

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORCEPOINT LLC,
Petitioner

v.

OPEN TEXT INC.,
Patent Owner

Case IPR2023-00784
Patent No. 8,438,386

**DECLARATION OF PROFESSOR ALESSANDRO ORSO
IN SUPPORT OF PATENT OWNER**

Mail Stop PATENT BOARD
Patent Trial and Appeal Board
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

IPR2023-00784
Open Text Inc. EX-2001

TABLE OF CONTENTS

EXHIBIT LIST	iii
I. QUALIFICATIONS	2
II. UNDERSTANDING OF RELEVANT LEGAL PRINCIPLES	6
III. STATE OF THE PRIOR ART	9
IV. THE ’386 Patent	10
A. Summary of the ’386 Patent.....	10
B. Claim Construction.....	16
1. Security History	17
C. Level of Ordinary Skill in the Art	19
V. Overview of the Prior Art.....	21
A. Overview Of Hubbard-495.....	21
B. Overview Of Hubbard-174.....	24
C. Overview Of Alperovitch.....	25
VI. Ground 1 Does Not Disclose or Render Obvious the Challenged Claims....	26
A. The Prior Art Does Not Disclose or Render Obvious the “Security History” Limitation	27
1. Hubbard-495 does not disclose a reputation vector comprising a “security history” factor	29
B. The Prior Art in Ground 2 Does Not Disclose or Render Obvious The “security history” Limitation.....	35

Declaration in Support of Patent Owner’s
Preliminary Response to Petition for *Inter Partes* Review
Patent No. 8,438,386

C.	There Was No Motivation to Combine Hubbard-495 and Hubbard-174 with Alperovitch	39
VII.	DEPENDENT CLAIMS.....	42
VIII.	OTHER LIMITATIONS NOT ADDRESSED	42
IX.	SECONDARY OBJECTIVE INDICIA OF NONOBVIOUSNESS	43
X.	CONCLUSION.....	43

Declaration in Support of Patent Owner’s
Preliminary Response to Petition for *Inter Partes* Review
Patent No. 8,438,386

EXHIBIT LIST

Exhibit	Description
2001	Declaration of Professor Alessandro Orso, Ph. D.
2002	<i>Curriculum Vitae</i> of Professor Alessandro Orso, Ph. D.
2003	<i>Sonrai Memory Ltd. v. Kingston Tech. Co. and Kingston Tech. Corp.</i> , Case No. 6:21-cv-1284-ADA, Order Denying Kingston Tech. Co. and Kingston Tech. Corp.’s Opposed Motion to Stay Pending Resolution of <i>Inter Partes</i> Review, Dkt. 94 (W.D. Tex., Oct. 18, 2022)
2004	<i>mCom IP, LLC v. Cisco Systems, Inc.</i> , Case No. 6:22-cv-00261-ADA, Order Denying Defendant’s Motion to Stay Pending <i>Inter Partes</i> Review, Dkt. 42 (W.D. Tex., Oct. 20, 2022)
2005	<i>Intellectual Ventures I LLC et al. v. Hewlett Packard Enterprise Co.</i> , No. 6:21-cv-00596-ADA, Order Denying Hewlett Packard Enterprise Company’s Opposed Motion to Stay Pending Resolution of <i>Inter Partes</i> Review, Dkt. 104 (W.D. Tex., Dec. 22, 2022)
2006	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.</i> , 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 Al-bright” (Law360 Mar. 14, 2023); https://www.law360.com/pulse/articles/1582438/print?section=pulse/courts
2008	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)”, <i>available</i> https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_dist_profile0331.2023.pdf

Declaration in Support of Patent Owner's
Preliminary Response to Petition for *Inter Partes* Review
Patent No. 8,438,386

Exhibit	Description
2009	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.</i> , Case No. 6:22-cv-243-ADA-DTG, Order Granting Fourth Amended Scheduling Order, Dkt. 160 (W.D. Tex. Jan. 22, 2023)
2010	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.</i> , Case No. 6:22-cv-243-ADA-DTG, Claim Construction Order, Dkt. 236 (W.D. Tex. Mar. 16, 2023)
2011	<i>Webroot, Inc. and Open Text Inc., v. Forcepoint LLC</i> , Case No. 6:22-cv-342-ADA-DTG, Defendant Forcepoint LLC's Preliminary Invalidity Contentions (W.D. Tex. Sept. 13, 2022) (excerpted)
2012	<i>Webroot, Inc. et al. v. AO Kaspersky Lab et al.</i> , No 6-22-cv-00243, Dkt. 121, Second Amended Complaint For Patent Infringement (<i>Forcepoint LLC</i> , Case No. 22-cv-00342-ADA-DTG) (W.D. Tex. Dec. 9, 2022)

Declaration in Support of Patent Owner's
Preliminary Response to Petition for *Inter Partes* Review
Patent No. Patent No. 8,438,386

I, Professor Alessandro Orso, 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 the petition for *Inter Partes* Review ("Petition") of U.S. Patent No. 8,438,386 ("the '386 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 '386 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 '386 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. 8,438,386 and supporting exhibits.

5. I have been asked to provide my technical opinions regarding the Petition and how a person of ordinary skill in the art would have understood the

Declaration in Support of Patent Owner's
Preliminary Response to Petition for *Inter Partes* Review
Patent No. 8,438,386

claims of the '386 patent at the time of the alleged invention. I have also been asked to provide my technical opinions on how concepts in the '386 patent specification relate to claim limitations of the '386 patent. In reaching the opinions provided herein, I have considered the '386 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 I set forth in my curriculum vitae (CV), which I submitted as Exhibit 2002.

7. I am currently a Professor in the School of Computer Science and the Interim Dean in the College of Computing, at the Georgia Institute of Technology (Georgia Tech). I received my MS degree in Electrical Engineering (1995) and my PhD in Computer Science (1999) from Politecnico di Milano, Italy. My main areas of expertise are program analysis, software testing and debugging, computer security, and program comprehension.

8. Overall, I have been working in the software field for almost 30 years. While preparing my MS thesis, in 1994, I worked for one year as the system administrator for a network of 16 public libraries, which involved setting up,

connecting, and maintaining a group of Linux servers that were exchanging updates overnight.

9. After getting my MS degree, in 1995, I worked for several months as a free-lance consultant, helping develop IT solutions for companies and performing Linux system installations.

10. Additionally, in my initial years at Georgia Tech, when I was working as a Postdoctoral Fellow, I was in charge of setting up my research group's lab, which involved installing operating systems and software, setting up networks, and configuring routers and firewalls for these networks. In the same period, I became a certified Linux system administrator.

11. During my PhD, I did research in the general area of software testing. My dissertation was about novel techniques for testing systems written using object-oriented languages. After completing my PhD, in 1999, and before moving to Georgia Tech, I worked for a year as a Postdoctoral Fellow at Politecnico di Milano, where I extended my dissertation work. In the same year, I spent the summer at the University of Illinois at Chicago as a visiting researcher.

12. I joined Georgia Tech in 2000 and worked there in different capacities: Postdoctoral Fellow (2000-2001), Research Scientist (2001-2004), Assistant Professor (2004-2008), Associate Professor with tenure (2008-2014), and Full Professor (2014 to date). From January 2015 to December 2017, I was Associate

School Chair, which involved various kinds of administrative responsibilities. I became an Associate Dean in 2020, and the Interim Dean of the College of Computing in August 2023.

