UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SOPHOS LTD. & SOPHOS INC.,

Petitioners

v.

OPEN TEXT INC.

Patent Owner

Case IPR2023-00732

Patent No. 8,719,932

DECLARATION OF RON SCHNELL
IN SUPPORT OF PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I. QUALIFICATIONS 2

II. UNDERSTANDING OF RELEVANT LEGAL PRINCIPLES 5

III. STATE OF THE PRIOR ART 7

IV. The ’932 Patent 9

A. Summary Of The ’932 Patent 9

B. Claim Construction 12

C. Level Of Ordinary Skill In The Art 12

V. OVERVIEW OF PRIOR ART 14

A. Overview Of Li 14

B. Overview Of Hartrell 15

C. Overview Of Yadav 16

D. Overview Of Mandujano 18

VI. LI IN VIEW OF THE SECONDARY ART DOES NOT DISCLOSE OR RENDER OBVIOUS THE CHALLENGED CLAIMS 19

A. Ground 1 19

1. Li and Hartrell Do Not Disclose “identifying… a reference to an identity of an externally networked source of the suspected pestware object” 20

1. Li and Hartrell do not disclose or render obvious “reporting… to an externally networked pestware research entity” ..... **Error! Bookmark not defined.**

1. Petitioners fail to show that a POSITA would have been motivated to Combine Li with Hartrell 27

B. Ground 2 27

1. Mandujano does not cure the deficiencies of Li and Hartrell identified in Ground 1. 27

2. A POSITA would not look to Mandujano to address shortfalls in Li and Hartrell because Mandujano relates to outbound monitoring.....28

C. Ground 3.....29

1. A POSITA Would Not Have Had A Motivation to Combine Li with Yadav.....30

2. Petitioners fail to show that Li in view of Yadav renders obvious "identifying… a reference to an identity of an externally networked source of the suspected pestware object" 31

3. Petitioners fail to show that Li in view of Yadav renders obvious "reporting the identity of the particular externally networked source to an externally networked pestware research entity" .....**Error! Bookmark not defined.**

D. Ground 4.....33

1. Mandujano does not cure the deficiencies of Li and Yadav identified in Ground 3. 35

2. Petitioner fails to identify any motivation to combine Li, Yadav, and Mandujano. 35

VII. CONCLUSION.....35

EXHIBIT LIST

Exhibit	Description
2001	Declaration of Ron Schnell
2002	*Curriculum Vitae* of Ron Schnell
2003	*Sonrai Memory Ltd. v. Kingston Tech. Co. and Kingston Tech. Corp.*, Case No. 6:21-cv-1284-ADA, Order Denying Kingston Tech. Co. and Kingston Tech. Corp.'s Opposed Motion to Stay Pending Resolution of *Inter Partes* Review, Dkt. 94 (W.D. Tex., Oct. 18, 2022)
2004	*mCom IP, LLC v. Cisco Systems, Inc.*, Case No. 6:22-cv-00261-ADA, Order Denying Defendant's Motion to Stay Pending *Inter Partes* Review, Dkt. 42 (W.D. Tex., Oct. 20, 2022)
2005	*Intellectual Ventures I LLC et al. v. Hewlett Packard Enterprise Co.*, No. 6:21-cv-00596-ADA, Order Denying Hewlett Packard Enterprise Company's Opposed Motion to Stay Pending Resolution of *Inter Partes* Review, Dkt. 104 (W.D. Tex., Dec. 22, 2022)
2006	*Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.*, Case No. 6:22-cv-243-ADA-DTG, Dec. 9, 2022 Transcript of Motions Hearing, Dkt. 133 (W.D. Tex. Dec. 15, 2022) (excerpted)
2007	Dani Kass, "Catching Up On Patent Litigation With Judge Albright" (Law360 Mar. 14, 2023); https://www.law360.com/pulse/articles/1582438/print?section=pulse/courts
2008	*Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.*, Case No. 6:22-cv-243-ADA-DTG, Order Granting Fourth Amended Scheduling Order, Dkt. 160 (W.D. Tex. Jan. 22, 2023)

Exhibit	Description
2009	U.S. District Courts—Federal Court Management Statistics–Profiles—During the 12-Month Periods Ending March 31, 2018 Through 2023, "Table N/A—U.S. District Courts–Combined Civil and Criminal Federal Court Management Statistics (March 31, 2023)", available https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distprofile0331.2023.pdf
2010	*Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.*, Case No. 6:22-cv-243-ADA-DTG, July 25, 2023 Claim Construction Order, Dkt. 391 (W.D. Tex. July 25, 2022)
2011	*Webroot, Inc. and Open Text Inc., v. CrowdStrike, Inc. and CrowdStrike Holdings, Inc.*, Case No. 6:22-cv-00241-ADA-DTG, Defendant's Preliminary Invalidity Contentions (W.D. Tex., Feb. 21, 2023) (excerpted)
2012	*Webroot, Inc. and Open Text Inc., v. Trend Micro, Inc.*, Case No. 6:22-cv-00239-ADA-DTG, Defendant's Preliminary Invalidity Contentions (W.D. Tex., Feb. 21, 2023) (excerpted)
2013	*Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab*, Case No. 6:22-cv-00243-ADA-DTG, Defendant's Preliminary Invalidity Contentions Appendix C (W.D. Tex., Feb. 21, 2023) (excerpted)
2014	Website: About ResearchGate, https://www.researchgate.net/about
2015	Website: "Google Announces Beta Release of Google Scholar," Univ. of Calif. (Nov. 17, 2004); *available* https://osc.universityofcalifornia.edu/2004/11/google-announces-beta-release-of-google-scholar/
2016	U.S. Patent 8,201,243 File History (Sophos Ex. 1002 IPR2023-00731)

I, Ron Schnell, declare as follows:

1. I have been engaged by King & Spalding LLP on behalf of OpenText Inc. ("Patent Owner"), to provide this Declaration concerning the technical subject matter relevant to Petitioner Sophos's petition for Inter Partes Review ("Petition") of U.S. Patent 8,719,932 ("the '932 Patent").

