this*

time, a filter can indicate a deferred action.” *Id.* 6:19-20 (emphasis added)).

Duvall then immediately begins to discuss the HTTP transmissions that are sent through a now-opened data stream. *See id.*, 6:20-25. Duvall explains that its deferred-action filter “searches for a GET command as the keyword in an outgoing data stream.” *Id.*, 6:20-22. And “[w]hen the client sends a transmission with a GET command ... the host server will respond with data for that directory.” *Id.*, 6:23-25.

91. This discussion confirms that by Step 130 of Fig. 4, the TCP stream must have been opened. Otherwise, the host server could not “respond with data for [the requested] directory.” *Id.*, 6:23-25. And this understanding is consistent with what I have explained about how Duvall’s patching code would work. Indeed, by that point, Duvall’s filtering system is not intercepting the open command, but instead filtering the HTTP transmissions.

92. Therefore, after Fig. 3, step 116, when Duvall’s system determines that deferred-action filters need to be applied, a POSA would recognize that Duvall inherently *opens* the TCP stream. Thereafter, Duvall monitors that stream for transmissions that can be matched with its deferred-action filters, *e.g.*, for HTTP transmissions. *See, e.g.*, EX1004 1:45-47, 6:19-27. Notably, this is also consistent with how Duvall itself describes the process of deferring. *See* EX1004, 1:45-47

(“The system can defer the decision whether to allow or block, and then monitor transmissions to search for a particular command and a particular filter pattern.”).

Duvall’s discussion of monitoring after deferring suggests that Duvall is not simply applying the deferred-action filters to the same data filtered by the direct-action filter. *See id.* But rather Duvall is monitoring subsequent transmissions and applying the deferred-action filter to those subsequently monitored transmissions. *See id.*

93. After opening the TCP stream, in Fig. 4, Duvall applies the deferred-action filters to any newly detected transmissions sent over the now-opened TCP stream. *See* EX1004, 5:19-20. By the time the deferred-action filters could be applied to any transmissions (*i.e.*, Fig. 4, Step 130), any previously filtered transmission to open the TCP stream (detected Fig. 3, step 100) must have already been allowed (after Fig. 3, step 116). *See, e.g.*, EX1004, 6:10-20. A POSA would recognize that this must necessarily be the case.

94. But because those transmissions subsequently sent after the TCP stream opened were never previously filtered, they cannot be “post-filtering residue” as Petitioner’s expert suggests. *See, e.g.*, EX1003, ¶135. Therefore, in my opinion, Duvall’s deferred-action filters do not perform the claimed “analysis of post-filtering residue” by operating in accordance with Duvall’s Figure 4.

5. **Petitioner's expert's suggested implementation of Duvall is technically nonsensical**

95. Based on Petitioner's expert's deposition it appears that, Petitioner's expert is not only misreading Duvall but is actually relying on an entirely different and undisclosed system that operates differently than what Duvall discloses. *See, e.g.,* EX2007, 98:6-13. This statement by Petitioner's expert captures some of his misunderstanding:

A So a person skilled reading Duvall would understand that the direction -- direction -- direct action filters are applied to every -- there's a test to determine if direct action filters **apply to every packet**, independent of whether or not any connection -- any -- independent of whether or not any TCP connection has been established or not.

EX2007, 98:6-13.

96. Based on Petitioner's expert's deposition, it appears Petitioner's expert is relying on a system that effectively performs deep packet inspection to filter *packets* rather than the application-level transmissions actually disclosed by Duvall. *See* EX2007, 99:6-8 (suggesting Duvall "look[s] at every packet"), 98:6-13, 103:10-18. In my opinion, even if Duvall could broadly apply to more than what is expressly disclosed, there is no support for the system that Petitioner's expert is relying on. As I will explain below, the implementation Petitioner is relying on fundamentally alters how Duvall operates and is inconsistent with

Duvall's explicit disclosures.

97. I initially note that Duvall's disclosure thoroughly details how it operates at the application level. *See, e.g.*, EX1004, 3:50-63, 9:13-11:16. Indeed, Duvall discusses patching the Winsock API and contains no mention of any packets. *See generally* EX1004, 9:13-11:16. However, Petitioner's expert suggested during his deposition 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 actually discloses applying its filters to any packets at all let alone applying direct and deferred action filters to the same packet (or even the same transmission).

98. I also note that Duvall provides no guidance on *how* deep packet inspection could even be implemented. Thus, even if it could be obvious (which, in my opinion it is not) for a POSA to try to implement Duvall as a deep packet inspection utility there is still no disclosure or any guidance on how that could be accomplished by a POSA at the time. As Petitioner's own expert conceded, "at the time this concept of deep packet inspection was ... a new thing." EX2007, 71:11-12. And I agree, that absent any disclosures as to how to perform deep packet inspection, a POSA would not have known how to do so.

99. Moreover, packet inspection would fundamentally change how Duvall

operates. It makes no technical sense given Duvall can already operate directly on application data. As Petitioner's expert conceded during his deposition, "Duvall is writing its disclosures in the context of the way that a[n] application developer would view the network communications." EX2007, 93:1-4. 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. I agree that Duvall's disclosures are written in the context of the way an application developer views the network. Indeed, a POSA would recognize that Duvall is disclosing an implementation that operates on application-level data, hence why its disclosure is written from that point of view. *See, e.g.*, EX1004, 9:13-11:16. Likewise, there is no disclosure or suggestion of performing packet inspection anywhere in Duvall because Duvall does not contemplate performing any packet inspection. *See generally*, EX1004.

100. Notably, 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. And once opened, you can read and write to the socket like you would a file. *See also* EX2007, 93:12-14. Petitioner's expert is correct that an operating system views a

socket as a file. Opening a socket is akin to creating a new file. Indeed, Duvall's direct-action filter is designed to block transmission by preventing such a socket from ever being created.

101. Likewise, reading and writing from the socket is how a system receives or transmits information through a TCP connection. And indeed, a POSA would recognize that reading and writing to a created socket is how Duvall's client contemplates receiving and sending transmissions through an open TCP data stream. *See, e.g.*, EX1004 6:19-27 (providing exemplary operation consistent with filtering data being written and read from TCP sockets). Duvall's deferred-action filters therefore operate directly on the data being read and written to these TCP sockets.

102. Importantly, Duvall also expressly teaches a POSA that the Winsock library is patched to run its filtering code. EX1004, 9:16-11:13. And a POSA would recognize that the Winsock library implements the required TCP socket handling for the Windows operating system. Indeed, based on Duvall's disclosure it is clear that Duvall's filtering code is run when the library makes a call to read and write from the socket. *Compare*, EX1004, 9:16-11:13, *with, id.*, 6:19-27. In this way, Duvall's deferred-action filters can directly analyze the content in the socket to match with keywords or filter patterns.

103. In contrast, Duvall does not teach a POSA how to match its 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 actually send the data over the network. Matching a keyword and filter pattern across multiple packets is not a trivial task and Duvall never discloses how this could be accomplished. Indeed, that would require the ability to perform deep packet inspection so that the transmitted content could be reconstructed based on the individual packets. But Duvall can simply analyze the content as it is written or read from a socket, which allows Duvall's system to avoid any need for deep packet inspection altogether. *See* EX1004, 9:16-11:13. Thus, Petitioner's expert's suggestion that Duvall would perform deep packet inspection makes no technical sense.

104. Moreover, using Duvall's deferred-action filter's additional criteria to try 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 the IP address and port. *See* EX1004, 4:37-58. Petitioner's own expert admits that the "connection establishment packet does not have a payload." EX2007, 94:15-16.

And indeed, it does not have a payload. Therefore, matching keywords (*cf.* Fig. 4, 134) and filter patterns (*cf.* Fig. 4, 136) would be entirely pointless. Petitioner's expert implicitly recognizes that Duvall's keywords and patterns relate to higher-level protocols by acknowledging that Duvall's deferred-action filters may need to be matched across multiple packets. Thus, Petitioner's expert's suggestion that Duvall's deferred-action filters would then be matched to an individual SYN packet makes no technical sense.

105. Likewise, it would not make technical sense to force Duvall's direct-action filters to apply to packets in an already opened stream. I note that there are no actions Duvall's direct-action filters could reasonably take when matched with such packets in an open stream. Indeed, the fact that a stream is even opened, can only mean that (1) Duvall's direct-action filter either previously ALLOWED the stream to open, or (2) there was no applicable direct-action filter (only deferred-action filters). *See* EX1004, 4:37-55, 6:10-18. 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. Likewise, if it was already determined that there was no applicable direct-action filter, then no direct-action filter will apply to any data in the open stream.

6. Duvall's disclosure, when properly understood, fails to

disclose “analysis of post-filtering residue”

106. I initially note that the patent examiner examining the Schneier application found that the “prior art does not disclose or suggest data neither discarded by negative or positive [filtering] is the residue that is sent for further analysis.” EX1002, 238. Given Duvall’s direct-action filters (*i.e.*, Figure 3) and deferred-action filters (*i.e.*, Figure 4) apply to different transmissions, there is also no “residue that is sent for further analysis” in Duvall. *Cf., id.*

107. As I have explained, 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.” Indeed, the residue is what is left over after the filters already been applied—and in this case no filter has been applied to the transmissions analyzed by Duvall’s deferred-action filters. Likewise, because the transmissions analyzed by Duvall’s deferred-action filters were never filtered, they also could not have been blocked or allowed by Duvall’s direct-action filters, nor discarded or selected by filtering. *See* EX1001, Claim 1(b).

