

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,

Petitioner,

v.

FORTINET, INC.,

Patent Owner.

IPR2027-00011
U.S. Patent No. 11,916,902

**DECLARATION OF MICHAEL FRANZ IN SUPPORT OF PETITION FOR
INTER PARTES REVIEW OF U.S. PATENT NO. 11,916,902**

TABLE OF CONTENTS

I.	INTRODUCTION AND QUALIFICATIONS.....	4
II.	EDUCATION	5
	A. Work Experience.....	5
	B. Publications	10
	C. Curriculum Vitae.....	10
	D. Materials Reviewed.....	11
III.	LEVEL OF ORDINARY SKILL IN THE ART	12
IV.	OVERVIEW OF THE '902 PATENT	14
	A. Priority Date of the Claims.....	14
	B. The Alleged Invention.....	14
	C. Prosecution History	18
	D. Claim Construction.....	19
V.	TECHNOLOGY LANDSCAPE AT THE TIME OF THE ALLEGED INVENTION	20
	A. Remote Network Access	20
	B. Network Access Control	21
	C. Insecure IoT Devices.....	21
	D. Virtual Private Networks.....	22
VI.	INVALIDITY BASED ON OBVIOUSNESS—LEGAL STANDARD	22
VII.	SPECIFIC GROUNDS.....	24
	A. Ground 1: Loza In View Of Bansal, Dupont, And Bareket Renders Claims 1-4, 6, 8-9, 11-14, and 16-18 Obvious.....	24
	1. Loza.....	24
	2. Bansal.....	25
	3. Dupont.....	27
	4. Bareket	30

Declaration of M. Franz ISO Petition for
Inter Partes Review Of U.S. Pat. No. 11,916,902

5.	Rationale to Combine Loza with Bansal, Dupont, and Bareket	31
6.	Element-by-Element Analysis	35
B.	Ground 2: Loza with Bansal, Dupont, Bareket, and Sahay Renders Claims 5, 7, 10, and 15 Obvious.....	55
1.	Sahay	55
2.	Rationale to Combine Loza, Bansal, Dupont, and Bareket with Sahay.....	56
3.	Element-by-Element Analysis	59
C.	Ground 3: Mishaev with Schwartz Renders Claims 1-18 Obvious	63
1.	Mishaev	63
2.	Schwartz.....	69
3.	Rationale to Combine Mishaev with Schwartz	75
4.	Element-by-Element Analysis	83
D.	Ground 4: Mishaev with Schwartz and Durbin Renders Claims 1-18 Obvious	108
1.	Durbin	108
2.	Rationale to Combine Mishaev and Schwartz with Durbin	110
3.	Analysis.....	111
VIII.	CONCLUSION.....	112

I. INTRODUCTION AND QUALIFICATIONS

1. I, Michael Franz, have been retained on behalf of Petitioner Netskope, Inc. (“Petitioner”) as a technical expert in connection with the above-captioned petition for *inter partes* review (“Petition”) of U.S. Patent No. 11,916,902 (the “’902 patent”) (Ex-1001). I have been asked to investigate and provide my opinion regarding the state of the art at the time of the alleged invention and whether claims 1-18 of the ’902 patent (the “Challenged Claims”) would have been obvious to a person of ordinary skill in the art (“POSITA”) in view of the prior art discussed below.

2. The opinions set forth in this declaration are based on my personal knowledge, my professional judgment, and my analysis of the materials and information referenced in this declaration and its exhibits.

3. I am being compensated for my consulting services, including time spent testifying at any hearing that may be held, at my standard consulting rate of \$800 per hour. I am also reimbursed for reasonable and customary expenses associated with my work in this case. I receive no other forms of compensation related to this case. My compensation does not depend on the outcome of this post-grant review or the co-pending district court litigation, and I have no other financial interest in this post-grant review.

4. It is my opinion, for the reasons explained in this declaration, that the Challenged Claims would have been obvious to a POSITA at the time of the alleged invention:

Ground	Basis	Reference(s)	Challenged Claims
1	§103	Loza with Bansal, Dupont, and Bareket	1-4, 6, 8-9, 11-14, and 16-18
2	§103	Loza with Bansal, Dupont, Bareket, and Sahay	5, 7, 10, and 15
3	§103	Mishaev with Schwartz	1-18
4	§103	Mishaev with Schwartz and Durbin	1-18

II. EDUCATION

5. I completed my undergraduate studies with a Diplomingenieur from the Swiss Federal Institute of Technology in Zurich (“ETH Zurich”) in 1989. In 1994, I obtained my Doctorate of Technical Sciences from ETH Zurich. My dissertation was entitled “Code-Generation On-the-Fly: A Key to Portable Software.”

A. Work Experience

6. I am a tenured Full Professor of Computer Science in the Donald Bren School of Information and Computer Sciences at the University of California, Irvine (“UCI”). I am also, by courtesy, a Full Professor of Electrical Engineering and Computer Science in the Henry Samueli School of Engineering at UCI. In 2016, the University awarded me the title of distinction of “Chancellor’s Professor” and in

2022, I was further elevated to “Distinguished Professor,” the highest campus-level title of distinction at my university. In 2025, I was additionally appointed as an “ICS Alumni Professor.” This endowed chair, which I hold concurrently with my other appointments, was donated by alumni of our school.

7. I have served as a visiting professor at ETH Zurich, the University of Klagenfurt in Austria, the Technical University of Brunswick in Germany, and the University of Ulm in Germany. I currently hold a courtesy appointment as a visiting professor at the Technical University of Berlin, Germany.

8. I have been elevated to Fellow of the Institute of Electrical and Electronics Engineers (IEEE), the global engineering society. Fellow is the highest of three grades of membership that are awarded based on merit. In every year, IEEE limits the number of new Fellows to one tenth of one percent of the membership, which currently stands at more than 530,000 members.

9. I have also been elevated to Fellow of the Association for Computing Machinery (ACM), the global professional society for computer scientists. Fellow is the highest of ACM’s four grades of membership. ACM’s rules for Fellows are even more restrictive than IEEE’s, limiting the total number of Fellows in absolute terms to 1% of the membership, which currently stands at about 110,000 members. In recent years, ACM has typically elevated no more than 50 individuals to Fellow

status in a single year; in 2015, the year I was advanced, there were 42 new Fellows. Furthermore, in July of 2026, I was named one of 80 Inaugural Members of the ACM SIGSOFT Software Engineering Academy. The Academy honors individuals whose cumulative contributions have shaped software engineering through research, innovation, and service.

10. I have also been elevated to Fellow of the American Association for the Advancement of Science (AAAS), the world's largest general scientific society, with over 120,000 members.

11. Lastly, I am a member of the inaugural cohort of Fellows of the International Federation for Information Processing (IFIP), the global organization for researchers and professionals working in the field of computing. Established in 1960 under the auspices of UNESCO, IFIP is recognized by the United Nations and links some 50 national and international societies and academies of science with a total membership of over half a million professionals. IFIP is an international, non-governmental organization that operates on a non-profit basis.

12. In April of 2021, the Association for Computing Machinery (ACM) named me the recipient of the ACM Charles P. "Chuck" Thacker Breakthrough in Computing Award. I am being recognized for the development of just-in-time compilation techniques that enable fast and feature-rich web services on the internet.

This is the third highest award across all of computer science given by a professional society, behind only the Turing Award (“the Nobel Prize of Computing”) and the ACM Prize in Computing (for early to mid-career contributions).

13. Furthermore, I am a recipient of the IEEE Computer Society’s Technical Achievement Award, “for pioneering contributions to just-in-time compilation and optimization and significantly advancing Web application technology.” At most 4 of these awards are given annually by the IEEE Computer Society, the largest of the IEEE’s technical societies with a current membership of more than 375,000 members. I am also a recipient of the Humboldt Research Award, also known as the “Humboldt Prize.” The award, given by the Alexander von Humboldt Foundation of Germany and funded by the German federal government, recognizes renowned researchers outside of Germany whose “fundamental discoveries, new theories or insights have had a significant impact on their own discipline and who are expected to continue producing cutting-edge achievements in the future.” It is the highest award given by the Foundation to researchers based outside of Germany. In 2025, I was awarded an “ERC Advanced Grant” by the European Research Council, the highest research award given to individual researchers by the European Union.

14. I have led pioneering research on downloadable code in client-server settings such as what we today call “Web 2.0.” This research has had a real and lasting impact on a great many people. I am the co-inventor (with one of my former Ph.D. students) of the “Trace Tree” compilation technique, for which the United States Patent and Trademark Office has awarded U.S. Patent No. 8,769,511. I collaborated with the non-profit Mozilla Foundation to incorporate this technique into the Firefox web browser, where it became the basis of the “TraceMonkey” JavaScript engine, eventually used by several hundred million people every day.

15. Over the course of my career so far, I have been the Principal Investigator on several high-profile research projects with a total budget of well over \$24M. My expertise in software systems with distinct emphases on performance and security of client-server and mobile computing has been sought out repeatedly by the Federal Government, and I have been participating in many high-level invitation-only meetings on Critical Infrastructure Protection and Cyber Security organized by the National Intelligence Community, the Department of Defense, the Department of Homeland Security, and the Department of Energy. The overwhelming majority of the federally-funded projects that I have worked on over the course of my career have been related to computer security.

16. Before I reached the maximum allowed number of consecutive terms on the editorial board, I was an Associate Editor of one of the flagship journals of the IEEE, the IEEE Transactions on Dependable and Secure Computing (TDSC). I have also served on the editorial boards of two further peer-reviewed scholarly journals focusing on software engineering, Software Practice and Experience (SPE) and Computer Science Research and Development (CSRD). I have served on the program committees of most major academic conferences that are related to the various themes of my research. I have served as the primary advisor to 41 completed Ph.Ds., served on the dissertation committees of a further 17 graduated Ph.Ds., and currently serve as the primary advisor on 7 further dissertations in progress.