2. I am over 18 years of age. I have personal knowledge of the facts stated in this Declaration and could testify competently to them if asked to do so.

3. I have reviewed and am familiar with the specification and the claims of the '932 Patent. In general, I will cite to the specification of a United States patent using the following formats: (Exhibit No. Col.:Line Number(s)) or (Exhibit No. Paragraph Number(s)). For example, the citation (EX-1001 1:1–10) points to the '932 Patent specification at column 1, lines 1–10. Also, for convenience, I use italics to denote limitations from the challenged claims.

4. All the opinions in this Declaration are based on the documents I reviewed and my knowledge and professional judgment. In forming the opinions expressed in this Declaration, I reviewed the Petition for *Inter Partes* Review of U.S. Patent No. 8,719,932 and supporting exhibits.

5. I have been asked to provide my technical opinions regarding how a person of ordinary skill in the art would have understood the claims of the '932 Patent at the time of the alleged invention. I have also been asked to provide my

technical opinions on how concepts in the ’932 Patent specification relate to claim limitations of the ’932 Patent. In reaching the opinions provided herein, I have considered the ’932 Patent, its prosecution history, and the references cited above and have drawn as appropriate on my own education, training, research, knowledge, and personal and professional experience.

I. QUALIFICATIONS

6. In formulating my opinions, I have relied on my knowledge, training, and experience in the relevant field, which I will summarize briefly. A more detailed summary of my background, experience, and publications is set forth in my curriculum vitae (CV), which is submitted as Exhibit 2002.

7. I am a Managing Director at Berkeley Research Group, LLC (“BRG”).

8. I have over 40 years of experience in the fields of computer science and software.

9. I have a master’s degree in computer science from Syracuse University and have a working knowledge of over 40 computer languages.

10. Over the course of my career, I have worked at many of the world’s largest computing companies, including (but not limited to) Bell Laboratories, IBM Corporation, and Sun Microsystems. I was also an early researcher on the Arpanet, which later became the Internet. In addition to working at large corporations, I have founded three start-up companies to date, including a backup and restore software

company and a .COM company that I sold to a public corporation in 2000.

11. Early in my career, I worked at the Artificial Intelligence Lab at the Massachusetts Institute of Technology.

12. Later, in approximately 1986, I worked at Bell Laboratories on the UNIX Operating System, writing many thousands of lines of source code representing portions of the core kernel of the UNIX operating system.

13. From 1988-1990, I worked at IBM Corporation on the kernel of their operating system called AIX (for the IBM 370 mainframe, as well as the IBM PS/2), as a programmer, and eventually a development manager.

14. From 1991-1992, I worked as a Principal Member of the Technical Staff at Encore Computer Corporation, on the kernel of their operating system called UMAX.

15. From 1992-1995, I worked at Sun Microsystems, on the kernel of their operating system called Solaris.

16. From 2002-2005, I was a Vice President at Equifax Corporation, one of the three major credit bureaus in the United States, leading software development in their Internet Marketing division. I was also the company expert on e-mail delivery, responsible for the delivery of over one billion e-mail messages per month.

17. I have also been on staff and consulted at numerous other companies and institutions, including (but not limited to) Syracuse University, Encore

Computing Corporation, Harris Computer Corporation, and ITT.

18. During my career I founded several startup companies, including two kernel software companies. I sold my last startup company to a public company in 2000.

19. I am currently an adjunct professor of computer science and a former advisory board member at the College of Engineering and Information Science at Nova Southeastern University.

20. From 2005 through 2011, I was responsible for monitoring Microsoft Corporation in connection with the antitrust litigations brought by the U.S. Department of Justice and the Attorneys General of 19 states in United States v. Microsoft and New York v. Microsoft. In this role, I had responsibilities akin to those of a Special Master and provided periodic compliance reports to Hon. Colleen Kollar-Kotelly of the United States District Court for the District of Columbia. I was responsible for directing the day-to-day enforcement of the final judgments against Microsoft and supervised a team of 93 people in performing these duties. In this role, I spent time auditing the Windows kernel, and used computer simulation models to detect noncompliance with the Final Judgments.

21. Two publications I have written in the field are: Jay L. Himes, Jason Nieh & Ron Schnell, "Antitrust Enforcement and Big Tech: After the Remedy Is Ordered," 1 Stanford Computational Antitrust 64 (2021), and Ron Schnell, "Hacking

101: Using Social Engineering Increases Security Attack Effectiveness," Coast Guard Journal of Safety & Security at Sea, Proceedings of the Marine Safety & Security Council 71, no. 4 (2014) 25–27.

II. UNDERSTANDING OF RELEVANT LEGAL PRINCIPLES

22. I am not a lawyer, and I will not provide any legal opinions. Although I am not a lawyer, I have been advised that technical experts apply certain legal standards when they form opinions about the meaning and validity of patent claims.

23. I understand that a patent claim is invalid if it is anticipated or obvious in view of the prior art, and that a claim can be unpatentable even if all of the requirements of the claim cannot be found in a single prior-art reference. I further understand that invalidity of a claim requires that the claim be anticipated or obvious from the perspective of a person of ordinary skill in the art at the time the invention was made.

24. I have been informed that a patent claim is invalid if it would have been obvious to a person of ordinary skill in the art. In analyzing the obviousness of a claim, I understand the following factors may be taken into account: (1) the scope and content of the prior art; (2) the differences between the prior art and the claims; (3) the level of ordinary skill in the art; and (4) any so called "secondary considerations" of nonobviousness if they are present.