108. In my opinion, a POSA would not read Duvall such that both direct and deferred actions could be taken with respect to the same transmission. Petitioner’s expert’s position is essentially modifying Duvall to the “residue that is

sent for further analysis.” *Cf.*, EX1002, 238. But such a modification fundamentally changes the way Duvall operates as compared to what was disclosed. Petitioner’s expert assumes this change would be obvious but does not actually provide any explanation of why or how it would be obvious besides merely suggesting it *could* be done.

109. Therefore, it is my opinion that a proper reading of 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.”

E. Claims 1-25 are valid over Duvall-Chu even under Petitioner’s Incorrect Interpretation of Duvall because Duvall fails to disclose “post-filtering residue” under a proper construction of that term

110. In my opinion, a POSA reading the Schneier claims would have understood that the filtering process that creates “post-filtering residue” must be distinct from the “analysis of post-filtering residue” that follows. This is evident from Schneier’s clear distinction between the anomaly engine and the filtering subsystems that perform these two separate steps. EX1001, 8:55-62; *see also compare, id.*, Fig. 2, 2020, 2030, *with, id.*, Fig. 2, 2050.

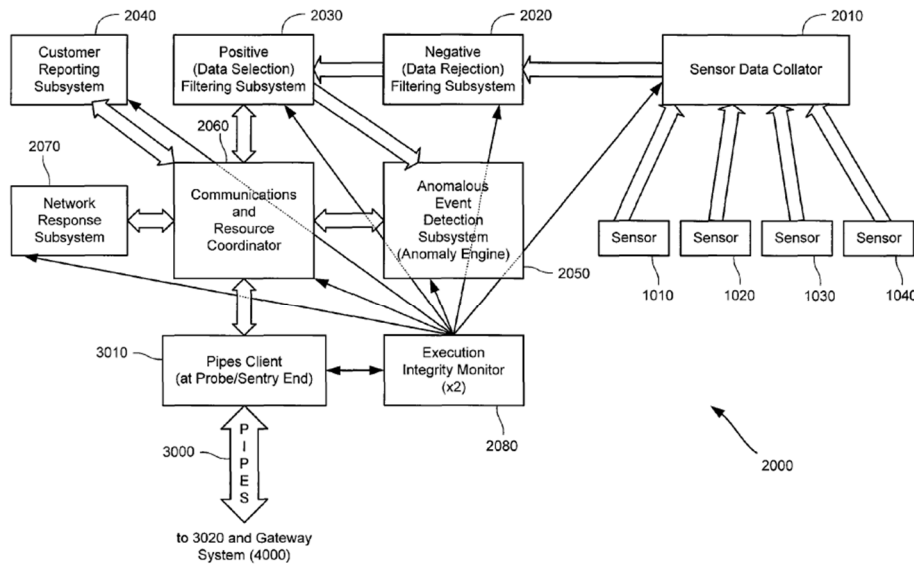


FIG. 2

EX1001, Fig. 2.

111. A POSA would obviously recognize that the anomaly engine can make use of other filters. But that does not mean the filters in the filtering subsystem can be artificially broken in half so that *some* of those filters would be treated as performing the “analysis of post-filtering residue.” In other words, a POSA would understand that the “analysis of post-filtering residue” cannot merely be applying filters from the same positive and negative filtering subsystems.

112. In my opinion, any proper construction of “post-filtering residue” as that term is used in Schneier must acknowledge that the filtering of status data (to select or discard status data) is first completed prior to the subsequent analysis,

regardless of whether that later analysis also uses filters.

113. I note that in Petitioner’s mistaken interpretation of Duvall, he suggests that Duvall’s direct and deferred-action filters are all applied to the same transmission, even though there is no such supporting disclosure. *See* EX1003, ¶105. Accordingly, even if you credit Petitioner’s reading of Duvall, its direct and deferred-action filters are just part of a single filtering subsystem that ultimately either blocks or allows each transmission. There is no basis for artificially breaking Duvall’s system in half to suggest that only certain filters in Duvall’s filtering subsystem are selecting and discarding, while the other filters—which operate in exactly the same way—are performing some *distinct* analysis. *See, e.g.,* EX1004, 1:30-50.

114. Indeed, even Petitioner’s own expert relies on Duvall’s disclosure that “the system can block the incoming data by discarding it,” which is in reference to Duvall’s deferred-action filters to show that Duvall’s system discards when it blocks, with respect to limitation 1(b). *See* EX1003, 133 (citing EX1004, 6:26-27). But if Duvall’s deferred-action filter is doing the discarding, it cannot also be performing the distinct and separate “analysis.” In other words, Petitioner’s use of deferred action filters as meeting both the filtering and analysis limitations makes clear that they are trying to read out limitations in Schneier.

F. Claims 1-25 are valid over Duvall-Chu because Petitioner’s expert never explains how Duvall-Chu selects, discards, or further analyzes “status data”

115. Petitioner’s expert overlooks Claim 1’s limitations regarding “status data.” The agreed-upon construction of “post-filtering residue” plainly requires “status data” to be selected and discarded. *See* EX1013 at 4. Moreover, the “analysis of post-filtering residue” must further analyze the residual “status data.” *See id.*

116. In light of these constructions, Petitioner must show that Duvall’s (1) direct-action filters select and discard status data, while Duvall’s (2) deferred-action filters analyze the residual status data. But Petitioner and its expert provides no explanation of either point as it relates specifically to “status data.” *See, e.g.*, EX1003, ¶133-136.

117. Petitioner’s expert only explains how traffic is blocked or allowed by Duvall and seems to equate blocking/allowing the traffic to selecting or discarding *traffic*. *See* EX1003, ¶133 (suggesting “data that is blocked is discarded data,” while “[d]ata that is allowed is selected data”). Indeed, Duvall’s disclosure only discusses blocking and allowing the traffic or its contents, rather than blocking/allowing or selecting/discarding status data. *See generally*, EX1004, 1:30-52.

118. But there is no explanation by Petitioner how selecting/discarding *traffic* relates to selecting/discarding *status data*, which are very different things. *See*, EX1003, ¶¶133-136. Indeed, a POSA would recognize that selecting and discarding status data is materially different than selecting and discarding the traffic. This is clearly evidenced by the fact that Schneier’s security system selects and discards things of an opposite nature to what Petitioner suggests is being selected and discarded by Duvall. *Compare*, EX1001, 8:51-55, *with*, EX1003, ¶¶133. Schneier selects the status data that relates to unwanted traffic (i.e., security threats) while discarding the status data that is benign. *See* EX1001, 8:51-55. But Duvall allows benign traffic, while blocking unwanted traffic. *See generally*, EX1004, 4:22-37. Thus, according to Petitioner, Duvall is selecting what is benign while discarding what is unwanted. EX1003, ¶¶133.

119. Likewise, Petitioner’s expert also never identifies in his declaration any “status data” that is being analyzed by Duvall’s deferred-action filters. *See* EX1003, ¶¶133-136. Indeed, it is not clear how Petitioner or its expert is suggesting Duvall’s deferred-action filter is analyzing status data. *See id.* Petitioner’s expert’s declaration 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*, ¶¶78-94 (explaining that Duvall’s deferred, and direct-

action filters analyze different transmissions). And the Petition fares no better—also failing to explain how the deferred-action filter analyzes anything besides traffic.

120. I note that during Petitioner's expert's deposition, he offered a new explanation of how the status data was being analyzed. However, this explanation was never presented in either the Petitioner nor his prior declaration.

Well, a person of skill in the art reading Duvall would understand that it discloses status data because, for example, it discloses things like IP addresses, which I understand previously was found to constitute status data. Duvall discloses these are operating on packets, just like a person of skill would understand the '641 is operating on, and so a person of skill in the art would understand that if a packet carrying an IP address is not subjected to allow filtering, not subjected to block filtering, it goes on to deferred action processing, that packet still carries with it the status data. So the status data is still there, and it's -- it's still -- things -- status data, such as, for example, the IP address are still in the packet when it hits the deferred action processing stage.

EX2007, 115:19-116:16.

121. I also note that this explanation could not have been inferred from his declaration given he is relying on the assumption that Duvall operates on packets, which is never disclosed anywhere in Duvall. Petitioner's expert also did not make this assumption clear in his declaration. Moreover, as I have explained, *supra*,

¶¶95-105, the idea that Duvall operates directly on packets is contrary to what a POSA would have understood when reading Duvall. Thus this new explanation comes completely out of left field.

G. Claims 1-17 are valid in view of Duvall-Chu because Petitioner never identifies an “analyst system”

122. A POSA’s understanding of the term “analyst system” would be informed by Schneier disclosure. For example, Schneier’s 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 also 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.