B. Publications

17. In addition to my dissertation, I co-authored “Automated Software Diversity,” released in 2015.

18. I have published 38 reviewed journal and magazine articles since 1993, and more than 120 conference and workshop papers.

19. I am an inventor on six issued U.S. patents.

C. Curriculum Vitae

20. A copy of my curriculum vitae is attached as Ex-1004 to the Petition.

D. Materials Reviewed

21. In forming my opinions, I have reviewed the '902 patent and its prosecution history, the prior art references discussed below, and the additional exhibits cited throughout this declaration. I have considered these materials in their entirety, even if only portions are discussed here. I have also relied upon my own knowledge, training, and decades of experience in the fields of computer science, software systems, and network security. The following is an exemplary list of the materials on which I based my opinion.

Exhibit	Description
1001	U.S. Pat. No. 11,916,902
1002	File History of the '902 patent
1004	Curriculum Vitae of Dr. Michael Franz
1005	U.S. Pat. App. Pub. No. 2005/0278777 ("Loza")
1006	U.S. Pat. App. Pub. No. 2020/0067949 ("Bansal")
1007	U.S. Pat. App. Pub. No. 2009/0307753 ("Dupont")
1008	U.S. Pat. No. 8,707,395 ("Sahay")
1009	U.S. Pat. App. Pub. No. 2020/0244646 ("Mishaev")
1010	U.S. Pat. No. 10,498,758 ("Schwartz")
1011	U.S. Pat. App. Pub. No. 2015/0365381 ("Durbin")
1012	RESERVED
1013	U.S. Pat. App. Pub. No. 2010/0005297 ("Ganesan")
1014	Dkt. 36-10 in <i>Netskope v. Fortinet</i> , Case 4:26-cv-08886-HSG (N.D. Cal. 2026) ("Complaint Ex. 10")

Exhibit	Description
1015	Souppaya, M. & Scarfone, K., (2016), <i>Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security</i> (NIST Special Publication 800-46 Rev. 2) National Institute of Standards and Technology. (“NIST SP 800-46”)
1016	Barker, E., Dang, Q., Frankel, S., Scarfone, K., & Wouters, P. (2020). <i>Guide to IPsec VPNs</i> (NIST Special Publication 800-77 Rev. 1). National Institute of Standards and Technology. (“NIST SP 800-77”)
1017	Joint Task Force (2020). <i>Security and Privacy Controls for Information Systems and Organizations</i> (NIST Special Publication 800-53, Rev. 5). National Institute of Standards and Technology. (“NIST SP 800-53”)
1018	U.S. Pat. App. Pub. No. 2018/0213574 (“Bareket”)
1019	U.S. Pat. App. Pub. No. 2022/0103523 (“Starr”)

III. LEVEL OF ORDINARY SKILL IN THE ART

22. I am not an attorney and offer no legal opinions. I have been informed about certain aspects of the law for purposes of my analyses and opinions.

23. I understand that in analyzing questions of invalidity, the perspective of a person having ordinary skill in the art (“POSITA”) is often implicated, and the Board may need assistance in determining that level of skill.

24. I understand that the claims and written description of a patent must be understood from the perspective of a POSITA. I have been informed that the following factors may affect the level of skill of a POSITA: (1) the educational level

of the inventor; (2) the type of problems encountered in the art; (3) the prior-art solutions to those problems; (4) the pace of innovation; (5) the sophistication of the technology; and (6) the educational level of active workers in the field. A person of ordinary skill in the art is also a person of ordinary creativity in the art.

25. In my opinion, a POSITA at the time of the alleged invention would have had at least a bachelor's degree in computer science, computer engineering, electrical engineering, or a related field, and at least two years of work or research experience with computer networks and computer network security. Work experience can substitute for formal education and vice versa. My opinions in this declaration are offered from the perspective of such a POSITA, and I am qualified to opine as a POSITA given my own education, training, and decades of experience in these fields.

26. Well before February 25, 2021, my level of skill in the art was at least that of a POSITA. My analysis and conclusions herein are from the perspective of a POSITA as of that date. A different priority date would not change my opinions, as all of the prior art relied upon in this declaration was published well before any potential priority date.

IV. OVERVIEW OF THE '902 PATENT

A. Priority Date of the Claims

27. I have been informed that a U.S. patent application may claim the benefit of the filing date of an earlier patent application if the earlier patent application sufficiently disclosed through its written description the invention claimed in the later-filed U.S. patent application.

28. I have also been informed that a patented claim is invalid if the claimed invention was patented, described in a printed publication, or in public use, on sale, or otherwise available to the public before the effective filing date of the claimed invention, or the claimed invention was described in an issued patent or in an application for patent published or deemed published and that was effectively filed before the effective filing date of the claimed invention.

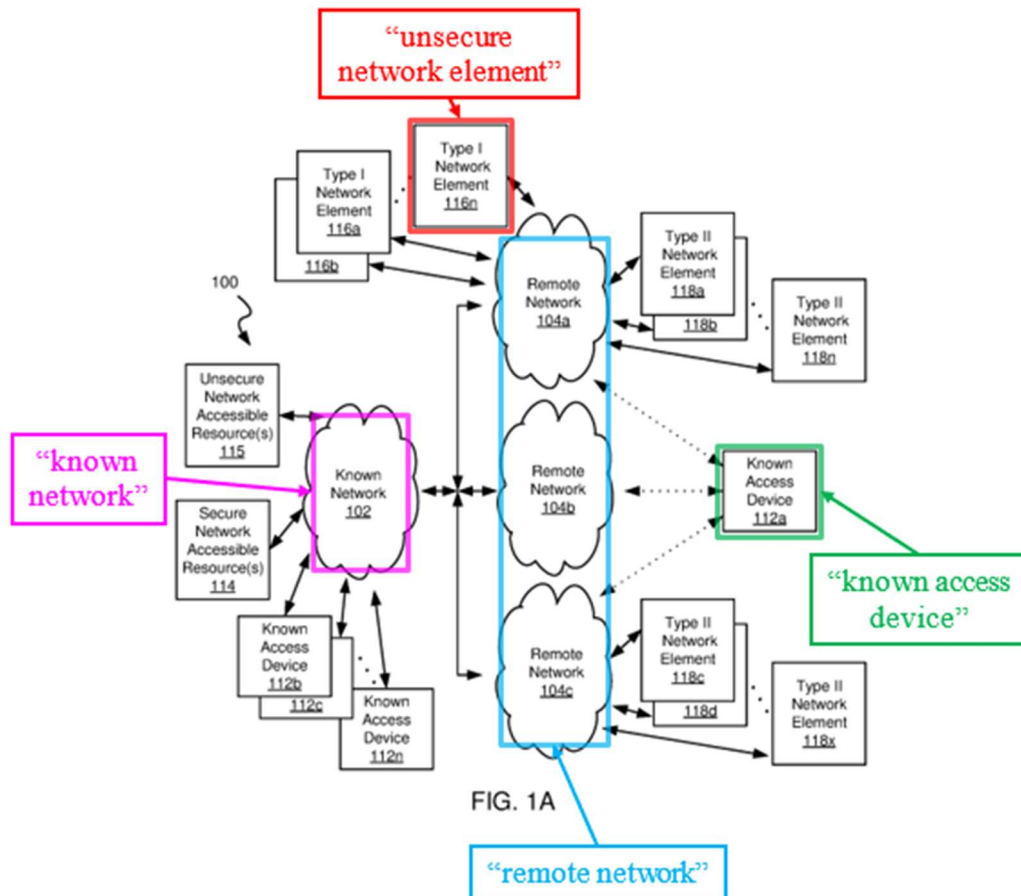
29. I have not been asked to review the priority chain of the '902 patent. For purposes of this declaration and my opinions, I assume the claims are entitled to the earliest available priority date, which is February 25, 2021.

B. The Alleged Invention

30. The '902 patent recognized what was already known in the art years prior, which I describe *infra* Section V.

31. The '902 patent describes “systems and methods for identifying potential threats included in a remote network by a network access device prior to

requesting access to a known secure network via the remote network.” Ex-1001, 1:43-47. The ’902 patent describes an example using its Fig. 1A, reproduced and annotated below:



32. As I discussed, the ’902 patent describes the familiar cast of components in the typical telework setting. *See id.*, 2:36-50. As found similarly in its claims, the ’902 patent’s Fig. 1A depicts a “known access device” (green)—e.g., a “corporate access device”—connected to at least one “remote network” (blue)—e.g., a “home network.” *Compare id.*, 8:8-10, 2:46-50, 3:8-10, Fig. 1A, with, e.g.,

id., limitation 1[a]. Upon request, the known access device may be granted access to a “known network” (pink)—e.g., a “corporate network”—and its “resource(s)” (unannotated) through a selected one of the remote networks, so long as the selected remote network contains no “unsecure network element” (red)—i.e., a “type I network element,” which may be a network element “not considered acceptably secure” as “designated by a network administration of the known network,” such as an “IOT device.” *Compare id.*, 8:11-20, 8:63-67, 9:39-45, 10:7-14, 13:36-47, *with, e.g., id.*, limitations 1[a]-[c], 1[e], claims 3-4.

33. As also recited in its claims, the '902 patent teaches that the known access device itself determines whether the selected remote network contains such an unsecure network element. *See id.*, 9:28-34, Fig. 1B, limitation 1[c]. This is done specifically through a “scan” of the remote network. *See, e.g., id.*, limitation 1[c], 9:28-34. As the '902 patent explains, such scans were already known in the art, such that the known access device could “use any process and/or circuitry known in the art for identifying network elements on the selected remote network.” *Id.*, 9:34-37 (item numbering omitted).