25. I have been informed that a claim can be obvious in light of a single

prior art reference or multiple prior art references. I understand that to prove that prior art or a combination of prior art renders a patent obvious, it is necessary to:

1) Identify the particular references that, singly or in combination, make the patent obvious;
2) Specifically identify which elements of the patent claim appear in each of the asserted references; and
3) Explain why a person of ordinary skill in the art would have combined the references, and how they would have done so, to create the inventions claimed in the patent. I further understand that exemplary rationales that may support a conclusion of obviousness include:
    - Combining prior art elements according to known methods to yield predictable results;
    - Simple substitution of a known element for another to obtain predictable results;
    - Use of known technique(s) to improve similar devices (methods or products) in the same way;
    - Applying a known technique to a known device (method or product) ready for improvement to yield predictable results;

- Choosing from a finite number of identified, predictable solutions with a reasonable expectation of success, which I am informed is the "obvious to try" standard;
- Known work in one field of endeavor may prompt variations of the work for use in either the same field or a different field based on design incentives or other market forces if the variations are predicable to a person of ordinary skill in the art; and
- Some teaching, suggestion, or motivation in the prior art that would have led a person of ordinary skill in the art to modify the prior art reference or to combine the prior art reference teachings to arrive at the claimed invention.

26. I have been informed that, in considering obviousness, hindsight reasoning derived from the patent at issue may not be used.

III. STATE OF THE PRIOR ART

27. My understanding is that the U.S. District Court for the Western District of Texas has construed "pestware" to mean "a trojan, spyware, adware program, or malware program that collects information about a person or an organization." (EX-2010 3; EX-1001 1:43-54.)

28. Viruses, trojans, worms, and similar programs are all types of pestware.

(EX-1001 at 1:14-17.) Different types of pestware work differently, and therefore, techniques that work to detect one type of pestware (*e.g.*, a virus) may be less effective against another type (*e.g.*, a worm). (*See generally* EX-1001 at 1:14-2:56.)

29. At the time of the invention in the ’932 Patent, many systems designed to address the threat of pestware focused on looking for previously known pestware. For example, antivirus software might have examined executable computer files for known signatures indicative of malware. A system would therefore be vulnerable again after the release of new malware until such malware was detected and defined, and a solution generated and released to users. Generally, this approach required human involvement. Thus, prior art systems were slow and inefficient at developing the required definitions for new pestware and at identifying behaviors associated with pestware.

30. Much of the prior art anti-pestware or anti-virus software focused on scanning and stopping ***known*** pestware based on previously created definitions of pestware. (EX-1001, 1:3-5.) These prior art methods for detecting known pestware suffered from inevitable extensive delay—either while waiting for the pestware to be detected and a definition generated or in locating the pestware to create the definitions in the first place. (EX-1001, 1:5-7).

31. Accordingly, there was a long-felt need for an improved technique to efficiently determine whether objects were safe or pestware.

IV. THE ’932 PATENT

A. Summary Of The ’932 Patent

32. The ’932 patent is titled “Backwards Researching Activity Indicative of Pestware.” The ’932 Patent seeks to find an identity of a source of activity that is indicative of pestware to create definitions for pestware removal software. (EX-1001-2:3-7; 2:24-37; 4:56-66.) Instead of looking for pestware files directly, the invention addressed in the ’932 patent monitors changes made to system resources, analyzes logs and traces of software execution, identifies patterns of behavior indicative of pestware, and classifies and categorizes detected pestware using heuristics and machine learning. (EX-1001 10:20-39.) The ’932 patent uses heuristics modules to compare the API call activities on the computer with weighted factors to make decisions relative to activities at the protected computer. (*Id*.) Unlike prior art systems, which focused on the internal origin through which an attack was made, the ’932 patent traces pestware activity both back to a pestware object ***and*** to a source that originated the pestware object. “As an example, if a pestware file is found on the file storage device 118, then the cache index 243 of the browser cache 242 may be searched to identify the name of the file, and if the originating URL is stored in connection with the file, the URL is identified as the source of the file.” (EX-1001 8:5-7.)

33. The ’932 Patent teaches a method that utilizes detection, quarantine,

removal, and heuristic engines in concert with shields. (EX- 1001 4:19-23.) The engines "compare files, processes, and registry entries… against known pestware definitions and characteristics," and quarantine and remove pestware objects. (EX-1001 4:23-28.) The shields are divided into operating system shields and browser shields and include two types of shields: behavior monitoring shields and definition-based shields. (EX-1001 at 4:33-40). The shields "monitor the protected computer for certain types of activities that generally correspond to pestware behavior," which include "a process spawning another process, an alteration to registry entries, communications with remote sites via the Internet, alterations to a startup folder, injection of a DLL into another process, and a change to the browser's home page and/or bookmarks." (EX- 1001 4: 41-48.) "The shields 120 inform the heuristics engine 110 about the activities and the heuristics engine 110 determines whether the research module 108 should be informed and/or whether the activity should be blocked." (EX- 1001 4:51-55.)

34. In one embodiment, the heuristics module conducts this analysis by comparing the activities on the computer with weighted factors. (EX- 1001 4:56-62.) "If the sum of the weighted factors that match the activity history exceed a threshold, then the activity is identified as pestware activity and the heuristics module 110 prompts the research module 108 to initiate research into the origin of the pestware initiating the activity." (EX- 1001 4:61-66.)

35. In other embodiments, the system uses an activity monitor that "monitors activities on the computer and stores information about the activities in the activity log 120 so as to assist the research module 108 in identifying activities associated with pestware and the source of the pestware." (EX-1001 5:33-37.) This monitor can also be a kernel-mode driver loaded during a boot sequence or anytime later, and is configured to log API calls and to intercept and log certain types of activities that correspond to pestware behavior. (EX-1001 at 5:53-55.)

36. Once indications of pestware are found, then the information recorded by the logs is traversed in order to identify the source of the pestware. (EX- 1001 at 7:47-51). The system disclosed in the '932 Patent can reference one piece (*e.g.*, an originating URL) or multiple pieces of data (*e.g.*, another process that spawned a pestware process, that second process's cache index, and the URL from which the process was downloaded) to identify the source of the pestware. (EX- 1001 7:52-8:4.) A research module 108 searches "the activity log 120 and/or one or more of the N files for information that associates the suspicious activity to one or more processes and the processes may be related to one or more files," to trace the origin of the suspicious objects that generated the suspicious activity. (EX- 1001 9:51-63.)

