EXHIBIT E

EXPERT REPORT OF AVIEL D. RUBIN

I. INTRODUCTION

1. I have been retained as an independent expert in this lawsuit by the law firm of Irell & Manella LLP on behalf of Juniper Networks, Inc. ("Juniper"). I have been asked to provide an opinion related to whether Claim 10 of U.S. Patent No. 8,677,494 ("the '494 Patent") contains an inventive concept sufficient to transform the claimed abstract idea into a patent-eligible application. As discussed in further detail in this declaration, it is my opinion that Claim 10 does not contain an inventive concept sufficient to transform the claimed abstract idea into a patent-eligible application.

2. In addition to opinions outlined in this report, I may also provide testimony (1) in rebuttal to Finjan's positions, including opinions of its experts and materials they discuss or rely upon, (2) based on any Orders from the Court, (3) based on documents, contentions, or other discovery that Finjan or others have not yet produced or were produced too late to be considered before my report was due, and/or (4) based on witness testimony which has not been given or was given too late to be considered before my report was due. I reserve the right to supplement or amend my opinions as further documentation and information is received.

3. If called to testify in this matter, I may use as exhibits various documents produced in this matter that refer or relate to the matters discussed in this report. I have not yet selected the particular exhibits that may be used. In addition, I may create or assist in the creation of certain demonstrative exhibits or summaries of my findings and opinions to assist me in testifying. Such exhibits have not yet been created.

II. BACKGROUND AND QUALIFICATIONS

4. I am being paid at my customary rate of $775 per hour for time spent on this case. I am also being reimbursed for reasonable and customary expenses. My compensation is not dependent in any way on the results of the lawsuit or the substance of my testimony.

5. I provide below an overview of my background and qualifications. Additional details of my education and employment history, professional service, patents, publications, and other testimony are set forth in my current curriculum vitae (CV), which can be found here:

29. In IPR2016-00159, the PTAB issued a Final Written Decision invalidating Claim 1 of the '494 Patent in view of a prior art article titled "Dynamic Detection and Classification of Computer Viruses Using General Behaviour Patterns" by Morton Swimmer *et al.* ("Swimmer"). IPR2016-0159, Paper 50 (Ex. 19) at 45. More specifically, the PTAB found that all of the overlapping limitations in Claim 10 (*i.e.*, everything from the limitations that is not bolded/underlined in the table above) was disclosed in the art before the priority date for the '494 Patent.

30. In reaching this conclusion, the PTAB applied a construction of the term "a list of suspicious computer operations" as "a list of all operations that could ever be deemed potentially hostile." Paper 50 at 33. That construction differs from the construction of the term applied by the Court in this proceeding of "a list of computer operations in a received Downloadable that are deemed hostile or potentially hostile." Dkt. No. 189 at 5. But the Board noted that its "ultimate conclusions regarding patentability of the challenged claims did not turn on [its] adoption of that construction…." Paper 50 at 33. Indeed, the Board found "that Swimmer discloses deriving security profile data including a list of suspicious computer operations even under Patent Owner's proposed construction," which was "a list of computer operations deemed suspicious." Paper 50 at 33-34. I agree with the Board that Swimmer discloses deriving "a list of computer operations deemed suspicious." In addition, Finjan's prior proposed construction is substantially similar to the construction adopted by the Court in this matter, and therefore it is my opinion that the Board's previous finding that Swimmer teaches all of the limitations in Claim 1 applies in this proceeding as well.

B. The Element Of A "Receiver For Receiving An Incoming Downloadable" Does Not Contain An Inventive Concept.

31. It is my opinion that using a "receiver" to receive an incoming Downloadable is not an inventive concept. Rather, receivers were well known, routine, and conventional in the art before the priority date of Claim 10 of the '494 Patent, and using a receiver to receive an incoming file (including Java files, HTML, PDFs, Microsoft Word, executables, etc.) was a routine and conventional use of a receiver.

32. For example, Swimmer teaches that a receiver can be used for receiving an incoming Downloadable in a malware detection system. Ex. 3 at 13 ("One possibility is to use it as a type of

firewall for ***programs entering a protected network***.”). I note that Finjan did not even challenge whether Swimmer taught a receiver during the IPR proceedings. *See generally* IPR 2016-00159, Paper 17 (Patent Owner’s Response) (Ex. 20).