13. In 2011, during my sabbatical year, I spent time as a visiting scholar at Politecnico di Milano, Italy (my alma mater), IBM Research, India, University of Lugano, Switzerland, and University of Buenos Aires, Argentina.

14. I have published over 100 refereed conference and journal papers in the general area of computer science. I have received several Distinguished Paper Awards and Best Paper Awards. I also received four Impact Awards, which are given to recognize the impact of research work in retrospect, typically considering the last ten years. I have been invited to give numerous guest lectures, talks, and distinguished lectures about my research. I have received grants to support my research from several major companies and national agencies, including Google, IBM, Microsoft, DARPA, DHS, Facebook, NSF, and ONR.

15. I have developed and taught several classes on software engineering, for both graduate and undergraduate students. I also developed an on-line class on software engineering that is being offered through the Udacity platform, as part of Georgia Tech's Online MSCS, and as part of Georgia Tech's professional education curriculum. My online class has been taken by thousands of students and has been

used by several colleagues as teaching material for their software engineering courses.

16. In addition to teaching in the academic context, I also taught a variety of professional education courses in various topics, including software quality, project management, software design, and system administration, to IT professionals in various companies and countries, including Argentina, Italy, Paraguay, South Africa, and United States.

17. I am an expert in the area of computer security. In the last 20 years, I have received multiple grants to support my security-related work from various agencies, including DARPA, DHS, NSF, and ONR, and I have published several well-cited papers about computer security. For example, one line of research that I successfully pursued in my career focuses on analysis and testing of applications developed using web technology. In particular, I have developed two new techniques that can detect and prevent injection attacks to web applications. Together the three main papers that describe these techniques have been cited over 2,000 times by the scientific community. One of these papers has also received a Most Influential Paper Award at the IEEE/ACM International Conference on Automated Software Engineering (ASE 2020). Developing these kinds of techniques requires a deep understanding of the concepts, mechanisms, and technologies involved, including

web and network security, multi-tier architectures, databases, JavaScript, SQL, HTML, HTTP and other underlying network protocols.

18. I am active in the software engineering research community in a variety of ways. I served as Program Chair for all the top conferences in my area and regularly serve on Program Boards and Program Committees for these conferences. I also regularly perform peer reviewing for various journals and for grant proposals submitted for funding to the National Science Foundation and other agencies (e.g., DARPA). I have been a member of the Steering Committee of the flagship conference in software engineering. I have also served on the Steering Committee for the two main conferences in the area of Software Testing and Program Analysis: The ACM International Symposium on Software Testing and Analysis (ISSTA) and the IEEE International Conference on Software Testing, Verification and Validation (ICST). Finally, I served as Associate Editor of the ACM Transactions on Software Engineering and Methodology and am currently serving as Associate Editor of the IEEE Transaction on Software Engineering.

19. I am a Distinguished Member of the ACM and an IEEE Fellow.

II. UNDERSTANDING OF RELEVANT LEGAL PRINCIPLES

20. I am not a lawyer, and I will not provide any legal opinions. Although I am not a lawyer, I have been advised certain legal standards are to be applied by

Declaration in Support of Patent Owner's
Preliminary Response to Petition for *Inter Partes* Review
Patent No. 8,438,386

technical experts in forming opinions regarding the meaning and validity of patent claims.

21. 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.

22. 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.

23. 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;

Declaration in Support of Patent Owner's
Preliminary Response to Petition for *Inter Partes* Review
Patent No. 8,438,386

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 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;
- “Obvious to try” – choosing from a finite number of identified, predictable solutions with a reasonable expectation of success;
- 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.

24. 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

25. The Internet is a worldwide, decentralized network of computers and data transmission paths through which the computers can communicate with other computers. EX-1001 3:44-48. Users often access the Internet using a web browser installed on the user's client computer. The web browser may download web pages from a server computer.

26. Hackers use these Internet communications to attack computers and other devices of users on the Internet. For example, a server may contain malicious data that, when downloaded onto a client computer, may grant the hacker with access to sensitive information stored on a user's client computer or otherwise force the client computer to operate in ways not intended by the user.

27. Ways to address these threats have been developed over time. (EX-1001 1:30-50, 1:62-2:32) One such approach is "content filtering," in which internet resources "are organized into categories and requests for Web content are matched against per-category policies and either allowed or blocked." (EX-1001 1:30-34)

Such approaches have various drawbacks, such as lack of precision and predictiveness. (*See* EX-1001 1:46-50)

28. Thus, as the '386 patent notes, there was a need for a system and/or method capable of assessing zero-day threats, determining whether a file or web page included malicious content in a more predictive and flexible manner. *Id.*

IV. THE '386 Patent

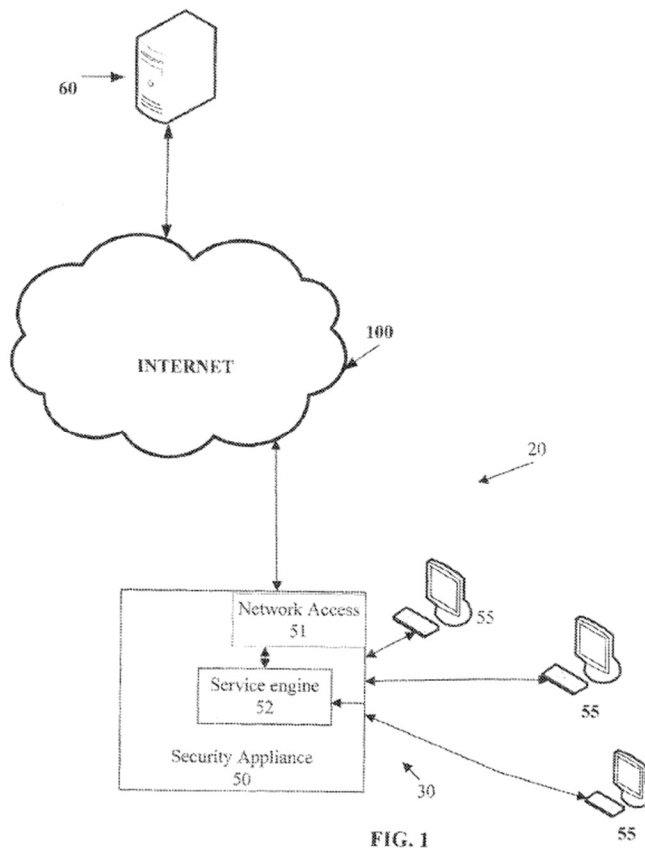
A. Summary of the '386 Patent

29. The '386 patent is entitled "System and Method for Developing a Risk Profile for an Internet Service," was filed on February 21, 2010, and was duly and legally issued by the United States Patent Office on May 7, 2013. (EX-1001 p. 1.) The systems and methods described and claimed in the '386 patent are directed to improved techniques for detecting and classifying a potentially malicious Internet resource based on the resources' reputation. (EX-1001 Abstract.)

30. To address the shortcomings of the prior art, the 386 patent describes and claims unconventional, novel systems and methods for controlling access to Internet resources, such as web pages. These enhanced computer systems and methods provide a technical solution to the technical problem of detecting and classifying potentially malicious resources on the Internet, thus improving network security while identifying and classifying malware threats in real-time without delays engendered by the use of human analysts or waiting until malicious Internet

resources have been identified and reported after they have already exploited other systems, networks, and/or client computers.