37. The identity of the externally networked source of the pestware is reported to an "externally networked pestware research entity." (EX-1001, claims 1, 6, 12). The research entity conducts further research on the suspicious pestware

objects and the externally networked source of pestware. "In this way, the suspicious objects and the [sources] originating the suspicious objects may be further researched to establish the extent to which they may be a threat." (*Id.* 8:46-49.)

B. Claim Construction

38. Petitioner does not construe any claim terms in its Petition. Accordingly, I don't take a position on claim construction at this point in the proceeding.

39. I understand that in the District Court's July 25, 2023 claim construction order, the Court determined that no terms of the '932 patent were indefinite and that all terms should be given their plain and ordinary meaning except for "pestware" and the order of steps limitations, whose constructions I summarize below. (EX 2010.)

"Pestware" ('932 patent, claims1, 2, 5, 7, 12, 13)	"a trojan, spyware, adware, or malware program that collects information about a person or an organization"
"monitor[ing] . . . stor[ing] . . . analyz[ing] . . . identify[ing] [a suspected pestware object] . . .	No order recited except for "identify[ing]" [a suspected pestware object], "identi[fying]"

identi[fying] [an externally networked source] . . . report[ing] . . .” (’932 patent, claims 1, 5, 12)	[an externally networked source], and “report[ing]” must occur in order.

40. I apply the Court’s construction or the plain and ordinary meaning of all the claim terms in accordance with the District Court’s July 25, 2023 order.

C. Level Of Ordinary Skill In The Art

41. I understand that certain issues relating to the validity of the ’932 Patent must be judged from the perspective of a person of ordinary skill in the relevant art.

42. I understand that Petitioner has defined the level of ordinary skill in the art or “POSITA” as:

> As of June 30, 2005, a person having ordinary skill in the art (POSITA) would be a person having a bachelor’s degree in computer science, computer engineering, or an equivalent, as well as two years of industry experience and would have had a working knowledge of host monitoring systems, software security analysis, and dynamic malware analysis. Additional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education.

(Petition 9.)

43. In my opinion, a POSITA at the time of the invention of the ’932 patent would have had a bachelor’s degree in an accredited program of electrical engineering, computer engineering, or computer science or in a similar discipline,

and have 2-3 years of practical work or research experience in the general fields of electrical engineering, computer science, networking, communications, and device and network security. More advanced degrees and/or training in a related discipline can compensate for shorter work experience.

44. Based on either standard, I was a person of at least ordinary skill in the art at the time of the invention of the ’932 Patent.

V. OVERVIEW OF PRIOR ART

A. Overview Of Li

45. Li discloses a unified logging architecture that captures and analyzes correlations among entries on different types of logs on a single computer. Li discloses six different types of logs that often are stored in different formats from different sources, such that insight from cross-log or common analysis is challenging. Li’s system (“UCLog”) processes the logs through monitors, which audit, filter, and compare the data collected by the various loggers. (EX-1005 8.) The monitors compare the data with existing models or signatures and send the compressed data to a centralized activity database for management and organization of the data. (EX- 1005 11.)

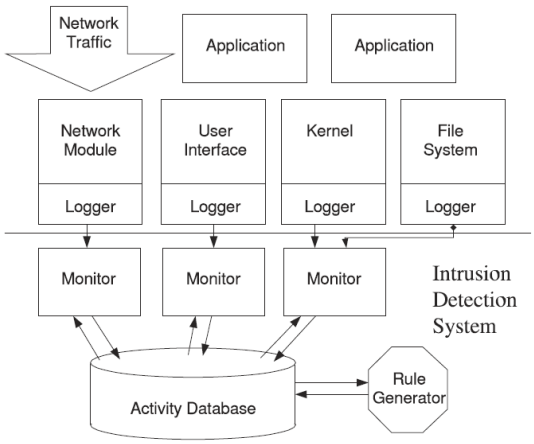

Figure 2. UCLog architecture

The monitors collaborate with other monitors of other loggers by sending queries through the activity database to find correlated activities. (EX- 1005 at 8, 11). Based on the queries and correlation, the rule generator "produces the models for normal or abnormal behavior and signatures for previous intrusions." (EX-1005 14.) Rules are stored in the activity database as training data or sent directly to the monitors. *Id*.

46. Li observed that some prior art intrusion detection systems detected attacks by monitoring manually defined "normal" and "abnormal" system or network behavior. (EX-1005 2.) Li observed that work had been done that identified abnormalities using machine learning or data mining to generate models, but criticized systems that focused on a single "source," which Li defines as a single log, file, or directory. (EX-1005 at 2, 3, 19-20.) (*See also* EX-1005 at 5 ("Most previous work on IDSs analyze a single component, ignoring the correlations among different components.")) Li criticized this single source technique as often resulting in false alarms because exploring activity correlations among heterogenous sources improved accuracy and reduced false positives. (EX-1005 3, 5.) Li therefore sought to provide a unified logging architecture to capture, correlate, and identify malware-related behaviors, while overcoming the "false alarm" problem it perceived in the prior art.

B. Overview Of Hartrell

47. Hartrell discusses a malware analysis system that initiates after a locally

executing anti-malware system detects an infection or suspected infection. (EX-1006, 2:39-44.) The system takes pre- and post-infection "snapshots" to provide a record of events and activities that occurred so that the collective snapshots can be used by experts to trace the sequence that led to an infection, understand how the infection spread through the system, and observe the impact on the system after the infection. (EX-1006, 2:48-57.) A "categorization component" of the malware analysis system processes the snapshots and normalizes the snapshot data by labeling and associating activities in the snapshots with predetermined categories of system activities. (EX-1006, 4:30-32.) The categorization process can be tuned by an administrator to improve the data's usefulness to a "commonality analysis component," which analyzes the output from the categorization component and labels activities as suspicious or potentially normal. (EX-1006, 4:32-37.) An administrator can then mark recurring suspicious activities as malicious. (EX-1006, 4:51-53.) A "response recommendation generator" also reviews the commonality analysis component output and makes recommendations for response to the system administrators. (EX-1006, 5:13-30.) Based on the analysis of the snapshots, a system administrator can reconfigure the security policies to prevent future infections. (EX-1006, 3:8-16.)

