

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NORMSHIELD INC. d/b/a BLACK KITE INC.,
Petitioner

v.

BITSIGHT TECHNOLOGIES, INC.,
Patent Owner

Case IPR2025-00276
Patent 11,777,976

**DECLARATION OF KEVIN C. ALMEROOTH, PH.D. IN SUPPORT OF
PETITION FOR INTER PARTES REVIEW OF
UNITED STATES PATENT NO. 11,777,976**

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	BACKGROUND AND QUALIFICATIONS.....	2
III.	LEGAL STANDARDS.....	14
	A. Obviousness	15
	B. Claim Construction.....	20
IV.	PERSON OF ORDINARY SKILL IN THE ART AND THE TIME OF THE ALLEGED INVENTION.....	21
V.	THE '976 Patent.....	22
	A. Technical Background.....	22
	B. Description of the '976 Patent's Specification	34
	C. The '976 Patent's Prosecution History	34
	D. Interpretation of the '976 Patent's Challenged Claims	35
VI.	PUBLIC AVAILABILITY OF CERTAIN EXHIBITS	36
	A. McNab	36
	B. Internet Archive Pages	37
	C. Public Videos	38
VII.	GROUND 1: TIPPETT RENDERS OBVIOUS CLAIMs 1, 2, 4-10, and 12-16	40
	A. Claim 1	40
	1. 1[pre]: A method for determining a security rating of an entity, the method comprising:.....	40
	2. 1[a]: determining an internal security rating comprising:	40
	3. 1[b]: obtaining data indicative of internal security from a plurality of internal data sources;	41
	4. 1[c]: extracting a plurality of internal security features from the obtained data;.....	43

5.	1[d]: applying a respective transformation function to each of the plurality of internal security features to determine a first plurality of transformed features; and	44
6.	1[e]: combining the first plurality of transformed features to form the internal security rating;	45
7.	1[f]: determining an external security rating comprising:	45
8.	1[g]: obtaining data indicative of external security from a plurality of external data sources;	47
9.	1[h]: extracting a plurality of external security features from the obtained data;.....	49
10.	1[i]: applying a respective transformation function to each of the plurality of external security features to determine a second plurality of transformed features; and.....	49
11.	1[j]: combining the second plurality of transformed features to form the external security rating; and	50
12.	1[k]: providing, via a reporting facility, a composite security rating for the entity based on the internal security rating and the external security rating, wherein at least one of the internal security features or the external security features indicates malicious activity associated with an IP address of the entity.	50
B.	Claim 2: The method of claim 1, further comprising: determining the composite security rating based on a weighted combination of the internal security rating and the external security rating.	53
C.	Claim 4: The method of claim 1, wherein at least one of the internal security features or the external security features comprise at least one of: a number of remotely exploitable vulnerabilities of the entity; a number of security incidents; or a number of vulnerable versions of software of the entity.	53
D.	Claim 5: The method of claim 1, wherein each respective transformation function is a normalization of the respective feature, and further comprising: when the normalization is applied to two or more of the internal security features or the external security features, summing the normalized features.	54
E.	Claim 6: The method of claim 1, wherein determining the internal security rating further comprises weighting the first plurality of transformed features.	56

F.	Claim 7: The method of claim 1, wherein combining the first plurality of transformed features comprises: summing the first plurality of transformed features; and normalizing the summed features by a set of normalization factors.	56
G.	Claim 8: The method of claim 1, wherein combining the second plurality of transformed features comprises: summing the second plurality of transformed features; and normalizing the summed features by a set of normalization factors.	58
H.	Claim 9	59
1.	9[pre]: A system for determining a security rating of an entity, the system comprising:.....	59
2.	9[a]: one or more computer systems programmed to perform operations comprising:.....	59
3.	9[b]: determining an internal security rating comprising:	60
4.	9[c]: obtaining data indicative of internal security from a plurality of internal data sources;	60
5.	9[d]: extracting a plurality of internal security features from the obtained data;.....	60
6.	9[e]: applying a transformation function to each of the plurality of internal security features; and.....	60
7.	9[f]: combining the transformed features to form the internal security rating;	60
8.	9[g]: determining an external security rating comprising:	61
9.	9[h]: obtaining data indicative of external security from a plurality of external data sources;	61
10.	9[i]: extracting a plurality of external security features from the obtained data;.....	61
11.	9[j]: applying a transformation function to each of the plurality of external security features; and.....	61
12.	9[k]: combining the transformed features to form the external security rating; and.....	61
13.	9[l]: providing, via a reporting facility, a composite security rating for the entity based on the internal security rating and the external	

	security rating, wherein at least one of the internal security features or the external security features indicates malicious activity associated with an IP address of the entity.	61
I.	Claim 10: The system of claim 9, wherein the one or more computer systems are further programmed to perform operations comprising: determining the composite security rating based on a weighted combination of the internal security rating and the external security rating.....	62
J.	Claim 12: The system of claim 9, wherein the internal security features and the external security features comprise at least one of: a number of remotely exploitable vulnerabilities of the entity; a number of security incidents; or a number of vulnerable versions of software of the entity.....	62
K.	Claim 13: The system of claim 9, wherein each respective transformation function is a normalization of the respective feature, and wherein the one or more computer systems are further programmed to perform operations comprising: when the normalization is applied to two or more of the internal security features or the external security features, summing the normalized features.	63
L.	Claim 14: The system of claim 9, wherein determining the internal security rating further comprises weighting the first plurality of transformed features.	63
M.	Claim 15: The system of claim 1, wherein combining the first plurality of transformed features further comprises: summing the first plurality of transformed features; and normalizing the summed features by a set of normalization factors.	63
N.	Claim 16: The system of claim 9, wherein combining the second plurality of transformed features further comprises: summing the second plurality of transformed features; and normalizing the summed features by a set of normalization factors.	63
VIII.	GROUND 2: TIPPETT AND MCGOVERN RENDER OBVIOUS CLAIMS 3 AND 11.....	64
A.	Rationale to Combine	64
B.	Claim 3: The method of claim 1, wherein the plurality of internal data sources comprises: vulnerability scan data of the entity; data indicating firewall rules of the entity; data from security incident reports corresponding to the entity; data indicative of computer network configurations of the entity; data indicative of software inventory of the entity; data indicative of security policies of the entity; data indicative of security controls of the entity; and data indicative of user behavior corresponding to the entity.....	68

C.	Claim 11: The system of claim 9, wherein the plurality of internal data sources comprises: vulnerability scan data of the entity; data indicating firewall rules of the entity; data from security incident reports corresponding to the entity; data indicative of computer network configurations of the entity; data indicative of software inventory of the entity; data indicative of security policies of the entity; data indicative of security controls of the entity; and data indicative of user behavior corresponding to the entity.....	72
IX.	CONCLUSION.....	72

I. INTRODUCTION

1. I have been retained by Normshield Inc. d/b/a Black Kite Inc. (“Petitioner”) as an independent expert consultant in this proceeding before the United States Patent and Trademark Office (“PTO”) against BitSight Technologies, Inc. (“Patent Owner”) regarding U.S. Patent No. 11,777,976 (“the ’976 Patent”) (Ex. 1001).¹ I have been asked to submit this Declaration on behalf of Petitioner.

2. I have been asked to consider whether certain references disclose or render obvious the features recited in claims 1-16 (collectively, the “Challenged Claims”) of the ’976 Patent. My opinions are set forth below. Based on my experience and expertise, it is my opinion that the prior art renders obvious all limitations of the Challenged Claims, as I discuss in detail below.

3. I am being compensated at a rate of \$850 per hour for my work in this proceeding. My compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of this or any other proceeding. I have no other interest in this proceeding.

4. All of my opinions stated in this Declaration are based on my own personal knowledge and professional judgment. I am over 18 years of age and, if I

¹ Where appropriate, I refer to exhibits that I understand are to be attached to the petition for *Inter Partes* Review of the ’976 Patent.

am called upon to do so, I would be competent to testify as to the matters set forth in this Declaration.

II. BACKGROUND AND QUALIFICATIONS

5. I am currently a Professor Emeritus in the Department of Computer Science at the University of California, Santa Barbara (UCSB). While at UCSB, I held faculty appointments and was a founding member of the Computer Engineering (CE) Program, Media Arts and Technology (MAT) Program, and the Technology Management Program (TMP). I also served as the Associate Director of the Center for Information Technology and Society (CITS) from 1999 to 2012. I have been a faculty member at UCSB since July 1997.

6. I hold three degrees from the Georgia Institute of Technology: (1) a Bachelor of Science degree in Information and Computer Science (with minors in Economics, Technical Communication, and American Literature) earned in June 1992; (2) a Master of Science degree in Computer Science (with specialization in Networking and Systems) earned in June 1994; and (3) a Doctor of Philosophy (Ph.D.) degree in Computer Science (Dissertation Title: Networking and System Support for the Efficient, Scalable Delivery of Services in Interactive Multimedia System, minor in Telecommunications Public Policy) earned in June 1997. During my education, I took a wide variety of courses as demonstrated by my minor. My undergraduate degree also included a number of courses more typical of a degree in

electrical engineering including digital logic, signal processing, and telecommunications theory.

7. One of the major concentrations of my research over the past 30+ years has been the delivery of multimedia content and data between computing devices, including through various network architectures. In my research, I have studied large-scale content delivery systems, and the use of servers located in a variety of geographic locations to provide scalable delivery to hundreds or thousands of users simultaneously.

8. I have also studied smaller-scale content delivery systems in which content is exchanged between individual computers and portable devices. My work has emphasized the exchange of content more efficiently across computer networks, including the scalable delivery of content to many users, mobile computing, satellite networking, delivering content to mobile devices, and network support for data delivery in wireless networks.

9. In 1992, the initial focus of my research was on the provision of interactive functions (e.g., VCR-style functions like pause, rewind, and fast-forward) for near video-on-demand systems in cable systems; in particular, how to aggregate requests for movies at a cable head-end and then how to satisfy a multitude of requests using one audio/video stream broadcast to multiple receivers simultaneously. This research has continually evolved and resulted in the

development of techniques to scalably deliver on-demand content, including audio, video, web documents, and other types of data, through the Internet and over other types of networks, including over cable systems, broadband telephone lines, and satellite links.

10. An important component of my research has been investigating the challenges of communicating multimedia content, including video, between computers and across networks including the Internet. Although the early Internet was used mostly for text-based, non-real time applications, the interest in sharing multimedia content, such as video, quickly developed. Multimedia-based applications ranged from downloading content to a device to streaming multimedia content to be instantly used.

11. One of the challenges was that multimedia content is typically larger than text-only content, but there are also opportunities to use different delivery techniques since multimedia content is more resilient to errors. I have worked on a variety of research problems and used a number of systems that were developed to deliver multimedia content to users. One content-delivery method I have researched is the one-to-many communication facility called “multicast,” first deployed as the Multicast Backbone, a virtual overlay network supporting one-to-many communication. Multicast is one technique that can be used on the Internet to provide streaming media support for complex applications like video-on-demand,

distance learning, distributed collaboration, distributed games, and large-scale wireless communication. The delivery of media through multicast often involves using Internet infrastructure, devices and protocols, including protocols for routing and TCP/IP.

12. Starting in 1997, I worked on a project to integrate the streaming media capabilities of the Internet together with the interactivity of the web. I developed a project called the Interactive Multimedia Jukebox (IMJ). Users would visit a web page and select content to view. The content would then be scheduled on one of a number of channels, including delivery to students in Georgia Tech dorms delivered via the campus cable plant. The content of each channel was delivered using multicast communication.

13. In the IMJ, the number of channels varied depending on the capabilities of the server including the available bandwidth of its connection to the Internet. If one of the channels was idle, the requesting user would be able to watch their selection immediately. If all channels were streaming previously selected content, the user's selection would be queued on the channel with the shortest wait time. In the meantime, the user would see what content was currently playing on other channels, and because of the use of multicast, would be able to join one of the existing channels and watch the content at the point it was currently being transmitted.