31. In particular, the '386 patent describes and claims embodiments including computer networks, such as a local area network ("LAN"), through which multiple client computers access the Internet. This system improves the operation of the computer network over traditional networks because, for example and as described in the '386 patent, it employs "a predictive approach based on a statistical model built on broad sampling of Internet resources with varying degrees of risk. [Such embodiments] focus[] on the reputation of a Web site, or any Internet-based service or resource." (EX-1001 4:34-38.) An example of this novel system is illustrated in the figure below, which shows multiple client-side devices 55 on a local area network 30 connecting to the Internet 100 to fetch an Internet resource (*e.g.*, a web site) from a remote server 60. (EX-1001 FIG. 1) Requests made on a client-side device 55 for the Internet resource may be routed to a security appliance 50 that assesses a reputation for the requested Internet resource to determine whether the Internet resource should be provided to the requesting client-side device 55:



(EX-1001 FIG. 1.)

32. The reputation for the requested Internet resource may be represented by a reputation index, which is determined using a reputation vector. (EX-1001 9:53-67.) A reputation vector is formed from the “set of features which characterize the reputation of the Internet resource” and is used to train a machine learning model that can then be used to evaluate a relative reputation of an Internet resource. (EX-1001 9:35-36, 13:3-14:56) The model may be trained using machine learning techniques such as support vector machine techniques, or variations thereof (*e.g.*, maximum entropy discrimination). (EX-1001 7:45-64, 9:28-41.) Vectors are used as

training data for machine learning classifiers, which is what is also taught by the '389 patent. (EX-1001 9:28-52.) A reputation vector may contain multiple features or factors, such as security history, legitimacy, behavior, associations, and location. (EX-1001 9:8-27.)

33. Security history may involve a history of security events for an Internet resource. For example, security history may involve the number of malware infections involving the Internet resource over a given period of time. (EX-1001 12:8-10.) As the '386 patent notes, for example, "the occurrence of a single security breach (the site gets hacked and is a danger to visitors) does not dramatically lower the reputation of a site. Repeated occurrences over time, however, will destroy the reputation of the site." (EX-1001 8:63-67.)

34. Legitimacy may be "determined by the top-level domain, the investment in the Internet resource (virtual hosting with non-affiliated sites, multiple hosting and SSL security), the traffic volume, the category age[,] the popularity rank. . . the consistency between the registering and hosting city region or country; and city, region or country associated with the IP address." (EX-1001 9:8-18.) Legitimacy may involve an assessment of the URL and/or IP address hosting the Internet resource. For example, an Internet resource having a reputable top-level domain (*e.g.*, google.com) may have a higher reputation than an Internet resource having a top-level domain that has been determined to be non-reputable (*e.g.*,

g00gle.com). As another example, an Internet resource having SSL security (e.g., SSL certificates for HTTPS access schemes) would increase the legitimacy of the resource. (See EX-1001 9:8-15 (“Legitimacy is determined by . . . the investment in the Internet resource (. . . SSL security).”).)

35. Behavior involves how the requested Internet resource operates when it is run on a device, and may involve particular run-time behaviors exhibited by the Internet resource, such as “the use of popup ads, browser hijacking and the use of auto-redirecting.” (EX-1001 9:19-20.)

36. Associations may involve how the requested Internet resource interacts with other resources on the Internet. For example, associations may involve “the number of sites linking into the site, the reputations of the linked in sites and the reputations of the linked-to sites.” (EX-1001 9:20-22.) The assessment of the Internet resource’s associations involves a different analysis than the top-level domain, URL, or IP address of the Internet resource itself. Rather, associations relate to how the Internet resource interacts with other Internet resources throughout the Internet. For example, a web page that contains links to known malicious Internet resources outside of its own host server, URL, domain, or IP address may be nonetheless found to have bad associations (given that it could be using its own otherwise benign domain to conceal its relationship with known malicious resources), reducing its reputability.

Declaration in Support of Patent Owner's
Preliminary Response to Petition for *Inter Partes* Review
Patent No. 8,438,386

37. Location may involve countries, municipalities, and other geographical factors associated with the Internet resource. For example, factors relating to location may include “the hosting country, the registration country, the region[,] the city[,] . . . [and] the consistency between the registering and hosting country and the country associated with the IP address.” (EX-1001 9:15-18.)

38. The table below provides examples of these five factors:

TABLE ONE			
Attribute	Description		
Country	2-letter code, 3-letter code or full name of country based on IP block	TABLE ONE-continued	
Top-level Domain	.com, .biz, .org, .gov, etc.	Attribute	Description
Domain Age	Number of months in existence on zone lists, or no less than the classification age	Latency	Number of milliseconds to return default page
Database Age	Months since Authority was entered into database	Rank	Numerical ranking, used as T if <2,000,000, F otherwise in modeling
Classification	Months that the Authority has held its current classification	Infected	T/F were infected download files found by AV tools during site analysis
Age		Security Trend	Number of malware infections in past 12 months
Hosts	Number of IP's associated with the Authority	Total Security	Total number of malware infections known
Virtually Hosted	T/F if the other authorities share associated IP's	Count	
Popups	T/F if the page opens new browser windows on its own	Redirect	Authority redirects to another Authority
Hijack	T/F does the default page alter the browser configuration	IP Address	Analysis of IP address for known threat sources, reserved IP ranges, and legacy IP address assignments
JavaScript	Count of <SCRIPT> blocks in default pages	ISP	Internet service provider
Executables	T/F does the authorities download executables to client	City	
Pictures	Count of pictures on default page	Region	

(EX-1001 11:50-12:16.)

39. A trained classifier may “use[] the reputation vector for a requested Internet service to evaluate its reputation index, a score which can be used with empirically developed threshold values to block access where the reputation index is deemed too low to be safe.” (EX-1001 9:30-41.) Threshold values may be established for different local area networks based on the needs and tolerances of a particular local area network.

Declaration in Support of Patent Owner's
Preliminary Response to Petition for *Inter Partes* Review
Patent No. 8,438,386

40. Accordingly, the '386 patent discloses and claims, among other things, an unconventional technological solution to the Internet-centric technical issue of identifying malware in computer systems. The solutions implemented by the '386 patent provide a specific and substantial improvement over prior Internet resource analysis and security systems, including machine learning and reputational elements combined in an unconventional manner. These approaches improve the function and working of computer network security services by, for example, utilizing machine learning techniques for predicting security threats, and doing so through relative reputational analysis. These elements and their combination represent a marked improvement in the functioning of computer systems used to identify and detect malicious Internet resources that could pose threats to computer networks.

B. Claim Construction

41. I understand that Petitioner applies the plain and ordinary meaning of all claim terms. (Petition 7.)

42. I understand that the District Court for the Western District of Texas issued a claim construction order on March 16, 2023, finding that the term “security appliance” should be construed to have their plain and ordinary meaning. (EX-2010 8.) Consistent with the Court’s order, I apply the plain and ordinary meaning of all claim terms.

43. I note that Petitioner's citations to Hubbard-495, Hubbard-174, and Alperovitch indicate a deviation from what a POSITA would understand the term "security history" to mean. Accordingly, I discuss the plain and ordinary meaning of this term as it would have been understood by a POSITA at the time of the invention claimed in the '386 patent.

1. Security History

44. At the time of the invention claimed in the '386 patent, a POSITA would have understood the plain and ordinary meaning of the term "security history" to mean "a history of security events for an internet resource."