34. If no unsecure network elements are identified in the scan, then the known access device can request a grant of access to—also called attempting a “network connection” with—the known network, such as by presenting an

“authorization credential” to the known network. *See id.*, limitation 1[e], claim 8, 9:66-10:6, 10:44-47, 8:67-9:3. However, if any unsecure network elements are identified, then the known access device can attempt “mitigation” instead to “cure any of the identified unsecure network elements”—e.g., by “connecting...to another remote network.” *Id.*, 5:56-61, claim 7.

35. If mitigation is unsuccessful—e.g., other remote networks do not exist, or any that do likewise contain unsecure network elements as identified in subsequent scans—then the known access device denies itself access to the known network. *Id.*, 16:60-17:9, 10:33-39, limitation 1[d]. Upon doing so, the known access device may also provide its user with a “message.” *E.g., id.*, 10:39-43, claim 5. However, if mitigation is successful—e.g., a scan of the other remote network identifies no unsecure network elements—then the grant of access is requested instead. *Id.*, 10:29-33, 17:13-17, claim 6.

36. Even after being granted access to the known network—e.g., as a result of the presented authorization credential being correct—the known access device may continue conducting scans to identify if any new unsecure network elements have been added the remote network. *Id.*, 10:4-6, 10:44-11:1, claim 8. If any are identified, then the known access device may disconnect from the known network, as well as provide its user with a message. *Id.*, 10:58-11:3, claims 9-10.

37. To carry out these scans, access request decisions, and other discussed functions of the known access device, the '902 patent explains that the known access device may include a “computer system,” which itself includes a “processing resource”—e.g., a general-purpose microprocessor—and memory storing instructions for the processing resource. *See id.*, 11:28-46, 11:55-12:7, Fig. 1C, claims 11-18. When these instructions are executed, the computer system—and thus the known access device—will then perform the discussed functions. *See id.*, 11:28-46, claims 14-18.

C. Prosecution History

38. The Examiner issued two successive Office Actions, each rejecting the application’s original claims 1-4, 6, 8-10, 12-15, and 17-20 over Loza, Bansal, and Dupont, and further rejecting (i) original claims 5, 7, 11, and 16 over these same references in view of Sahay and (ii) original claims 8 and 18 over these same references in further view of Ex-1018. Ex-1002, 133-56, 180-99.

39. Between the two Office Actions, the Examiner said that “bring[ing] in claim 8 into the independent claims” would result in “compact prosecution of the case.” *Id.*, 165. The Applicant did not agree with the Examiner. *Id.*

40. Following the Applicant’s Request for Continued Examination, the Examiner indicated in an interview that the claims would be allowable if original

claim 8 were incorporated into the independent claims. *Id.*, 49. The Applicant ultimately agreed, authorizing an Examiner's amendment to cancel original claims 8 and 18 and move their subject matter into the independent claims, such that Claim 1 would recite the "wherein" clause directed to starting a VPN application and requesting access over a VPN (i.e., limitation 1[f]). *Id.* The Examiner allowed the claims on this basis, finding that the "prior arts of record fail to teach" the amended claim language. *Id.*, 46.

41. The claims as issued in the '902 patent, however, omitted this VPN limitation. Ex-1001, 18:41-44, 19:47-50; 20:15-18. The '902 patent's owner subsequently obtained a Certificate of Correction adding this omitted clause to the independent claims. Ex-1002, 1.

D. Claim Construction

42. I have been instructed that claim terms in an IPR are construed according to the "plain and ordinary" meaning standard of *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) and 37 C.F.R. § 42.100(b). I understand this to mean that the claim terms are interpreted as a POSITA would have understood the claim terms according to their plain and ordinary meaning as informed by the specification and prosecution history. I do not see the need to construe any claim term outside its plain and ordinary meaning.

V. TECHNOLOGY LANDSCAPE AT THE TIME OF THE ALLEGED INVENTION

43. In this section, I summarize the state of the art at the time of the alleged invention, which in my opinion establishes that each individual element recited in the Challenged Claims was well known, and that these elements were already being combined in practice, well before the earliest priority date of the Challenged Claims.

A. Remote Network Access

44. For decades, organizations controlled access to their computing resources by physically securing their networks and requiring users to be on-premises to connect, with a password serving as an additional layer of security. Ex-1009, ¶0002. That model was gradually displaced as cloud computing and remote connectivity matured, and employees, contractors, and other users came to access organizational networks and services from locations outside the organization's own premises as a matter of course. *Id.*, ¶0003-04. Known systems implemented remote access using established methods, including VPN and dialup connections integrated with wired and wireless local access. Ex-1007, ¶0005.

45. By 2016, telework and remote access were ubiquitous and it was well understood that telework technologies should be secured against the assumption that external networks and devices “contain hostile threats that will attempt to gain access to the organization's data and resources,” and that communications over such

external, uncontrolled networks are “susceptible to eavesdropping, interception, and modification.” Ex-1015, 8.

B. Network Access Control

46. This shift to remote access was understood to introduce a corresponding security gap, since a device connecting from outside an organization’s own network could not be assumed to be as trustworthy as a device connecting from within it. Ex-1009, ¶¶0005, ¶¶0007. To address that gap, it became standard industry practice to evaluate a device’s security posture, or the security of the network through which it was connecting, before granting that device access to a protected network—rather than relying on authentication alone. Ex-1015, 23. This general scan-before-access approach was implemented in numerous commercial and patented network access control products and systems well before the challenged patent, in which a connecting device or its network would be assessed for vulnerabilities, and access would be granted, denied, or conditioned on the results of that assessment. Ex-1005, ¶¶0040-41; Ex-1007, ¶¶0005-08, ¶¶0060; Ex-1009, ¶¶0009; Ex-1010, Figs. 2, 5.

C. Insecure IoT Devices

47. It was also widely recognized that the proliferation of Internet of Things (“IoT”) devices—cameras, printers, home entertainment systems, IP phones, thermostats, and home security systems—created new network vulnerabilities, since such devices are “notorious for poor security” and often run on default usernames

and passwords, making them common vectors for malware, DDOS attacks, and data theft that go undetected by traditional point security solutions. Ex-1006, ¶0003. It followed that a device sharing a network with one or more such insecure devices faced materially elevated risk, and detecting the presence of such devices on a network was a known and sensible precondition to trusting that network for sensitive communications (e.g., network scanning, fingerprinting, etc.). *Id.*, Abstract, ¶0034.

D. Virtual Private Networks

48. A virtual private network (“VPN”) was a well-known mechanism for establishing a secure, encrypted channel between a client device and a remote network gateway, particularly where the device’s local network connection could not be trusted, and VPN-based access was already an established part of integrated network access control systems. Ex-1007, ¶0005. While VPN connections were traditionally initiated manually by a user, it was also known to automate that process well before the challenged patent. Ex-1011, Fig. 1; Ex-1018, Abstract, ¶0066.

VI. INVALIDITY BASED ON OBVIOUSNESS—LEGAL STANDARD

49. As I discussed above, I have been informed of the legal standards governing patent invalidity based on prior art. I further understand that a patent cannot be properly granted for subject matter that would have been obvious to a person of ordinary skill in the art at the time of the alleged invention, and that a

patent claim directed to such obvious subject matter is invalid under 35 U.S.C. § 103.

50. It is also my understanding that in assessing the obviousness of claimed subject matter, one should evaluate obviousness in light of the prior art from the perspective of a POSITA at the time the alleged invention was made (and not from the perspective of either a layman or a genius in that art).

51. I understand that obviousness may also be shown by a combination of prior art references where a POSITA would have had a motivation to combine the references, with a reasonable expectation of success. I have applied these standards, together with the ordinary meaning of the claim terms as would be understood by a POSITA and as informed by the specification and prosecution history, in forming the opinions below.

52. I understand that the question of obviousness is to be determined based on: (1) the scope and content of the prior art; (2) the differences between the subject matter of the claim and the prior art; (3) the level of ordinary skill in the art at the time of the alleged invention; and (4) any relevant objective factors (the “secondary indicia”) indicating nonobviousness—including commercial success, a long-felt need, failed attempts by others, copying, unexpected results, praise by others in the field, the taking of licenses, and expressions of surprise by those skilled in the art—

or indicating obviousness, such as independent invention by others before or at about the same time. I reserve the right to address any secondary considerations raised by the Patent Owner—but I am unaware of any at this time.

VII. SPECIFIC GROUNDS

A. Ground 1: Loza In View Of Bansal, Dupont, And Bareket Renders Claims 1-4, 6, 8-9, 11-14, and 16-18 Obvious

53. In my opinion, Loza in view of Bansal, Dupont, and Bareket renders claims 1-4, 6, 8-9, 11-14, and 16-18 obvious.

1. Loza

54. Loza disclosed a system and method for enforcing secure network connections for remote and mobile users. Ex-1005, Abstract. Loza provided “a method of providing a warning of an insecure network connection between a client device and a server.” *Id.*, ¶0013; Fig. A (reproduced below).

