

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

SUPPLEMENTAL DECLARATION OF WENKE LEE
IN SUPPORT OF PATENT OWNER'S SUR-REPLY

I. INTRODUCTION

1. My name is Wenke Lee, and I hereby declare as follows:

2. I am over the age of twenty-one (21) years, of sound mind, and capable of making the statements set forth in this Declaration. I am competent to testify about the matters set forth herein. All facts and statements contained herein within my personal knowledge are true and correct, and I believe those items stated herein on information and belief to be true and correct.

3. I submitted a prior declaration in this matter (Ex. 2016), which I understand was filed on February 21, 2024. I have been retained on behalf of BT Americas Inc. (“BT”) for the above-captioned inter partes review proceeding to provide my expert opinions and expert knowledge. I understand that this proceeding involves U.S. Patent No. 7,895,641 (“the ‘641 patent,” Ex. 1001), which is titled “Method and system for dynamic network intrusion monitoring, detection and response,” and is currently assigned to BT Americas Inc.

4. My background and qualifications were provided in paragraphs 2, 5, and 14-21 of my prior declaration, and my CV was provided as Ex. 2020. My statements in my prior Declaration regarding my review of the ‘641 patent and related materials remain unchanged, as do my understandings of the relevant legal principles.

5. I confirm that, to the best of my knowledge, the exhibits

accompanying my prior declaration and the exhibits accompanying this declaration are true and accurate copies of what they purport to be and that an expert in the field would reasonably rely on them to formulate opinions such as those set forth in this declaration. I further confirm that 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.

6. Since my last declaration, I have reviewed and considered the following additional materials:

- Petitioner’s Reply to Patent Owner Response (“The Reply,” Paper 20), and all exhibits cited by Petitioner in connection therewith;
- Daria Zhuravleva, “Most Common Spam Emails You Can Encounter in 2024,” May 8, 2022, available at <https://selzy.com/en/blog/spam-email-examples/> [Ex. 2023].
- “The Worst Phishing Attacks in History,” January 05, 2023, available at <https://www.graphus.ai/blog/worst-phishing-attacks-in-history/> [Ex. 2024].
- Micke Ahola, “The 7 most damaging phishing attacks of all time,” available at <https://blog.usecure.io/famous-phishing-attacks> [Ex. 2025].
- Patchen Barss, “Ten indispensable technologies built by the pornography industry,” June 5, 2011, available at <https://patchenbarss.com/2011/06/05/ten->

indispensable-technologies-built-by-the-pornography-industry/ [Ex. 2026].

- Cezary Jan Strusiewicz, “5 Ways Porn Created the Modern World,” *Cracked*, December 11, 2010, available at https://www.cracked.com/article_18888_5-ways-porn-created-modern-world.html [Ex. 2027].
- Doug Gross, “In the tech world, porn quietly leads the way,” *CNN*, April 23, 2010, available at <https://edition.cnn.com/2010/TECH/04/23/porn.technology/index.html?hpt=Sbin> [Ex. 2028].
- Any other materials cited herein.

II. REPLY TO CERTAIN ARGUMENTS RAISED BY PETITIONER AND DR. JEFFAY

A. Duvall Is Directed to a Concept Orthogonal to Computer Security

7. Claim 1 recites “identify[ing] potentially *security*-related events,” and claim 18 likewise recites “an identified potentially *security*-related event.” In my view, a person of ordinary skill in the art (POSITA) would understand that, broadly speaking, this plain language positions the claims in the computer security world. I have reviewed Duvall numerous times, and it does not mention computer security at all. As I discuss in greater detail below, a POSITA would understand that Duvall is directed to an orthogonal issue with no practical bearing on the computer security world. In my opinion, a POSITA would understand that trying to identify objectionable material, including objectionable pornographic material, in the manner taught by Duvall has no practical bearing on identifying potentially

security-related events as claimed.