45. The plain language of the term "security history" is self-explanatory – the history of an internet resource's security. A POSITA would understand this security history to involve information such as the history of security events for the internet resource. A POSITA would also understand that this history of security events can be used to determine the reputation of the resource. This is consistent with the disclosure of the '386 patent, which indicates that the number of times an internet resource's security has been compromised is a factor in the reputation of the resource:

While security threats are transitory since they come up suddenly and are mitigated as quickly as possible, reputation is built up over a period of time and is a more enduring quality. ***Reputation can be lost, or become bad, over a period of time with repeated security events***, bad associations, and bad behavior. ***For that reason, the occurrence of a***

single security breach (the site gets hacked and is a danger to visitors) does not dramatically lower the reputation of a site. Repeated occurrences over time, however, will destroy the reputation of the site.

(EX-1001 8:58-67 (emphasis added)).

46. Furthermore, the claim language explains that a security history refers not to some vague “historical data” as Petitioner claims, but rather the actual history of an internet resource’s security. (EX-1001 cl. 1 (“method for controlling access to an Internet resource” that includes steps of transmitting a request for the internet resource receiving the request for the Internet resource, and then determining if a reputation index for the Internet resource is at or above a threshold value...where the reputation index is generated from a reputation vector for the Internet resource that includes ***a plurality of factors for the Internet resource,” with one of those enumerated factors being the Internet resource’s “security history.”***) (emphasis added).)

47. As an example, the ’386 patent refers to a “Security Trend,” which a POSITA would understand to refer to historical security events that provide a trend or trajectory of an internet resource’s reputation. This “Security Trend” could be, for example, a “[n]umber of malware infections in the past 12 months.” As another example, the ’386 patent refers to a “Total Security Count” attribute, which could be, for example, the “[t]otal number of malware infections known.” (EX-1001

12:8.) A POSITA would understand these to be references to an internet resource's security history.

48. Accordingly, it is my opinion that the term "security history" should be construed consistent with its plain and ordinary meaning – a history of security events for an internet resource.

C. Level of Ordinary Skill in the Art

49. I understand that certain issues relating to the validity of the '386 patent must be judged from the perspective of a person of ordinary skill in the relevant art, as I discuss below. I have been asked to define the level of a "person having ordinary skill in the art" or "POSITA" that someone would have had at the time the alleged invention as claimed was made. In deciding the level of a POSITA, I have considered the following factors, which I have been informed are relevant in determining the level of ordinary skill in the art:

- The levels of education and experience of persons working in the field;
- The types of problems encountered in the art;
- The prior art solutions to these problems;
- The rapidity with which innovations are made; and
- The sophistication of the technology.

Declaration in Support of Patent Owner's
Preliminary Response to Petition for *Inter Partes* Review
Patent No. 8,438,386

50. Based on these considerations, it is my opinion that a POSITA at the time of the invention of the '386 patent had a bachelor's degree in an accredited program of electrical engineering, computer engineering, or computer science, or a similar discipline, and have 2-3 years of practical work experience in the general fields of electrical engineering, computer science, networking, communications, and/or device and network security. More advanced degrees and/or training in a related discipline can compensate for shorter work experience.

51. I understand that Petitioner has defined the level of ordinary skill in the art as:

A person having ordinary skill in the art (a "POSITA") relative to the '386 Patent would have at least a four-year undergraduate degree in computer science or a closely related field and at least two years of experience in the field of computer and network security. (EX-1002 Declaration by Michael Goodrich, Ph.D., ¶¶22-25.) Additional education could substitute for professional experience and vice versa. (*Id.*)

(Petition 6-7.)

52. The minor variations in these two positions would not alter my opinions expressed in this Declaration.

53. Based on either standard, I was at least a person of ordinary skill in the art at the time of the invention of the '386 patent.

V. Overview of the Prior Art

A. Overview Of Hubbard-495

54. Hubbard-495 is directed to a “system and method . . . for identifying active content in websites on a network.” (EX-1004 Abstract.) Hubbard-495 discloses that when a user operating a computer requests access to a website, a system searches a database of categorized URLs to determine whether that request for access should be granted.

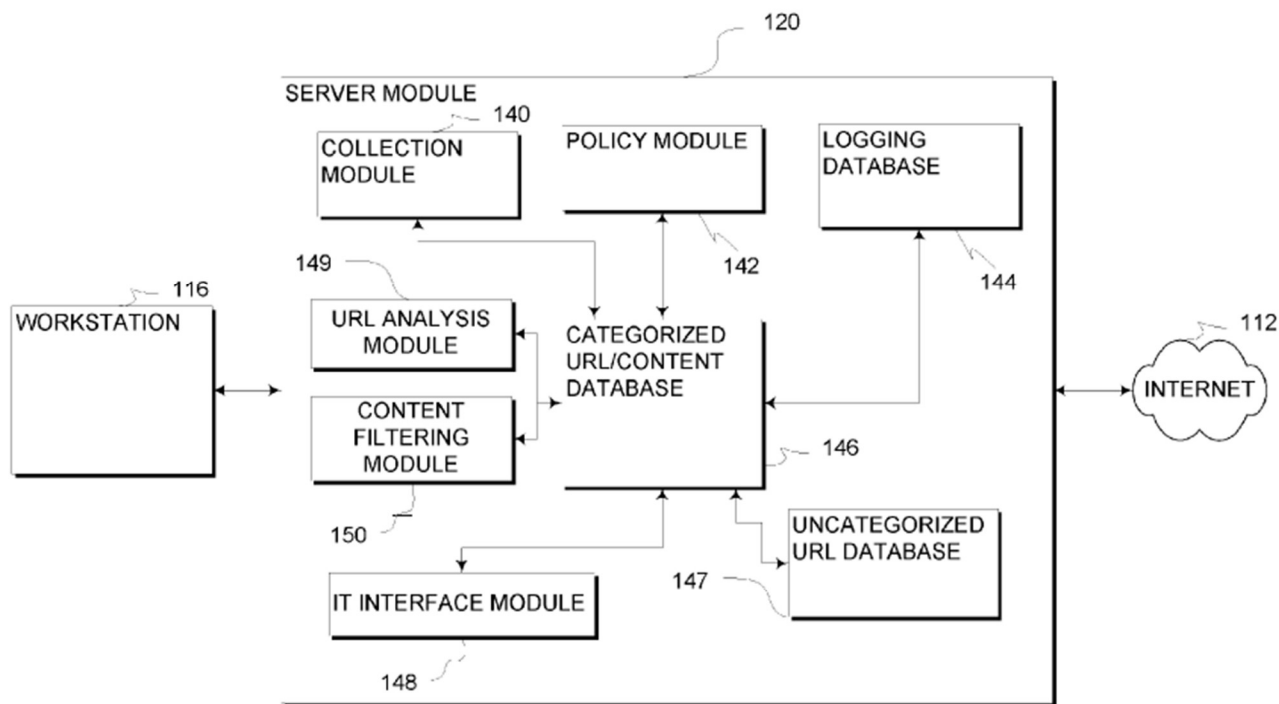
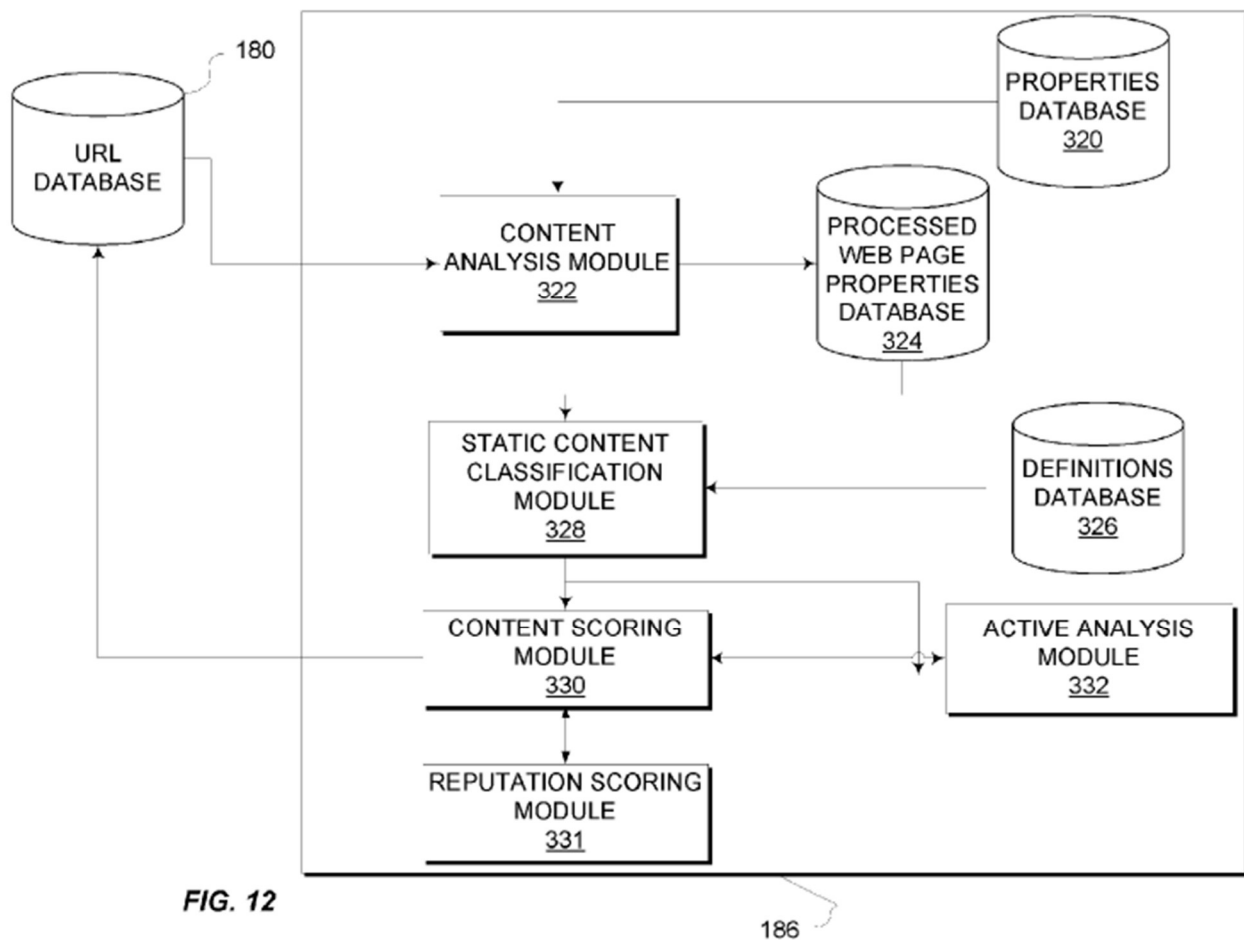