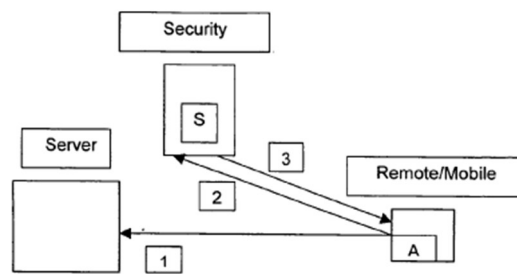


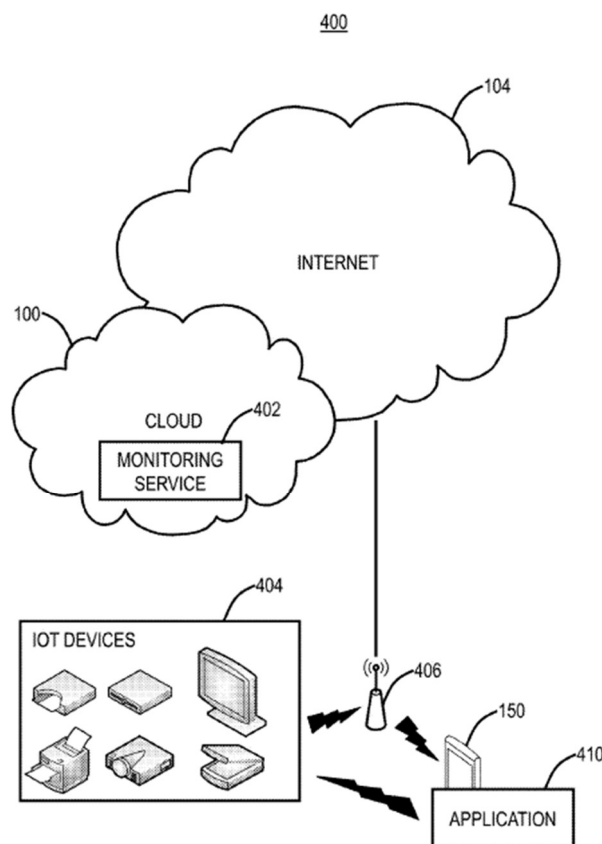
Figure A. Remote user establishing a network connection to a corporate server and requesting security scan on its network connectivity

55. In Loza, every time a remote user attempts to connect to a corporate server, an agent on the remote user’s machine automatically connects to a security

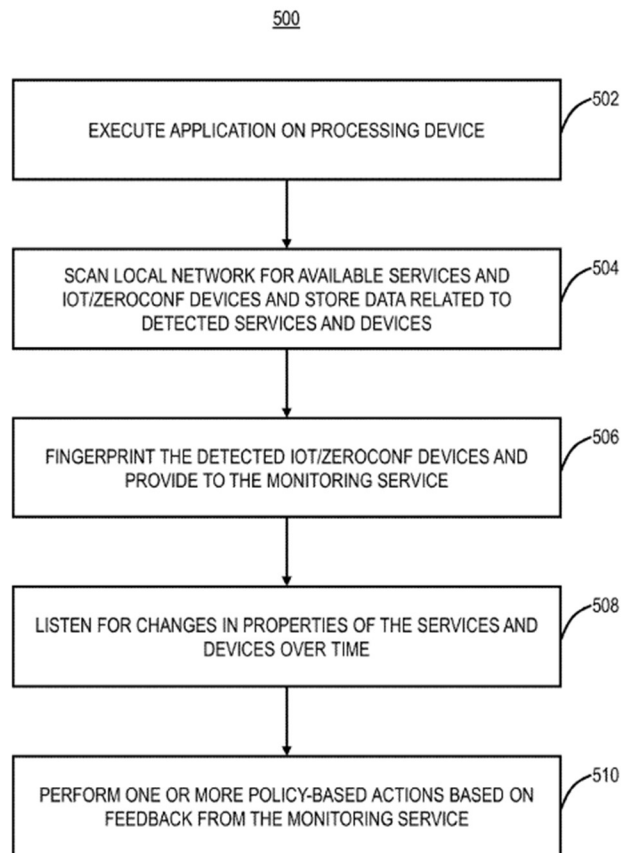
scanner, which assesses the security of the machine's external network connectivity and identifies the number and severity of any discovered vulnerabilities. *Id.*, ¶¶0040-41, ¶0048. Based on a configurable security policy, an agent installed on the machine can then notify the user that the connection is insecure or prevent the machine from establishing any network connection at all. *Id.*, ¶0042. Loza further disclosed that an IT administrator can set the applicable security policy centrally, including triggering a message instructing the user to install a required security measure before access is granted. *Id.*, ¶0053.

2. **Bansal**

56. Bansal disclosed systems and methods for security and control of Internet of Things ("IoT") and ZeroConf devices using cloud services. Ex-1006, Abstract.; Fig. 4 (reproduced below).

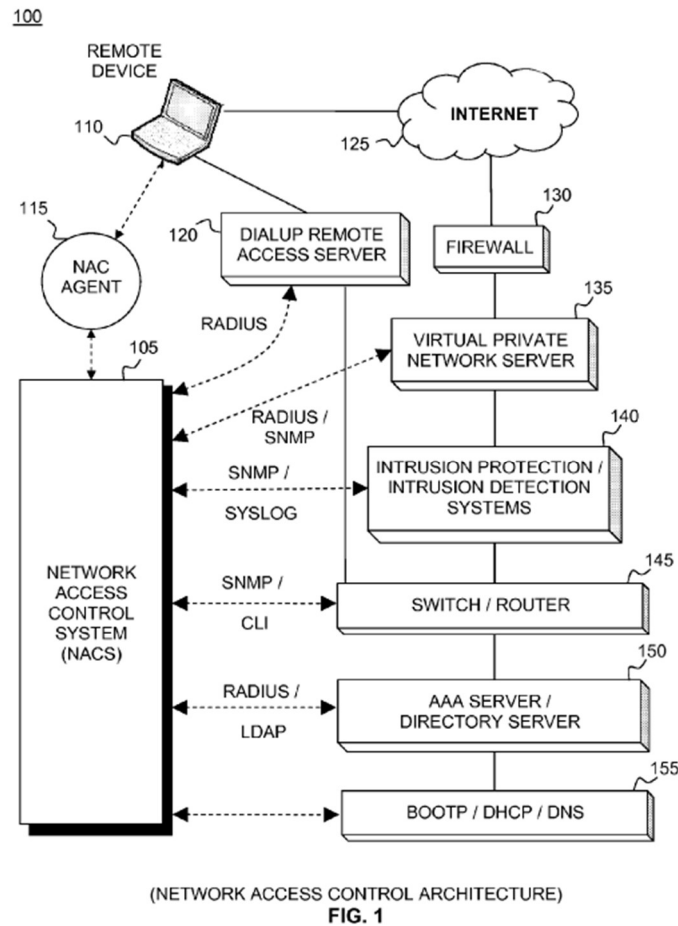


57. An application running on a user's device operates in a promiscuous mode to look for potentially vulnerable and compromised machines on the local network, fingerprinting IoT and ZeroConf devices based on their static and dynamic behavior. *Id.*, Abstract; Fig. 5 (reproduced below). The application discovers all hosts on the network and uses a cloud-based service to detect potentially malicious IoT devices with known vulnerabilities. *Id.*, ¶0014; Fig. 5 (reproduced below).

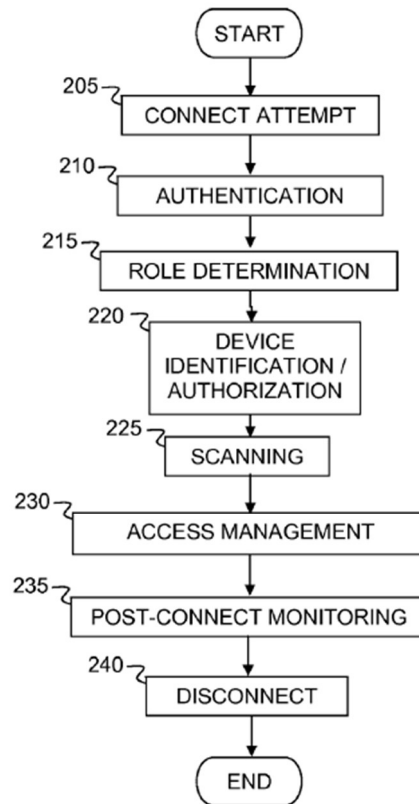
**FIG. 5**

3. Dupont

58. Dupont disclosed a network access control (“NAC”) system and method for devices connecting to a network using remote access control methods. Ex-1007, Abstract; Fig. 1 (reproduced below).



59. Dupont's system automatically performs authentication, assessment, authorization, provisioning, and remediation of a connecting host by collecting information about the user and the host from sources, the remote access device, and an on-host agent, builds a model of the host, and uses that model to govern the host's actual network access once it connects. *Id.*, Abstract; Fig. 2 (reproduced below).



(OPERATIONAL STAGES / PHASES)

FIG. 2

60. Dupont disclosed that a successful vulnerability scan results in a host identity being created for the connecting device, after which the system removes the access-restricting filters for that session, effectively granting it network access. *Id.*, ¶0060. Once connected, Dupont's system performs ongoing passive monitoring, including periodic vulnerability scanning, and if a vulnerability is later discovered

the host is marked at-risk and either disconnected or has its filters reapplied. *Id.*, ¶0061.

4. Bareket

61. Bareket disclosed a method of automatically establishing a VPN connection over an unsecure wireless network. Ex-1018, Abstract; Fig. 1 (reproduced below).

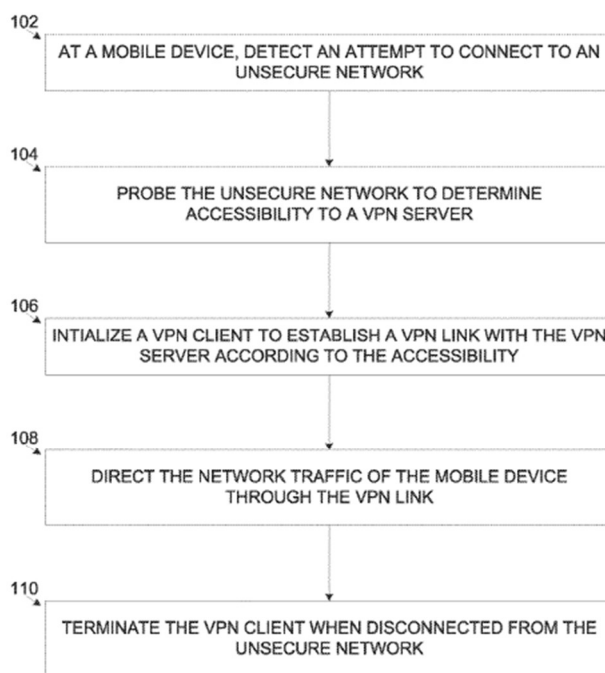


FIG. 1

62. A mobile device detects an attempt to connect to the internet via an unsecure wireless network and probes that unsecure network to determine whether

a VPN server is accessible. *Id.*, Abstract; ¶¶0060-61. Based on that determination, the mobile device automatically initializes a VPN client, which establishes a VPN link to the VPN server over the unsecure wireless network. *Id.*, ¶0066. The device then directs its network traffic through that VPN link, and automatically terminates the VPN client when the device disconnects from the unsecure network. *Id.*, Abstract; ¶0066.