123. Although a POSA would recognize that an analyst system is not limited to just SOCRATES, the Schneier patent’s description of SOCRATES is still highly instructive to how a POSA would understand the meaning of “analyst system” when reading Schneier’s claims. For example, it would be clear to a POSA that when Schneier uses the term analyst system, Schneier is not referring to just a group of analysts or some system used by an end-user. Instead, it plainly denotes a technological system that is designed to be used *by the analysts* rather than the end-user and is designed to assist the analysts in their role.

124. I note that although Petitioner’s expert suggests that Duvall-Chu’s “human intervention would be performed by an analyst system,” EX1003, ¶142, he provides no explanation of where this analyst *system* comes from or what it even is in Duvall-Chu. At best, Petitioner’s expert seems to argue why it would have been obvious to have an *analyst* manage Duvall-Chu’s system, but I see no explanation of what system those analysts would be using. *See generally*, EX1003, ¶139-145.

125. I would also note, that simply because a user can now be characterized as an analyst, a POSA would recognize that it would not automatically change the nature of any system used by that user into an analyst system. For example, a POSA would understand that just because an “analyst”

happens to be using one of the monitored devices—a generic computer for example, that would not suddenly and automatically transform that monitored device into an “analyst system” as this term is used by Schneier. Rather, the analyst system must be a system designed to assist an analyst in their role.

126. I would also note that Petitioner and its expert’s rationale for including an analyst in the first place seems to be based on obviousness in light of references other than Duvall and Chu. *See id.*, ¶¶142-143 (citing EX1037-1039). But none of those other cited references show that transmitting to an analyst system would be *inherent* to Duvall-Chu. *See id.*

127. I also note that Petitioner’s expert also never explains why it would be obvious to add an analyst *system* to Duvall-Chu. *See id.* In fact, Petitioner’s expert never even specifies what the analyst system in Duvall-Chu is. *See generally*, EX1003, ¶¶139-145. Notably, even if the other references taught that including an *analyst* into Duvall-Chu would be obvious, there is still no disclosure of any analyst system used by those analysts. *See generally*, EX1037-1039. In fact, there is no discussion of an analyst system in any of the cited prior art. *See generally*, EX1004, EX1005, EX1037-1039. Likewise, there is no disclosure how an analyst system could be implemented or how it is even used by analysts. *See generally*, EX1004, EX1005, EX1037-1039. Without any disclosure it would not

have been obvious to a POSA what the “analyst system” is or how to implement it.

128. For example, Petitioner relies on EX1037 as evidence that outsourcing the responsibility for editing an IDS’ filters has previously been done. *See* EX1003, ¶143. Presumably, Petitioner is suggesting that the third parties involved with the disclosed outsourcing are akin to analysts. But EX1037 provides no actual disclosure of *how* such outsourcing was accomplished, nor any disclosure of the systems used by the third-party. *See* EX1037, 224. Notably, the fact that outsourcing was only provided for NetRanger, but not other IDS’ clearly shows that the third parties did not have a one size fits all solution. *See* EX1037, 224. Thus, there is no evidence that whatever system was used for NetRanger could also work for Duvall-Chu. This disclosure is insufficient to show a POSA how to modify Duvall-Chu’s system to include an analyst system, even if an analyst were introduced into Duvall-Chu.

129. As I will explain further below, neither Duvall nor Chu discloses any system that could even receive the transmissions (*i.e.*, prompt) sent by Duvall’s probe after being combined with Chu, besides the same device that was originally trying to access illicit material (or trying to download the file in Chu). *See* EX1004, 8:11-12; EX1005, 44. In other words, both Duvall and Chu only teach returning information back to the original user at the client device rather than to an

analyst. *See* EX1004, 8:11-12; EX1005, 44. And a POSA would understand that the client device being used to access content would clearly not be an analyst system. Thus, neither reference contains any disclosure of any analyst systems capable of receiving what was sent from the probe.

130. Duvall clearly lacks any analyst systems because there is no disclosure or even any suggestion that Duvall's editing manager would receive any information from Duvall's probes. *See* EX1004, 8:1-16. Rather, a POSA would recognize Duvall is merely disclosing a standard database editing utility that is linked to the filtering database.

131. Likewise, Chu also lacks an analyst system. *See* EX1005, 44. Chu implements a trust management system on devices like personal computers. *See, e.g.,* EX1005, 23-25. Therefore, a POSA would understand that when Chu's policy says, "prompt me for attention," Chu is referring to the user that is currently using the computer and trying to download the file. *Id.* Indeed, Chu does not even disclose another device or another way to send a prompt specifically to the user that edited the policies. *Cf.* EX2007, 136:3-5 (suggesting "the prompt is being sent to the person that has generated Chu's filtering rules"). Rather, a POSA would recognize, that Chu is simply referring to a standard prompt on that same device the user is using to download the file. *See* EX1005, 44.

132. Therefore, Chu only teaches displaying a prompt on the device of the same user attempting to download a file. EX1005, 44. There is no teaching or suggestion that whoever is attempting to download the file would have any sort of special expertise. Indeed, 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)). And it is in no way similar to Duvall's editing manager.

133. Moreover, there is no disclosure in Chu of how to implement the type of "analyst system" that Petitioner suggests is needed for Duvall-Chu. Petitioner suggests a prompt would be sent to someone that is "not the user trying to access the illicit content." *See* EX1003, ¶143. But Chu does not disclose any way to do that because there is only a single device, which is being used by the same user trying to download the file.

H. Claims 1-17 are valid in view of Duvall-Chu because Petitioner fails to show Duvall-Chu is reasonably capable of dynamic modification

134. As I understand Petitioner's expert's explanation of how Duvall satisfies limitation 1(e), he suggests that the use of a database by Duvall inherently allows the filtering system to perform dynamic modification. *See* EX1003, ¶¶149-154. This is false. Petitioner's expert conflates a *database's* ability to be edited

without taking anything else down and an *application's* ability to rely on such a database dynamically. *See id; see also* EX2007, 153:18-154:20 (answering “you certainly don’t have to take an application using a database offline *to update a database*” (emphasis added) when asked whether “an application using the database would[] need to be taken offline”).

135. Notably, a POSA reading Duvall would actually recognize that Duvall does not even contemplate dynamic modification as an option. At minimum, dynamic modification is not inherent to any of Duvall’s embodiments. Indeed, Duvall provides many suggested improvements without ever considering whether it would affect the ability of its system to perform dynamic modification because a POSA would recognize that Duvall presumes it is simply not an option. *See, e.g.,* EX1004, 8:28-61, 3:46-49. For example, Duvall suggests that its server-based system performs pre-processing, which is clearly incompatible with dynamic modification. *See* EX1004, 8:28-61. But Duvall never considers the cost of giving up the ability to dynamically modify, because Duvall never presumes its system would perform dynamic modification in the first place.

136. As another example, Duvall suggests maintaining the database on the hard-drive and copying the database into RAM during operation. *See* EX1004, 3:46-49. A POSA would recognize that this was a well-known way to avoid the

problems related to enabling dynamic modification. Indeed, by relying on a RAM copy Duvall can sidestep any additional solutions needed to enable its system to rely on the database dynamically. The RAM copy of the database does not automatically reflect the latest filters in the hard-drive. Rather, a POSA would recognize that copying to RAM allows Duvall's system to utilize the RAM copy independent of any changes to the database maintained on the hard drive. The filtering system will only modify its analysis capability upon restarting the system when the hard drive version of the database is copied into memory again. There is no evidence that dynamic modification would have been obvious to a POSA.

137. Notably, Petitioner's expert, during his deposition, tried to ignore Duvall's explicit disclosure of using a RAM copy by suggesting the server-based embodiment was different:

Q Okay. Edits to the database on the hard drive aren't going to be automatically reflected in the RAM copy until it's copied again into RAM, right?

A So this is describing the client-side filtering system, which is not the embodiment in Duvall that I'm relying on.

Q And you're relying on the server embodiment?

A Correct.

Q Okay. Where in Duvall does it discuss how the database is stored in the server embodiment?

A I don't know that Duvall discloses that detail, because that's just simply an implementation detail that's well within the knowledge of a person of ordinary skill in the art. Again, because it's saying that -- you know,

because you're using known database editing techniques, I think a person of skill in the art would understand that you're just using known database technology. Duvall isn't claiming any innovation in databases, so that detail isn't specified here, but that's well within the knowledge of the person of ordinary skill in the art's knowledge.

EX2007, 160:12-161:6.

138. But Duvall explicitly discloses that the server-based “version of the filtering system uses the same type of filter database as a client-based filtering system, but the filter database is located on server 30.” EX1004, 2:23-27.

139. I also note that during Petitioner’s expert’s deposition, he appeared to suggest that Duvall might be using of a specific type of caching with the RAM copy. EX2007, 161:16-162:13, 163:7-15 (suggesting that despite Duvall’s disclosure of a RAM copy, “[t]he database is the thing that is searched”). But not only does Petitioner’s expert never provide any evidence of this specific type of caching solution at the time, but Petitioner’s expert also admits that even such caches do not inherently allow for dynamic modification. *See* EX2007, 165:1-5 (“Caches can certainly be out of date, which is why any system, in particular a database system, would be known to run a cache consistency protocol to make sure the cache always has fresh contents.”). Rather, these caches face an additional problem related to maintaining cache consistency which has an entire field of art devoted to resolving such problems. Thus, a POSA would actually have two

problems to solve: (1) cache consistency, and (2) how to allow Duvall's filtering system to rely on a database dynamically. Petitioner's expert thus provides no evidence of any dynamic modification solutions known to a POSA at the time that would work with Duvall's system.