14. The IMJ service combined the interactivity of the web with the streaming capabilities of the Internet to create a jukebox-like service. It supported true Video-on-Demand when capacity allowed, but scaled to any number of users based on queuing requested programs. As part of the project, we obtained permission from Turner Broadcasting to transmit cartoons and other short-subject content. We also connected the IMJ into the Georgia Tech campus cable television network so that students in their dorms could use the web to request content and then view that content on one of the campus's public access channels.

15. More recently, I have also studied issues concerning how users choose content, especially when considering the price of that content. My research has examined how dynamic content pricing can be used to control system load. By raising prices when systems start to become overloaded (i.e., when all available resources are fully utilized) and reducing prices when system capacity is readily available, users' capacity to pay as well as their willingness can be used as factors in stabilizing the response time of a system. This capability is particularly useful in systems where content is downloaded or streamed on-demand to users.

16. As a parallel research theme, starting in 1997, I began researching issues related to wireless devices and sensors. In particular, I was interested in showing how to provide greater communication capability to "lightweight devices," i.e., small form-factor, resource-constrained (e.g., CPU, memory, networking, and

power) devices. Starting in 1998, I published several papers on my work to develop a flexible, lightweight, battery-aware network protocol stack. The lightweight protocols we envisioned were similar in nature to protocols like Bluetooth, Universal Plug and Play (UpnP) and Digital Living Network Alliance (DLNA).

17. From this initial work, I have made wireless networking—including ad hoc, mesh networks and wireless devices—one of the major themes of my research. My work in wireless networks spans the protocol stack from applications through to the encoding and exchange of data at the data link and physical layers.

18. At the application layer, even before the large-scale “app stores” were available, my research looked at building, installing, and using apps for a variety of purposes, from network monitoring to support for traditional computer-based applications (e.g., content retrieval) to new applications enabled by ubiquitous, mobile devices. For example, my research has looked at developing applications for virally exchanging and tracking “coupons” through “opportunistic contact” among mobile wireless devices (i.e., communication among devices moving into communication range with each other). In many of the courses I have taught there is a project component. Through these projects I have supervised numerous efforts to develop new “apps” for download and use across a variety of mobile platforms.

19. Toward the middle of the protocol stack, my research has also looked to build wireless infrastructure support to enable communication among a set of

mobile devices unaided by any other kind of network infrastructure. These kinds of networks are useful either in challenged network environments (e.g., when a natural disaster has destroyed existing infrastructure) or when suitable support for network communication never existed. The deployment of such networks (or even the use of traditional network support) are critical to support services like disaster relief, catastrophic event coordination, and emergency services deployment.

20. Yet another theme is monitoring wireless networks, in particular different variants of IEEE 802.11 compliant networks, to (1) understand the operation of the various protocols used in real-world deployments, (2) use these measurements to characterize use of the networks and identify protocol limitations and weaknesses, and (3) propose and evaluate solutions to these problems. I have successfully used monitoring techniques to study wireless data link layer protocol operation and to improve performance by enhancing the operation of such protocols. For wireless protocols, this research includes functions like network acquisition and channel bonding.

21. One theme in my wireless network research has been cross-layer solutions and innovations. As mentioned above, with greater wireless device use and network support, we envisioned new application paradigms and services, for example, when mobile devices come into contact with each other. Instead of relying on existing infrastructure to relay communication, the devices are able to discover

each other and communicate directly. Other examples include discovering and using location information to enhance users' experiences. Network support and novel applications span use a variety of network architectures supporting users on foot, in vehicles, and across varying terrains and environments. Finally, we studied how communication efficiency can be supported through intelligent handoffs as well as location and movement prediction.

22. Protecting networks, including their operation and content, has been an underlying theme of my research almost since the beginning of my research career. Starting in 2000, I have been involved in several projects that specifically address security, network protection, and firewalls. After significant background work, a team on which I was a member successfully submitted a \$4.3M grant proPOSITAl to the Army Research Office (ARO) at the Department of Defense to propose and develop a high-speed intrusion detection system. Key aspects of the system included associating streams of packets and analyzing them for viruses and other malware. Once the grant was awarded, we spent several years developing and meeting the milestones of the project. A number of my students worked on related projects and published papers on topics ranging from intrusion detection to developing advanced techniques to be incorporated into firewalls. I have also used firewalls, including their associated malware detection features, in developing

techniques for the classroom to ensure that students are not distracted by online content.

23. My recent work ties some of the various threads of my past research together. I have investigated content delivery in online social networks and proposed reputation management systems in large-scale social networks and marketplaces. On the content delivery side, I have looked at issues of caching and cache placement, especially when content being shared and the cache has geographical relevance. We were able to show that effective caching strategies can greatly improve performance and reduce deployment costs. Our work on reputation systems showed that reputations have economic value, and as such, creates a motivation to manipulate reputations. In response, we developed a variety of solutions to protect the integrity of reputations in online social networks. The techniques we developed for content delivery and reputation management were particularly relevant in peer-to-peer communication and recommendations for downloadable “apps.”

24. As an important component of my research program, I have been involved in the development of academic research into available technology in the market place. One aspect of this work is my involvement in the Internet Engineering Task Force (IETF). The IETF is a large and open international community of network designers, operators, vendors, and researchers concerned with the evolution

of the Internet architecture and the smooth operation of the Internet. I have been involved in various IETF groups including many content delivery-related working groups like the Audio Video Transport (AVT) group, the MBone Deployment (MBONED) group, Source Specific Multicast (SSM) group, the Inter-Domain Multicast Routing (IDMR) group, the Reliable Multicast Transport (RMT) group, the Protocol Independent Multicast (PIM) group, etc. I have also served as a member of the Multicast Directorate (MADDOGS), which oversaw the standardization of all things related to multicast in the IETF. Finally, I was the Chair of the Internet2 Multicast Working Group for seven years.

25. My involvement in the research community extends to leadership positions for several academic journals and conferences. I am the co-chair of the Steering Committee for the ACM Network and System Support for Digital Audio and Video (NOSSDAV) workshop and on the Steering Committees for the International Conference on Network Protocols (ICNP), ACM Sigcomm Workshop on Challenged Networks (CHANTS), and IEEE Global Internet (GI) Symposium. I have served or am serving on the Editorial Boards of IEEE/ACM Transactions on Networking, IEEE Transactions on Mobile Computing, IEEE Network, ACM Computers in Entertainment, AACE Journal of Interactive Learning Research (JILR), and ACM Computer Communications Review. I have co-chaired a number of conferences and workshops including the IEEE International Conference on

Network Protocols (ICNP), IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), International Conference on Communication Systems and Networks (COMSNETS), IFIP/IEEE International Conference on Management of Multimedia Networks and Services (MMNS), the International Workshop On Wireless Network Measurement (WiNMee), ACM Sigcomm Workshop on Challenged Networks (CHANTS), the Network Group Communication (NGC) workshop, and the Global Internet Symposium, and I have served on the program committees for numerous conferences.

26. Furthermore, in the courses I taught at UCSB, a significant portion of my curriculum covered aspects of the Internet and network communication including the physical and data link layers of the Open System Interconnect (OSI) protocol stack, and standardized protocols for communicating across a variety of physical media such as cable systems, telephone lines, wireless, and high-speed Local Area Networks (LANs). The courses I have taught also cover most major topics in Internet communication, including data communication, multimedia encoding, and mobile application design. My research and courses have covered a range of physical infrastructures for delivering content over networks, including cable, Integrated Services Digital Network (ISDN), Ethernet, Asynchronous Transfer Mode (ATM), fiber, and Digital Subscriber Line (DSL). For a complete list of courses I have taught, see my curriculum vitae (CV).

27. In addition, I co-founded a technology company called Santa Barbara Labs that was working under a sub-contract from the U.S. Air Force to develop very accurate emulation systems for the military's next generation internetwork. Santa Barbara Labs' focus was in developing an emulation platform to test the performance characteristics of the network architecture in the variety of environments in which it was expected to operate, and, in particular, for network services including Ipv6, multicast, Quality of Service (QoS), satellite-based communication, and security. Applications for this emulation program included communication of a variety of multimedia-based services, including video conferencing and video-on-demand.

28. In addition to having co-founded a technology company myself, I have worked for, consulted with, and collaborated with companies for nearly 30 years. These companies range from well-established companies to start-ups and include IBM, Hitachi Telecom, Turner Broadcasting System (TBS), Bell South, Digital Fountain, RealNetworks, Intel Research, Cisco Systems, and Lockheed Martin.

29. Through my graduate education, leadership with CITS, involvement in TMP, role in the development of the Internet2 infrastructure, and consulting with ISPs, I have gained a strong understanding in the role of the Internet in our society and the challenges of deploying large-scale production networking infrastructure. CITS, since its inception, has looked at the role of the Internet in society, including

how the evolution of technology have created communication opportunities and challenges, including, for example through disruptive technologies like P2P. TMP looks to focus on non-purely technical issues, including, for example, state-of-the-art business methods, strategies for successful technology commercialization, new venture creation, and best practices for fostering innovation. Through my industry collaborations and Internet2 work, I have developed significant experience in the challenges of deploying, monitoring, managing, and scaling communication infrastructure to support evolving Internet services like streaming media, conferencing, content exchange, social networking, and e-commerce.

30. I am a Member of the Association of Computing Machinery (ACM) and a Fellow of the Institute of Electrical and Electronics Engineers (IEEE).

31. Additional details about my employment history, fields of expertise, courses taught, and publications are further included in my CV attached as Ex. 1004.

32. Based on my professional experience, I believe I am qualified to testify as an expert on matters related to the patent at issue.

III. LEGAL STANDARDS

33. Petitioner' attorneys have explained to me the legal standards that apply in this case. My understanding of those standards is described below. I am not an attorney, and I do not have formal training in the law regarding patents. I have

used my understanding of the following legal principles set forth in this section in reaching my opinions.

34. I understand that, in this proceeding, Petitioner have the burden of proving that the challenged claims are invalid by a preponderance of the evidence.

A. Obviousness

35. I have been informed that a claim is invalid as obvious under 35 U.S.C. § 103 (pre-AIA) if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time of the invention to a person of ordinary skill in the art. I have been informed that the following matters are relevant to determining whether the claimed invention would have been obvious: (1) the scope and content of the prior art, (2) the difference or differences between the patent claim and the prior art, (3) the level of ordinary skill in the art at the time the invention of the patent, and (4) any secondary considerations or objective indicia of non-obviousness.

36. I have been informed that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. When a claim simply arranges prior art elements with each performing the same function it had been known to perform and yields no more than one would expect from such an arrangement, then such a combination is obvious. When a patent claims a structure already known in the prior art altered by the mere

substitution of one element for another known in the field, the combination is likely to be obvious unless the combination yields an unpredictable result.

37. I have been informed that when a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill in the art can implement a predictable variation, such a variation is likely unpatentable. For the same reason, if a technique has been used to improve one device, and one of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill. One question to consider is whether the improvement is more than predictably using prior art elements according to their established functions.

38. I have been informed that it may often be necessary, in a validity analysis, to consider whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue. This can be accomplished by looking to interrelated teachings of multiple patents or other publications or pieces of prior art; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by one of ordinary skill in the art.

39. I have been informed that a validity analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim; it is

appropriate to take account of the inferences and creative steps that a person of ordinary skill in the art would employ. I have been informed that a person of ordinary skill in the art is a person of ordinary creativity, not an automaton.

40. I have been informed that a claim composed of several elements is not proved obvious merely by demonstrating that each element was, independently, known in the prior art. I have been informed that it can be important to identify a reason that would have prompted a person of ordinary skill in the art in the relevant field to combine the elements in the way the claimed new invention does. I am told that one way that subject matter can be proved obvious is by noting there existed at the time of the invention a known problem for which there was an obvious solution encompassed by the patent's claims. I have been informed that any need or problem known in the field of endeavor at the time of the claimed invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.