FIG. 3

(EX-1004 FIG. 3.)

55. If the URL is not in the database (*i.e.*, it is uncategorized), the system employs, among other things, a reputation scoring module 331 “that generates a score or other data representative of a reputation of the URL.” (EX-1004 9:29-33.)



(EX-1004, FIG. 12.)

56. “One embodiment may include a method of generating a score indicative of the reputation, or likelihood that a website associated with an uncategorized URL contains active or other targeted content based on an analysis of the URL.” (EX-1004 Abstract, 9:25-33.)

57. Scores resulting from the analysis of URLs are categorized based on those scores falling within particular ranges associated with those categories. Hubbard-495 discloses that policies are implemented in accordance with a URL Access Policy Database, which stores rules and conditions for determining the circumstances in which a user's request will be transmitted via the Internet to fetch the content identified by the requested URL.

158

URL Access Policy Database

User	Category	Always block?	Allowed Times
asmith	Malicious	Yes	
bnnguyen	Gambling		6pm – 8 am
cle	Spyware	Yes	
	Politics		6pm – 8 am

160 162 164 166

FIG. 5

(EX-1004, FIG. 5.)

58. Hubbard-495 also teaches an *ad hoc* process for categorizing a URL in order to determine if the user's request should be allowed in accordance with the policies stored in the URL Access Policy Database. (EX-1004, 9:29-33, 18:53-19:22.)

B. Overview Of Hubbard-174

59. Hubbard-174 discloses systems and methods for removing objectionable content from webpages. Hubbard-174 concerns “Google-bombing” or “Spamdexing,” wherein “operators of websites having undesirable or malicious content may utilize misleading techniques with the purpose of having their malicious content included in the web feeds” or search engine results. (EX-1005, 1:13-26.)

60. Hubbard-174 discloses “removing certain portions of the data such as malicious or otherwise objectionable content.” (EX-1005, Abstract.)

61. Hubbard-174 uses a “policy module including instructions for modifying content based on the category of the content, and a content filtering module configured to modify at least some of the content based at least in part on the instructions.” (EX-1005, 2:5-9.)

62. Hubbard-174 describes a content filtering module 149 that may remove content from webpages located at those URLs. The content filtering module 149 performs this filtering by utilizing a link analysis chart 250, which identifies content that should be removed from a webpage being accessed by a user.

Declaration in Support of Patent Owner's
Preliminary Response to Petition for *Inter Partes* Review
Patent No. Patent No. 8,438,386

250

ITEM TYPE	URL	ACTION TAKEN	CATEGORY	CODE
a,href	http://www.coolscreensavers.com/	Allow	Search Engines	76
a,href	http://www.verycoolscreensavers.com/	Allow	Search Engines	76
a,href	http://www.verycoolscreensaver.com/	Observe	Free Software	99
a,href	http://www.somewhatcoolscreensavers.com/	Allow	Search Engines	76
a,href	http://www.downloadacoolscreensaver.com/	Observe	Free Software	99
img,src	http://www.adultcoolscreensavers.com/sample.gif	Block	Adult Content	66
a,href	http://www.thebestscreensavers.com/	Allow	Search Engines	76
a,href	http://www.artisticscreensavers.com/	Allow	Search Engines	76
img,src	http://www.verycoolscreensavers.com/save.jpg	Allow	Search Engines	76
a,href	http://www.trickyscreensavers.com/	Block	Spyware	154
a,href	http://www.basicscreensavers.com/	Observe	Free Software	99

252 254 256 258 260

FIG. 11B

(EX-1005, FIG. 11B.)

C. Overview Of Alperovitch

63. Alperovitch is directed to systems and methods for improved spam filters for messaging systems, such as emails. To improve such filters, Alperovitch discloses readily identifying spam communications, namely emails, by assigning reputations to certain “communications entities,” such as email addresses.