C. Overview Of Yadav

48. Yadav discloses an integrated intrusion detection system that uses a

dynamically controlled firewall for integrated network intrusion detection. Yadav's system integrates firewall filtering information with network intrusion analysis and only monitors blocked network communications, thereby reducing the amount of network traffic that needs to be monitored. (EX-1008 3:1-14.) The system of Yadav only performs intrusion analysis on packets blocked by a firewall. (EX- 1008 3:5-10.) That blocked traffic's patterns are checked for patterns spanning multiple channels or communication channels. (EX-1008 4:27-30.) An application behaving abnormally is added to a watchlist and monitored more frequently. (EX-1008 4:52-58.)

49. Under Yadav, when an unauthorized communication is received, a copy is sent to the intrusion detector component, and the communication is blocked. (EX-1008 at 8:25-33.) If an intrusion prelude pattern is detected, then the source of the communication is added to the list of potential intruders to be monitored. (EX-1008 8:56-59.)

50. Based on an administrator's post hoc review of the snapshots, the response recommendation generator generates recommendations, which are made available to system or security administrators. (EX-1008 5:13-30.) The administrators can then decide what corrective measures to implement based on the recommendation. (*Id*.)

D. Overview Of Mandujano

51. Mandujano discloses a score-based system to determine whether an outbound object is malware, using outbound intrusion detection (sometimes referred to as "OID"). Outbound intrusion detection does not protect local resources from being compromised by other systems, but rather prevents local resources from compromising other systems. (EX-1007 67.) Outbound intrusion detection in Mandujano can identify attempts to compromise remote systems by monitoring outbound activity. (*Id*). According to Mandujano, "[a]n advantage of the OID approach … is broader visibility: a host has total access and control over its own resources." (*Id*. 70.) Specifically, Mandujano discloses using the in-depth knowledge of the internal structures to detect patterns that indicate abnormal behavior and define signatures of illicit activity. (*Id*. 78.) Armed with a more thorough understanding of the origin of the actual attack program and underlying commands used, an outbound intrusion detection system can provide potential victims with targeted security measures, thereby conserving resources. (*Id*. 71.) A request for initiating a data transfer is the primary event that triggers the signature detection algorithm. (*Id*. at 84). Because each system is responsible for monitoring its own outbound traffic, the processing strategy is scalable. (*Id*. 73.)

VI. LI IN VIEW OF THE SECONDARY ART DOES NOT DISCLOSE OR RENDER OBVIOUS THE CHALLENGED CLAIMS

52. The petition presents four grounds challenging the claims of the ’932 Patent:

Ground 1	Section 103(a)	Obvious over Li in view of Hartrell	Claims 1-14
Ground 2	Section 103(a)	Obvious over Li in view of Hartrell and Mandujano	Claims 1-14
Ground 3	Section 103(a)	Obvious over Li in view of Yadav	Claims 1-14
Ground 4	Section 103(a)	Obvious over Li in view of Yadav and Mandujano	Claims 1-14

53. I disagree with the arguments in the Petition and the opinions set forth by Dr. Houh for at least the reasons that I discuss in further detail below.

A. Ground 1

54. Petitioners’ obviousness grounds fail for at least the following three reasons: (1) neither Li nor Hartrell disclose or render obvious “reporting… to an externally networked pestware research entity;” (2) neither Li nor Hartrell disclose or render obvious “identifying… a reference to an identity of an externally networked source of the suspected pestware object;” and (3) a POSITA would not

have been motivated to combine Li and Hartell.

1. Li and Hartrell do not disclose or render obvious "reporting… to an externally networked pestware research entity"

55. Li does not disclose an externally networked pestware research entity. As shown in Figure 2, Li's system design does not include any kind of research entity, let alone an externally networked pestware research entity:

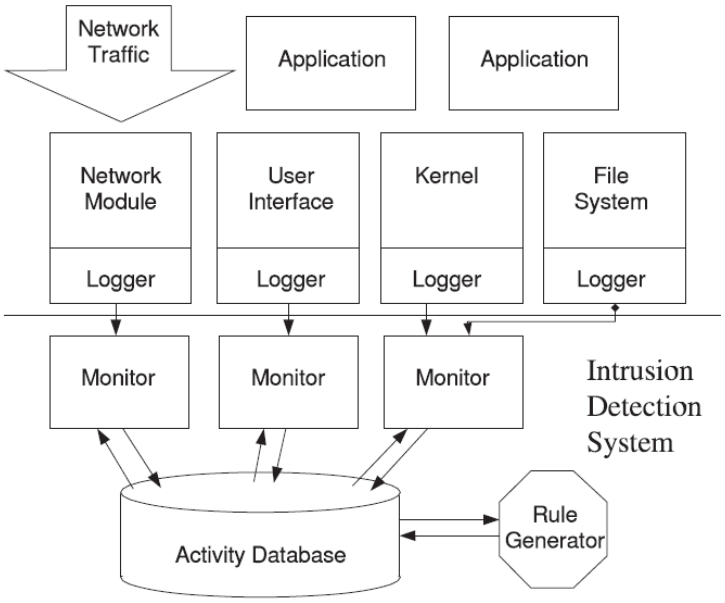

Figure 2. UCLog architecture

(EX-1005 8, Figure 2.)

56. Dr. Houh correlates "*externally networked research entity*" with Li's disclosure of a human reviewer. Petitioners claim that this limitation is met because "Li states that the user interface of an IDS 'enables an administrator to view the

output from the system,'" and because that interface is on a separate system, then the administrator is externally networked. (EX-1003 ¶ 110). A POSITA would not understand a human administrator, whether working on a separate workstation on the same network as the UCLog system or not, to be an "externally networked" entity, let alone an "externally networked research entity."