41. I have been informed that one should not assume that a person of ordinary skill in the art attempting to solve a problem will be led only to those elements of prior art designed to solve the same problem. Instead, I have been informed that since familiar items may have obvious uses beyond their primary purposes, in many cases a person of ordinary skill in the art will be able to fit the teachings of multiple prior art references together like pieces of a puzzle.

42. I have been informed that, when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, persons of ordinary skill in the art have good reason to pursue the known options within their technical grasp. If this leads to the anticipated success, the product was likely not accomplished by innovation but by using ordinary skill and common sense. I have been informed that, in such an instance, the fact that the combination was obvious to try may show that the combination was obvious.

43. I have been informed that, when determining whether a claimed combination would have been obvious, the correct analysis is not whether a person of ordinary skill in the art, writing on a blank slate, would have chosen the particular combination of elements described in the claim. Instead, I have been informed that the correct analysis considers whether one of ordinary skill, facing the wide range of needs created by developments in the field of endeavor, would have seen a benefit to selecting the combination claimed.

44. I have been informed that, when determining whether a claimed invention is obvious, any “secondary considerations” of non-obviousness identified by the patentee should also be considered. These secondary considerations can include:

- commercial success of the invention, causally related to the invention itself rather than to companion factors, such as advertising or attractive packaging;
- the invention taught away from the technical direction followed by those skilled in the art;
- a long-felt but unsatisfied need for the invention while the needed implementing arts and elements had long been available;
- the invention achieves results unexpected to those skilled in the art;
- copying of the invention by competitors as distinguished from their independent development
- unsuccessful attempts by those skilled in the art to make the invention;
- acquiescence by the industry to the patent's validity by honoring the patent through taking licenses or not infringing the patent, or both; and

- skepticism, disbelief in or incredulity by those skilled in the art that the patentee's approach worked.

45. I have been informed that, for the above information to impact the obviousness of a patent claim, there must be a nexus between the alleged secondary considerations and the claims. In addition, I have been informed that the burden of introducing evidence of secondary considerations generally is on the Patent Owner. If the Patent Owner or its expert should assert secondary considerations of non-obviousness, I reserve the right to provide a Declaration addressing assertions of non-obviousness due to secondary considerations.

B. Claim Construction

46. I have been informed that claim terms are typically given their plain and ordinary meanings, as would have been understood by a person of ordinary skill in the art at the time of the earliest alleged priority date. I have further been informed that when considering the meaning of any terms in the Challenged Claims of the '976 Patent, I should apply the plain and ordinary meaning of those terms. I have further been informed that in considering the meaning of the claims, one must consider the language of the claims, the specification, and the prosecution history of record.

47. I have been informed that in general, a preamble limits the invention if it recites essential structure or steps, or if it is necessary to give life, meaning, and vitality to the claim. I have further been informed that a preamble is not limiting

where a patentee defines a structurally complete invention in the claim body and uses the preamble only to state a purpose or intended use for the invention. I have further been informed that dependence on a particular disputed preamble phrase for antecedent basis may limit claim scope because it indicates a reliance on both the preamble and claim body to define the claimed invention. I have further been informed that clear reliance on the preamble during prosecution to distinguish the claimed invention from the prior art transforms the preamble into a claim limitation because such reliance indicates use of the preamble to define, in part, the claimed invention.

IV. PERSON OF ORDINARY SKILL IN THE ART AND THE TIME OF THE ALLEGED INVENTION

48. I have been asked to assume that the '976 Patent is entitled to its earliest alleged priority date of September 24, 2010. *See* Ex. 1001. Beyond this assumption, I have not undertaken an analysis to determine the earliest priority date to which the '976 Patent is entitled.

49. Based on the materials and information I have reviewed and based on my experience in the technical areas relevant to the '976 Patent, a person of ordinary skill in the art at the time of the alleged invention of the '976 Patent would have had at least a Bachelor's degree in Computer Science or similar field and at least two years of industry experience in network security. More education can supplement practical experience and vice versa. Based on my knowledge and experience,

including as discussed above in Section II, I was a person of ordinary skill in the art at the time of the alleged invention of the '976 Patent and can provide opinions regarding the knowledge of a person of ordinary skill in the art as of that time. My opinions herein are, where appropriate, based on my understandings as to a person of ordinary skill in the art at that time. I myself had these capabilities at the time of the alleged invention of the '976 Patent.

V. THE '976 Patent

A. Technical Background

50. Below, I provide a brief background summary of the technology at issue.

51. U.S. Pat. No. 11,777,976 (the "'976 Patent") is directed to collecting information about network resources, generally from external information sources. Prior to 2010, ordinary artisans in the field were aware of numerous techniques for collecting information about a network and its resources using what are known as Open Source Intelligence ("OSINT") tools, "open source" indicating that such information could be collected without access to or permission from the target organization.

52. For example, there were a number of well-known OSINT tools for collecting IP address information about assets. The McNab reference (Ex. 1005) devotes an entire chapter to such methods for "Internet Host and Network

Enumeration,” i.e. enumerating the various hosts within a network, including their IP addresses.

53. For example, McNab describes a tool called “whois,” which can look up various information about a domain name, including its authoritative name servers. McNab at 22.

Example 3-1. Obtaining the domain WHOIS record for blah.com

```
$ whois blah.com
```

```
Domain Name: BLAH.COM
Registrar: NETWORK SOLUTIONS, LLC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com
Name Server: NS1.BLAH.COM
Name Server: NS2.BLAH.COM
Name Server: NS3.BLAH.COM
Status: clientTransferProhibited
Updated Date: 04-oct-2006
Creation Date: 20-mar-1995
Expiration Date: 21-mar-2009
```

54. McNab also describes a well-known, free tool called “dig” which can perform a number of functions related to DNS queries. McNab describes using the “dig” command to retrieve a list of hostnames for a specified domain name (“ucia.gov” in the example below) from a specified name server (“relay2.ucia.gov” in the example below), using a technique called a “DNS zone transfer.” McNab at 33.

Example 3-8. Using dig to perform a DNS zone transfer

```
$ dig @relay2.ucia.gov ucia.gov axfr
```

```
; <<>> DiG 9.2.4 <<>> ucia.gov @relay2.ucia.gov axfr
;; global options: printcmd
ucia.gov. 3600 IN SOA relay1.ucia.gov. root.ucia.gov.
511210023 7200 900 604800 900
ucia.gov. 3600 IN NS relay1.ucia.gov.
ucia.gov. 3600 IN NS relay7.ucia.gov.
ucia.gov. 3600 IN NS auth100.ns.uu.net.
ucia.gov. 3600 IN MX 5 mail2.ucia.gov.
ain.ucia.gov. 3600 IN A 198.81.128.68
ain-relay.ucia.gov. 3600 IN CNAME relay1.ucia.gov.
ain-relay-int.ucia.gov. 3600 IN CNAME ain-relay1-int.ucia.gov.
ain-relay1.ucia.gov. 3600 IN CNAME relay1.ucia.gov.
ain-relay1-ext.ucia.gov. 3600 IN CNAME relay1.ucia.gov.
ain-relay1-int.ucia.gov. 3600 IN A 192.168.64.2
ain-relay2.ucia.gov. 3600 IN CNAME relay2.ucia.gov.
ain-relay2-ext.ucia.gov. 3600 IN CNAME relay2.ucia.gov.
ain-relay2-int.ucia.gov. 3600 IN A 192.168.64.3
ain-relay7.ucia.gov. 3600 IN CNAME relay7.ucia.gov.
ain-relay7-ext.ucia.gov. 3600 IN CNAME relay7.ucia.gov.
ain-relay7-int.ucia.gov. 3600 IN A 192.168.64.67
ex-rtr.ucia.gov. 3600 IN CNAME ex-rtr-129.ucia.gov.
ex-rtr-129.ucia.gov. 3600 IN A 198.81.129.222
ex-rtr-129.ucia.gov. 3600 IN HINFO "Cisco 4000 Router" "NP-1E Board"
ex-rtr-191-a.ucia.gov. 3600 IN A 192.103.66.58
ex-rtr-191-b.ucia.gov. 3600 IN A 192.103.66.62
foia.ucia.gov. 3600 IN NS relay1.ucia.gov.
foia.ucia.gov. 3600 IN NS auth100.ns.uu.net.
mail1.ucia.gov. 3600 IN A 198.81.129.68
mail1out.ucia.gov. 3600 IN A 198.81.129.71
mail2.ucia.gov. 3600 IN A 198.81.129.148
mail2out.ucia.gov. 3600 IN A 198.81.129.146
relay.ucia.gov. 3600 IN CNAME relay1.ucia.gov.
relay-int.ucia.gov. 3600 IN CNAME ain-relay1-int.ucia.gov.
relay1.ucia.gov. 3600 IN A 198.81.129.193
relay1-ext.ucia.gov. 3600 IN CNAME relay1.ucia.gov.
relay1-int.ucia.gov. 3600 IN CNAME ain-relay1-int.ucia.gov.
relay2.ucia.gov. 3600 IN A 198.81.129.194
relay2-ext.ucia.gov. 3600 IN CNAME relay2.ucia.gov.
relay2-int.ucia.gov. 3600 IN CNAME ain-relay2-int.ucia.gov.
relay2a.ucia.gov. 3600 IN A 198.81.129.200
relay2y.ucia.gov. 3600 IN A 198.81.129.68
relay2z.ucia.gov. 3600 IN A 198.81.129.69
relay7.ucia.gov. 3600 IN A 198.81.129.186
relay7-ext.ucia.gov. 3600 IN CNAME relay7.ucia.gov.
relay7a.ucia.gov. 3600 IN A 198.81.129.197
relay7b.ucia.gov. 3600 IN A 198.81.129.198
res.ucia.gov. 3600 IN A 198.81.129.116
wais.ucia.gov. 3600 IN CNAME relay2.ucia.gov.
```

55. Once the network hosts have been enumerated, they can then be scanned to assess information about the network. McNab itself explains that

“Network scanners are used to perform bulk automated scanning of IP ranges to identify vulnerable network service components. The two most popular open source network scanners are Nmap and Nessus.” McNab at 13. Nessus, for example, “is a vulnerability assessment package that can perform many automated tests against a target network, including ICMP, TCP, and UDP scanning, testing of specific network services (such as Apache, MySQL, Oracle, Microsoft IIS, and many others), and rich reporting of vulnerabilities identified.” *Id.* By identifying vulnerabilities, the network can be given a risk assessment score.

56. This process of enumerating network assets and performing vulnerability scans to generate risk assessment scores was described by other sources as well. For example, a 2001 paper titled “An Introduction to Internet Attack & Penetration” (Ex. 1015) describes an “Anatomy of a Hack” that lists the following steps:

1. Identification of Internet-based points of presence
2. Network scanning & reconnaissance
3. Accessing the target system or network
4. Carrying out objectives
5. Manipulation of logs and system files

57. The paper then goes on to describe attacks such as the exploitation of vulnerabilities, or various forms of malware. Ex. 1015 at 9-14.

58. In 2002, the National Institute of Standards and Technology (“NIST”) (an organization part of the U.S. Department of Commerce) published a paper called

“Risk Management Guide for Information Technology Systems” (Ex. 1016), which provides guidelines and methodologies for conducting risk assessments, mitigating risks, and ensuring the security of IT systems within the federal government. Section 3.1.2 of the paper outlines various information-gathering techniques, such as “Automated Scanning Tool[s]” such as “network mapping tool [to] identify the services that run on a large group of hosts and provide a quick way of building individual profiles of the target IT system(s).” Ex. 1016 at 11-12. This results in a “picture of the IT system environment, and delineation of system boundary.” *Id.* The paper then goes on in Chapter 3.3 to discuss scanning these services to identify vulnerabilities, noting that “[t]he analysis of the threat to an IT system must include an analysis of the vulnerabilities associated with the system environment.” *Id.* at 15. Based on this analysis, the paper recommends producing a risk rating, which is derived “by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact,” resulting in various “risk levels of High, Medium, and Low” within a risk-level matrix. *Id.* at 24.