140. I have been informed by counsel that limitation 1(e) has been construed to require only "reasonable capability." However, I have also been informed that "reasonable capability" does not refer to mere possibility. Instead, I have been informed that the term recognizes that a system need not perform the claimed functionality in all modes of operation, but instead must be "reasonably capable" of performing the claimed functionality at least some of the time and without "significant alteration." For example, I understand that if a system already has the required functionality, but it is just not enabled, the system would be "reasonably capable" of performing the required functionality. Likewise, if a system performed the claimed functionality only under certain circumstances, that system would also be "reasonably capable" of performing the required functionality. However, just because it would be possible to add the claimed functionality to a system during certain modes of operation, does not mean that system is "reasonably capable" of performing the required functionality.

141. Based on this understanding, and in my opinion, Duvall is not

“reasonably capable” of dynamic modification. As I have explained in paragraph 135, Duvall’s system is clearly not inherently capable of dynamic modification in any mode of operation. Thus, Duvall’s system would have to be significantly altered. Likewise, as I explained in paragraphs 136-139, there is also no evidence that a POSA would have known how to modify Duvall’s system at the time of invention to perform dynamic modification (in any mode of operation). While it is certainly not impossible to imagine some way to implement a form of dynamic modification with today’s technology, there is no evidence that it would have been obvious to do at the time of Schneier’s invention.

I. Claim 6 is valid in view of Duvall-Chu because Petitioner fails to show how Duvall-Chu performs analysis in a SOC as part of the “*identifying step*”

142. In my opinion, Petitioner has completely failed to show how its combination of Duvall-Chu reads on Claim 6. Petitioner and its expert’s discussion of Claim 6 only argues why the analyst system that Petitioner suggests exists in Duvall-Chu for Claim 1(c), would be located at a remote SOC. Pet., 44-46; EX1003, ¶¶186-174. But this is not what Claim 6 requires. In my opinion, Claim 6 narrows the “identifying step” of Claim 1(b). Petitioner’s expert apparently agrees this is the case based on his deposition. *See* EX2007, 168:16-17 (“I believe that Claim 6 narrows the disclosures – the limitations of B of Claim

1.”).

143. The only analysis Petitioner suggests would be performed by Duvall-Chu’s purported analyst system occurs after the “identifying step” is already complete. *See* Pet., 44-46 (citing Pet., §VI.A.5). According to Petitioner’s Duvall-Chu combination for Claim 1, once Duvall’s filtering system completes the “identifying step,” (i.e., Claim 1(b)) it then prompts an unspecified analyst system (as part of the transmitting step in Claim 1(c)). *See generally*, Pet., §VI.A.5. With respect to Claim 1, Petitioner suggests the analyst at this supposed analyst system will perform some analysis based on that prompt. *See generally*, Pet., §VI.A.5. This analysis clearly occurs *after* the Claim 1(b) “identifying step” instead of as part of it based on Petitioner’s mapping of Duvall-Chu.

144. Petitioner never identifies any other analysis performed by the analyst system, which could be part of the Claim 1(b) “identifying step.” *See generally*, Pet., §VI.A.5; *see also* Pet., 44-46. Therefore, even if the analyst system was located in a SOC as Petitioner argues, there is still no analysis being done in the SOC as part of the “identifying step,” which is required by Claim 6.

J. Claim 15 is valid in view of Duvall-Chu because Petitioners mapping requires showing that the prior art performs the dynamic modification step of Claim 1(e)

145. In my opinion, Petitioner fails to show how any combination of prior

art references teaches or discloses Claim 15. Petitioner's attempt to show that its Duvall-Chu combination discloses the limitations of Claim 15 relies on Duvall-Chu also performing the dynamic modification step referenced in limitation 1(e). In my opinion, because Petitioner's Duvall-Chu combination does not actually perform the dynamic modification step, it also cannot satisfy the limitations of Claim 15.

146. I initially note that I am aware that the Board previously construed limitation 1(e) to only require "mere capability." Paper 9, 39. I have been informed by counsel that there is a dispute about whether "mere capability" requires Duvall-Chu to actually perform the dynamic modification step at least some of the time or whether Duvall-Chu merely needs to be capable of being modified to perform that capability. In my opinion, regardless of what Claim 1 would require with respect to "mere capability," Petitioner's Duvall-Chu combination relies on actually performing dynamic modification in order to satisfy the limitations of Claim 15.

147. Petitioner's expert admitted during his deposition that he only considered how Duvall-Chu would satisfy the limitations of Claim 15 by performing this dynamic modification step. 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.").

And I agree Petitioner's Duvall-Chu combination would need to perform the dynamic modification step in order to satisfy the limitations of Claim 15 as presented by Petitioner and its expert. Therefore, Petitioner must show that the dynamic modification step is actually performed by Duvall-Chu as a condition precedent to satisfying Claims 15. As I explain in paragraphs 134-141, Petitioner's Duvall-Chu combination does not perform the dynamic modification step recited in Claim 1(e) at any point in time.

148. Therefore, in my opinion, Claim 15 is not taught by Duvall-Chu.

K. Claims 7-16 are valid in view of Duvall-Chu-Trcka because Petitioner's expert fails to consider the technical realities of Trcka's implementation

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

149. In my opinion, Petitioner's motivation to combine Trcka with Duvall-Chu is deeply flawed because, as I will discuss below, the techniques disclosed by Trcka are incompatible with Duvall-Chu's system despite Petitioner's expert's conclusory opinions to the contrary.

150. Indeed, much of Petitioner's expert's opinion is founded on false assumptions that a POSA would not make. For example, Petitioner's expert opines

the following:

Indeed, Duvall performs filtering based on data contained in network packets, such as “port number and IP address,” EX1004, 3:64-4:55. Trcka similarly captures and presents packet-level data, including “headers of all packets transferred over the network,” EX1014, ¶¶38-39. Duvall and Trcka thus operate upon similar traffic data, indicating that Trcka’s analysis techniques would apply equally well to the data in Duvall-Chu’s system.

EX1003, ¶186.

151. I initially note that Petitioner’s expert’s statement that “Duvall performs filtering based on data contained in network packets,” *id.*, is not fully accurate. EX1003, ¶186. For example, if Duvall blocks an outgoing transmission, the filtered data will not relate to any network packets because those packets will never be created or sent (because the stream was blocked from being opened). So, while it is true that occasionally some of the data that Duvall filters might also be contained in network packets, that observation really has no bearing on how Duvall’s system actually operates.

152. Moreover, Petitioner’s expert appears to actually be suggesting that Duvall’s filters *operate* on network packets, which would be false and contrary to Duvall’s disclosure. Indeed, after explaining how Trcka relies on network packets, Petitioner’s expert then concludes that “Duvall and Trcka thus operate upon similar traffic data.” EX1003, ¶186. But as I explain in paragraphs 95-105, Duvall does

not operate on packets at all.

153. In fact, a POSA would recognize that Duvall’s system actually has no visibility into the network packets—making it incompatible with Trcka. Duvall’s filtering system patches the operating system (*e.g.*, a Winsock API), EX1004, 9:16-11:13, and applies its filters to Duvall’s attempts to execute an open command (*i.e.*, direct-action filter) or read/write from a TCP socket (*i.e.*, deferred-action filter). *See* EX1004, 6:10-27; *see also* EX1004, 4:37-58; 5:7-40. Therefore, Duvall’s filtering system does not detect, record, analyze, monitor, or even filter any network packets.

154. Trcka, on the other hand, as Petitioner’s expert recognizes, does operate directly on network packets. In fact, access specifically to the raw packets is “[a]n important benefit of [Trcka’s] recording process.” EX1014, ¶12. And it is due to recording the raw packets that these “recordings can therefore be used to perform [the] wide range of network analysis [techniques]” taught by Trcka. *Id.* I also note that Trcka not only requires the raw packet data, but it requires *all* the raw network traffic from a monitoring point. *See id.*, ¶12, ¶38 (explaining recording process “involves passively capturing, at the data link level [], all network traffic that is present at [a] network monitoring point”). This is because Trcka’s analysis techniques rely on the ability to “fully-reconstruct and evaluate

virtually any type of network transaction.” *Id.*, ¶12.

155. Therefore, in my opinion Petitioner’s expert’s opinion that “Trcka’s analysis techniques would apply equally well to Duvall-Chu” is actually false. *Cf.* EX1003, ¶186. On the contrary, as I explained above, Duvall-Chu and Trcka are incompatible with each other because Duvall-Chu does not have visibility into the network packets that Trcka’s analysis requires. And besides Petitioner’s expert’s conclusory statements, which I have just explained are not accurate, Petitioner and its expert provide no further evidence that this assumption is true.