57. The '932 patent claims generally refer to the pestware research entity as the "externally networked pestware research entity." (*See* EX- 1001, claims 1, 5, 12.) Otherwise, the "research entity" is referred to in the specification as the "remote research entity." (*Id*. 9:61-62.) The research entity is distinguishable from the research module. The research module searches activity logs and N files for information associating an object's suspicious activity to processes, which are related to "one or more files." (*Id*. 9:48-55.) This search provides information about the identity of the source of a suspicious process and/or files," and the source is then reported to a remote research entity. (*Id*. 9:61-63.) ("Once the source of the suspicious object(s) is identified (Block 510), the source is then reported (e.g., to a remote research entity) (Block 512).")

58. In this regard, Li is similar to the art the patent owner already distinguished during prosecution, U.S. 2005/0268112 ("Wang"). Applicant distinguished Wang: "the event log described by Wang is not an externally networked pestware research entity. The event log is a file that resides within the

computer that runs Wang's Gatekeeper engine software...Wang does not describe providing the event log to any externally networked entity...." (EX-1002 71). The Applicant distinguished the prior art based on the fact that the prior art involved activities that were entirely internal to the computer without any external network involved, while the claims recited an externally networked entity. (*Id*.)

59. As shown in Figure 2, all of the activities involved in Li's IDS are internal to the computer, and involve no externally networked pestware research entity. Figure 2 indicates that all activities occur on the "internal" side of the network traffic arrow, with no indication that any information is ever fed back into an external network. There is no indication anywhere in Li that operating a server externally would be necessary or advantageous.

60. Hartrell does nothing to cure the deficiencies of Li. Like Li, Petitioners point to Hartrell's disclosure of alerting the system operator or administrator to a pattern and providing recommendations to the same system administrator. (Petition 28-29, EX-1006, 5:13-30.) The reliance on a human decision for the execution and completion of these processes, however, does not disclose reporting to an ***externally networked*** pestware research entity.

2. Li and Hartrell Do Not Disclose "identifying… a reference to an identity of an externally networked source of the suspected pestware object"

61. Dr Houh points primarily to Li to support his argument that the prior

art disclosed the limitation "identifying… a reference to an identity of an externally networked source of the suspected pestware object." I disagree that a POSITA would have understood the "source" disclosed in Li to mean the same as the "externally networked source" disclosed in the '932 patent. As demonstrated by Li's references to "network activity," Li is concerned with monitoring and protecting *internal networks* against pestware.

62. Li describes an intrusion detection system (IDS) as one that "attempts to detect attacks by monitoring system or network behavior." (EX-1005 2.) Li does not disclose a system or method that can identify an externally networked source of a suspected pestware object. Instead, Li discloses monitoring file input and output (or "I/O") at specific files or directories, which Li refers to as sources. (EX-1005 19-20.) Specifically, Li discusses monitoring and correlating an "additional source"—the c:\recycler\ directory. (*Id*.) Li states adding this "additional source" could improve intrusion detection system ("IDS") accuracy because it was a common technique for worms and viruses to create files inside that directory. (*Id*. 20.) That passage does not disclose tracing the origin or source of pestware that caused the file to be created, but rather generating a warning that the behavior at the internal directory, file, or component is behaving abnormally. (*Id*.) Further, Li discloses its system "organizes all audit logs from heterogeneous sources." (*Id*. 3.) Even Dr. Houh refers to the logs as "sources." (EX-1003 ¶70.) A POSITA would therefore

know Li's use of the term "source" to mean an internal file, directory, or component.

63. An internal file or directory, as disclosed in Li, is distinguishable from the '932 patent's use of the term "source," which means an externally networked object or actor. The '932 patent makes multiple references to the identity of the source being externally networked – not strictly an internal file or directory. (*See* EX-1001 3:52-54 ("the identities (e.g., I.P. address, URL, email client or program name) of sources (e.g., web sites, email or program) of the pestware"); *id*. 3:60-64 ("the N files 130 include one or more files with information that assist the research module 108 in tracing information in the N files130 to an identity (e.g., URL) of the source of pestware 122, 124 on the computer 100."); *id*. 3:67-4:4 (N files "may include information such as process IDs, registry entries, file names, cookies and URLs among other information that is used to trace from an identified pestware file, pestware process and/or pestware activity to an originating source (e.g., URL or IP address) of the infection.").)

64. Li is similar to the art examined and overcome during the prosecution of the related '243 patent. During prosecution, the examiner pointed to U.S. 2004/0024864 ("Porras") in which all the detection activity occurs solely within an internal network—no external network is involved. For example, Applicant stated that Porras is limited to the confines of the host computer: "Porras is expressly limited to finding and taking action, on the host computer, against only the host

computer session that attacks the host computer. The universe of activity in Porras is limited to the confines of the host computer and its user sessions and process sessions." (EX-2016 166-167.) Porras is therefore confined to the host computer. As Dr. Houh noted, Applicant argued during prosecution that the "'source' of the object is an 'externally networked source,' which the applicant argued was different from a source of an attack within the host computer." (EX-1003 ¶60.) Dr. Houh also noted that Applicant distinguished Porras from the '243 patent because "Porras is interested not in an externally networked source suspected of originating an attack." (*Id.* (*citing* (EX- 2016 168.).) Similarly, Li, which only correlates data on a single computer, does not disclose "identifying… a reference to an identity of an externally networked source of the suspected pestware object."

65. In the singular reference to "source" identified by Petitioners and Dr. Houh, Li refers to "the source and the execution path of the occurring intrusion." (*Id*.) The execution path of the source refers to its functions within the system itself. This provides no disclosure of identifying a source that is externally networked. This stands in stark contrast to the '932 patent, which expressly describes identifying the URL from which a pestware originated:

> As an example, if a pestware file is found on the file storage device 118, then the cache index 243 of the browser cache 242 may be searched to identify the name of the file, and if the originating URL is stored in connection with the file, **the URL is identified as the source of the file**. As another example, if a pestware process is identified, a search of

> the activity log 220 may lead to the identity of a second process that spawned the pestware process, and additional searching of the activity log 220 using the name of the second process may lead to the identification of a pestware file associated with the second process. In turn, a search of the cache index 243 for the name of the pestware file may lead to **the URL from which the pestware file was downloaded**.