5. Rationale to Combine Loza with Bansal, Dupont, and Bareket

63. In my opinion, a POSITA would have found it obvious to modify Loza using the teachings of Bansal, Dupont, and Bareket, as detailed below.

a. A POSITA Would Have Used Bansal's Unsecure Element Identification in Loza

64. The Examiner found that Loza disclosed a method of scanning a remote network and denying access to a known network if vulnerabilities are found but does not itself specify that those vulnerabilities relate to at least one unsecured network element—e.g., an IoT device. Ex-1002, 138. The Examiner found that Bansal closes that gap by disclosing an application that discovers all hosts on the network can be used to “detect potentially malicious IoT devices with known vulnerabilities.” *Id.*, citing Ex-1006, ¶0014. I agree with the Examiner.

65. The Examiner found that Loza and Bansal were “analogous references to the claimed invention as they both pertain to a method of scanning a network and

identifying vulnerabilities,” and that it “would have been obvious to one of ordinary skill in the art, before the effective filing date of the claimed invention, to modify Loza using the method of identifying an unsecured network element as taught by of Bansal.” Ex-1002, 138. The stated rationale was that “[s]uch modification enables protecting the known network since attackers can gain access to secured networks through an unsecured network element on a remote network that a user is using to connect to the secured network.” *Id.*, 146. The Examiner stated that “[t]he combination of Loza and Bansal teaches a method of scanning a network and identifying an unsecure element.” *Id.*, 139, 146. I agree with the Examiner.

66. A POSITA would have had reason to incorporate Bansal’s IoT-device detection into Loza’s existing scan-and-decide framework to address the known threat that an unsecured device on the remote network poses to the secured network the user is trying to reach, since both references are directed to the same underlying problem of scanning a network to identify security vulnerabilities before permitting a connection to proceed.

b. A POSITA Would Have Modified Loza and Bansal to Grant Access When No Unsecure Network Element Is Found and to Make Mitigation Decisions

67. The Examiner found that the combined teaching of Loza and Bansal described scanning a remote network to identify an unsecure network element as a

basis for denying access but that combination did not address what should happen if no vulnerabilities are discovered—i.e., when no unsecure network element is found. Ex-1002, 139. Dupont closes that gap by disclosing that a “successful scan” results in a “host identity” being created and any access-restricting filters being removed for that session, effectively granting the host network access. *Id.*, citing Ex-1007, ¶0060. I agree with the Examiner.

68. The Examiner found that Loza, Bansal, and Dupont were “analogous references to the claimed invention as they pertain to a method of scanning a network and identifying vulnerabilities,” and that it “would have been obvious to one ordinary skill in the art, before the effective filing date of the claimed invention, to modify the combination of Loza and Bansal using the method of requesting access to a network after the scanning confirms that there are no unsecured elements in the network.” Ex-1002, 139. The stated rationale was that “[s]uch modification will reduce network threats since the network where remote access is requested from is confirmed to be secure.” *Id.* I agree with the Examiner.

69. The Examiner also stated that “[t]he combination of Loza, Bansal, and Dupont teaches a method of mitigating security vulnerabilities of unsecured network.” *Id.*, 154. The Examiner found that it would have been obvious to a POSITA “to further modify the combined teaching of Loza and Bansal in claim 1

by using the method of mitigating vulnerabilities and requesting access as taught by Dupont” to “enable to selectively allow users to connect to a known network if vulnerabilities are mitigated and not permanently block them.” *Id.*, 142, 185, 187. I agree with the Examiner.

70. A POSITA would have had reason to incorporate Dupont’s grant-of-access, credentialing, and ongoing-monitoring teachings into the combined Loza-Bansal scan-and-decide framework, because doing so completes the logical cycle that Loza and Bansal leave open-ended—what to do, and how to keep monitoring, once a connecting device’s remote network has been scanned using the same type of network-access-control architecture already contemplated by Loza and Bansal.

c. A POSITA Would Have Modified Dupont to Perform Mitigation Using a VPN

71. The Examiner found that the combined teaching of Loza, Bansal, and Dupont described mitigating a detected security issue and, following that mitigation, requesting renewed access to the known network but that combination did not specify starting a VPN application as the mitigation mechanism or routing the renewed access request over a VPN. Ex-1002, 154. Bareket closes that gap by disclosing that upon detecting an unsecure wireless network, a probe agent automatically initializes a VPN client, which establishes a VPN link to a VPN server

over the unsecure wireless network and directs the device's network traffic through that encrypted link. *Id.*, 154-55 citing Ex-1018, ¶0066. I agree with the Examiner.

72. The Examiner found that it “would have been obvious to one of ordinary skill in the art, before the effective filing date of the claimed invention, to modify the combined teaching of Loza, Bansal and Dupont...by starting a VPN application and requesting access through the VPN application as taught by Bareket.” Ex-1002, 155. The stated rationale was that “[s]uch modification will make the known network more secure since a VPN provides a secure encrypted connection.” *Id.* I agree with the Examiner.

73. A POSITA would have had reason to incorporate Bareket's automatic VPN-initiation teaching into the combined Loza-Bansal-Dupont framework as the specific mitigation-and-reconnection mechanism, because doing so uses a well-known, readily available technique—establishing an encrypted VPN link—to make the renewed connection to the known network more secure than relying on the unsecure remote network alone, which is precisely the security gap that Loza, Bansal, and Dupont are each independently concerned with closing.

6. Element-by-Element Analysis

- a. **1[pre], 11[pre], 14[pre]: A method for reducing network threats, the method comprising/A system comprising: one or more processing resources; a non-transitory computer-readable medium couple to one or**

more processing resources, wherein the non-transitory computer-readable medium has store thereon instructions that when executed by one or more processing resources cause the one or more processing resources to/A non-transitory computer-readable storage medium embodying a set of instructions, which when executed by one or more processing resources of a computer system, causes the one or more processing resources to perform a method comprising:

74. To the extent the preamble is limiting in Claims 1, 11, and 14, Loza disclosed or rendered obvious these limitations.¹ The Examiner found that Loza disclosed “a method for reducing network threats” by disclosing “a method of providing a warning of an insecure network connection between a client device and a server.” Ex-1002, 147 citing Ex-1005, ¶0013. Loza also disclosed “a system comprising” by disclosing “a system for enforcing secure network connection for remote/mobile users comprises.” Ex-1002, 144 citing Ex-1005, ¶0010. Loza further disclosed “one or more processing resources” by disclosing “an agent installed on a machine connected to the network and accepting connections from remote users.” Ex-1002, 144 citing Ex-1005, ¶0010. I agree with the Examiner.

¹ The Certificate of Correction changed “a processing resource” to “one or more processing resources.” Ex-1002, 1. This does not impact my analysis of this limitation.

75. The Examiner also found that Bansal taught “non-transitory computer-readable medium coupled to one or more processing resources, wherein the non-transitory computer-readable medium has stored thereon instructions that when executed by one or more processing resources cause the one or more processing resource to” by disclosing “[m]oreover, some exemplary embodiments may include a non-transitory computer-readable storage medium having computer readable code stored thereon for programming a computer, server, appliance, device, processor, circuit, etc. each of which may include a processor to perform functions as described and claimed herein.” Ex-1002, 145, 148 citing Ex-1006, ¶0054. I agree with the Examiner.

76. Accordingly, Loza in view of Bansal disclosed or rendered obvious these limitations.

- b. 1[a], 11[a], 14[a]: receiving, by a processing device, a request to access a known network from a known access device connected through a remote network,**

77. Loza disclosed or rendered obvious these limitations.

78. The Examiner found that Loza disclosed the “receiving, by a processing device, a request to access a known network” element by disclosing that “a program or agent on the remote user’s machine (i.e., processing device) may automatically

connect to a security scanner upon the user's attempt (i.e., request) to connect to the corporate server." Ex-1002, 137 citing Ex-1005, ¶0048. I agree with the Examiner.

79. The Examiner found that Loza further disclosed or rendered obvious the "from a known access device connected through a remote network" element. Ex-1002, 118. In the Advisory Action, the Examiner found Loza's scanned network is "remote" because the "[t]he network connected machine starts scanning the external (i.e., remote) network once it gets the external (i.e., remote) IP address as envisaged in paras. [0038-42]" and "[t]he network connected machine is not responsible for the security of, or not known or not governed by the external network (i.e., remote) as indicated by the application's spec." *Id.* The Examiner also stated that "a local/external network whose channel is sought by a connecting device to connect to the external resource(s), shall consider the local network as remote," because "the security of such a network connection is not known, not governed nor controlled by the connecting entity, as the entity seeks the external IP" and "[t]he entity (network connected machine), shall scan the security of the its external network, is typically 'remote' to such a network as envisaged in the prior art." *Id.* The Examiner also cited Fig. 1 in Bareket "for knowledge and clarification purposes" to corroborate that an entity's own external network is typically "remote" to it. *Id.* I agree with the Examiner.