8. During my cross-examination, Petitioner's counsel misstated or mischaracterized my written and oral testimony many times. Over and over again, I had to say "[t]hat's not what I said" or otherwise correct the record. Now, page 2 of the Reply says that I said during my deposition that "I would think everything is potentially related to security, including your email, including PDF documents." Petitioner takes this quote completely out of context. My statement there was to show how absurd Petitioner's position was that porn was a potentially security-related event. *See* Ex. 1046, 178:22-6 ("I would think everything is potentially related to security.... If you go that route, anything you touch, open up your computer, connect to Internet, potentially you be infected. You want to go that route, yeah, everything is potentially."). But as I then explained during my cross-examination:

My point is for security concern, yeah, downloading anything from anywhere is a potential non-zero probability that something is bad, but on the other hand as a security person you cannot say, well, how do I secure my machine? Don't connect to the Internet. Duh. No USBs, duh. What do you do? Do nothing. Then the machine will be secure. Come on.

So my point is secure people will know -- a POSA will tell you I want to monitor everything, but I'm using evidence, information, knowledge, and experience, other sources of information, even your insights or connection to underground world, whatever, to basically collect enough security-related intelligence so you can decide what to block, what to allow.

Ex. 1046, 186:9 to 187:2.

9. Both Dr. Jeffay and I agree that a POSITA would have to take into account context to separate potentially security-related events from non-potentially security-related events. I agree with Dr. Jeffay when he said, “[I]t depends on the context and it would certainly depend on the type of network....”). Ex. 2007, 29:14-16. He made similar statements elsewhere during his cross-examination, all to the effect that one needs to take into account contextual information when distinguishing between potentially security-related events and non-potentially security-related events. *See, e.g., id.*, 29:20-30:2, 31:2-11. That contextual information is ultimately what is important here, whereas whether something is objectionable is distinct from whether that data is potentially security-related.

10. During my cross examination, I offered similar testimony about contextual information mattering when determining whether something was potentially security-related, or not. For example, as I said, “You don’t say, wow, this is porn. You look at other contextual information to say is this reasonable thing to do?” Ex. 1046, 179:14-15. I further explained that “I use contextual information, knowledge information to decide what to block, what not to block. You can never say just because porno sites are blocked. That’s completely irrelevant to the security operation that a POSA would understand.” *Id.*, 188:10-12. Likewise, a POSITA would not say “just because a website has a curse word, it means it has a virus. That’s – that’s a leap that a POSA would not make, and a

POSA would say, okay, curse word, so what?” *Id.*, 180, 10-14. I talked more about contextual information, and why pornographic websites cannot simply be considered unsecure, throughout my deposition. *See, e.g., id.*, 180:14-19, 186:17-187:7, 188:10-12.

11. In my view, a POSITA reading Duvall would find no teaching or suggestion of the additional context needed to convert Duvall into a security monitoring system. Remember, Duvall does not even mention security. As I stated during my cross-examination, “Duvall is talk[ing] about objectionable contents. It doesn’t talk about blocking access to a site for security.” *Id.*, 192:4-6. These are just two different, orthogonal concepts. *See id.*, 192:7-10, 192:22-193:6.

12. The Reply on page 3 cites Exhibits 1026 and 1030 for the assertion “it was common for computer viruses to use objectionable materials to lure users into downloading the virus.” These exhibits include information about the Melissa Virus. But the Melissa Virus did not use objectionable materials to lure users into downloading the virus. Instead, the Melissa Virus sent an email with a header reading “Important Message From <name>” where the name was taken from an Outlook address book. Ex. 1030, 4. At the very least, the subject line made the email seem benign to trick individuals to open it. The exploit itself was the result of a macro embedded in an attachment to the email, which ran as soon as the attachment was opened. The attachment in the email contained a list of

pornographic sites, but that is irrelevant to the lure and the exploit. Both the lure and the exploit would have worked exactly the same if the attachment contained a list of the patents most recently issued by the USPTO, entries from the Oxford English Dictionary, an organization chart, a restaurant menu, or anything else. In fact, replacing the list of pornographic sites with this kind of benign information could have made the virus worse, because it could have more easily bypassed some spam filters in operation at the time. Thus, Exhibits 1026 and 1030 actually contradict the points raised in the Reply.

13. Research from email marketing platforms, and phishing and spam defense and awareness companies, have come to the same conclusion as me, *i.e.*, identifying objectionable material is a distinct consideration from identifying potentially security-related events. For example, email marketing platform Selzy notes that the reasons why people get spam email (Ex. 2023, 2-3), and the most common phishing and spam examples currently (*id.*, 4-11), have nothing to do with objectionable material such as pornographic material. Pornographic material is not even in the top 10, according to this list. Phishing and spam defense company Graphus likewise cataloged the worst phishing attacks in history, and none involved objectionable material such as pornographic material. *See generally* Ex. 2024. Human Risk Management (HRM) company “usecure,” which provides security awareness training, came to the same conclusion for the seven most

damaging/costly phishing attacks of all time. *See generally* Ex. 2025.