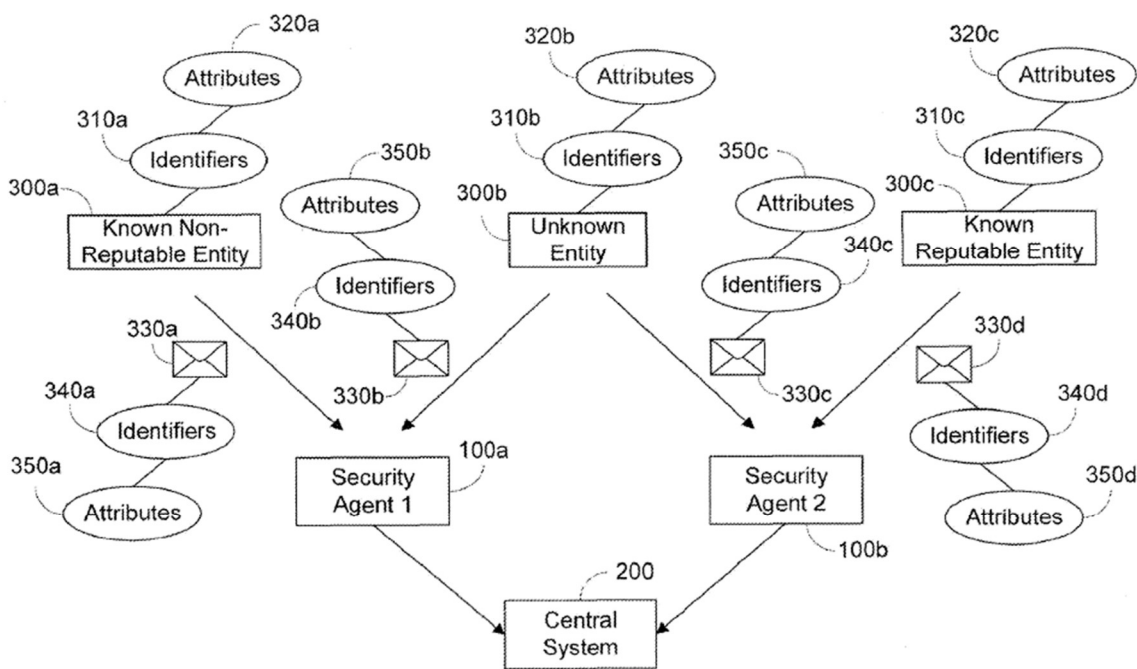


FIG. 3

(EX-1006, FIG. 3.)

64. Alperovitch discloses that a communication entity's reputation may be based on observed behavior. (EX-1006 [0045].) This observed behavior may include "a specific set of sending patterns, blacklist events, or specific attributes of the evidentiary data." (EX-1006 [0048].) Alperovitch does not explain what a "blacklist event" is.

VI. Ground 1 Does Not Disclose or Render Obvious the Challenged Claims

65. Petitioner and its expert allege that Hubbard-495 and Hubbard-174 render obvious every limitation of claims 1-13, 15, 16, and 18.

Declaration in Support of Patent Owner's
Preliminary Response to Petition for *Inter Partes* Review
Patent No. Patent No. 8,438,386

Ground 1	Section 103(a)	Obvious over Hubbard-495 in view of Hubbard-174	Claims 1-13, 15, 16, and 18
-----------------	----------------	--	--------------------------------

66. I Disagree with the arguments in the Petition and the opinions set forth by Dr. Goodrich for at least the reasons that I discuss in further detail below.

67. Petitioner's arguments based on Hubbard-495 in combination with Hubbard-174 fail because the petition fails to establish that this combination discloses or renders obvious every limitation of the independent claims, including in particular the "security history" limitation. For these reasons, and as further addressed herein, Petitioner has not shown that it is reasonably likely to prevail on the patentability of any of the challenged claims.

A. The Prior Art Does Not Disclose or Render Obvious the "Security History" Limitation

68. Petitioner relies on a combination of Hubbard-495 and Hubbard-174 as disclosing the limitations listed in the table below. (Petition 25–26, 52, 58.) However, as addressed below, these references fail to disclose these limitations.

Declaration in Support of Patent Owner's
Preliminary Response to Petition for *Inter Partes* Review
Patent No. Patent No. 8,438,386

Limitation	Claim Language
1[c2]	<i>“determining if a reputation index for the Internet resource is at or above a threshold value established for the local area network, the reputation index generated from a reputation vector for the Internet resource, the reputation vector comprising a plurality of factors for the Internet resource comprising security history, legitimacy, behavior, associations and location”</i>
7[e3]	<i>“the security appliance having a service engine for analyzing a reputation vector for the Website and generating a reputation index for the Web site from the reputation vector, the reputation vector comprising a plurality of factors for the Internet resource comprising security history, legitimacy, behavior, associations and location”</i>
11[c2]	<i>“constructing a reputation vector for the Internet resource at the data collection site, the reputation vector comprising a plurality of factors for the Internet resource comprising security history, legitimacy, behavior, associations and location”</i>

13[c2]	<i>“the reputation vector comprising a plurality of factors for the Internet resource comprising security history, legitimacy, behavior, associations and location,”</i>
--------	---

1. Hubbard-495 does not disclose a reputation vector comprising a “security history” factor

69. The ‘386 patent’s claim language recites that the “security history” factor requires two things: (1) that the security history be for an internet resource, and (2) that the security history be used in a reputation vector factor to determine the reputation index of the internet resource. The ‘386 claims recite a security history for an internet resource. As discussed above, the term “security history” refers to a history of security events for an internet resource. *See*, Section IV.B, *supra*. The claim language also supports this. (EX-1001 cl. 1, 15:66-16:14) (reciting a “method for controlling access to an Internet resource” that includes the step of “determining if a reputation index for the Internet resource is at or above a threshold value . . .” where the reputation index is generated from a reputation vector for the Internet resource that includes “a plurality of factors for the Internet resource,” with one of those enumerated factors being the Internet resource’s “security history.”). This claim language also indicates that the “security history” is a factor “for the Internet resource”. Each challenged independent claim includes similar language. (EX-1001 (cl. 7, 16:63-17:1 “the reputation vector comprising a

plurality of factors for the Internet resource comprising security history...”), claim 11, 17:28-39 “accessing a reputation index for the Internet resource, the reputation index based on a reputation vector for the Internet resource comprising security history...”), *id.* cl. 13, 18:1-20 (“constructing a reputation vector for the Internet resource...the reputation vector comprising a plurality of factors for the Internet resource comprising security history...”).)

70. The claims further recite that the security history must be used as a part of a reputation vector in determining the reputation index of the internet resource whose reputation index is being determined. The claims recite that the reputation vector includes “a plurality of factors for the Internet resource.” One of those enumerated factors is the Internet resource’s “security history” and further state that “the reputation index is generated from the reputation vector. (EX-1001 cl.1; *see also* cl. 7 (“generating a reputation index for the Web site from the reputation vector, the reputation vector comprising a plurality of factors for the Internet resource comprising security history...”); cl. 11 (17:28-39 “accessing a reputation index for the Internet resource, the reputation index based on a reputation vector for the Internet resource comprising security history...”).) A POSITA would have understood that the “security history” is a factor in the reputation vector in order for the reputation index of the internet resource to take the resource’s security history into account. (*See* EX-1001 8:58-67)

71. Petitioner conflates “security history” with “legitimacy” in its argument that this limitation is present in Hubbard-495. First, Petitioner claims that Hubbard-495 discloses “historical data,” and speculates that this could include historical security data. As I noted above, the claimed term “security history” refers to the history of the security of the internet resource being analyzed. *See* Section IV.B, *supra*.