80. Additionally, the Examiner found that Loza's machine as the device scanning the remote network. *Id.* Loza's machine met the '902 Patent's own definition of a "known access device" where the specification defined it as "a device that includes a module governing access to a known network via a remote network." Ex-1001, 3:11-13. I agree with the Examiner.

81. Loza disclosed that its "network connected machine" has an "agent (A) installed on [the] machine connected to the Internet/network" that causes the network server to respond to a network connection request from the network connected machine, after which the "[n]etwork connected machine start[s] assessing security of its own external network connectivity by using its built-in scanner." Ex-1005, ¶0040. The agent may then "notify a user that this particular location that is used to connect to the Internet/network is insecure, or prevent user's machine to establish any network connection." *Id.*, ¶0042.

82. Accordingly, Loza disclosed or rendered obvious these limitations.

- c. **1[b], 11[b], 14[b]: wherein the known network is a private network that authorizes credentials associated with the known access device, and the remote network is external to the known network;**

83. Loza disclosed or rendered obvious these limitations.

84. Loza disclosed the element "wherein the known network is a private network that authorizes credentials associated with the known access device" by

disclosing that a remote machine may be required to first connect to a security scanner before obtaining “permission to connect to the corporate network server” given “by way of a unique key to the remote machine, or a message to the corporate server to accept a connection or another method that would fulfill the function of signalling permission of the remote machine to connect to the corporate system.” *Id.*, ¶0048. These are all various forms of authorizing credentials that the corporate network employs to authorize access, associated with the specific remote machine.

85. In the typical teleworking scenario that was well established by the time of the alleged invention and that is still common practice today, corporations and similar entities typically run their own private networks (i.e., “known networks”) and control access to these private networks by requiring certain credentials to connect. Common is the scenario in which a teleworker uses a “known device” to connect “back” to the known corporate network—for example, a laptop or mobile device issued to them by the corporation, or a “bring your own device (BYOD)” with installed BYOD management software that enables the corporation’s IT staff to securely manage corporate data on the personally-owned device. In either case, both the known device and the known network are ultimately under the common control of the corporation’s IT administration staff, so that arranging for such a

roaming device to be associated with credentials that enable it to connect “back” is straightforward.

86. The Examiner found that Loza also disclosed “the remote network is external to the known network” element. In the Advisory Action, the Examiner equated “external” with “remote,” explaining that “[t]he network connected machine starts scanning the external (i.e., remote) network once it gets the external (i.e., remote) IP address,” and that the network connected machine’s external network is “typically remote.” Ex-1002, 118. I agree with the Examiner.

87. Loza described its invention as “equally applicable to other types of networks in which security breaches on connections from outside of a particular known network could be a concern.” Ex-1005, ¶0049. This language treats the network from which the remote machine connects, and the “particular known network” it is trying to reach, as two separate network environments, proving that the remote network is external to the known network.

88. Accordingly, Loza disclosed or rendered obvious these limitations.

- d. **1[c], 11[c], 14[c]: scanning, by the processing device of the known access device, the remote network through which access to the known network is to be established, wherein the scanning is configured to identify an unsecure network element on the remote network;**

89. Loza disclosed or rendered obvious these limitations.

90. The Examiner found that Loza disclosed the element of “scanning, by the processing device of the known access device, the remote network through which access to the known network is to be established” by disclosing that “[n]etwork connected machine starts assessing security of its own external network connectivity by using its built-in scanner (S).” Ex-1005, ¶0040. I agree with the Examiner.

91. The Examiner also found that Loza disclosed the element “wherein the scanning is configured to identify an unsecure network element on the remote network” by disclosing that “[t]he built-in security scanner identifies a number and a severity level of discovered, if any, security vulnerabilities for this particular machine’s external network connection.” Ex-1005, ¶0041. I agree with the Examiner.

92. Additionally, Loza taught a “processing device of the known access device” in the form of a network connected machine with an agent. The agent in Loza is software and it would have been obvious to a POSITA that there is a processing device on which the software runs. *See* 1[a-b]/11[a-b]/14[a-b].

93. Accordingly, Loza disclosed or rendered obvious these limitations.

- e. **1[d], 11[d], 14[d]: based at least in part on identifying at least one unsecure network element on the remote network, denying, by the processing device, access to the known network; and**

94. Loza in view of Bansal disclosed or rendered obvious these limitations.

95. The Examiner found that Bansal taught the element of “identifying at least one unsecure network element on the remote network” by disclosing that where “the application discovers all hosts on the network and uses a cloud service...to detect potentially malicious IOTs with known vulnerabilities.” Ex-1002 citing Ex-1006, ¶0014. I agree with the Examiner.

96. The Examiner also found that Loza disclosed the element of “denying, by the processing device, access to the known network” by disclosing that “[b]ased on a security policy, an agent (A) installed on this particular machine that is connected to the Internet/network may notify a user that this particular location that is used to connect to the Internet/network is insecure, or prevent user’s machine to establish any network connection.” Ex-1002, 138 citing Ex-1006, ¶0042. I agree with the Examiner.

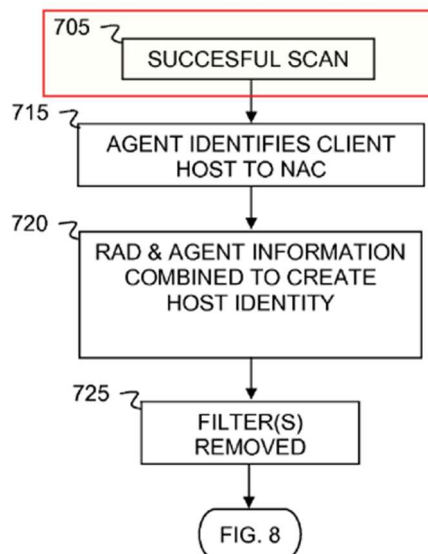
97. The Examiner stated that “[t]he combination of Loza and Bansal teaches a method of scanning a network and identifying an unsecure element” and that it would have been obvious to a POSITA “to modify Loza using the method of identifying an unsecured network element as taught by of Bansal” to “enable[] protecting the known network since attackers can gain access to secured networks through an unsecured network element on a remote network that a user is using to connect to the secured network.” Ex-1002, 139, 146. I agree with the Examiner.

98. Accordingly, Loza in view of Bansal disclosed or rendered obvious these limitations.

- f. **1[e], 11[e], 14[e]: based at least in part upon on failure to identify any unsecure network element on the remote network, requesting a grant of access from the known network to the processing device.**

99. Loza in view of Bansal and Dupont disclosed or rendered obvious these limitations.

100. The Examiner found that Dupont taught the element of “based at least in part upon on failure to identify any unsecure network element on the remote network” by disclosing a “successful scan” in Fig. 7, reproduced and annotated below. Ex-1002, 139 citing Ex-1007, Fig. 7. I agree with the Examiner.



101. The Examiner also found that Dupont also taught the element of “requesting a grant of access from the known network to the processing device” by

disclosing that “[a] successful scan 705 is accompanied by host characteristics that identify the client host to NACS 715” —which the Examiner equated to “requesting access.” Ex-1002, 139 citing Ex-1007, ¶0060. I agree with the Examiner.

102. The Examiner stated that it would have been obvious to a POSITA “to modify the combination of Loza and Bansal using the method of requesting access to a network after the scanning confirms that there are no unsecured elements in the network” to “reduce network threats since the network where remote access is requested from is confirmed to be secure.” Ex-1002, 139. I agree with the Examiner.

103. Accordingly, Loza in view of Bansal and Dupont disclosed or rendered obvious these limitations.

- g. 1[f], 11[f], 14[f]: wherein mitigating a security issue of the unsecure network element includes starting, by the processing device, a virtual private network application, and wherein requesting the grant of access from the known network to the processing device is done over a virtual private network.**

104. Loza in view of Bansal, Dupont, and Bareket disclosed or rendered obvious these limitations.

105. The Examiner found that Bareket disclosed the first half of this limitation (“wherein mitigating a security issue...a virtual private network application”) by disclosing that “the probe agent 222 automatically initializes (invokes, launches) the VPN client 224 according to the determined accessibility,

i.e. the probe agent 222 invokes the VPN client 224 in case the accessibility is determined valid (feasible).” Ex-1002, 154-55 citing Ex-1018, ¶0066. I agree with the Examiner.

106. The Examiner found that Bareket disclosed the second half of this limitation (“wherein requesting the grant of access...over a virtual private network”) by disclosing that “[t]he VPN client 224 then establishes the VPN link with the VPN server 214 over the unsecure wireless network 210.” Ex-1002, 154-55 citing Ex-1018, ¶0066. I agree with the Examiner.

107. The Examiner also stated that it would have been obvious to a POSITA “to modify the combined teaching of Loza, Bansal, and Dupont...by starting a VPN application and requesting access through the VPN application as taught by Bareket” to “make the known network more secure since a VPN provides a secure encrypted connection.” Ex-1002, 155. I agree with the Examiner.

108. Accordingly, Loza in view of Bansal, Dupont, and Bareket disclosed or rendered obvious these limitations.

109. Thus, Loza in view of Bansal, Dupont, and Bareket disclosed or rendered obvious claims 1, 11, and 14.

- h. 2, 12: ...wherein access by the processing device to the known network is granted upon a combination of the requesting a grant of access from the known network to the processing device and a correct authorization**

**credential presented by the processing device to the
known network.**

110. Loza in view of Bansal and Dupont disclosed or rendered obvious these claims.

111. Dupont taught the element “wherein access by the processing device to the known network is granted” by disclosing that “NACS commands the RAD to remove the filters for the affected session 725.” Ex-1002, 140 citing Ex-1007, ¶0060. I agree with the Examiner.

112. Dupont also taught the element “upon a combination of the requesting a grant of access from the known network to the processing device” by disclosing that “[a] successful scan 705 is accompanied by host characteristics that identify the client host to NACS.” Ex-1002, 140 citing Ex-1007, ¶0060. I agree with the Examiner.