14. During my deposition, I was asked several times about the relationship between objectionable pornographic content and security. I explained that pornographic websites, by themselves, were not known to pose security risks. *See* Ex. 1046, 184:4-6. I disagreed with the suggestion that, in the 1990s, “it was well-known that pornographic sites were very susceptible to having malware and spyware and viruses.” *Id.*, 9-16.

15. I offered further testimony about what was going on in the security industry at the time of the invention, specifically with regard to pornographic websites. For example, when I was asked about whether, in the 1990s, pornographic sites were susceptible to having malware, spyware, and viruses, I explained:

I clearly remember porn sites among the first sites that implement secure [sockets] layer because they want to charge you. They want you to pay to get some contents.

In fact, I would say that [was] a driver for a lot of web security technology that we know of today....

...[T]o say going to porn site you get infected is completely opposite to what I know.

Id., 182:3-21.

16. I mentioned pornographic sites being among the first sites to implement Secure Sockets Layer (SSL), which I recall being developed by Netscape around 1995. As is well known by now, SSL is a standard technology

for securing an internet connection by encrypting data sent between two systems—oftentimes a website and a browser, or between two servers. When you see a URL with “HTTPS,” it means that the website is secured by an SSL certificate (or by a transport layer security (TLS) certificate, TLS being a successor to SSL). SSL is oftentimes used in e-commerce applications. Websites selling pornography were some of the earliest e-commerce applications available on the Internet.

17. The goal of SSL was to ensure privacy, authentication, and data integrity in Internet communications. In this regard, it is quite apparent why pornographic sites would want to offer a high degree of privacy. SSL certificates can also authenticate the identity of a website owner, which provides an added layer of trust by which users can verify who is sending them information. And data integrity helps verify that the data has not been tampered with before reaching its intended recipient. Because of these features, pornographic sites were secure and quite resistant to cyberattacks.

18. Pornographic websites were early adopters of security-related technology, and they also were driving security-related technology developments throughout the 1990s and even to today. This has been written about extensively. For example, the founder of “Danni’s Hard Drive”—which garnered a million hits” in its first week and was the busiest site on the web for the next two years—along with other pornography companies “pioneered the e-commerce and security

solutions that paved the way for PayPal, eBay, Amazon, and the commercialization of the Internet.” Ex. 2026, p.2.

19. One article, citing the research of Professor Jonathan Coopersmith from Texas A&M University, observed that “almost every piece of modern internet technology can be traced back to the adult trade.” Ex. 2027, 20.

Companies like Google, Yahoo, and AOL have studied the adult industry to copy their business strategies. *Id.*, 22. Even CNN explained that “a widely acknowledged but seldom-spoken truth of the technology world” is that “[w]henver there’s a new content platform, the adult-entertainment industry is one of the first to adopt it -- if they didn’t help create it in the first place.” Ex. 2028, p. 1. And according to CNN, “[w]ebsites that require memberships, encryption coding, speedier file-sharing technology -- all can trace their roots back to the adult industry.” *Id.*, p. 2.

20. In my view, a POSITA, aware of what was happening in the industry, would understand that a system like Duvall’s would not be modified or extended to handle security. Security was already being addressed by pornographic sites themselves, and required different context and considerations compared to Duvall’s objectionable content filter. Moreover, the pornographic sites detected by Duvall were more likely to be secure because they implemented SSL and depended on secure e-commerce as their business model. As I mentioned earlier, in my

view, a POSITA would not modify Duvall as Petitioner proposed because the concepts of securing against objectionable material and securing against potentially security-related events are orthogonal.

B. The Reply’s Latest Attempt to Justify Introducing Features from Chu Into Duvall Is Incorrect.

21. Dr. Jeffay’s arguments that Duvall had a problem with filtering “too much or too little,” while also conceding “nothing more [was] needed” beyond what was already disclosed by Duvall to address this supposed issue, are inconsistent. Dr. Jeffay’s testimony also contradicts the alleged rationale for looking to Chu, as there is no motivation “to seek additional techniques for more accurately resolving the status of residue data transmissions,” because “given the operation of Duvall, a [POSITA] would understand that nothing more is needed.” See *id.* (comparing Ex. 1003, 107, with Ex. 2007, 133:17-22). I see that the Reply is now arguing that the earlier-alleged motivations “are directed to improving the process for determining when to edit filters.” But there are problems with the reliance on Duvall and Chu, even if this is the reason why they are being combined.