156. The incompatibility between Duvall-Chu and Trcka also directly affects Petitioner’s suggested motivation to combine Trcka into Duvall-Chu. Petitioner suggests 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.’” Pet., 51. But this motivation is flawed because Trcka’s disclosed techniques cannot be used to determine whether Duvall-Chu’s filtering system is filtering too much or too little as a technical matter. In fact, Trcka’s disclosed techniques cannot even determine on a technical level what is being blocked or allowed by Duvall’s filtering system.

157. Trcka’s disclosed analysis techniques can only analyze an archive of network traffic that is created by monitoring the packets that are sent through the

network. *See* EX1014, ¶¶35-67, 108-109. As these data packets pass through a monitoring point, Trcka routes that traffic to an archive. *See* EX1014, ¶38. That archive can then be analyzed using Trcka’s interactive analysis tools. EX1014, ¶53, 108-109.

158. But Duvall’s filtering system blocks and allows transmissions *inside* the operating system. *See* EX1004, 9:14-15 (describing “patching code for the client computer’s operating system”). As a result, the data recorded in Trcka’s analysis tools will not and cannot reflect the decisions Duvall’s client has made to either block or allow the traffic. *Cf.* EX1014, ¶38. For example, when Duvall blocks outgoing data, that data is simply not sent over the network. *See, e.g.,* EX1004, 4:56-58. There are thus no packets for Trcka to record, and no way for Trcka to know that something was blocked by monitoring any point on the network. Likewise, traffic received by Duvall’s system over the network will eventually be blocked or allowed in Duvall’s operating system. *See, e.g.,* EX1004, 6:19-27. Thus, Trcka will record that traffic in its archive regardless of whether Duvall ultimately decides to block or allow that traffic internally.

159. If Duvall’s filtering system is integrated in a firewall rather than at a client endpoint, then Trcka’s techniques will also be unable to distinguish between the firewall and Duvall’s filtering system. *Cf.* EX1014, ¶38. So, Trcka’s disclosed

techniques are actually unable to “to enable the user to analyze whether ‘the filtering system is filtering too much or too little.’” *Cf.*, EX1003, ¶186. In my opinion a POSA would not have been able to combine Trcka with Duvall-Chu for this specifically-alleged purpose with a reasonable expectation of success. Therefore, in my opinion, Petitioner’s motivation to combine Trcka into Duvall-Chu is deeply flawed. *Cf. id.*

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

160. I separately note that Petitioner and its expert never explains exactly how Trcka’s analysis is being incorporated into Duvall-Chu’s system. *See generally*, EX1003, ¶¶184-206. There is no discussion of the components, systems, or methods that are being modified or added into Duvall-Chu’s existing system. *See id.* And no discussion of the components, systems, or methods taken from Trcka’s disclosure besides the resulting functionality of Trcka’s techniques. *See id.* Petitioner and its expert’s discussion is insufficient to inform a POSA about what their combination of Duvall-Chu-Trcka actually is, what it looks like, or how it operates.

161. This problem with Petitioner’s lack of explanation as to how Trcka is combined with Duvall-Chu is exacerbated by the fact that Petitioner is relying on

the same disclosure of Trcka to teach two distinct functionalities that needs to be performed in entirely separate portions of Duvall-Chu's system. *Compare*, EX1003, ¶¶189-195, *with, id.*, ¶¶196-202. Indeed, Petitioner and its expert appear to be relying on only a single combination of Duvall-Chu-Trcka, but the limitations supposedly taught by this combination relate to entirely different portions of Duvall-Chu's system. *Compare*, EX1001, Claims 7-9, 12-13, *with, id.*, Claims 10-11.

162. Petitioner argues that its Duvall-Chu combination performs the “identifying step” of Claim 1(b) within Duvall's filtering system. *See* EX1003, ¶¶137-138. Claims 7-9 and 12-13 all relate to this “identifying step” of Claim 1(b), which would be performed by Duvall's filtering system. EX1001, Claims 7-9, 12-13. After the “identifying step” is complete, Petitioner's Duvall-Chu's combination prompts an analyst at an analyst system, in order to satisfy limitation 1(c). *See* EX1003, ¶¶139-145. Petitioner relies on its arguments for Claim 6 to argue that Duvall-Chu's purported analyst system would be located in a remote SOC. *See* EX1003, ¶197. Claims 10-11 relate to the computerized analysis that occurs in that SOC. *See* Claims 10-11.

163. Therefore, to read on both sets of Claims, Petitioner must modify Duvall-Chu in at least two different ways. First, the portions of Duvall-Chu that

performs the “identifying step” (i.e., Duvall’s filtering system) must be modified.

Second Duvall-Chu’s analyst system, which Petitioner contends would be located in a SOC, would also have to be modified. But Petitioner and its expert never acknowledge this or even discuss any relevant modifications in relation to even one of these portions of Duvall-Chu’s system.

164. Instead, Petitioner’s expert appears to just be concluding that the ultimate functionality described by Trcka could somehow be incorporated into Duvall-Chu without actually implementing any of the technology thoroughly disclosed by Trcka. *See generally*, EX1003, ¶¶184-206. This conclusion cannot be correct. Trcka’s analysis techniques are closely tied to its underlying technology and disclosed implementation details. *See generally*, EX1014. For example, much of Trcka’s analysis techniques are enabled by having an archive of raw packet data available to analyze. *See, e.g.*, EX1014, ¶¶12, 39-40, 108-135. Indeed, Trcka dedicates a large portion of its disclosure teaching a POSA how to collect the necessary data that would enable Trcka’s analysis techniques in the first place. *See, e.g.*, EX1014, ¶¶34-107.

- 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

165. Although Petitioner never even discusses how Duvall-Chu would be

modified, I note that there are also several important differences between Trcka's techniques and the portions of Duvall-Chu's system that performs the "identifying step." Petitioner's expert fails to consider these differences that make Duvall-Chu's system unsuitable for combining with Trcka. *See generally*, EX1003, ¶¶184-195.

166. One immediate difference between Duvall and Trcka is that Duvall operates directly on live traffic while Trcka's techniques 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 a system that operates using patching code to inspect live traffic and one that operates entirely on archived historical data. EX1003, ¶186. This leads to three distinct, but interrelated, problems.

167. *First*, Trcka's analysis applications only operate on the archived traffic data "in an 'off-line' mode." EX1014, ¶15. So, unlike firewalls or Duvall's filtering system, 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 that traffic after-the-fact. *Id.* But

Duvall's "identifying step" operates on live data, as it is intercepted by the operating system. *See, e.g.*, EX1004, 6:10-29. Duvall therefore has no visibility into historical traffic besides the very transmission it is analyzing right then and there. In other words, Trcka teaches a stateful analysis, which is facially incompatible with Duvall-Chu's system. I note that during Petitioner's expert deposition, he admitted that "there are certain analyses that you can do on archived traffic that you fundamentally can't do on live traffic, and stateful inspection is an example of that." EX2007, 181:14-16. And indeed, that is why Trcka's analysis techniques are incompatible with Duvall-Chu's system. Notably, the need for this historical data also leads to the next problem.

168. *Second*, Trcka's analysis applications only operate on "archived traffic data." EX1014, ¶15. Therefore, without such an archive, Trcka's analysis techniques simply will not work. 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. Thus, Trcka's ability to analyze is heavily impacted by the location of the monitoring point. Modifying Duvall-Chu to implement Trcka's archive is therefore necessary to combining Trcka's analysis techniques with Duvall-Chu. But Petitioner's expert never considers *how* this archive could be created or even

where the monitoring point would be in Duvall-Chu's system. Indeed, Petitioner's expert provides no showing of how such a modification would be obvious to a POSA.

169. Notably, given that Duvall-Chu never captures, records, or processes any data at the packet-level (as I explained in paragraphs 95-105) and Trcka cannot determine what is blocked or allowed by Duvall-Chu's filters (as I explained in paragraphs 149-159), Trcka's techniques for creating an archive would not work in Duvall-Chu. A different archive than what is taught or disclosed by Trcka would be needed for Duvall-Chu's system. But there is no disclosure in the prior art on how to create this different archive for Duvall-Chu. A POSA would therefore not have found it obvious because there is no guidance on how to properly modify Duvall-Chu.

170. *Third*, Trcka's analysis applications are also "interactive analysis applications." EX1014, ¶109. This is related to the fact that Trcka's analysis techniques are offline. Indeed, Trcka's analysis applications are only designed to be used by "authorized user[s]," EX1014, ¶15, as opposed to automatically. In contrast, the portions of Duvall's filtering system that performs the "identifying step" happens *automatically* by applying filters. See, *e.g.*, EX1004, 6:10-29; 9:14-11:19. Indeed, Duvall intercepts live transmissions and can "discard[] incoming

data ... or replac[] parts of received data” as it is received. *See, e.g.*, EX1004, 1:39-40.

171. 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. *See generally*, EX1003, ¶¶184-206. Indeed, Trcka’s interactive analysis tool is unsuitable for Duvall’s “identifying step” because requiring a user to manually perform the analysis is facially incompatible with Duvall’s need for automatic analysis.