33. There are numerous other prior art references that disclosed using a “receiver” to receive a Downloadable. *See, e.g.*, U.S. Patent No. 5,802,275 (Ex. 29) (filed June 22, 1994) at Claim 6 (“a receiver for receiving [] programs”); U.S. Patent No. 6,065,118 (Ex. 30) (filed September 24, 1996) at Claim 11 (“importing to the system a data stream containing at least one mobile program component which is to execute on the computer system from an external source”) and Claim 7 (“the program components which are to be intercepted and run within the execution location are Applets”).

34. Indeed, firewalls and network gateways were well-known long before the priority date of the ‘494 Patent, and all firewalls and network gateways must necessarily have a receiver for receiving files to be processed. *See, e.g.*, U.S. Patent No. 6,065,118 (Ex. 30) at Claim 5 (“the execution location is provided with at least one firewall between the execution location and one of the external sources of data and the end user system”).

C. The Element Of “A Downloadable scanner coupled with said receiver, for deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable” Does Not Contain An Inventive Concept

35. It is my opinion that using a “Downloadable scanner” to derive security profile data for a Downloadable, including a list of suspicious operations that may be attempted by the Downloadable was not an inventive concept at the time of the priority date for the ‘494 Patent.

36. As noted above, the PTAB found that Swimmer disclosed the function of “deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable,” as recited in Claim 1. The PTAB determined, however, that the Petitioner had not demonstrated that Swimmer taught a “scanner,” because Swimmer’s system was a dynamic analyzer—as opposed to a more traditional “scanner” such as a static analyzer. IPR2016-00159, Paper 50 at 51-52.

37. I understand that the Court in this matter has since construed the term "scanner" to mean "software that searches code to identify suspicious patterns or suspicious computer operations." Dkt. No. 189 at 13. I further understand that the Court has interpreted its construction to include dynamic analyzers. Dkt. No. 189 at 14. If dynamic analyzers are included within the scope of the term "scanner," then Swimmer clearly discloses this element of Claim 10. Ex. 3 at, e.g., 9-10 ("The audit system was integrated into an existing PC emulation by placing hooks into the module for processing all opcodes corresponding with the events (see fig. 4). These are primarily calls to the DOS functions. … Internally, the audit trail complies to a canonical format, which is [] very generic, and allows most types of records to be implemented.").

38. Whether or not the construction of "scanner" includes dynamic analyzers, it is my opinion that the use of a "scanner" to derive security profile data (including suspicious computer operations) was conventional as of the priority date of the '494 Patent and is not an inventive concept.

In fact, at the time of the priority date for the '494 Patent, one of the most typical ways for a program to determine whether a file was malicious was by using "software that searches code to identify suspicious patters or suspicious computer operations." One example of malware detection that used a "scanner" is static analysis, where the features and characteristics of a file are analyzed without actually executing the code and checking, for example, for specific byte sequences or other patterns in the code, or using heuristic analysis that identifies features such as if the file has an invalid digital signature, has a high entropy, or has no publisher information. Static analyzers have existed since at least the mid-1980s.

39. By the early 1990s, scanners performing static analysis that used parsing techniques[1] to decompose code and flag specific extracted components (including operations) that were suspicious were commonly used. *See, e.g.*, Ex. 4 at p. 5 ("Hexadecimal patterns may be used to detect the presence of the virus with . . . a dedicated virus scanner."; Ex. 3 at p. 3 ("Scanning techniques are further

[1] At the lowest level, computer instructions are in numerical form called "machine code" that is only legible to a computer, which are directly executable by a computer's central processing unit. A "disassembler" can be used to abstract the machine code into a low-level but human-readable language known as "assembly language." Instructions written in assembly language, however, are still generally difficult for a human to understand, so for analysis purposes, programs are often parsed to "decompile" the machine code into source code, which is the more human-understandable language in which a computer program is generally written. Parsing involves identifying and separating various parts of a program into the instructions and parameters that make up the program.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.