113. Dupont further taught the element “and a correct authorization credential presented by the processing device to the known network” by disclosing that “[i]f authentication 310 is successful 325, the process flows to capture user identity 335, capture RAD location 340, and determine authorization 345” and “RADIUS is used to provide authentication for connecting users and to integrate RAD with NACS.” Ex-1002, 140 citing Ex-1007, ¶0047. I agree with the Examiner.

114. The Examiner also stated that it would have been obvious to a POSITA “to further modify the combined teaching of Loza, Bansal, and Dupont in claim 1 by using the method of presenting authorization credential as taught by Dupont” to “reduce the threat to the known network since both the user/device and the network from which connection is requested from are authenticated.” Ex-1002, 140. I agree with the Examiner.

115. Accordingly, Loza in view of Bansal and Dupont disclosed or rendered obvious these claims.

i. 3, 13: ...wherein the unsecure network element is an Internet of Things (IoT) device.

116. Loza in view of Bansal and Dupont disclosed or rendered obvious these claims.

117. The Examiner found that Bansal taught that “[t]he application discovers all hosts on the network and uses a cloud service such as via a cloud-based system to detect potentially malicious IOTs with known vulnerabilities.” Ex-1002, 140-41 citing Ex-1006, ¶0014. I agree with the Examiner.

118. The Examiner also stated that it would have been obvious to a POSITA “to further modify the combined teaching of Loza, Bansal, and Dupont in claim 1 by using the method of detecting an unsecured IoT device in a network as taught by Bansal” to prevent threats from IoT devices that are abundant in many remote works

which in turn will increase the security of a known network. Ex-1002, 140. I agree with the Examiner.

119. Accordingly, Loza in view of Bansal and Dupont disclosed or rendered obvious these claims.

j. 4: ...wherein administration of the processing device and the known network is controlled by a common administration entity.

120. Loza in view of Bansal and Dupont disclosed or rendered obvious this claim.

121. The Examiner found that Loza disclosed the element “wherein administration of the processing device and the known network” by disclosing that “the IT administrator...by setting the policy could require it prior to granting access”—which the Examiner equated to “administering the processing device”—where the set policy would “automatically prevent access further into a network”—which the Examiner equated to “administration of network.” Ex-1002, 141 citing Ex-1005, ¶0053. I agree with the Examiner.

122. The Examiner found that Loza further disclosed the element “is controlled by a common administration entity” by its multiple references to “IT administrator” that set these policies. Ex-1002, 141 citing Ex-1005, ¶0019, ¶¶0052-53. I agree with the Examiner.

123. Accordingly, Loza in view of Bansal and Dupont disclosed or rendered obvious this claim.

- k. 6[a], 6[b], 16[a], 16[b]: ...mitigating a security issue of the unsecure network element; and based at least in part upon mitigating the security issue of the unsecure network element, requesting a grant of access from the known network to the processing device.**

124. Loza in view of Bansal and Dupont disclosed or rendered obvious these claims.

125. The Examiner found that Dupont disclosed the element “mitigating a security issue of the unsecure network element” by disclosing that “[u]sers may be required 620 to disconnect to remediate 630 or remediate from the restricted network while still connected 625.” Ex-1002, 142 citing Ex-1007, ¶0058. I agree with the Examiner.

126. The Examiner found that Dupont also disclosed the element “based at least in part upon mitigating the security issue of the unsecure network element” by disclosing “[o]nce remediation is complete.” Ex-1002, 142 citing Ex-1007, ¶0058. I agree with the Examiner.

127. The Examiner found that Dupont further disclosed the element “requesting a grant of access from the known network to the processing device” by disclosing that “[i]f the user does disconnect to remediate, he then returns to the steps

of FIG. 2 with another connect attempt”—which the Examiner equated to “requesting grant of access.” Ex-1002, 142 citing Ex-1007, ¶0058. I agree with the Examiner.

128. The Examiner also stated that it would have been obvious to a POSITA “to further modify the combined teaching of Loza, Bansal and Dupont in claim 1 by using the method of mitigating vulnerabilities and requesting access as taught by Dupont” to “enable to selectively allow users to connect to a known network if vulnerabilities are mitigated and not permanently block them.” Ex-1002, 142, 185, 187. I agree with the Examiner.

129. Accordingly, Loza in view of Bansal and Dupont disclosed or rendered obvious these claims.

- I. **8[a], 8[b], 17[a], 17[b]: ...using, by the processing device, a network connection between the processing device and the known network; and while using the network connection between the processing device and the known network, scanning, by the processing device, the remote network through which access to the known network is established, wherein the scanning is configured to identify an unsecure network.**

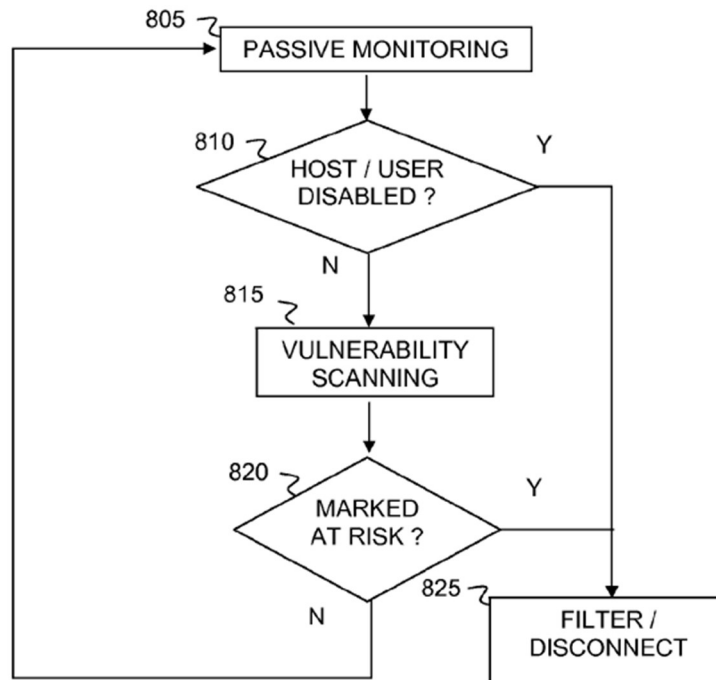
130. Loza in view of Bansal and Dupont disclosed or rendered obvious these claims.

131. The Examiner found that Dupont taught the element “using, by the processing device, a network connection between the processing device and the

known network” by disclosing that “NACS commands the RAD to remove the filters for the affected session 725”—which the Examiner equated to “using network connection.” Ex-1002, 142-43 citing Ex-1007, ¶¶0058. I agree with the Examiner.

132. The Examiner found that Dupont also taught the element “while using the network connection between the processing device and the known network” by disclosing Fig. 8 (reproduced below) which “is a simplified flow chart of an embodiment of post-connect monitoring 800.” Ex-1002, 143 citing Ex-1007, ¶¶0061. I agree with the Examiner.

800



133. The Examiner found that Dupont further taught “scanning, by the processing device, the remote network through which access to the known network is established” by disclosing that “[p]assive monitoring 805 determines the client state 810 within NACS and involves optional periodic vulnerability scanning 815 where a client may be marked at-risk 820.” Ex-1002, 143 citing Ex-1007, ¶0061. I agree with the Examiner.

134. The Examiner found that Dupont further taught “wherein the scanning is configured to identify an unsecure network element on the remote network” by disclosing that “if a client fails a security compliance scan or is found to be disabled 810, it proceeds to be filtered or disconnected 825.” Ex-1002, 143 citing Ex-1007, ¶0061. I agree with the Examiner.

135. The Examiner also stated that it would have been obvious to a POSITA “further modify the combined teaching of Loza, Bansal and Dupont in claim 1 by using the method of scanning a network after access has been granted as taught by Dupont” to “further reduce threat to a known network by continuously monitoring a remote network and identifying potential vulnerabilities that might arise after access has been granted.” Ex-1002, 143. I agree with the Examiner.

136. Accordingly, Loza in view of Bansal and Dupont disclosed or rendered obvious these claims.

- m. 9, 18: ...upon identifying an unsecure network element on the remote network while using the network connection between the processing device and the known network disconnecting, by the processing device, the processing device from the known network.**

137. Loza in view of Bansal and Dupont disclosed or rendered obvious these claims.

138. The Examiner found that Dupont taught the element “upon identifying an unsecure network element on the remote network while using the network connection between the processing device and the known network” by disclosing that “[p]assive monitoring 805 determines the client state 810 within NACS and involves optional periodic vulnerability scanning 815 where a client may be marked at-risk 820.” Ex-1002, 144 citing Ex-1007, ¶0061. I agree with the Examiner.

139. The Examiner found that Dupont also taught the element “disconnecting, by the processing device, the processing device from the known network” by disclosing that “[i]f a client is marked at risk, it may be disconnected” or “if a client fails a security compliance scan or is found to be disabled 810, it proceeds to be...disconnected 825.” Ex-1002, 144 citing Ex-1007, ¶0061. I agree with the Examiner.

140. The Examiner also stated that it would have been obvious to a POSITA “to further modify the combined teaching of Loza, Bansal and Dupont of claim 8 by

using the method of disconnecting a device from a known network when vulnerabilities are discovered as taught by Dupont” to “reduc[e] threats to known network by isolating vulnerable devices.” Ex-1002, 144.