172. Despite at least these three technical hurdles, Petitioner concludes—without any further explanation—that a “POSA would encounter no technical hurdles.” Pet., 52; *see also* EX1003, ¶187. In my opinion, Petitioner and its expert’s conclusion is therefore without merit and contrary to the evidence.

b. Petitioner’s expert fails to consider *how* to implement Trcka’s analysis into Duvall-Chu’s remote SOC

173. Likewise, for Claims 10-11, even though Petitioner’s expert provides no discussion of *how* Trcka is being combined into Duvall-Chu at all, I highlight various problems a POSA would encounter when incorporating Trcka’s analysis techniques to be usable from a remote SOC.

174. I first note that 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’....”).

175. But as I have already explained, 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 techniques could be used to analyze whether Duvall’s system was “filtering too much or too little” from the SOC. *See* EX1003, ¶¶186, ¶¶196-202.

176. Notably, a remote SOC does not innately have access to a local archive of traffic data that is created using Trcka’s techniques. The fact that the SOC is remote to the monitored network is significant because unlike transmitting data locally, transmitting large amounts of data remotely is non-trivial. And Petitioner itself suggests the SOC would be remote. *See* Pet., 45. Therefore, a POSA would recognize that this is a problem that would need to be addressed. Yet Petitioner never discusses *how* Trcka’s archive could even be made available to a remote SOC. *See* Pet., 54-57. And Petitioner’s expert provides no evidence that a POSA would be able to do so with a reasonable expectation of success. EX1003,

¶¶196-202.

177. Importantly, Petitioner's failure to discuss *how* Trcka would be combined with Duvall-Chu actually conceals the glaring security and privacy concerns inherent to providing a remote SOC with access to such an archive. In my opinion, 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 full access to a network's raw packet data. A POSA would have recognized that there were at the time (and still are to this day) privacy and security concerns related to providing third parties with access to raw traffic data. Yet for Trcka's analysis to work in a SOC the SOC needs access to that raw traffic archive. *See* EX1014, ¶12. And access to such an archive taught by Trcka means every single packet sent or received on the network will be accessible from the SOC. *See* EX1014, ¶12. A POSA would therefore recognize several privacy and security concerns, which Petitioner's expert does not address.

178. *First*, providing remote access to Trcka's archival unit greatly increases the risk that sensitive information would be exposed. A POSA would have recognized that the attack surface to obtain such sensitive information would inherently be tripled. For example, attackers need not only target the corporate network, but can now alternatively target the remotely accessible archival unit,

which contains a recording of every single piece of packet data that was transmitted over the network. Likewise, attackers can also alternatively target the SOC, which has access to that archive, or can target transmissions as they are being sent from the archive to the SOC.

179. This is a problem unique to trying to force Trcka's techniques into Duvall-Chu's SOC. Indeed, Trcka's archive is not ordinarily remotely accessible. *See generally*, EX1014. And because Trcka's archival unit contains raw packet data, rather than, *e.g.*, status data, an attacker would have full visibility into the corporate network by accessing the archival unit. *See* EX1004, 12. For the very same reasons why having the packet data is so valuable to Trcka's techniques, that packet data also greatly enhances the risk that sensitive information would be exposed. *See, e.g.*, EX1014, ¶12 (explaining the value of packet-level data). Moreover, this visibility into the network's raw packets could also be used to find even further weaknesses in the corporate network. These problems inherent to combining Trcka into Duvall-Chu in this way would be plainly obvious to a POSA. In my opinion, a POSA would not have made such a modification to Duvall-Chu without at least addressing this security risk. But Petitioner's expert never considers and provides no explanation of how such risks could be addressed by a POSA.

180. *Second*, providing third parties with access to a corporate networks' raw traffic would also have raised privacy concerns separate from the security concerns I just discussed. Indeed, to my knowledge, providing *all* of a network's raw traffic to a third-party was unheard of at the time and even to this day. To my knowledge, 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 in the form of raw packet data. Instead, managed security monitoring systems typically 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).

181. Petitioner's expert seemed to suggest during his deposition that there were commonly known ways to address such privacy issues that would have been known to a POSA. But the only evidence Petitioner's expert provides is his own paper, which he explains is an example of how such privacy concerns could be addressed. Indeed, Petitioner's expert said the following in his deposition:

And there's any number of very obvious, very well-known techniques that you can use to mitigate any privacy concerns you have, some of which are -- for example, are discussed in my 2001 paper that we talked about, "What TCP/IP Protocol Headers Can Tell Us About the Web."

EX2007, 195:17-196:1.

182. Notably, his paper addresses these privacy concern by simply *not* viewing the HTTP header information at all. *See* EX2005. Therefore, the solution suggested by Petitioner's expert is to not implement an archive like Trcka's at all. Indeed, an archive of raw packet data necessarily exposes those HTTP headers along with the actual traffic. Thus, Petitioner's paper teaches away from combining Trcka into Duvall-Chu in this way. And in my opinion, without addressing such privacy concerns, a POSA would not have found it obvious to make such a modification to Duvall-Chu's SOC.

183. *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 at least once. Petitioner's expert seems to believe this is trivial, but a POSA would not have found it to be trivial at the time. Indeed, because Trcka collects every single packet, it would essentially require the corporate network to double its bandwidth. *See* EX1014, ¶¶12, 38. A POSA would have resisted such a solution even today, and the cost of bandwidth at the time was many times what it is today. *See, e.g.*, EX2019 (noting a 92% decrease in cost of bandwidth just from 2008 to 2018). 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 all the associated privacy and security risks that would inherently follow. Petitioner never discusses any alternatives, and the cited prior art does not teach a POSA how to address this problem.

184. In my opinion, a POSA would—at minimum—need to address these three concerns before finding it obvious to combine Trcka’s techniques into Duvall-Chu’s SOC. Petitioner’s expert’s opinions—which are Petitioner’s only support—are therefore deficient, in my view, because he failed to consider any of the same considerations that a POSA would have considered.

L. Claims 14 and 15 are valid in view of Duvall-Chu-Trcka-Ziese because Petitioner’s combination requires an initial modification to Duvall-Chu-Trcka that Petitioner’s expert failed to consider

185. In my opinion Petitioner’s motivation to combine Ziese is flawed because a POSA would not be motivated to even look for Ziese until Duvall-Chu-Trcka’s system is first modified as Petitioner suggests. *See generally*, EX1003, ¶¶207-212. Petitioner’s expert first suggests modifying Duvall to be used in a distributed corporate network and then suggests Duvall would use multiple servers as a result. *See* EX1003, ¶¶209-211. Neither of these modifications accord with Petitioner’s prior combination of Duvall-Chu, or Duvall-Chu-Trcka. Nor are they supported by the disclosures of any cited prior art.

186. Petitioner’s actual proffered motivation for combining Ziese into

Duvall-Chu is because Duvall would need Ziese's techniques in order to operate while having multiple servers. *See* EX1003, ¶211. In effect, Petitioner's motivation to combine Ziese into Duvall-Chu is only because Duvall was first modified to need Ziese's techniques. *See* EX1003, ¶¶207-212. But Petitioner's expert never provides any motivation for its initial series of modifications to Duvall-Chu-Trcka in the first place. *See* Pet., 58-63.

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

187. I initially note that Petitioner's expert appears to agree that Petitioner's motivation requires first modifying Duvall-Chu-Trcka twice. During Petitioner's expert's deposition he stated the following:

A I'm reading to you from paragraph 209 on page 108, as motivation for clients being distributed widely beyond a traditional local area network, which motivates a distributed corporate network as discussed in paragraph 210, which then motivates employing multiple servers.
EX2007, 200:22-201:5.

188. Indeed, Ziese only 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. A POSA would therefore recognize that there is no need for Ziese if there are not already multiple servers that need updates. Indeed, Ziese itself provides no motivation for making Duvall-Chu-Trcka use multiple servers.

189. Therefore, Petitioner’s motivation to combine Ziese assumes that 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, I would agree that Duvall only discloses a single server. Likewise, Petitioner’s own combination of Duvall-Chu-Trcka also contains only a single server. *See* Pet., 27-28; *see also* Pet., 50-58. Accordingly, there cannot be any motivation to look for Ziese yet, because there is only one server in Duvall-Chu-Trcka. *See* Pet., 59-60; EX1004, 8:18-26.

190. In my opinion, 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. And as Petitioner’s expert recognizes, Duvall would require additional “techniques [to] resolve this problem,” which are not contemplated by Duvall. *Id.* Moreover, Petitioner’s expert also

acknowledges that “Duvall already suggests the use of centralized updates.”

EX1003, ¶212. And this is accomplished by having only a single server that contains the filtering database.

191. In my opinion, Duvall thus teaches away from using multiple servers because such a configuration defeat Duvall’s goal of centralizing updates while unnecessarily creating problems for Duvall’s system. Indeed, Petitioner’s expert never explains what benefit there is to forcing Duvall to use multiple servers in the first place besides so that Ziese can be introduced into the mix.

2. **Petitioner’s expert never provides any motivation for modifying Duvall to use multiple servers**

192. As I explain herein, Petitioner’s expert provides no real motivation for a POSA to add multiple servers to Duvall-Chu-Trcka. *See generally*, EX1003, ¶¶207-212. In my opinion, none of Petitioner’s cited prior art provides any such motivation. I note that Petitioner’s expert simply 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’”). Not only is this presumption unsupported by evidence, but Petitioner’s expert also does not explain why Duvall-Chu-Trcka would be

modified for a distributed corporate environment in the first place.