1. A POSITA Would Consider More than Just When Something (Allegedly) is Happening.

22. In my opinion, when assessing what Chu teaches, a POSITA would consider what Chu specifically teaches about who is making a change to filters,

where the change is being made, and why the change is being made in the first place—and not just when a change allegedly is to be made. In this regard, my view is that the “who” and “where” in Chu are wrong. Chu teaches allowing end-users to make determinations on their own computers about whether to navigate to certain sites even if warnings indicating that trust decisions cannot be reached are presented. Duvall’s desire is to restrict access to objectionable material, so this combined behavior could end up being catastrophic. For example, minors would be able to make their own decisions about whether to visit pornographic sites right at their own computers. Chu basically teaches how to bypass the very protections Duvall seeks to provide. And these protections would be bypassed regardless of whether Duvall were modified to handle computer security or just objectionable material. What Chu tries to accomplish with its prompt is fundamentally counter to what Duvall’s system tries to accomplish. In fact, the resulting combination would be particularly vulnerable to a host of exploits, such as phishing and spoofing exploits, because the end-user (rather than a trained analyst) would be the one to make an on-the-fly trust decision.

2. Making an On-the-Fly Trust Decision Would Hurt Duvall’s System.

23. The policy relied on from Chu in essence allows a party to make an on-the-fly determination of whether to trust a particular site after it fails to match any filters. But a POSITA would understand that empowering any party to make a

trust/do-not-trust decision as taught by Chu in Duvall's context at best would be counterproductive. For example, allowing end-users to make determinations on their own computers would create the very sorts of problems Duvall seeks to avoid. Even assuming for the sake of argument that a remote analyst would determine whether to trust a particular website, that determination in this context likely would result in objectionable pornographic material being provided to Duvall-Chu's end-user. And in the security context, analysts are simply not capable of making such determinations on-the-fly. There is just too much information to consider in a relevant time period.

24. As I explained above (e.g., in paragraphs 12-14) and previously, a POSITA would recognize that non-objectionable material is *at least* equally likely to raise security concerns compared to objectionable material. Ex. 2016, 36-37. Both the greeting card example I previously gave, and Dr. Jeffay's Melissa Virus example, are in agreement on this point. *See id.*, 36-38; Ex. 1030, 4. And as I discussed above (e.g., in paragraphs 15-20), sites offering pornographic material were early adopters of security-related technologies; they were "a driver for a lot of web security technology that we know of today." Ex. 1046, 182:10-21.

25. In my view, a POSITA would understand that a trained analyst making security-related trust decisions would reasonably permit pornographic material to reach the end-user. Such material would be expected, i.e., trusted, to be

reasonably secure given the security measures pornographic sites were implementing at the time of the invention. This follows from the use of SSL and other technologies as I discussed in detail above. This expected operation ultimately would harm Duvall's system, not improve it. Therefore, in my opinion, a POSITA considering this factual background would not have made the alleged combination.

3. The New Asserted Motivation Is Unrealistic.

26. The Reply on page 3 states "[t]he motivations provided in the Petition do not propose a new filter-editing mechanism in Duvall," but on page 4 states "the Duvall-Chu combination provides a 'suitable' improvement to Duvall's default 'block or allow' operation." There is no separate filter editing for "Duvall's default 'block or allow' operation." To me, then, it seems that the Reply is proposing some "new filter-editing mechanism in Duvall."

27. In my view, a POSITA would find the newly-proposed motivation to be unrealistic. The relied-upon policy from Chu does not even contemplate editing filters. For example, Chu's whitelist and blacklist are not modified after an end-user makes a trust/do-not-trust decision. I see no teaching or suggestion in Chu to modify filters (much less a default filter applied after all other individual filters are applied), as the Reply apparently is now alleging.