72. However, Hubbard-495 does not disclose such a security history. In fact, Hubbard-495 never teaches what “historical data” means, let alone that it includes “security history.” Further, the “historical data” referenced by Hubbard-495 vaguely refers to an IP address history rather than a security history. Hubbard-495 provides no indication that this IP address history bears any relationship with a security history. The examples that the Petition purports to be “security history” are also never represented by Hubbard-495 to be such examples, and a POSITA would not understand those examples to be indicative of “security history” of an internet resource. In fact, the Petition’s purported examples are among a list of “scoring criteria” disclosed in Hubbard-495 without any significant detail, and none of these criteria is described as being a security history or examples of a security history:

The reputation scoring module 331 may generate the scores ***based on information about the URL of the web page (e.g., scoring criteria) such as*** one or more of URL content strings, Geo-location data associated with the URL (e.g., the URL host or host domain), the name server

that provides the IP address of the URL host or its domain, the network or blocks of IP addresses associated with the host IP address or its domain, ***active content previously identified with reference to the host, the hosts' domain, or the URL path, historical data associated with the IP address of the URL host***, creation date or expiration date associated with the registration of the URL host, whether search engine results exist for the URL or the URL host, ***certificate details associated with the URL*** (e.g., for secure (such as HTTPS) access schemes), meta tag categories associated with other URLs associated with the URL host (e.g., such as in the URL database 180 or the processed web page properties database 324), categories associated with other URLs of the URL host (e.g., in the URL database 180), ***a fingerprint*** (e.g., a digest or hash) associated with the content of the URL for comparison to such data of previously categorized URLs (and to generate reputation data depending on whether URLs with the same fingerprint had targeted content), and scoring based on site (host or domain) access statistics (e.g., generate higher reputation scores for frequently visited sites than for infrequently visited sites because frequently visited sites (for other URLs that do not have targeted content) are less likely to have targeted content in newly visited URLs).

(EX-1004 18:61-19:22 (emphasis added).)

73. “Certificate details associated with the URL (e.g., for secure (such as HTTPS) access schemes)” are not security history. As the '386 patent explains, certificate details refer to the “legitimacy” factor. Certificate details provide information as to whether a URL is secured via a security protocol known as Secure Sockets Layer (SSL), thereby increasing the likelihood that an Internet resource has a high legitimacy (hence the certificate). This is consistent with the '386 patent,

Declaration in Support of Patent Owner's
Preliminary Response to Petition for *Inter Partes* Review
Patent No. Patent No. 8,438,386

which identifies that Internet resources known to be encrypted or secured by other means are more likely to be legitimate. As explained in the '386 patent, "[l]egitimacy is determined by the top-level domain, the investment in the Internet resource (virtual hosting with non-affiliated sites, multiple hosting and **SSL security**).” (EX-1001 9:10-14 (emphasis added).) SSL security refers to a security protocol known as Secure Sockets Layer, which is employed under HTTPS access schemes for encryption and authentication.

74. Similarly, “active content previously identified with reference to the host, the hosts’ domain, or the URL path” is not a security history – it relates to the “behavior” factor described in the '386 patent. As such, it provides insight into behavioral qualities of the Internet resource:

Security solutions, such as anti-virus products, examine file or Web page content to discover known patterns or signatures that represent security threats to users, computers, or corporate networks. These focus not on the subject matter of a site [content], but look for viruses and other malware that are currently infecting the site.

(EX-1001 1:41-46 (emphasis added).)

75. In fact, “active content” is not inherently malicious. “Active content” is simply content in an Internet resource that provides interactive or dynamic qualities to the website. “Active content” includes GIFs, JavaScript, and streaming audio and/or video. (See EX-1004 1:34-52) These qualities are in contrast to security history, which would include, for example, a history of security events involving the

Internet resource, such as whether or not the resource's security has been compromised in the past. (*See, e.g.*, EX-1001 8:61-67, 12:1-16 (Table One).)

76. As such, a POSITA would not understand how merely referencing “active content” refers to a history of the security of an internet resource. Hubbard-495 also does not provide guidance to a POSITA to come to such a conclusion.

77. Similarly, a “fingerprint” is not a history of the security of an internet resource. In fact, a fingerprint would fit within the “behavior” factor, as it involves actively analyzing the content of an internet resource and comparing that content against a database of content that can be identified as malicious or “active content.” A POSITA would not have considered such a “fingerprint” to be indicative of security history at all. In fact, a POSITA would not have even considered such a “fingerprint” to be indicative of historical data for an internet resource, given that the fingerprint is used to assess the current state of an internet resource being analyzed. Petitioner does not explain how Hubbard-495 teaches that a fingerprint would provide information about a history of security events that could be used as a “security history.”

**B. The Prior Art in Ground 2 Does Not Disclose or Render Obvious
The “security history” Limitation**

78. Petitioner and its expert allege that Hubbard-495, in combination with Hubbard-174 and Alperovitch, renders obvious every limitation of claims 1-13, 15, 16, and 18.

Ground 2	Section 103(a)	Obvious over Hubbard-495, Hubbard- 174, and Alperovitch	Claims 1-13, 15, 16, and 18
-----------------	----------------	---	--------------------------------

79. Petitioner relies on Alperovitch as disclosing the limitation “security history” in claim elements 1[c2], 7[e3], 11[c2], and 13[c2].

Limitation	Claim Language
1[c2]	“the reputation index generated from a reputation vector for the Internet resource, the reputation vector comprising a plurality of factors for the Internet resource comprising <i>security history</i> , legitimacy, behavior, associations and location,”
7[e3]	“the reputation vector comprising a plurality of factors for the Internet resource comprising <i>security history</i> , legitimacy, behavior, associations and location,”

Declaration in Support of Patent Owner's
Preliminary Response to Petition for *Inter Partes* Review
Patent No. 8,438,386

11[c2]	“the reputation index based on a reputation vector for the Internet resource comprising <i>security history</i> , legitimacy, behavior, associations and location,”
13[c2]	“the reputation vector comprising a plurality of factors for the Internet resource comprising <i>security history</i> , legitimacy, behavior, associations and location,”

80. However, as addressed below, Alperovitch does not disclose this limitation.

81. Petitioner relies on Alperovitch's reference to a “behavioral profile” as disclosing the “security history” claimed in the '386 patent. However, Petitioner conflates “security history” with “behavior.” Petitioner and its expert point to nothing in Alperovich's behavior profile that discloses or teaches the claimed “security history” factor. While Petitioner asserts that Alperovich discloses that a “behavior profile” may include “a specific set of sending patterns” and “blacklist events,” (Petition at 73), neither of these references refers to a “security history” factor. “Sending patterns” and “blacklist events” are only parts of a larger “behavior profile.”

82. The behavior profile alone does not constitute a “security history” at least because it includes much information that is not historical data. (EX-1006

[0048]) Alperovich does not disclose how a behavioral profile that includes information such as sending patterns, blacklist events, or other similar behavioral information that is not historical and does not describe security events would constitute a history of security events for any particular internet resource. Alperovich also fails to describe how such a “behavior profile” is used as a factor to generate a reputation index of a particular internet resource to account for the extent of that resource’s history of security events.

83. Further, Petitioner is incorrect in arguing that “[a] POSITA would understand that blacklist events would be previous security events that would flag a site for placement on the ‘blacklist’ or a list of entities that are blocked from communicating with or logging into a computer, site, or network, and that a ‘specific set of sending patterns’ would reference historical data about the entity’s prior communications.” (Petition 73.)

84. Petitioner’s argument overlooks the fact that Alperovitch explicitly refers to blacklist events as behavioral and indicative of an entity sending messages via, for example, email or instant message, rather than indicative of whether an Internet resource has been compromised in the past. Further, Petitioner claims that blacklist events would be previous security events that “would flag a site for placement on the ‘blacklist.’” (Petition 73.) This is in stark contrast to, for example, the actual placement of a user, messaging account, or other such entity on a blacklist,

Declaration in Support of Patent Owner's
Preliminary Response to Petition for *Inter Partes* Review
Patent No. 8,438,386

as discussed in Alperovitch. (EX-1006 [0048]) Petitioner thus describes Alperovitch as disclosing conduct of a user, messaging account, or the like, consistent with bad behavior, rather than a history of instances in which a webpage is compromised.