(EX- 1001 7:59-8:4.)

66. The ’932 patent expressly discloses, and claims, identifying a source that can be traced back to an external network. Li provides no such disclosure.

67. Thus, a POSITA would not have understood Li, which only correlates data on a single computer, to disclose “identifying… a reference to an identity of an externally networked source of the suspected pestware object.”

68. Hartrell cannot cure the deficiencies of Li because Hartrell is not concerned with pestware *objects* at all. Instead, the disclosed “malware analysis system” of Hartrell “monitors and records computer system *activities*.” (EX-1006 Abstract.) There is no disclosure of tracing a specific *object* back to an externally networked source. The “objects” described in Hartrell are not pestware objects but “operating system objects that were manipulated.” (*Id.* 3:6-7.) Determining that “four infected machines visited the same web site prior to being infected” does not disclose, or require, identifying a “pestware object” that caused the infection. (*Id.* at 3:48-49.) Because Hartrell does not disclose identifying a pestware object, it cannot disclose identifying the externally networked source ***of*** a pestware object.

3. Petitioners fail to show that a POSITA would have been motivated to Combine Li with Hartrell

69. I disagree with Dr. Houh that a POSITA would be motivated to "aggregate the system-wide unified log information disclosed in Li within the centralized database described in Hartrell." (EX- 1003 ¶85). Li *already discloses* an "activity database" to aggregate log information. (EX- 1005 12-14.) Li expressly contemplates that such a log may be used in a "large-scale network"—that is, a network running multiple computers—and offers solutions to manage such network-wide logging in an efficient manner. (*Id.* 13-14.) Dr. Houh fails to explain why a POSITA would abandon the database disclosed in Li for a different database, much less explain what advantages that database of Hartrell offers over Li's.

B. Ground 2

1. Mandujano does not cure the deficiencies of Li and Hartrell identified in Ground 1.

70. In Ground 4, Dr. Houh relies upon Mandujano to support disclosure of limitations 1B, 1C, 6B, 12B, and 12C. Dr. Houh does not rely on Mandujano to cure any of the deficiencies identified in Ground 1 above. Nor could he as Mandujano does not address limitations 1E, 1F, 5C, or 5D discussed above. Thus, Ground 2 fails for the same reasons I described above.

2. A POSITA would not look to Mandujano to address shortfalls in Li and Hartrell because Mandujano relates to outbound monitoring

71. I disagree with Dr. Houh that a POSITA would have "found it obvious to implement the predictions (including the calculations from Mandujano) based on heuristics and thresholds in a separate module." (Petition 55.) Dr. Houh only provides a conclusory statement that "A POSITA would have understood that the disclosed components could be implemented in a single heuristics module, as these implementations are all parts, or steps, in the process of determining whether activity amounts to an intrusion." (EX- 1003 ¶186.) However, a POSITA would not rely on or combine Mandujano with the other prior art because the other art involves monitoring inbound or internal communications and activities, but Mandujano strictly involves the monitoring of outbound communications. (*See generally,* EX-1007). In fact, Mandujano discloses that its primary focus, outbound intrusion detection, "is a variant of the intrusion detection problem. Its objectives vary from those of traditional intrusion systems…." (EX-1007 67.) In describing its architecture and implementation, Mandujano specifically discloses that "***only outgoing packets are being captured***…" (EX-1007 112.)

72. By contrast, Li uses a multitude of data points to monitor, analyze, and detect all abnormal behaviors inside of an internal system (EX-1005 11). Li discloses a broad series of loggers that capture broad varieties of data, well beyond "only

outgoing packets." (EX-1005 9-10.) Indeed, the key benefit of the UCLog disclosed in Li is that it "enables the intrusion detection system to make some sense of the *myriad of different* available logs and *correlate* the information the logs present to enhance the intrusion detection process." (*Id.* 1.) A POSITA would not be motivated to improve upon Li's system of aggregating myriad sources of data by combining it with the system of Mandujano, which focuses on only one source.

73. Similarly, Hartrell discloses using a "commonality analysis" of "snapshots" to identify statistically significant commonalities for pre- and post-infection malware states. (EX-1006 5:13-30). A POSITA would not have been motivated to combine Hartrell's reactive commonality approach with Mandujano's proactive, pre-infection, and single point of reference approach. A POSITA would not have looked to an incident-based approach to address perceived shortfalls in a systems-based approach.

74. Mandujano teaches monitoring for intrusions by focusing on a far narrower subset of data than Li and Hartrell. A POSITA would therefore not have looked to Mandujano to fill the gaps in the primary references.

C. Ground 3

75. Dr. Houh claims Li, in light of Yadav, would have rendered obvious the following limitations: 1[p]; 1[d]; 1[e]; 2[a]; 4[a]; 5[a]; 6[p]; 6[c]; 6[d]; 12[p].

1. Petitioners fail to show that Li in view of Yadav renders obvious "reporting the identity of the particular externally networked source to an externally networked pestware research entity"

76. I disagree with Dr. Houh that Yadav discloses reporting the "externally networked source" of a pestware object to an "externally networked pestware research entity" because, as explained above, Yadav is not concerned with identifying an "externally networked source" at all. Rather, Yadav may "report the intrusion to the central security server 292." (EX-1003 ¶200; *see also*, Petition 61 (*citing* EX-1008 10:25-28).) Yadav's "intrusion" is not a source of a suspected pestware object—that is the origin of a program residing on the computer. An intrusion is not an "object" or "source" at all, but rather an event—"an attempt to break into and/or misuse a computing system." (EX-1008 2:60-61.) Reporting the existence of an "intrusion" is not the same as reporting an identity of an "externally networked source" of a "suspected pestware object."