193. With regards to modifying Duvall for a distributed corporate network, Petitioner's expert appears to be relying on Duvall and Ziese. *See* EX1003, ¶¶209-210. 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 the portions of Duvall that Petitioner's expert cites to in support of its opinion does not suggest to a POSA that Duvall's clients would ever be distributed widely outside of a traditional LAN. *See* EX1004, 2:35-39. On the contrary, Duvall only explains that its clients may be part of a LAN or a broad-based commercial service. *Id.* In my opinion, Duvall's identification of a "broad-based commercial service" as an alternative to LAN actually tends to teach against the use of Duvall in a distributed corporate network because Duvall never mentions a distributed corporate network at all. *See id.* Indeed, a distributed corporate network is neither a LAN nor a broad-based commercial service. Even Petitioner's own expert appears to recognize that this is the case. EX2007, 200:1-3 (recognizing three alternatives where "the clients can be distributed, they can be part of a LAN, [or] they can be part of a broadband network."). A POSA would therefore recognize that Duvall neither teaches nor suggests that it could be used in

a distributed corporate network. *See* EX1004, 2:38-39.

194. Likewise, Ziese’s disclosure of how to distribute updates to multiple devices contains no motivation for a POSA to modify a system like Duvall-Chu-Trcka into a distributed corporate network (not to mention that a POSA would not even look for Ziese yet in the first place). *See* EX1015, 1:26-31, 2:29-32, 2:41-44.

195. I also note that even if there was a valid motivation to modify Duvall-Chu-Trcka into a distributed corporate network, Petitioner’s expert never explains how that necessitates adding multiple servers. *See* EX1003, ¶¶209-211. And indeed, it would not. Rather, Petitioner’s expert’s proffered motivation “for a distributed corporate network to *centrally* analyze and update filters” actually suggests that a POSA would have been motivated to do the opposite. Rather than using multiple servers, which would just create problems for Duvall, a POSA could just keep using a single centralized server. *See* EX1003, ¶211 (emphasis added). Petitioner’s expert thus fails to explain why a POSA would ever modify Duvall-Chu-Trcka to use multiple servers.

196. Separately, I note that because Petitioner never clearly explained how Trcka was incorporated into Duvall-Chu’s system, I am unable to properly analyze what modifications would have been needed with respect to Trcka’s techniques when combining Ziese into Duvall-Chu-Trcka. Indeed, depending on where and

how Trcka's techniques are implemented, a POSA could be faced with additional technical hurdles when converting Duvall-Chu-Trcka's system into a distributed corporate network or adding multiple servers. I also note that Petitioner and its expert's discussion of combining Ziese into Duvall-Chu-Trcka ignores Trcka and its techniques altogether. *See generally*, EX1003, ¶¶207-212. Rather Petitioner and its expert only discusses how Duvall's system would be modified. *See id.*

M. Claims 18-25 are valid in view of Duvall-Chu-Cogger because Petitioner's expert's opinion is unsupported by evidence

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

197. In my opinion, a POSA would not be motivated to combine Cogger into Duvall-Chu. Notably Cogger in an entirely different field of art as compared to Duvall and Chu. Cogger discloses an interface to a trouble ticketing system for a telecommunications network. *See* EX1033, 2:6-12 (discussing "legacy system for the telecommunications industry [] known as a fault management system which can provide a range of services to larger customers of the enterprise"). Duvall discloses a censorship tool and Chu discloses a trust management system. *See* EX1004, 1:12-24 (discussing "parents are particularly concerned that their children can get access to such objectionable materials"); EX1005, 3 ("My thesis will identify what trust management is in the context of the World Wide Web and

propose a general architecture to close the gap between trust and cryptography”).

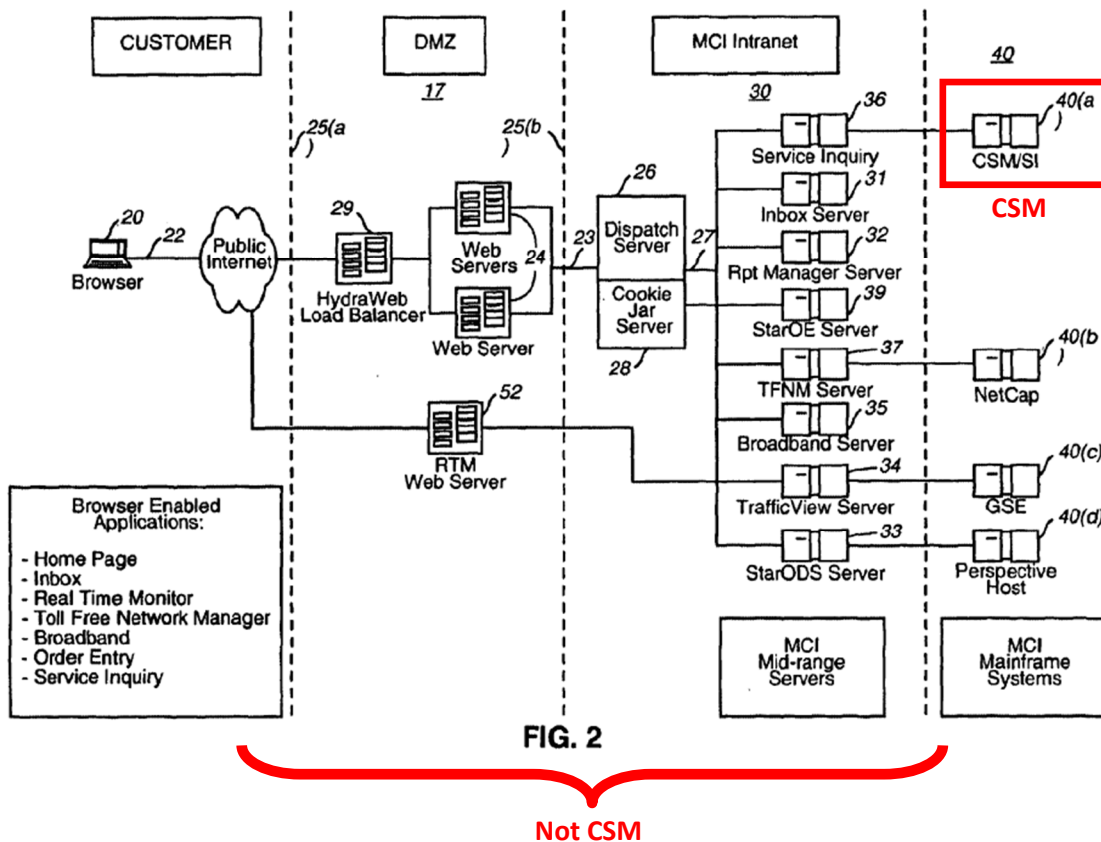
There is no relation between Cogger’s field of art and that of either Duvall or Chu.

198. Moreover, the “CSM” that Petitioner’s expert specifically provides would need to be implemented (in order to combine Cogger with Duvall-Chu) is not sufficiently disclosed by the Cogger reference. *See* EX1003, ¶230. Indeed, Petitioner relies on its expert’s conclusory suggestion that in Duvall-Chu-Cogger, “a POSA would have implemented Cogger’s CSM.” EX1003, ¶230.

199. However, Petitioner and its expert do not cite to any of the systems or processes that form Cogger’s CSM. *See generally* EX1003, ¶¶228-224. Notably, Petitioner’s expert purports to describe Cogger’s CSM by citing various parts of Cogger, but those cited portions of Cogger do not actually describe the CSM. *See* EX1003, ¶¶228-224.

200. 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, Fig. 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)."). Though the connection between the customer's browser and the CSM may be secure, there is no evidence that the CSM itself has been secured (or even how to secure it).



EX1033, Fig. 2 (annotations added).

201. As a matter of fact, Cogger only discloses the interface between a customer's browser and a pre-existing CSM. This interface relies on a complex architecture of other various pre-existing telecommunications servers and systems. *See, e.g.,* EX1033, Fig. 2, MCI Intranet. But disclosure of this interface and complex architecture does not teach or disclose how to implement the underlying CSM. Indeed, Cogger merely discloses that it exists, and teaches a POSA how to securely access it. *See generally* EX1033.

202. Petitioner's own expert has acknowledged during his deposition that Cogger does not actually disclose how to implement the CSM.

Q Can you show me where in Cogger it discloses how to implement the CSM?

A 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 person of ordinary skill in the art.

EX2007, 206:9-15.

203. Rather, Petitioner's expert suggests a POSA could figure out how to implement it on their own based on descriptions of the functions the CSM is capable of. *See id.* Notably, Petitioner's expert likens this lack of disclosure to the Schneier patent's disclosure. *See id.*, 206:16-207:1. But the Schneier patent's disclosure is actually very thorough in describing the actual systems and components that form its ticketing system. Indeed, the Schneier patent details how

to secure and isolate the ticketing system, how the system is used by the analyst, and more. *See, e.g.*, EX1001, 6:15-10:44; *see also* EX1001, Fig. 1, Fig. 3-9. In my opinion, Cogger’s description of solely how a customer can securely interface with the CSM does not sufficiently teach a POSA how to implement or secure the CSM itself.