85. Second, Petitioner conflates a “site” with a “communications entity.” Alperovitch is entirely focused on messaging systems, as opposed to web browsing. Thus, Petitioner’s contention that a POSITA would understand that blacklist events would be previous events that would flag a “site” for placement on a blacklist is incorrect. Rather, a POSITA would understand that “blacklist events” pertain to the message sender being scrutinized. Messaging systems and websites raise different security concerns, and a POSITA would not have falsely equated “sites” with, for example, email senders.

86. Similarly, Petitioner again conflates behavior and security history by pointing to “a specific set of sending patterns” as disclosing the “security history” limitation. A specific set of sending patterns by a source of electronic communications (*e.g.*, an individual or email account that sends emails) does not bear any clear relationship with a website’s reputation for having vulnerabilities exploited or for being caught exploiting vulnerabilities.

87. Accordingly, Ground 2 neither discloses nor renders obvious the “security history” limitation.

C. There Was No Motivation to Combine Hubbard-495 and Hubbard-174 with Alperovitch

88. A POSITA would not have been motivated to combine Hubbard-495 and Hubbard-174 with Alperovitch because these references are not analogous art, are not in the same field of endeavor, and there is no evidence that shows how a POSITA would have combined or modified these references as claimed in the '386 patent. Hubbard-495 relates to categorizing webpages and websites. Hubbard-174 is directed to filtering active content from webpages, namely search engine results. Alperovitch is directed to securing messaging systems, such as emails and instant messages.

89. In fact, rather than focusing on websites, Alperovitch is entirely focused on protecting against disreputable individuals, and URLs for websites are only mentioned as possible malicious content in messages (rather than as targets of user requests). As such, the attributes that would be involved in assessing the reputation of a message sender are largely different from the factors involved in categorizing or filtering content from webpages. For example, Alperovitch identifies the following attributes as relevant to reputation: “a specific set of sending patterns, blacklist events, or specific attributes of the evidentiary data. Some examples include: Sender/Receiver Identification; Time Interval and sending patterns; Severity and disposition of the payload; Message construction; Message quality;

Protocols and related signatures; Communications medium.” These factors are largely absent in the disclosures of Hubbard-495 and Hubbard-174. (*See, e.g.*, EX-1004 18:53-19:61; *see generally* EX-1005 (lacking any reference to reputation analysis).)

90. Moreover, Hubbard-495 and Hubbard-174 focus on identifying risk factors associated with a URL host. (*See generally* EX-1004 Abstract; EX-1005 Abstract.) Such risk factors would not be applicable to Alperovitch because dangerous activity could easily be masked using a Gmail account, granting a sender a higher reputation merely for using a known, reputable email server to send suspicious or dangerous emails. In contrast, a large number of disreputable email senders may weaken the reputation of the email host despite there being little to no relationship between the sender and the host.

91. While Alperovitch states that “hackers often attempt to use various network-type applications (e.g., e-mail, web, instant messaging (IM) etc.),” Alperovitch does not disclose how to address web-based threats. (EX-1006 [0032]) Rather, Alperovitch refers to identifying dangerous e-mail and instant messaging accounts, but does not make any reference to identifying risks associated with webpages or URLs as described in Hubbard-495 or Hubbard-174. None of examples of its “behavioral profile” or “sending patterns” is suggested by any of Petitioner’s references as being relevant to the URLs described by Hubbard-495 and Hubbard-

174. By Petitioner's logic, any system or method involving cybersecurity or reputation would have been obvious to a POSITA to combine, regardless of their field of endeavor, teachings, and goals for improvement over the art.

92. Further, Alperovitch teaches that the categorizations of message senders differ from that of websites. Where Alperovitch discloses categorizing senders as "Spammer," "Scammer," and "Legitimate Sender," (EX-1006 [0048]), Hubbard-495 and Hubbard-174 disclose categorizing websites as "Malicious," or by the subject matter of the webpage or website at large, such as "Gambling," or "Spyware." (EX-1004 FIG. 6A.)

93. Alperovitch is also not reasonably pertinent to the '386 patent, as it seeks to solve different problems from those targeted by the '386 patent. For example, the '386 patent seeks to prevent users in a network seeking access to Internet resources that would include malicious or inappropriate content from being granted access to those resources. In stark contrast, Alperovitch seeks to identify individuals who would seek to send malicious or inappropriate content to message recipients. The kinds of vulnerabilities, vectors for exploitation, and protocols for communication are very different in the two cases, and a POSITA would not have looked at email, VoIP, instant messaging, or other similar systems when the goal is to identify dangerous Internet resources such as webpages. Furthermore, in the '386 patent, these Internet resources are *specifically requested* by users, whereas in

Alperovitch, the users are being protected from messages that *may* contain links to Internet resources and are sent to them from potentially malicious entities; these are two diametrically opposite perspectives, and a POSITA would have no reason to combine such opposite approaches.

94. Based on the above, it is my opinion that Hubbard-495, Hubbard-174, and Alperovitch are not in the same field of endeavor, are not reasonably pertinent to the particular problem with which the inventors of the '386 patent were involved, and are non-analogous to the '386 patent. Further, it is my opinion that Petitioner does not explain how a POSITA would combine or modify Hubbard-495, Hubbard-174, and Alperovitch. Accordingly, Petitioner's Section 103(a) grounds should be rejected.

VII. DEPENDENT CLAIMS

95. Because Petitioner has failed to establish that any of its grounds render obvious all limitations of independent claims 1, 7, 11, and 13, I understand that Petitioner cannot make a showing that such grounds render obvious dependent claims 2-6, 8-10, 12, 15, 16, and 18.

VIII. OTHER LIMITATIONS NOT ADDRESSED

96. It is my understanding that this declaration is being provided in support of Patent Owner's Preliminary response. I have provided analysis of key limitations

not included in the prior art. The fact that I have not analyzed particular limitations or claims in no way indicates or supports that these limitations or claims are disclosed or rendered obvious by the prior art, and I reserve the right to supplement my analysis if asked to do so.

IX. SECONDARY OBJECTIVE INDICIA OF NONOBVIOUSNESS

97. I understand that in determining obviousness of the claimed invention, objective evidence of secondary considerations pertaining to nonobviousness must be considered, including long-felt but unsolved needs, failure of others, commercial success, etc. Petitioner does not address or consider any such evidence in its petition. (*See generally* Petition.)

98. As discussed above, a long-felt and persistent need existed to improve network forensics methods before the invention of the '386 patent. *See* Section III, *supra*. Prior attempts to develop reliable network security were limited in their ability to do so effectively and efficiently. *See* Section III, *supra*.

99. These secondary indicia further support my opinion that the '386 patent was non-obvious.

X. CONCLUSION

100. For at least the foregoing reasons, it is my opinion that Petitioner's grounds do not render obvious any of the challenged claims of the '386 patent.

Declaration in Support of Patent Owner's
Preliminary Response to Petition for *Inter Partes* Review
Patent No. Patent No. 3,438,386

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 17th day of August, 2023 in Atlanta, Georgia.

Respectfully submitted,

A handwritten signature in cursive script, appearing to read 'Alessandro Orso', is written over a horizontal line.

Alessandro Orso, Ph.D.