Table 3-6. Risk-Level Matrix

Threat Likelihood	Impact		
			<i>High</i> (100)
<i>High</i> (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
<i>Medium</i> (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
<i>Low</i> (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

*Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)*⁸

59. A 2007 presentation given at the Blackhat conference provides an overview of “gathering and discovery techniques, with a concentration on third-party services and new tools” and then using such tools to “gain[] access to a target network.” Ex. 1017 at 4. Thus, in Chapter 3, the paper states “[t]he first step to any security engagement is the initial discovery process,” and describes “discovery techniques, starting from the outside.” *Id.* at 7. The chapter goes on to provide resources for discovering employees of an organization, such as through Google searches, or using a tool called Evolution that “is able to cross-reference information from a large set of public data sources.” *Id.* at 8. The chapter then explains how to use tools to perform “network discovery” using “DNS zone transfers, Whois requests, and reverse DNS lookups.” *Id.* at 9. The chapter then provides descriptions of more advanced tools such as a “‘Domain Dossier’ service which combines the various DNS and Whois requests into [a] single report, with the option to perform a

quick port scan as well.” *Id.* There is also the “DomainTools.com web site” which “accepts an IP address or host name as an input and provides a list of all domains that reverse back to that IP.” *Id.*

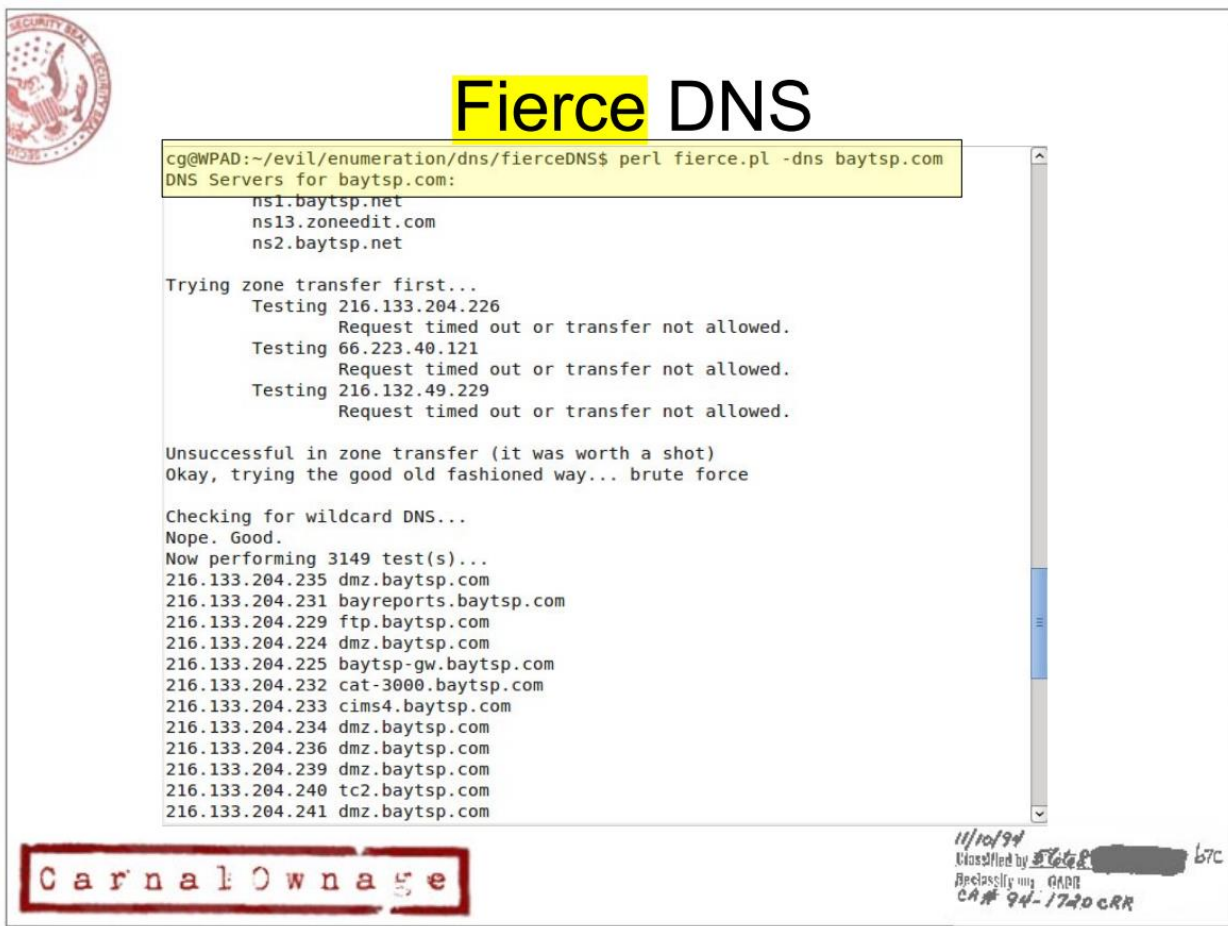
60. The paper also describes using “the Metasploit Framework” which “includes a number of application discovery modules ... to detect services that are difficult to find otherwise.” *Id.* at 14. For example, the below output searched on an IP range and returned DNS and SNMP services running on hosts within that IP range:

```
[*] Sending 6 probes to xxx.xxx.xxx.0->xxx.xxx.xxx.255 (256 hosts)
[*] Discovered DNS on xxx.xxx.xxx.19 (TinyDNS)
[*] Discovered DNS on xxx.xxx.xxx.249 (BIND 8.4.6-REL-NOESW)
[*] Discovered DNS on xxx.xxx.xxx.250 (Microsoft)
[*] Discovered SNMP on xxx.xxx.xxx.170 (Ethernet Routing Switch)
[*] Discovered SNMP on xxx.xxx.xxx.171 (ProCurve J8692A)
```

Id. The paper goes on to describe various ways to attack these services. *Id.* at 19-33.

61. In 2008, a well-known security researcher named Chris Gates delivered a presentation called “New School Information Gathering” (Ex. 1018). The presentation describes a “[b]lack box approach to info gathering” where “the customer wants you to find everything about them you can via ‘open source’ methods.” Ex. 1018 at 5. OSINT information gathering involves “no direct contact with victim’s servers OR no non-standard traffic directed toward victim.” *Id.* at 9.

The presentation then describes several tools for gathering such information. For example, the presentation describes one tool called Fierce DNS which “locate[s] likely targets both inside and outside a corporate network.” *Id.* at 18. Fierce DNS uses a number of DNS queries to find hosts on the same domain and IP blocks used by the domain. *Id.* at 20. The below output for “bytsp.com” shows the various hosts for that domain name. *Id.* at 21-22.





Fierce DNS

```
216.133.204.246 dmz.baytsp.com
216.133.204.247 dmz.baytsp.com
216.133.204.248 dmz.baytsp.com
216.133.204.249 dmz.baytsp.com
216.133.204.250 dmz.baytsp.com
216.133.204.251 dmz.baytsp.com
216.133.204.252 dmz.baytsp.com
216.133.204.253 dmz.baytsp.com
216.133.204.254 dmz.baytsp.com
216.133.204.255 dmz.baytsp.com
216.133.204.240 demo.baytsp.com
216.133.204.229 dl.baytsp.com
216.133.204.227 mail.baytsp.com
216.133.221.24 pop.baytsp.com
216.132.49.228 vpn.baytsp.com
206.135.194.198 w3.baytsp.com
216.133.221.15 webmail.baytsp.com
68.178.254.204 www.baytsp.com
68.178.254.204 .baytsp.com
```

```
Subnets found (may want to probe here using nmap or unicornscan):
206.135.194.0-255 : 1 hostnames found.
216.132.49.0-255 : 1 hostnames found.
216.133.204.0-255 : 29 hostnames found.
216.133.221.0-255 : 2 hostnames found.
68.178.254.0-255 : 2 hostnames found.
```

```
Done with Fierce scan: http://hackers.org/fierce/
Found 35 entries.
```

Have a nice day.

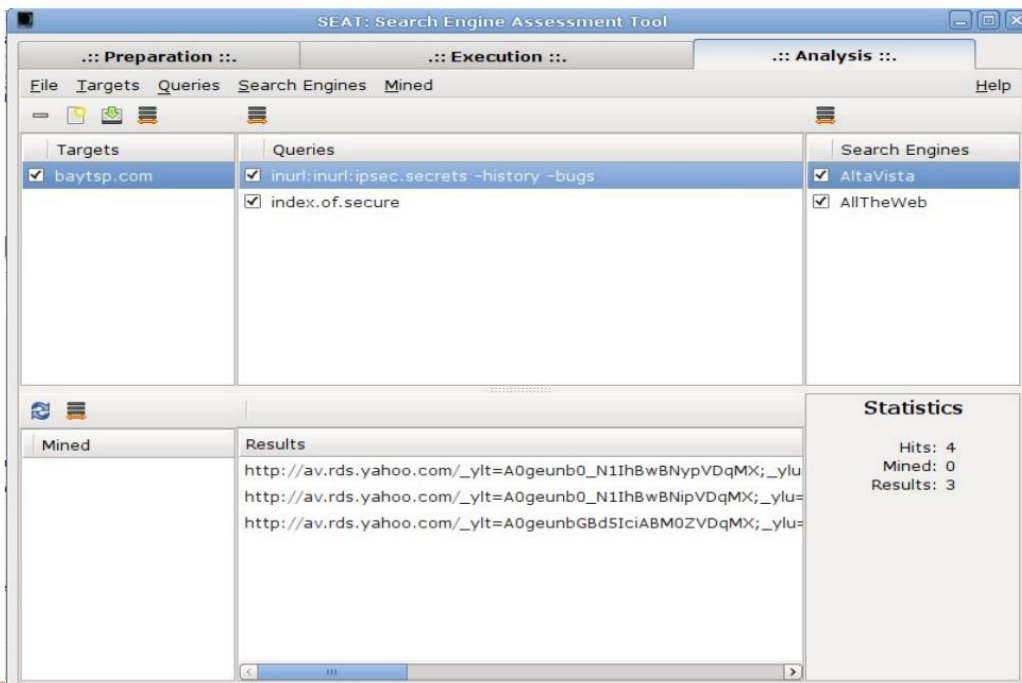
CarnalOwne

Classified by SP 6068
Declassify on: OADR
CA# 94-1720 CRR b7c

62. Another tool called “SEAT (Search Engine Assessment Tool)” “uses information stored in search engine databases, cache repositories, and other public resources to scan a site *for potential vulnerabilities*.” *Id.* at 24 (emphasis added). The tool involves providing a domain name as input (such as “baytsp.com” as used in the slides) and returning a set of results about that domain. *Id.* at 26.



SEAT (Search Engine Assessment Tool)



CarnalOwne

Classified by 3166
Declassify on: OADR
CA# 94-1740 CRR b7c

63. The presentation also describes methods for harvesting email addresses from the provided domain name. *Id.* at 28-32.

64. Another tool called Metagoofil searches for PDF, Word, and other documents found on the provided domain name and extracts metadata from those documents to, for example, “[r]eveal the creator of a document,” “[r]eveal the application that created the document,” “[r]eveal create date,” all in order to “deliver a directed client side attack for something installed in the enterprise.” *Id.* at 35-40.