28. A POSITA would understand that Chu's policy is about enabling an

end-user to make a “one-off” override decision. A POSITA therefore would not modify Duvall to have a trained remote analyst make such snap decisions for all navigation attempts reaching uncertain determinations. This would be unrealistic in practice because of the vast amount of information to be considered and the need to consider that information carefully and based on empirical analysis. Moreover, a POSITA would understand that a decision to make a one-off determination in no way motivates a change to a multi-use, multi-user filter intended for future application. The proposed combination is even more farfetched because the alleged “improvement [is] to Duvall’s default ‘block or allow’ operation.” *See* Reply, 4 (emphasis added). A POSITA would not expect to modify a default operation based on a one-off override decision. Again, this is inconsistent with the empirical operation and decision-making appropriate in this art.

C. The Board Should Consider Duvall as a Whole, and for What It Actually Teaches.

29. The Reply emphasizes the presence of block 100 in Duvall’s Fig. 3 by looking at the figure out of context. The Reply (and Dr. Jeffay) fails to consider the meaning of col. 4:40-43. This text from Duvall indicates that the open command, shown in block 100, is contemplated for execution. Col. 4:56-58 of Duvall confirms the open command is not necessarily successful. These portions of Duvall contradict Petitioner’s superficial reading of Duvall.

30. The Reply at pages 7-8 compounds this error in asserting “both direct- and deferred-action filters are searched for the *same* message transmitted through the data stream.” The Reply is incorrect. The Reply cites to col. 4:45-55 and col. 4:65-5:1 of Duvall, but these portions discuss retrieving filters. Thus, what is the same is the subset of retrieved filters that are applied, NOT the data being filtered. At best, these portions are about applying retrieved filters to the same overall stream. But the data considered by direct and deferred action filters are ultimately different data within that same stream.

31. Simply stated, direct action filters are not searched for a message transmitted through a data stream. Direct action filters determine whether to allow a data stream to be opened. The deferred action filters do not act on the same data considered by the direct action filters, but rather act on the content being transmitted, i.e., the payload, which presumably would require deep packet inspection which would be highly inefficient to implement—and is therefore at odds with the ‘641 patent, which bases the analysis on status data. Thus, when Duvall is properly considered as a whole, it is clear that Fig. 3 operates on different data than Fig. 4.

D. Petitioner’s Misreading of Duvall Discloses a Single Filter Database with Filters Acting Together in Concert, Which Still Does Not Meet the Claim Language.

32. Petitioner’s Reply at page 10 alleges it is “[c]lear from Figures 3 and

4, Duvall's deferred-action filters are not a continuation of the direct-action filters but come afterwards as their own discrete set of analyses." Reading Duvall as Petitioner does, I conclude that simply is false. Rather, this is only true if Figures 3 and 4 operate on different data as I have explained they do.

33. Duvall discloses a single filter database with filters. Each filter entry has a field specifying whether it is a direct or deferred action filter. Ex. 1004, 4:12-15. Filter entries are retrieved and "first scanned for entries that require direct action." *Id.*, 4:17-21. Duvall prefers to store its filters "so that the system searches ALLOW filters first, BLOCK filters next, and deferred action filters last." *Id.*, 4:27-30. And Duvall preferably "takes action based on the first matched filter." *Id.* Under the proper view of Duvall, the ordering of filters allows the system to take action based on the first matched filter in accordance with Figs. 3 and 4. Because Fig. 3, which applies direct-action filters to transmissions opening a stream, must be performed first, the direct-action filters are preferably stored before the deferred-action filters. Accordingly, when a deferred action filter is reached at Fig. 3, step 116, Duvall will open the stream and then continue to Fig. 4.

34. But under PAN's view, Fig. 3 and Fig. 4 applies to the same data. Thus, Duvall has a single collection of both direct- and deferred-action filters that are stored together, searched together, and applied to data in the same way. Under PAN's view then, changing the ordering of filters would also change which filter

gets applied first. Under this view, there is really no difference between the direct and deferred action filters besides the additional fields. But those additional fields are just exemplary and there is no reason why a direct-action filter—under PAN’s view—could not also contain the additional fields of the deferred-action filter. In this sense, the operation of direct- and deferred-action filters are indistinguishable from each other.

35. Therefore, taking an expansive view of Duvall as urged by Petitioner actually contradicts the Reply, because Duvall would teach that deferred-action filters are basically no different than the direct-action filters. They merely act depending on whichever match happens to come first based and on whichever order the filters happen to be stored in. Importantly, the alleged sequential relationship between boxes 104 and 116 in Duvall’s Fig. 3 would merely represent an exemplary situation where direct actions *happen* to come first—rather than showing that Fig. 3 and Fig. 4 are performing discrete sets of analysis. Therefore, I conclude that even under Petitioner’s view of Fig. 3 and Fig. 4, Duvall does not perform the claimed “filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering.”