77. Additionally, I disagree with Dr. Houh that Yadav discloses reporting *of any kind* to an externally networked pestware research entity. The single cited reference to a "central security server" provides no detail regarding the composition or capabilities of this server. (Petition 61 (citing EX-1008 10:25-28).) Dr. Houh points to nothing that indicates the server is externally networked. On the contrary, Yadav makes clear that a key aspect of "network security is to install a firewall,

which restricts and controls the flow of traffic between networks, *typically between an enterprise network and the Internet*." (EX-1008 1:51-54.) Yadav is expressly directed at "integrating firewall filtering information with network intrusion analysis" by "performing intrusion analysis on packets blocked by a firewall." (*Id.* 3:1-10.) In other words, the express purpose of Yadav is to protect an internal network (an enterprise network) from an external network (the Internet). Given this context, it is clear that the "central security server" would be networked to the computer submitting a report via the protected internal network.

78. Indeed, while Yadav is focused on the protecting of the internal network, Yadav knows how to specifically identify an external network when it wants to. (*Id.* 1:54 ("the Internet"); *id.* 4:12 ("an IP network").) That Yadav uses no such term to describe the networking of the "central security server" further indicates that the server communicates via the internal network. Yadav offers no disclosure that the "central security server" is externally networked, nor is it a necessary or obvious aspect of the disclosed system.

2. Petitioners fail to show that Li in view of Yadav renders obvious "identifying… a reference to an identity of an externally networked source of the suspected pestware object"

79. I disagree with Dr. Houh's assessment that Li discloses "identifying an externally networked source" of the suspected pestware object for the reasons I

described above with respect to Ground 1. I also disagree with Dr. Houh that Yadav cures this deficiency.

80. Dr. Houh states that a POSITA would have been motivated to combine Li and Yadav because both references "pertain to the same field of endeavor: the detection and prevention of intrusions." (EX-1003 ¶192.) Yadav does not disclose identifying an "externally networked source of a suspected pestware object" because Yadav does not concern itself with identifying pestware objects at all. The '932 patent describes its invention in part as "identifying … a suspected pestware object on the computer." (EX-1001 2:32-33.) The patent further explains that pestware is a "type of program[]." (*Id.* 1:50-61.) The claimed invention attempts to identify the "originating source…of the infection." (*Id.* 4:3-4.) Dr. Houh points to no disclosure in Yadav that identifies a program residing on the computer that is a suspected pestware object, let alone any disclosure of an attempt to identify the origin of the suspected pestware object.

81. Rather than attempting to identify the source of a program residing on the computer, Yadav discloses identifying "a source of [an] intrusion prelude," as Dr. Houh notes. (EX- 1003 ¶192; Petition 60 (citing EX-1008 4:31-41).) An "intrusion" is defined by Yadav as "an attempt to break into and/or misuse a computing system," and defines an "intrusion prelude" as "communication activities that typically precede an intrusion." (EX- 1008 2:60-63.) In other words, Yadav

attempts to identify and stop an *on-going* attempt to access or misuse the computer. By contrast, the ’932 patent attempts to identify the source of a *previous* event that originated the suspected pestware object.

3. A POSITA Would Not Have Had A Motivation to Combine Li with Yadav

82. I disagree with Dr. Houh that a POSITA would be motivated to “aggregate the log information, including information about the source of pestware, within the central security server described in Yadav.” (EX-1003 ¶192.) Li *already discloses* an “activity database” to aggregate log information. (EX-1005 12-14.) Li expressly contemplates that such a log may be used in a “large-scale network”—that is, a network running multiple computers—and offers solutions to manage such network-wide logging in an efficient manner. (*Id.* 13-14.) Dr. Houh fails to explain why a POSITA would abandon the database disclosed in Li for a different database, much less explain what advantages the central server of Yadav offers over Li’s activity database.

83. A POSITA would not look to Yadav to modify Li because the two differ in their purpose and implementation. First, while Li focuses on holistic analysis and correlation of logs to understand system activities, Yadav focuses on targeting malicious activities and unauthorized access attempts on specific network traffic channels. (*Compare* EX-1005 at 8 *with* EX-1008 3:5-10.) Second, Li aims to provide

a comprehensive view of system activities to improve long term analysis, prevention, and response, while Yadav monitors and reacts to network traffic in real time.

84. A POSITA would not have looked to an intrusion detection system focused on real-time reactions to unauthorized network traffic to modify the log correlation system in Li. A POSITA would not have looked to a system with a much more restricted scope to fulfill the now-perceived shortfalls of the whole-system approach disclosed in Li. Certainly, a POSITA would not have looked to Yadav's system for an externally networked pestware research entity since such an entity was not disclosed in Yadav. Thus, even if a POSITA had sought to modify Li to incorporate an externally networked pestware research entity (they would not have), they would not have turned to Yadav for guidance. A POSITA would not have looked to Li in view of Yadav to disclose or render obvious any limitation of the '932 patent.

D. Ground 4

85. Ground 4 fails for the same reasons as I described in Ground 3. None of the deficiencies found in Ground 3 are cured by Mandujano. Even if they were, a POSITA would not be motivated to combine Mandujano with Li and Yadav to arrive at the claimed invention.

1. Mandujano does not cure the deficiencies of Li and Yadav identified in Ground 3.

86. In Ground 4, Dr. Houh relies upon Mandujano to support disclosure of limitations 1B, 1C, 6B, 12B, and 12C. Dr. Houh does not rely on Mandujano to cure any of the deficiencies identified in Ground 3. Nor could he as Mandujano does not address limitations 1E, 1F, 5C, or 5D discussed above. Thus, Ground 4 fails for the same reasons I described above.

2. Petitioner fails to identify any motivation to combine Li, Yadav, and Mandujano.

87. I disagree that a POSITA would have been motivated to combine the teachings of Li and Yadav with Mandujano for the same reasons a POSITA would have been motivated to combine Li, Hartrell, and Mandujano. Hartrell and Yadav are two different references. Petitioners offer no explanation at all for why a POSITA would substitute the two in this combination. Petitioners have failed to meet their burden to show motivation to combine.

VII. CONCLUSION

88. For at least the foregoing reasons, it is my opinion that Petitioners' grounds do not render obvious any of the challenged claims of the '932 Patent.

I hereby declare that all statements made herein of my own knowledge 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.

Executed this 10th day of August, 2023 in Sunrise, Florida.

Respectfully submitted,

Ron Schnell