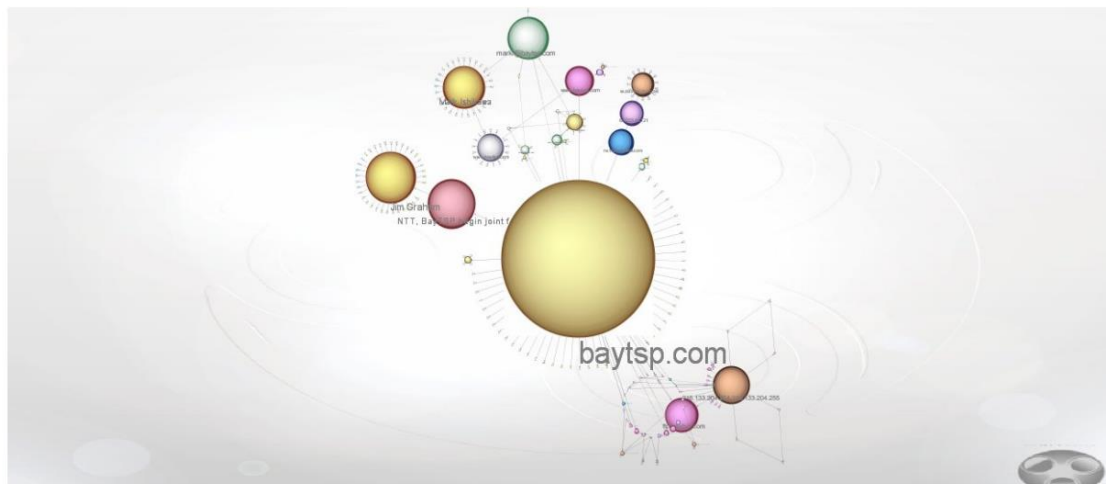
65. Finally, the presentation describes a tool called Maltego, which can perform many of the above functions automatically in one piece of software.

Maltego “is a program that can be used to determine the relationships and real world links between: People ... Companies ... Web sites ... Internet infrastructure such as: Domains, DNS names, Netblocks, IP addresses” and it does this “using open source intelligent (OSINT).” *Id.* at 67. Maltego can enumerate network assets given a domain name, such as by finding “MX and NS servers” for the domain name and determining “what hostnames are shared by the DNS servers,” and “brute forc[ing] our domain names and resolve them to IPs.” *Id.* at 67-72. From there, email addresses and documents can be harvested. *Id.* at 73-77. The presentation explains that Maltego can also search blogs, social networks and incoming links. *Id.* at 82. Maltego also provides graphical representations of the mapped network assets, showing them being associated with various entities. *Id.* at 80.



Maltego

- Sort your views to see relationships



Carnal O w n a g e

11/10/94
Classified by 57668 [redacted] b7c
Declassify on: OADR
CAF 94-1720 CRR

66. Maltego is further described and shown at Exhibit 1021, which is a 2009 video entitled “Social Engineering Using Maltego.” The video shows how Maltego can be used to discover network assets for a particular domain, as well as additional domains that share a DNS name server.

67. Thus, as shown above, ordinary artisans had long had experience seeking information from various sources to enumerate network assets and collect information for providing a risk assessment score.

B. Description of the '976 Patent's Specification

68. The '976 Patent to Boyer *et al.* was filed October 13, 2020 and claims priority to a provisional application filed September 24, 2010.

69. The '976 Patent is directed to conventional techniques for measuring the security vulnerability of a network from external observances. Specifically, it can “creat[e] a composite security rating” from data that is “derived from externally observable characteristics.” Ex. 1001 at Abstract. The claims of the '976 Patent further require generating that composite security rating from internal data sources. *See, e.g., id.*, cl. 1. In particular, the independent claims recite an internal security and an external security rating, which are then combined to a composite security rating. *Id.*

C. The '976 Patent's Prosecution History

70. I have reviewed the prosecution history of the '976 Patent and summarize it below.

71. The initial set of claims were significantly different from the claims that were eventually allowed. Below is the language of the original claim 1 when the application was submitted:

1. (Original) A method of evaluating information security of a third party computer system, the method comprising:
collecting at least two security characterizations of the third party computer system;
generating a composite security rating using the at least two security characterizations;
wherein the two security characterizations are derived from externally observable characteristics of the third party computer system.

72. During prosecution, the examiner issued a non-final rejection over U.S. Pub. No. 2006/0212925 (“Shull”). The applicant then canceled the claims and drafted a completely new set of claims, arguing that Shull did not disclose an internal security rating, an external security rating, or providing a composite security rating. The examiner then issued a notice of allowance.

D. Interpretation of the ’976 Patent’s Challenged Claims

73. For the purposes of my analysis in this IPR proceeding, I understand that the words of a claim are given their plain meaning that those words would have had to a POSITA at the time of the alleged invention. I also understand that the structure of the claims, the specification, and the prosecution history may also be used to better construe a claim insofar as the plain meaning of the claims cannot be understood. Moreover, I understand that even treaties and dictionaries may be used, albeit under limited circumstances, to determine the meaning attributed by a POSITA to a claim term at the time of filing. Furthermore, I understand that a Patent Owner’s own apparent interpretation of certain terms in related proceedings can be considered to determine the meaning of patent claims in an IPR proceeding.

74. I have followed this approach in my analysis, and I have applied the plain and ordinary meaning of those terms as they would have been interpreted by a POSITA at the time the invention was made (not today). For purposes of my analysis here, I have used the September 24, 2010 filing date of the '976 Patent as the date of the invention.

VI. PUBLIC AVAILABILITY OF CERTAIN EXHIBITS

75. I have been asked to opine on the public availability of certain exhibits and specifically whether they were publicly available by September 24, 2010.

A. McNab

76. In my opinion, McNab was publicly available by 2008.

77. McNab is a book published by O'Reilly Media. I am familiar with O'Reilly Media and know that they are a very well-known and reputable publisher of books related to computer technology. I have reviewed dozens of O'Reilly-published books and have cited many such books in my own publications.

78. In my opinion, based on both my expertise in the field and from my personal experience, a POSITA would have considered O'Reilly Media to be a reputable publisher such that the copyright dates on their publications are a reliable and trustworthy indicator of when the publication was published. Ordinary artisans rely on the copyright date printed on the inside of O'Reilly-published books. I am

not aware of nor have I heard of any O'Reilly-published book having a copyright date that is not commensurate with the date of its public availability.

79. In my opinion, Exhibit 1005 is also an authentic copy of McNab as it was available in 2008. Based on my significant experience as a reader of O'Reilly-published books, Exhibit 1005 is complete and has no visible alterations. Exhibit 1005 also has all the hallmarks of an authentic copy of an O'Reilly-published book, including a cover page, a copyright page, a table of contents, an index, and a back cover page. There are also no missing pages from Exhibit 1005. Thus, in my opinion, Exhibit 1005 is a true and authentic copy of McNab as it was published in 2008.

B. Internet Archive Pages

80. Several of the exhibits I have reviewed are from the Internet Archive, including Exhibits 1015, 1017, 1020, and 1022. I am familiar with the Internet Archive and have reviewed the declaration of Mr. Frank-White regarding the operation of the Internet Archive.

81. The Internet Archive exhibits are printouts of web pages or files that were archived by the Wayback Machine. Each link to the Wayback machine has a date and timestamp which indicates the date and time that the link was archived. In my experience this date and time an accurate reflection of when the Wayback Machine archives that particular page. Being familiar with the operation of the

World Wide Web and crawlers like those used by the Wayback Machine, a page could not be archived by the Wayback Machine unless it was available to the public. Moreover, crawlers generally operate by accessing pages that were linked by other pages, and therefore a page that was archived by the Wayback Machine is typically archived because it was linked from at least one other webpage. This further indicates that the archived webpage was publicly available at the time it was archived.

C. Public Videos

82. Exhibits 1019 and 1020 are printouts of webpages that host a video that was publicly available on Vimeo and YouTube, respectively.

83. Exhibit 1019 (available at <http://vimeo.com/2745624>) is a video on the Vimeo website entitled “Toorcon X Gates: New School Information.” This video is of Chris Gates presenting the presentation “New School Information Gathering,” a copy of which is at Exhibit 1018. The webpage states that it was uploaded on January 6, 2009. In my opinion, the upload date on a Vimeo webpage is generally a reliable indicator of when a video was publicly available. Ordinary artisans would have found the date on a Vimeo webpage to be a reliable indicator of public availability. I also note that Exhibit 1019 is a confirmation from an employee at Vimeo that the video was uploaded on January 6, 2009.

84. In addition, I note that Exhibit 1020 is the version of Exhibit 1019 as it was archived by the Wayback Machine on March 2, 2009. This indicates that the video was at least publicly available by March 2, 2009.

85. Thus, in my opinion, Exhibits 1018, 1019 and 1020 were all publicly available by early 2009. It is also my opinion that they are true and correct copies of the video on the date they were published, since the video or webpage does not have any indication it was edited or altered since its upload date.

86. Exhibit 1021 (available at <https://www.youtube.com/watch?v=qiv4-wy3mx0>), is a video on the YouTube website entitled “Social Engineering Using Maltego.” Exhibit 1031 are screenshots of relevant portions from this video. The webpage states it was uploaded on September 14, 2009 and that it has thousands of views. In my opinion, the upload date on a YouTube webpage and its view count is generally a reliable indicator of when a video was publicly available. Ordinary artisans would have found the date on a YouTube webpage to be a reliable indicator of public availability. Moreover, the metadata for this video indicates that it was “published[]At” September 14, 2009 and has a “view[]Count” of 60,168 views, thereby further indicating its public availability by 2009. Ex. 1030.

87. I also note that the video itself, which is of a person using the Maltego software, often displays various dates. All of these dates are consistent with a public

availability date of 2009. For example, at 0:20, the video shows an NS record that is dated March 23, 2009.

88. This in my opinion, Exhibit 1021 was publicly available by 2009. It is also my opinion that they are true and correct copies of the video on the date they were published, since the video or webpage does not have any indication it was edited or altered since its upload date.

VII. GROUND 1: TIPPETT RENDERS OBVIOUS CLAIMS 1, 2, 4-10, AND 12-16

A. Claim 1

1. 1[pre]: A method for determining a security rating of an entity, the method comprising:

89. In my opinion, Tippetts discloses this limitation.

90. Tippetts discloses a method for determining a “security risk index,” *i.e.* **security rating**, for an entity. One of the security risk indices disclosed by Tippetts is a “local security risk index representing the security of ... information resources associated with [an] entity 224A.” Tippetts at ¶46. Information resources include an entity’s “databases,” “computer terminals,” or “servers.” *Id.* at ¶32. Tippetts discloses that an “entity” can “include ... an organization; ... or any other entity,” as well as “consultants, vendors, customers, home users.” *Id.*

2. 1[a]: determining an internal security rating comprising:

91. In my opinion, Tippetts discloses this limitation.

92. Tippet discloses that determining the “local security risk index,” *i.e.* **consolidated security rating**, includes determining a “local vulnerability factor,” *i.e.* **internal security rating**. Tippet at ¶47. Specifically, Tippet discloses that the local security risk index is expressed as “ $LSRI=GT*LV*GI$ ” where “LV may be associated with a local vulnerability factor.” *Id.* Tippet further discloses that the “local vulnerability factor” includes “**internal** factor component[s]” such as a “mitigating measure designed to secure [the entity’s] information resources, a past history of at least one type of security breach, a future plan for securing the information resources associated with the entity 224A, or any other type of query related to the local vulnerability of the information resources associated with the entity 224A,” thereby indicating that the “local vulnerability factor” is an **internal security rating**. Tippet at ¶¶24, 49. In addition, as I discuss in the next limitation, because the “local vulnerability factor” is generated from information from internal data sources, it is an **internal security rating**.

3. 1[b]: obtaining data indicative of internal security from a plurality of internal data sources;

93. In my opinion, Tippet discloses or renders obvious this limitation.

94. Tippet discloses that generating the “local vulnerability factor,” *i.e.* **internal security rating**, comprises gathering “local vulnerability factor components,” which involves obtaining **data indicative of internal security**. Tippet teaches that such local vulnerability factor components are generated from

information relating to “a mitigating measure designed to secure [the entity’s] information resources, a past history of at least one type of security breach, a future plan for securing the information resources associated with the entity 224A, or any other type of query related to the local vulnerability of the information resources associated with the entity 224A,” each of which are ***data indicative of internal security*** since they indicate the vulnerability of the entity based on internal past events or internal mitigating measures. Tippet at ¶49. Because such information is indicative of the internal state of the entity’s network, in my opinion, a POSITA would understand that such information is obtained from ***a plurality of internal data sources***.