36. A POSITA simply would not artificially divide Duvall’s single filtering process. In my view, a POSITA would understand the combination

according to Petitioner's misread would involve a single filter system lacking any sort of distinct analysis of post-filter residue that follows positive and negative filtering, even under the Reply incorrect reading of Duvall.

E. The Reply's "Reasonable Capability" Arguments Are Incorrect.

37. In my view, Duvall does not disclose dynamically modifying the probe during operation thereof as set forth in limitation 1(e). The Reply at page 16 asserts that "[t]he Petition explains, 'a POSA would have recognized that Duvall's "analysis capability of said probe" is "dynamically modified ... during operation thereof" because taking the system offline each time an update [to Duvall's filters] was required would be disadvantageous.'" But a POSITA would not have found it obvious to address this suboptimal implementation based on the cited art.

38. The Reply at page 17 asserts "the recited dynamic modification capability requires nothing more than use of 'known database editing techniques' that have been known for decades." Of course, it is unclear whether Petitioner is talking about claim 1, or an alleged teaching from Duvall. Either way, there are serious problems with the Reply's reasoning.

39. In particular, the Reply focuses on showing dynamic modification of the wrong component—i.e., dynamically modifying the database, not the probe.

Even if the database could be dynamically modified¹, that does not mean the probe's analysis can be inherently (i.e., necessarily) dynamically modified. For example, when Duvall's database is copied into RAM, the actual database can still be updated dynamically (on the disk). But that does not mean the probe's capabilities are dynamically updated since those changes will not be reflected in the RAM copy. Whether the probe can be dynamically updated depends on the implementation of the probe itself and whether that implementation is capable of detecting or reacting to dynamic updates. But Duvall does not provide a mechanism to detect or react to changes to the filters during operation. As just one example, if a stream was already opened, but a new direct-action filter says close that stream, Duvall's system is already past the point where that direct-action filter could be applied. Even though the stream should now be closed, Duvall's system

¹ I note that a database is just an organized collection of structured information. It does not make much sense to say that the database can be modified without being taken offline as there is no such concept for a mere collection of data. During the cross-examination, Petitioner's line of questioning about dynamically modifying the database was confusing for this reason. However, upon reading Petitioner's Reply, it appears Petitioner is actually referring to modifying a database without taking the application that hosts the database offline. However, the question of whether the application that hosts the database must be taken offline is very different than the question of whether the application that **relies on** the database (e.g., the probe's application) must be taken offline.

would just continue allowing data through that stream. Duvall's filtering system as disclosed is not inherently capable of dynamic modification simply because the underlying database can be dynamically modified. As can be seen, then, dynamic modification would depend on application implementation details, not just the mere existence of a database).

F. Secondary Considerations

40. Contrary to the Reply's contentions, I mapped the claim limitations to the product (*see* Ex. 2016, 214), identified which claims the product embodies (*see id.*, 215, stating "Counterpane MSM embodies the challenged claims"), and discussed the analysis of post-filtering residue (*see id.*, stating "[t]he Sentry also utilizes an analysis engine to further analyze post-filtering residue which is then sent to the SOC and Socrates) and dynamic modifications (*see id.*, 221-222). All of this was confirmed during my deposition. *See, e.g.*, Ex. 1046 36:17-19; 37:10-13. It is true that I have not personally reviewed "internal documents" about how exactly certain functions were implemented in the commercial product. *Id.*, 45:22-46:2. However, my opinion was formed based on cited industry report and references. I knew this technology very well. I specially relied on Exhibits 2009-2015 and 2017, which match my recollection of the technology, both from what I knew of it being familiar computer security industry and also what I knew of it from attending a conference where Bruce Schneier was presenting. *See* Ex. 2016,

213.

III. CONCLUSION

41. In signing this declaration, I recognize that this declaration will be filed as evidence in an inter partes review before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required, I will appear for cross-examination within the United States during the time allotted.

42. I hereby declare that all statements made herein are made of my own knowledge and are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Dated: June 24, 2024



Wenke Lee