204. 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 actual 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”).

205. In short, Cogger’s CSM is only disclosed as a black box. At best, Cogger 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)).

206. But Cogger fails to teach a POSA how to implement the actual underlying CSM system. For example, Cogger does not disclose any systems or processes used to create, store, or manage the trouble tickets in the CSM. *See generally*, EX1033. Notably, while Cogger's interface separately relies on its own storage and processing mechanisms, once that ticket is sent to the CSM, there is no disclosure of anything is handled by the CSM. EX1033, 15:66-17:49. As another example, Cogger does not disclose any systems or processes that allow a customer service representative to access or use the CSM. *See generally*, EX1033.

Importantly, Cogger also does not disclose any systems and processes related to securing the CSM itself, rather than the customer's connection to it. *See generally*, EX1033. For example, there is no evidence that the customer service representative's connection to the CSM is secure, nor is there any disclosure of the systems or processes that the representatives would use to access the CSM. *See generally*, EX1033. Petitioner's expert's suggestion that "a POSA would have implemented Cogger's CSM" is therefore unsupported by any evidence.

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

207. Notably, even if Cogger's CSM could be implemented by a POSA, I note that there is no guidance on how it could be incorporated into Duvall-Chu's system to do what Petitioner suggests.

208. Petitioner relies on its Duvall-Chu combination as discussed for Limitation 1(b) and 1(c) to teach the "event record" that is created in accordance with Claim 18. *See* EX1003, ¶232. Importantly, Petitioner's expert suggests this "event record" would be placed into a problem ticket along with various other information. *Id.* Petitioner's expert also 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.

209. But although Cogger's problem tickets are disclosed as containing those various information, Petitioner's expert ignores Cogger's disclosures as to how to populate that information. Based on Cogger's disclosure, that information is actually manually populated by the customers. *See, e.g.*, EX1033, 21:21-22:30. But Petitioner and its expert fails to show *how* that Duvall-Chu could be modified to populate any information in the problem tickets.

210. Indeed, Petitioner's Duvall-Chu combination automatically prompts the network administrator whenever a transmission does not match any of Duvall's direct or deferred-action filters. *See* Pet., §VI.A.1-2. Thus, based on Petitioner's Duvall-Chu combination, there is no opportunity for a customer to manually populate new trouble tickets related to each "event record." In contrast, this is exactly how Cogger populates that information. *See* EX1033, 21:21-22:30.

211. Moreover, Petitioner's expert relies specifically on Cogger's disclosure of a customer manually populating the trouble ticket as evidence that Cogger teaches a "symptom record." *See* EX103, ¶¶235-236. Cogger discloses that its front-end user interface "asks the customer the problem/identifier type" and then asks the customer to "narrow down the problem by having the customer choose from a list of Product types, Service types, and Trouble Descriptions." EX1033, 21:27-30. The customer must then answer additional questions until all the required information is available. *Id.*, 21:37-41. Cogger explains that the "questions that need to be asked to open a ticket vary by product and problem type." EX1033, 22:58-59. And Petitioner's expert suggests that these answers from the customer are what "relate to '*symptom[s]*' of a particular problem." Pet., 236 (alterations in original).

212. In fact, Petitioner's expert does not even appear to consider this

question at all. Thus, in my opinion, Petitioner and its expert have failed to adequately explain how Cogger is actually being combined into Duvall-Chu's system. There is no evidence that Cogger could actually be incorporated into Duvall-Chu with a reasonable expectation of success because Petitioner and its expert simply assume that Cogger's trouble tickets will have the necessary information, without considering or explaining how that information got there.

VI. SECONDARY CONSIDERATIONS INDICATE THE CHALLENGED CLAIMS WERE NOT OBVIOUS

213. I am aware of the Counterpane's Managed Security Monitoring ("Counterpane MSM") service created by Bruce Schneier and offered by Counterpane Internet Security, Inc. in 2000. The descriptions and discussions of Counterpane MSM in EX2009-EX2015; EX2017 matches my recollection. *See* EX2009-EX2015; EX2017. In my opinion, Counterpane MSM is an embodiment of the Schneier patent and is captured by the claims. *See* EX2011, 2 (noting Counterpane MSM is "patented technolog[y] developed by Counterpane.")

214. 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). 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.”). The Sentries collect data from network devices and utilize over 20,000 filters to filter potential security threats. EX2009, 6. The Sentry also utilizes an analysis engine to further analyze post-filtering residue which is then sent to the SOC and Socrates. EX2009, 12. Trained security analysts work with the Socrates program to “filter[] out the chaff” and refine the potential security threat information that is presented to customers. EX2012, 2.

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

215. In my opinion, Counterpane MSM embodies the challenged claims and 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. Moreover, the claims provided an architecture that also enabled reactive responses to potential threats. In my opinion, the need recognized by the Schneier patents and solved by Counterpane’s MSM were missing in the network security industry in 2000.

216. As the inventor’s 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 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).

217. Moreover, in my opinion, there was a long felt need for the ability to detect the threats that these static systems could not detect. *See, e.g.*, EX1001, 2:8-10 ("Buried in all that information may be the footprints of ongoing network attacks or intrusions."). The inventors recognized that information regarding unknown security threats likely resided within the post-filtering residue leftover after filtering performed at the probe (i.e., the Sentry of Counterpane MSM). *See, e.g.*, EX1001, 5:25-29. But prior art detection did not have a good way of analyzing the residue due to the complexity of the analysis that would be required. *See, e.g.*, EX1001 1:29-33, ("But because such products cannot be relied upon to work perfectly, and because security butts may exist in other software or hardware, complete network security also requires monitoring, detection and response in

event of a breach.”).

218. Likewise, although theoretically possible with human analysts, prior art systems could not actually utilize human analysts to monitor such data for threats due to the sheer volume of the residue data. *See, e.g.*, EX1001, 1:36-43 (“System administrators normally do not have the time or ability to read through large amounts of constantly updated audit information, looking for attacks on their systems. They also do not have the time to continuously monitor hacker activities, looking out for new tactics, tools and trends. Finally, they do not have the time to become experts on every kind of intrusion and to maintain that expertise.”).

219. Indeed, when Counterpane MSM entered this space with its new approach to managed security monitoring, its competitors were mainly IDS 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.

220. The claimed solution therefore provided a novel architecture to solve these long-felt needs. *See, e.g.*, EX1001, Claim 1-27. The claimed filtering and analysis of status data at the probe reduces the volume of data that needs to be further analyzed, so that identified information can be sent to an analyst system. This claimed architecture allowed for the identification of security threats that were

previously undetectable using prior art systems. *See, e.g.*, EX1001, 8:51-62. The analyst system functions to reduce the number of false positives and trained analysts can use the tools and databases available to them to home in on the most credible threats. *See, e.g.*, EX1001, 2:13-24. This claimed architecture also enabled the use of analysis techniques such as cross-probe correlation that was previously impossible due to the isolated nature of prior art detection tools. *See, e.g.*, EX1001, 2:35-40.

221. Moreover, because Counterpane analyzed status data, as claimed, rather than raw traffic, the claimed solution also sidestepped many of the security and privacy concerns related to sending raw traffic to remote third parties. *See, e.g.*, EX2005. The claimed feedback at the probe also updates the capabilities of the probe, which enabled reactive responses to newly detected threats. *See, e.g.*, EX1001, 2:30-40.

222. Accordingly, Counterpane MSM was able to meet a long-felt need that existed for internet security, which not met until Counterpane's MSM service was released.

B. Industry Praise and Commercial Success of Counterpane MSM

223. 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”).

224. When compared to the competition, others in the industry have recognized “only Counterpane is positioned to be a vendor-agnostic monitoring-focused service.” EX2014, 4; *see also id.* at 7 (“Even if there were a company sharing Counterpane’s model, and there seems not to be, there would still be a sufficient market for multiple vendors.”).

225. In my opinion, the industry acclaim awarded to Counterpane and its Counterpane MSM service, specifically, is also complemented by Counterpane’s commercial success in the industry. For example, the “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.” EX2010, 3.

226. In fact, The Regence Group spent \$450,000 on Counterpane every year. EX2015. And by 2006 it was acquired “for a sum of more than \$20 million.” EX2017.

227. In my opinion, the evidence that Counterpane MSM met a long-felt but unresolved need, was given industry praise, and was commercially successful indicates that Schneier's claims were non-obvious.

VII. CONCLUSION

228. For the foregoing reasons, it is my opinion that all claims of Schneier are patentable.

I declare under penalty of perjury under the laws of the United States of America that all statements made herein based on my own personal knowledge are true and correct, that statements made on the basis of information and belief are believed to be true, and the opinions expressed in this declaration are my own. If called to testify as to the contents of this declaration, I could and would do so, competently.

These statements are made with knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under section 1001 of title 18 of the United States Code.

Dated: February 21, 2024

A handwritten signature in black ink, appearing to read "Wenke Lee", is written over a horizontal line.

Wenke Lee