95. Moreover, Tippet describes that such components are “internal factor component[s],” thereby indicating that the data is ***obtained from a plurality of internal data sources***. Tippet at ¶24. In fact, Tippet discloses that the security risk index “determining unit” receives information from the entity via “an information link” or “one or more networks,” and that an entity has “various information resources ... such as one or more databases 232, one or more computer terminals 234, one or more computer networks 236, one or more servers 238,” *i.e. a plurality of data sources that are internal to the entity’s network*. Tippet at ¶¶31-32.

96. In my opinion, a POSITA also would have found it obvious that the local vulnerability factor components are obtained from a plurality of internal data

sources. I believe a POSITA would have been motivated to store information such as the entity's mitigating measures, history of security breaches, or future security plans (Tippett at ¶49) within **internal** data sources because such information would be unique to the entity as well as sensitive and confidential to the entity and therefore undesirable to be stored outside of the entity's control. A POSITA would also be motivated to store such information within a **plurality** of data sources because multiple data sources provide redundancy and parallelization, thereby increasing efficiency. Moreover, Tippett already teaches that the entity's information resources include multiple "databases," *i.e.* **internal data stores**, and that the entity sends information to the security risk index determining unit, thus further motivating a POSITA to store such information within the already-present internal data stores. Tippett at ¶¶31-32. It is also my opinion that a POSITA would have a reasonable expectation of success because storing security information in databases was conventional and well-within the skill of an ordinary artisan.

4. 1[c]: extracting a plurality of internal security features from the obtained data;

97. In my opinion, Tippett discloses this limitation.

98. Tippett discloses that "local vulnerability factor components," *i.e.* **plurality of internal security features**, are extracted from the internal security data. In particular, such factor components are "**determined based on** the at least one standard or customized local vulnerability query related to the presence of at least

one mitigating measure designed to secure information resources, a past history of at least one type of security breach, a future plan for securing the information resources associated with the entity 224A, or any other type of query related to the local vulnerability of the information resources associated with the entity 224A.” Tippet at ¶49.

5. **1[d]: applying a respective transformation function to each of the plurality of internal security features to determine a first plurality of transformed features; and**

99. In my opinion, Tippet discloses this limitation.

100. Tippet discloses that the local vulnerability factor components, *i.e.* ***internal security features***, are weighted, *i.e.* ***applied a respective transformation function***. In particular, Tippet discloses that the “local vulnerability factor component weighting operation” yields a “weighted local vulnerability factor component,” *i.e.* ***a first plurality of transformed features***. Tippet at ¶51. Tippet describes that the weighting process includes “evaluating the effectiveness of the specific implemented mitigating measure according to one or more different aspects of mitigation.” Tippet at ¶52. Tippet also describes a weighting process wherein “more than one implemented mitigating measure may safeguard against a same specific type of security event,” which uses the following formula:

$$LVFC=1-((1-E_1)\cdot(1-E_2)\cdot\ldots(1-E_n)),$$

101. This weighting process would be used for a “local vulnerability factor component for the specific type of security event.” *Id.* at ¶53. In other words, Tippet describes at least a weighting process for a local vulnerability factor component representing a mitigating measure and a weighting process for a component representing a security event (such as a breach). Thus, Tippet describes *respective transformation functions* depending on the type of component, *i.e. internal security feature*.

6. 1[e]: combining the first plurality of transformed features to form the internal security rating;

102. In my opinion, Tippet discloses this limitation.

103. Tippet teaches that the weighted local vulnerability factor components, *i.e. first plurality of transformed features*, are “combined ... using statistical mathematics, Bayesian logic, sampling and mitigating measurement, or another method” to generate the “local vulnerability factor,” *i.e. internal security rating*. Tippet at ¶54.

7. 1[f]: determining an external security rating comprising:

104. In my opinion, Tippet discloses this limitation.

105. Tippet discloses that determining the “local security risk index,” *i.e. consolidated security rating*, includes determining a “general threat factor,” *i.e. external security rating*. Tippet at ¶47. Specifically, Tippet discloses that the local security risk index is expressed as “ $LSRI = GT * LV * GI$ ” where “GT may be

associated with a general threat factor.” *Id.* Tippet further discloses that the “general threat factor” includes information about “new types of security events and their severity, information relating to future security events discovered in chat rooms or on message boards, current trends in the implementation of security events, or any other data related to security events that have transpired on the network 228.” *Id.* at ¶37. Tippet further clarifies that a “security event may be any event that threatens the security of one or more information resources, such as, an electronic event, a physical event, an intentional event, an unintentional event, a man-made event, a natural event, an internal event, an external event, a system event, a non-system event, or other event.” *Id.*

106. A POSITA would have understood that the “general threat factor” is an **external security rating**. As an initial matter, as discussed in the next limitation, because the information to generate the “general threat factor” is obtained from external data sources, that is in my opinion enough to constitute an **external security rating**. In addition, the “general threat factor” is a characteristic of “network 228,” of which the comprises the networks of multiple entities. Tippet at ¶¶37, 32, Fig. 2. This is analogous to the ’976 patent’s disclosure of “industry reports” as an external source for the external security rating, which indicates that the external security rating can be a characteristic of a larger network of which the entity is just one part. Ex. 1001, 14:47-49.

107. If Patent Owner argues that the *external security rating* must be a characteristic specific to just the entity, then it is my opinion that is also disclosed in Tippet. Specifically, Tippet discloses that the “general threat factor” is generated from information from “information sources 242.” Tippet at ¶37. Such information sources contain information “pertaining to security events that threaten the security of the *information resources* ... on the network 228,” which Tippet discloses are resources of an entity. *Id.* at ¶¶33, 32 (“The entity 224A may be associated with various *information resources* ... such as one or more databases 232, one or more computer terminals 234, one or more computer networks 236, one or more servers 238, and one or more other information resources 240.”). In other words, because the external information sources contain information about specific information resources on the network, this would include information about resources belonging to the entity.

8. 1[g]: obtaining data indicative of external security from a plurality of external data sources;

108. In my opinion, Tippet discloses this limitation.

109. Tippet discloses that generating the “general threat factor,” *i.e.* *external security rating*, comprises gathering “general threat factor components,” which involves obtaining *data indicative of external security*. In particular, the general threat factor components are generated from obtained data “pertaining to security events that threaten the security of the information resources and the

frequency or rate at which they occur on the network.” Tippet at ¶37. Such data includes “new types of security events and their severity, information relating to future security events discovered in chat rooms or on message boards, current trends in the implementation of security events, or any other data related to security events that have transpired on the network 228.” *Id.* In my opinion, a POSITA would understand that such data is ***indicative of external security*** because they include “external event[s]” and are information directed to events that are external to the entity and not specific to the entity, such as information about new vulnerabilities or mitigating measures found on “chat rooms or on message boards.” *Id.* I note that the “general threat factor components” are data pertaining to security events on “the network,” which is broader than the particular entity and contains multiple entities. *See id.* at ¶¶31-32.

110. Tippet further discloses that such information is obtained “from the plurality of information sources 242,” which include ***external data sources*** such as “public databases, network chat forums, network message boards, scholarly journals, periodicals, personal and commercial web pages, sensors, machine records, trust values, or any other source of information.” Tippet at ¶¶37, 33. In my opinion, because such information is about security events or mitigating measures that are not specific to an organization, and may be of interest to any security researcher, a

POSITA would understand that such sources are **external** and not within the control of the entity.

9. 1[h]: extracting a plurality of external security features from the obtained data;

111. In my opinion, Tippet discloses this limitation.

112. Tippet discloses that “global threat factor components,” *i.e. plurality of external security features*, are extracted from the external security data. In particular, such factor components are generated by “**obtaining data** ... pertaining to security events that threaten the security of the information resources and the frequency or rate at which they occur on the network 228.” Tippet at ¶37.

10. 1[i]: applying a respective transformation function to each of the plurality of external security features to determine a second plurality of transformed features; and

113. In my opinion, Tippet discloses this limitation.

114. Tippet discloses that the global threat factor components, *i.e. external security features*, are normalized and weighted, *i.e. applied a respective transformation function*. In particular, Tippet discloses that a “general threat factor component ... may be in the form of a rate, a frequency, a count, a scale, or another form” and therefore must be “convert[ed] ... into a common format” by a “normalizing operation.” Tippet at ¶38. A POSITA would understand that the normalization operation, *i.e. transformation function*, is specific to the form of the component, and therefore is a **respective transformation function**.

115. Tippet also discloses that the global threat factor components are “weighted,” such as “based on ... the severity of a possible security event, the probability of a future security event, the predictability of a possible security event, or any other basis.” Tippet at ¶¶38-39. Thus, the weighting formula is also a ***respective transformation function***.

116. Once these transformation functions are applied, this results in a “normalized and weighted” “general threat factor component,” *i.e. a second plurality of transformed features*.

11. 1[j]: combining the second plurality of transformed features to form the external security rating; and

117. In my opinion, Tippet discloses this limitation.

118. Tippet teaches that the normalized and weighted general threat factor components, *i.e. second plurality of transformed features*, are “combined ... using statistical mathematics, Bayesian logic, sampling and measurement, or another method” to generate the “general threat factor,” *i.e. external security rating*. Tippet at ¶39.

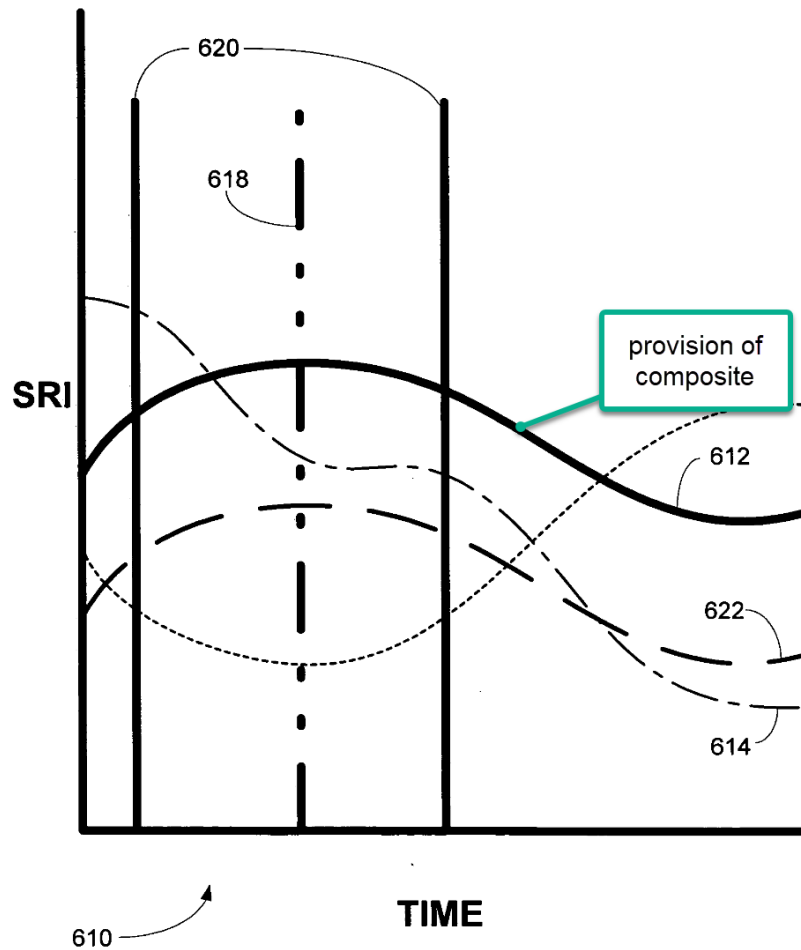
12. 1[k]: providing, via a reporting facility, a composite security rating for the entity based on the internal security rating and the external security rating, wherein at least one of the internal security features or the external security features indicates malicious activity associated with an IP address of the entity.

119. In my opinion, Tippet discloses this limitation.

120. ***“a composite security rating for the entity based on the internal security rating and the external security rating”***: Tippetts discloses that it combines the “local vulnerability factor” (i.e. ***internal security rating***) and the “general threat factor” (i.e. ***external security rating***) to generate a “local risk index representing the security of ... information resources associated with [an] entity 224A,” i.e. ***a composite security rating for the entity***. Tippetts at ¶46. In particular, the “local risk index” can be calculated using the formula “ $LSRI=GT*LV*GP$ ” where “LV may be associated with a local vulnerability factor” and “GT may be associated with a general threat factor.” *Id.* at ¶47.

121. ***“providing, via a reporting facility, a composite security rating”***: Tippetts discloses a “graphical representation,” i.e. ***a reporting facility***, to provide a “local security risk index” for a particular entity. Tippetts at ¶57. Figure 6 is an example of the graphical representing, where elements 612 and 614 are different local security risk indices for different entities. *Id.*

FIG. 6



122. *“wherein at least one of the internal security features or the external security features indicates malicious activity associated with an IP address of the entity”*: Tippet discloses that the “local vulnerability factor” (i.e. *internal security feature*) is generated from information about “a past history of at least one type of *security breach*” that occurred on the entity’s network. Tippet at ¶¶49, 48 (“This may include adding or subtracting at least one local vulnerability query such as, a type of possible security breach that is *unique ... to the entity 224A.*”). In my

opinion, a POSITA would understand that a security breach of a network is ***malicious activity associated with an IP address of the entity***, because a security breach is almost always a breach of a network node which contains an IP address that belongs to the entity's network. For example, information about a breach of a computer belonging to an entity's employee would be ***malicious activity associated with an IP address*** of that employee's computer, which is an ***IP address of the entity***.

B. Claim 2: The method of claim 1, further comprising: determining the composite security rating based on a weighted combination of the internal security rating and the external security rating.

123. In my opinion, Tippetts discloses this limitation.

124. As I discussed above for limitation 1[k], the “local security risk index” (i.e. ***composite security rating***) is generated by ***combining*** the “general threat factor” (i.e. ***external security rating***) and “local vulnerability factor” (i.e. ***internal security rating***). Tippetts at ¶47. In my opinion, this combination is a ***weighted combination***, because as I discussed in limitations 1[d] and 1[i], the “general threat factor” and “local vulnerability factor” are made up of weighted components. As a result, each factor as a whole is also weighted in accordance with the weight of its components.

C. Claim 4: The method of claim 1, wherein at least one of the internal security features or the external security features comprise at least one of: a number of remotely exploitable

vulnerabilities of the entity; a number of security incidents; or a number of vulnerable versions of software of the entity.

125. In my opinion, Tippet discloses this limitation.

126. Tippet discloses that at least one of the components of the “local vulnerability factor” (i.e. ***internal security feature***) is derived from data regarding the “past history of at least one type of security breach.” Tippet at ¶49. In my opinion, a POSITA would understand that a history of security breaches of the entity would include ***a number of security incidents***, specifically the number of times that type or types of security breach occurred in the recorded history.

D. Claim 5: The method of claim 1, wherein each respective transformation function is a normalization of the respective feature, and further comprising: when the normalization is applied to two or more of the internal security features or the external security features, summing the normalized features.

127. In my opinion, Tippet discloses or renders obvious this limitation.

128. As I discussed for limitation 1[i], Tippet discloses performing a ***respective transformation function*** on ***external security features*** in the form of a “normalizing operation.” Tippet at ¶38.

129. If Patent Owner argues that the claim requires that the ***internal security features*** also be normalized, then in my opinion, a POSITA would have found it obvious to normalize the “local vulnerability factor components,” i.e. ***internal security features***. A POSITA would be motivated to normalize the local vulnerability factor components because, as taught by Tippet itself, normalizing

provides the benefit of “convert[ing]” a component “into a common format,” which is needed if the component “may be in the form of a rate, a frequency, a count, a scale, or another form.” Tippet at ¶38. A POSITA would have understood that the “local vulnerability factor components” may also come in different forms, especially since they are described as having different forms, *i.e.* “a mitigating measure,” “a past history ... of security breach,” or “a future plan.” *Id.* at ¶49. Thus a POSITA would be motivated to normalize these components into a common format so that they can be combined into the local vulnerability factor. In my opinion, a POSITA would have had a reasonable expectation of success in doing so because normalization is itself taught by Tippet and would have been well within the skill of a POSITA, such as by converting the factor component into a common scale. For example, both a mitigating measure and future plan can be normalized to a scale of 1-10 depending on their known efficacy against vulnerabilities.

130. Tippet further discloses that the normalized factor components are “combined ... using statistical mathematics, Bayesian logic, sampling and measurement, or another method.” Tippet at ¶¶39, 54. A POSITA would understand that such methods of combination would include ***summing*** the components (*i.e. the normalized features*), since summing is the simplest and most straightforward method of using “mathematics” to combine the components.

E. Claim 6: The method of claim 1, wherein determining the internal security rating further comprises weighting the first plurality of transformed features.

131. In my opinion, Tippet discloses this limitation.

132. As discussed for limitation 1[d], Tippet discloses that the local vulnerability factor components are weighted. See Tippet at ¶¶51-52. Furthermore, as discussed for claim 5, a POSITA would have found it obvious to normalize the local vulnerability factor components as the transformation function that results in a *first plurality of transformed features*. Thus, for the same reasons, a POSITA would have also found it obvious to perform the weighting as taught by Tippet after the normalization, especially since Tippet expressly teaches that other factor components are “normalized and weighted.” See, e.g., Tippet at ¶39.

F. Claim 7: The method of claim 1, wherein combining the first plurality of transformed features comprises: summing the first plurality of transformed features; and normalizing the summed features by a set of normalization factors.

133. In my opinion, Tippet discloses this limitation.

134. As discussed in limitations 1[d] and 1[e], Tippet discloses that the local vulnerability factor components are weighted to result in *a first plurality of transformed features*. Tippet further discloses that the weighted components are “combined ... using statistical mathematics, Bayesian logic, sampling and mitigating measurement, or another method” to generate the “local vulnerability factor.” Tippet at ¶54. In my opinion, a POSITA would understand that such

methods of combination would include **summing** the components, since summing is the simplest and most straightforward method of using “mathematics” to combine the components.

135. Tippet further discloses that the “local vulnerability factor,” *i.e.* **summed features**, are normalized by multiplying it with the “general impact factor,” *i.e.* **set of normalization factors**. Tippet at ¶47. The “general impact factor” is the combination of various components that “reflect all ... effects associated with a security breach” such as “the hard and soft costs of a security breach such as the cost of previous security breaches, the future cost of predicted security breaches, public sentiment with regard to security breaches, or other information” and represents “an expected cost of a breach of the security of the information resources.” Tippet at ¶¶43, 23. Thus, in conjunction with the “local vulnerability factor,” which “represent[s] ... a likelihood of a security event breaching the security of the information resources” (Tippet at ¶23), the “general impact factor” acts as a **set of normalization factors** for each of the “local vulnerability factor components” that make up the “local vulnerability factor.” This is because each “general impact factor component” describes the effect of a security event and each “local vulnerability factor component” describes the likelihood of the security event, and thus when they are multiplied together, it normalizes the “local vulnerability factor components”

into a value that represents the security event's expected harm (*i.e.* probability of harm multiplied by the magnitude of harm) particular to an entity.

G. Claim 8: The method of claim 1, wherein combining the second plurality of transformed features comprises: summing the second plurality of transformed features; and normalizing the summed features by a set of normalization factors.

136. In my opinion, Tippet discloses this limitation.

137. As discussed in limitations 1[i] and 1[j], Tippet discloses that the general threat factor components are weighted to result in ***a second plurality of transformed features***. Tippet further discloses that the weighted components are “using statistical mathematics, Bayesian logic, sampling and measurement, or another method” to generate the “general threat factor.” Tippet at ¶39. A POSITA would understand that such methods of combination would include ***summing*** the components, since summing is the simplest and most straightforward method of using “mathematics” to combine the components.

138. Tippet further discloses that the “general threat factor,” *i.e.* ***summed features***, are normalized by multiplying it with the “general impact factor,” *i.e.* ***set of normalization factors***. Tippet at ¶47. The “general impact factor” is the combination of various components that “reflect all ... effects associated with a security breach” such as “the hard and soft costs of a security breach such as the cost of previous security breaches, the future cost of predicted security breaches, public sentiment with regard to security breaches, or other information” and represents “an

expected cost of a breach of the security of the information resources.” Tippett at ¶¶43, 23. Thus, in conjunction with the “general threat factor,” which “represent[s] ... a rate or frequency of security events that threaten the security of the information resources” (Tippett at ¶23), the “general impact factor” acts as a *set of normalization factors* for each of the “general threat factor components” that make up the “general threat factor.” This is because each “general impact factor component” describes the effect of a security event on a network and each “general threat factor component” describes the rate of the security event threatening a network and thus when they are multiplied together, it normalizes the “general threat factor components” into a value that represents the security event’s expected harm (*i.e.* probability of harm multiplied by the magnitude of harm) to a network.

H. Claim 9

1. 9[pre]: A system for determining a security rating of an entity, the system comprising:

139. In my opinion, Tippett discloses this limitation for the same reasons I discussed above for limitation 1[pre]. Tippett further discloses a “system.” Tippett at Abstract.

2. 9[a]: one or more computer systems programmed to perform operations comprising:

140. In my opinion, Tippett discloses this limitation. Tippett discloses that its system and methods are performed through “software modules running in a

distributed computing environment,” *i.e. computer systems programmed to perform operations*. Tippett at ¶30.

3. 9[b]: determining an internal security rating comprising:

141. In my opinion, Tippett discloses this limitation for the same reasons I discussed above for limitation 1[a].

4. 9[c]: obtaining data indicative of internal security from a plurality of internal data sources;

142. In my opinion, Tippett discloses this limitation for the same reasons I discussed above for limitation 1[b].

5. 9[d]: extracting a plurality of internal security features from the obtained data;

143. In my opinion, Tippett discloses this limitation for the same reasons I discussed above for limitation 1[c].

6. 9[e]: applying a transformation function to each of the plurality of internal security features; and

144. In my opinion, Tippett discloses this limitation for the same reasons I discussed above for limitation 1[d]. I note that this limitation is broader than limitation 1[d] as it does not require that the transformation function be a “*respective* transformation function.”

7. 9[f]: combining the transformed features to form the internal security rating;

145. In my opinion, Tippett discloses this limitation for the same reasons I discussed above for limitation 1[e].

8. 9[g]: determining an external security rating comprising:

146. In my opinion, Tippet discloses this limitation for the same reasons I discussed above for limitation 1[f].

9. 9[h]: obtaining data indicative of external security from a plurality of external data sources;

147. In my opinion, Tippet discloses this limitation for the same reasons I discussed above for limitation 1[g].

10. 9[i]: extracting a plurality of external security features from the obtained data;

148. In my opinion, Tippet discloses this limitation for the same reasons I discussed above for limitation 1[h].

11. 9[j]: applying a transformation function to each of the plurality of external security features; and

149. In my opinion, Tippet discloses this limitation for the same reasons I discussed above for limitation 1[i]. I note that this limitation is broader than limitation 1[i] as it does not require that the transformation function be a “*respective* transformation function.”

12. 9[k]: combining the transformed features to form the external security rating; and

150. In my opinion, Tippet discloses this limitation for the same reasons I discussed above for limitation 1[j].

13. 9[l]: providing, via a reporting facility, a composite security rating for the entity based on the internal security rating and the external security rating, wherein at least one of the

internal security features or the external security features indicates malicious activity associated with an IP address of the entity.

151. In my opinion, Tippet discloses this limitation for the same reasons I discussed above for limitation 1[k].

I. Claim 10: The system of claim 9, wherein the one or more computer systems are further programmed to perform operations comprising: determining the composite security rating based on a weighted combination of the internal security rating and the external security rating.

152. In my opinion, Tippet discloses this limitation for the same reasons I discussed above for Claim 2.

J. Claim 12: The system of claim 9, wherein the internal security features and the external security features comprise at least one of: a number of remotely exploitable vulnerabilities of the entity; a number of security incidents; or a number of vulnerable versions of software of the entity.

153. In my opinion, Tippet discloses this limitation.

154. As I discussed above for claim 4, Tippet discloses that the “local vulnerability factor” (*i.e. internal security feature*) comprises **a number of security incidents**. If Patent Owner argues that this claim also requires that the external security features comprise one of the above pieces of information, Tippet discloses that the “general threat factor components” (*i.e. external security features*) can be derived from “data related to security events [*i.e. security incidents*] that have transpired on the network 228.” Tippet at ¶37. In addition, Tippet discloses that the general threat factor “represent[s] ... a rate or frequency of security events that

threaten the security of information resources.” *Id.* at ¶23. Thus, in my opinion, a POSITA would understand that the rate of security events would include ***a number of security incidents***, since a POSITA would understand that a “rate” is the number of occurrences divided by time.

- K. Claim 13: The system of claim 9, wherein each respective transformation function is a normalization of the respective feature, and wherein the one or more computer systems are further programmed to perform operations comprising: when the normalization is applied to two or more of the internal security features or the external security features, summing the normalized features.**

155. In my opinion, Tippet discloses this limitation for the same reasons I discussed above for Claim 5.

- L. Claim 14: The system of claim 9, wherein determining the internal security rating further comprises weighting the first plurality of transformed features.**

156. In my opinion, Tippet discloses this limitation for the same reasons I discussed above for Claim 6.

- M. Claim 15: The system of claim 1, wherein combining the first plurality of transformed features further comprises: summing the first plurality of transformed features; and normalizing the summed features by a set of normalization factors.**

157. In my opinion, Tippet discloses this limitation for the same reasons I discussed above for Claim 7.

- N. Claim 16: The system of claim 9, wherein combining the second plurality of transformed features further comprises: summing the**

second plurality of transformed features; and normalizing the summed features by a set of normalization factors.

158. In my opinion, Tippetts discloses this limitation for the same reasons I discussed above for Claim 8.

VIII. GROUND 2: TIPPETT AND MCGOVERN RENDER OBVIOUS CLAIMS 3 AND 11

159. Claims 3 and 11 recite that the internal data sources from which information is collected comprise of a number of different types of information. While Tippetts discloses several of such types of information, it does not expressly disclose all of them. However, McGovern discloses collecting information from such data sources to generate a network security assessment. As I discuss below, it is my opinion that it would have been obvious to combine such teachings with Tippetts.

A. Rationale to Combine

160. In my opinion, a POSITA would have been motivated to incorporate McGovern's teachings of collecting various types of information for performing a security assessment of a network.

161. McGovern teaches a "method for information security assessment" that uses various "security parameters [that] relate to a plurality of aspects of an information system." McGovern at ¶29. Such parameters "may encompass the key aspects of information security as described above, such as identity management, vulnerability management, threat management, trust management, and disaster

recovery plans” as well as “the basics of an information system, such as hardware and software configuration, network size and scale, which may also have an impact on security risks.” *Id.* For example, “[v]ulnerability management ... involve[s]... receiving vulnerability updates and applying security patches to software and firmware components” as well as “the use of software tools for security scanning and vulnerability removal.” *Id.* at ¶23. Similarly, “identity and access management” involves information about firewalls and their “implementation of access policies, enforcement of user roles and entitlements, strength of encryption algorithms, and even the availability and quality of directory services.” *Id.* at ¶25. McGovern uses these security parameters to measure “degrees of compliance” which is then quantified and used to perform a security assessment of the network. *Id.* at ¶¶35-37.

162. As I discussed in Ground 1, Tippetts discloses generating a “local vulnerability factor” using various types of information “related to the local vulnerability of the information resources associated with the entity.” Tippetts at ¶49. Tippetts further discloses that the local vulnerability factor is used to generate a local security risk index which “represent[s] the security” of an entity’s network. Tippetts at ¶46. In my opinion, a POSITA would have been motivated to incorporate McGovern’s teachings of “security parameters,” all of which were well-known and commonly collected information for assessing a network’s security, as additional sources of information to be used with calculating Tippetts’s local vulnerability

factor. Since Tippet discloses that the “local vulnerability factor” uses any information related to the security vulnerability of the entity, a POSITA would be motivated to give effect to that teaching by using other well-known sources of information about a network’s vulnerabilities and security such as those described in McGovern. A POSITA would have known that additional sources of information would improve the accuracy of Tippet’s local vulnerability factor, as well as its use in generating a local security risk index. In fact, Tippet describes that the local security risk index is “used to certify the security” of the entity’s network, which is used to “verify to outside parties such as clients, partners, insurers, vendors, consultants, associates, competitors, or other parties” that the network is secure. Tippet at ¶62. Thus, a POSITA knowing the importance of the local security vulnerability factor in certifying the entity’s network would desire to improve its accuracy and be as comprehensive as possible in assessing all aspects of a network’s security, which could be accomplished by making use of the sources of information described by McGovern.

163. Consistent with these teachings in Tippet, McGovern teaches that the “security parameters” can be used to assess “degrees of compliance ... for each security parameter,” which “qualitatively and/or quantitatively describe what is in place in an information system with respect to the corresponding security parameter.” McGovern at ¶35. In other words, McGovern expressly teaches that its

security parameters are used to assess a network's security, and a POSITA would be motivated by such teachings to use McGovern's security parameters as part of calculating Tippet's local vulnerability factor.

164. In my opinion, a POSITA would have had a reasonable expectation of success in combining Tippet and McGovern. McGovern provides detailed descriptions on the types of information that is collected for each "security parameter," which were information that was well-known and well-within the skill of an ordinary artisan to implement within a conventional network. In addition, McGovern also explains that the security parameters can be "quantif[ied] ... to ultimately reach an overall risk assessment," which would be compatible with Tippet's teachings of normalizing and weighing the local vulnerability factor components into a quantifiable amount to be used to calculate the local security risk index. McGovern at ¶36; Tippet at ¶47.

165. Finally, in my opinion, Tippet and McGovern are directed to the same field of endeavor as the '976 patent because all three describe performing security assessments of a network. Ex. 1001 at Abstract ("A method and system for creating a composite security rating from security characterization data of a third party computer system."); Tippet at Abstract ("A system and method for assessing the risk to information resources that may include the generation and/or use of a security

risk index.”); McGovern at Abstract (“Methods for information security assessment and data risk scoring are disclosed.”).

B. Claim 3: The method of claim 1, wherein the plurality of internal data sources comprises: vulnerability scan data of the entity; data indicating firewall rules of the entity; data from security incident reports corresponding to the entity; data indicative of computer network configurations of the entity; data indicative of software inventory of the entity; data indicative of security policies of the entity; data indicative of security controls of the entity; and data indicative of user behavior corresponding to the entity.

166. In my opinion, Tippet and McGovern together disclose each of the claimed ***internal data sources***. As I discussed above, it would have been obvious to combine Tippet and McGovern.

167. “***vulnerability scan data of the entity***”: McGovern discloses that information about “vulnerability management” is collected to perform an information security assessment. McGovern at ¶¶28-29. According to McGovern, “[v]ulnerability management ... involve[s] ... the use of software tools for ***security scanning and vulnerability removal***.” *Id.* at ¶23. McGovern also discloses collecting information related to “virus scan logs.” *Id.* at ¶60. Such information is ***vulnerability scan data of the entity***, including “virus scan logs,” since a POSITA would understand that viruses typically exploit network and entity vulnerabilities.

168. McGovern further discloses that such information is collected by “data sources” that “include ***internal*** data records maintained by the organization,” *i.e.* ***internal data sources***.

169. ***“data indicating firewall rules of the entity”***: McGovern discloses that information about “identity management” is collected to perform an information security assessment. McGovern at ¶¶28-29. According to McGovern, “identity and access management” of “firewall[s]” involves “implementation of access policies, enforcement of user roles and entitlements, strength of encryption algorithms, and even the availability and quality of directory services.” *Id.* at ¶25. Such information is ***data indicating firewall rules of the entity*** because it is indicative of firewall rules and policies related to access, user roles and permissions, and encryption algorithms.

170. McGovern further discloses that such information is collected by “data sources” that “include ***internal*** data records maintained by the organization,” *i.e.* ***internal data sources***.

171. ***“data from security incident reports corresponding to the entity”***: Tippet discloses that information about the entity’s “a past history of at least one type of security breach” is collected from ***internal data sources***. Tippet at ¶49. Such information is ***data from security incident reports*** since a security breach is a ***security incident*** and the past history of security breach will include ***reports*** of such incidents.

172. ***“data indicative of computer network configurations of the entity”***: McGovern discloses that information about “hardware and software configuration” and “network size and scale” is collected to perform an information security

assessment. McGovern at ¶¶28-29. Such information is ***data indicative of computer network configurations of the entity*** because it is indicative of how the network is configured in terms of the hardware and software configuration of its network nodes as well as its configuration with respect to size and scale.

173. McGovern further discloses that such information is collected by “data sources” that “include ***internal*** data records maintained by the organization,” *i.e. internal data sources*.

174. ***“data indicative of software inventory of the entity”***: McGovern discloses that information about “vulnerability management” is collected to perform an information security assessment. McGovern at ¶¶28-29. According to McGovern, “[v]ulnerability management ... involve[s]... receiving vulnerability updates and applying security patches to software and firmware components” as well as “the use of software tools for security scanning and vulnerability removal.” *Id.* at ¶23. Such information is ***data indicative of software inventory of the entity*** because it is indicative of the inventory of software patches and software tools installed on an entity’s network.

175. McGovern further discloses that such information is collected by “data sources” that “include ***internal*** data records maintained by the organization,” *i.e. internal data sources*.

176. ***“data indicative of security policies of the entity”***: Tippetts discloses that information about a “mitigating measure designed to secure information resources” and “a future plan for securing the information resources associated with the entity” are collected from ***internal data sources***. Tippetts at ¶49. Such information is ***data indicative of security policies of the entity*** since they reflect the entity’s policy on mitigating security events and securing the entity’s information resources.

177. ***“data indicative of security controls of the entity”***: Tippetts discloses that information about a “mitigating measure designed to secure information resources” is collected from ***internal data sources***. Tippetts at ¶49. Tippetts further discloses that mitigation includes “deterrence,” “protection,” “detection,” and “recovery.” *Id.* at ¶52. Thus, such information is ***data indicative of security controls of the entity*** since it reflects how the entity controls its information sources to deter or protect from security events.

178. ***“data indicative of user behavior corresponding to the entity”***: McGovern discloses that information about “identity management” is collected to perform an information security assessment. McGovern at ¶¶28-29. According to McGovern, information about “identity management” includes “how often a network user is required to change his or her login password.” *Id.* at ¶36. Such

information is *data indicative of user behavior corresponding to the entity* because it is indicative of how often users within the entity's network change their passwords.

179. McGovern also discloses collecting information "corresponding to ... authorized users" and "attempted unauthorized logins." McGovern at ¶38. Such information is also *data indicative of user behavior corresponding to the entity* because it is indicative of login behaviors for users belonging to the entity or attempting to gain access to entity.

180. McGovern further discloses that such information is collected by "data sources" that "include *internal* data records maintained by the organization," *i.e. internal data sources*.

C. Claim 11: The system of claim 9, wherein the plurality of internal data sources comprises: vulnerability scan data of the entity; data indicating firewall rules of the entity; data from security incident reports corresponding to the entity; data indicative of computer network configurations of the entity; data indicative of software inventory of the entity; data indicative of security policies of the entity; data indicative of security controls of the entity; and data indicative of user behavior corresponding to the entity.

181. In my opinion, Tippet and McGovern render obvious this limitation for the same reasons I discussed above for Claim 3.

IX. CONCLUSION

182. I hereby declare that all statements made of my own knowledge are true and that all statements made on information and belief are believed to be true. I further declare 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 the Title 18 of the United States Code and that such willful false statements may jeopardize the validity of this proceeding.

Executed on this December 10, 2024 by:



Kevin C. Almeroth, Ph. D.