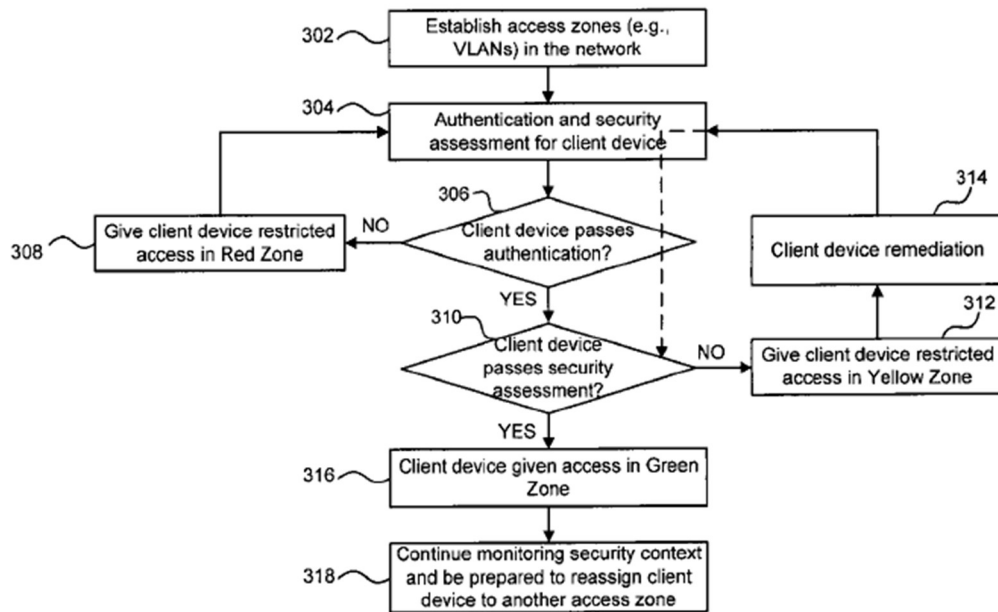
141. Accordingly, Loza in view of Bansal and Dupont disclosed or rendered obvious these claims.

B. Ground 2: Loza with Bansal, Dupont, Bareket, and Sahay Renders Claims 5, 7, 10, and 15 Obvious

142. In my opinion, Loza in view of Bansal, Dupont, Bareket, and Sahay renders claims 5, 7, 10, and 15 obvious.

1. Sahay

143. Sahay disclosed a technique for providing secure network access by establishing a plurality of access zones in a network, in which client devices assigned to different access zones have different access privileges and are isolated from one another. Ex-1008, Abstract, Fig. 3 (reproduced below).



144. A client device is assigned to one of the access zones based on an assessment of a security context associated with the device and its connection to the network. *Id.*, Abstract. Sahay further disclosed that a client device may continue to be monitored for its security context after connecting, and that an access controller may reassign the client device to another access zone or VLAN based on one or more triggering events, including a change in the security context, a security violation by the client device, a security violation detected in the network, or an operator-initiated request to reassign the client device. *Id.*, 3:37-44.

2. Rationale to Combine Loza, Bansal, Dupont, and Bareket with Sahay

145. A POSITA would have found it obvious to modify the teachings of Loza, Bansal, Dupont, and Bareket with Sahay, as detailed below.

a. A POSITA Would Have Modified the Denial/Disconnection Response to Redirect Access to Another Remote Network

146. The Examiner found that the combined teaching of Loza, Bansal, and Dupont described denying access to the known network upon detecting an unsecure element and disconnecting the processing device from the known network upon later detecting an unsecure element during an established connection, together with providing the user a message following denial or disconnection. Ex-1002, 151-53. However, that combination did not specify that the message to the user requests the user to access the known network via another remote network, nor that mitigating the security issue includes connecting the processing device to another remote network. *Id.* Sahay closes that gap by disclosing that, upon a triggering event such as a security violation or a change in security context, the access controller reassigns the client device to another access zone or VLAN. *Id.*, 151-53 citing Ex-1008, 3:37-44. I agree with the Examiner.

147. The Examiner also stated it “would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to modify the combined teaching of Loza, Bansal, and Dupont using a method of prov[id]ing a message to a user requesting to access a known network via another network as taught by Sahay.” Ex-1002, 151-52. The stated rationale was that

“[s]uch modification helps reduce threat[s] to a known network by preventing access from a vulnerable remote network.” *Id.*, 152.

148. Although the Examiner did not refer to Bareket in his analysis of Sahay because the Examiner’s rejection based on Bareket was for a set of dependent claims that were moved into the independent claims via amendment *after* the Examiner’s multiple rejections. Still, a POSITA would have found it obvious to combine Sahay with Loza, Bansal, Dupont, and Bareket because combining Sahay’s access-zone/VLAN reassignment teaching with the VPN-based mitigation-and-reconnection mechanism disclosed by Bareket would have been a straightforward application of known techniques, each addressing the same underlying security gap—preventing continued or renewed access to the known network through a remote network shown to pose a security risk—using predictable means and yielding no more than the predictable result of a more secure, appropriately rerouted connection.

149. A POSITA would have had reason to incorporate Bareket’s automatic VPN-initiation teaching into the combined Loza-Bansal-Dupont framework as the specific mitigation-and-reconnection mechanism, because doing so uses a well-known, readily available technique—establishing an encrypted VPN link—to make the renewed connection to the known network more secure than relying on the

unsecure remote network alone, which is precisely the security gap that Loza, Bansal, and Dupont are each independently concerned with closing.

3. Element-by-Element Analysis

- a. **5, 15: ...upon denying access to the known network by the processing device, providing a message to a user of the processing device requesting the user to access the known network via another remote network.**

150. Loza in view of Bansal, Dupont, and Sahay disclosed or rendered obvious these claims.

151. The Examiner found that Loza disclosed the first half of this limitation (“upon denying access...requesting the user to”) by disclosing that “the present invention can be used as a trigger to provide a message to a user to download and properly install a particular security measure on the remote machine, as directed by a corporate IT policy etc.” which “would enable an IT administrator to set a policy, so as to automatically prevent access further into a network until the security measure is installed and working on the remote machine.” Ex-1002, 151 citing Ex-1005, ¶0053. I agree with the Examiner.

152. The Examiner found that Sahay disclosed the second half of this limitation (“access the known network via another remote network”) by disclosing that “the access controller may reassign the client device to another access zone or VLAN based on one or more triggering events” that may include “a change in

security context, security violation by the client device, a security violation detected in the network, and an operator-initiated request to reassign the client device.” Ex-1002, 151 citing Ex-1008, 3:37-44. I agree with the Examiner.

153. The Examiner also stated that it would have been obvious to a POSITA “to modify the combined teaching of Loza, Bansal and Dupont using a method of proving a message to a user requesting to access a known network via another network as taught by Sahay” to “help[] reduce threat[s] to a known network by preventing access from a vulnerable remote network.” Ex-1002, 151-52. I agree with the Examiner.

154. Accordingly, Loza in view of Bansal, Dupont, and Sahay disclosed or rendered obvious these claims.

b. 7: ...wherein mitigating the security issue of the unsecure network element includes connecting, by the processing device, the processing device to another remote network.

155. Loza in view of Bansal, Dupont, and Sahay disclosed or rendered obvious this claim.

156. The Examiner found that Sahay disclosed this claim by disclosing that “the access controller may reassign the client device to another access zone or VLAN based on one or more triggering events” such as “a change in security context, security violation by the client device, a security violation detected in the network,

and an operator-initiated request to reassign the client device.” Ex-1002, 152 citing Ex-1008, 3:37-44. I agree with the Examiner.

157. The Examiner also stated that it would have been obvious to a POSITA “to modify the combined teaching of Loza, Bansal and Dupont using a method of proving a message to a user requesting to access a known network via another network as taught by Sahay” to “help[] reduce threat[s] to a known network by preventing access from a vulnerable remote network.” Ex-1002, 152. I agree with the Examiner.

158. Accordingly, Loza in view of Bansal, Dupont, and Sahay disclosed or rendered obvious this claim.

- c. **10: ...upon disconnecting the processing device from the known network by the processing device, providing a message to a user of the processing device requesting the user to access the known network via another remote network.**

159. Loza in view of Bansal, Dupont, and Sahay disclosed or rendered obvious this claim.

160. The Examiner found that Loza disclosed the first half of this claim (“upon disconnecting...to a user of the processing device”) by disclosing that “the present invention can be used as a trigger to provide a message to a user to download and properly install a particular security measure on the remote machine, as directed

by a corporate IT policy etc.” which “would enable an IT administrator to set a policy, so as to automatically prevent access further into a network until the security measure is installed and working on the remote machine.” Ex-1002, 153 citing Ex-1005, ¶0053. I agree with the Examiner.

161. The Examiner found that Sahay disclosed the second half of this limitation (“access the known network via another remote network”) by disclosing that “the access controller may reassign the client device to another access zone or VLAN based on one or more triggering events” that may include “a change in security context, security violation by the client device, a security violation detected in the network, and an operator-initiated request to reassign the client device.” Ex-1002, 153 citing Ex-1008, 3:37-44. I agree with the Examiner.

162. The Examiner also stated that it would have been obvious to a POSITA “to modify the combined teaching of Loza, Bansal and Dupont using a method of proving a message to a user requesting to access a known network via another network as taught by Sahay” to “help[] reduce threat[s] to a known network by preventing access from a vulnerable remote network.” Ex-1002, 153.

163. Accordingly, Loza in view of Bansal, Dupont, and Sahay disclosed or rendered obvious this claim.

C. Ground 3: Mishaev with Schwartz Renders Claims 1-18 Obvious

164. Other prior art beyond that which was in front of the Office, including Mishaev and Schwartz, only further confirm my opinion that the claimed concepts were well-known before the priority date of the '902 patent.

1. Mishaev

165. Like the '902 patent, Mishaev taught an “apparatus and method of remote access computer security” targeted towards the “many enterprises t[hat] allow a mobile workforce to remotely access protected enterprise computing services” and the simultaneous “growing number of sophisticated cyber attacks that [have] targeted organizational computing resources and cloud services.” *Compare* Ex-1009, ¶0001-05, *with* Ex-1001, 2:21-56. Fig. 1B is reproduced and annotated below:

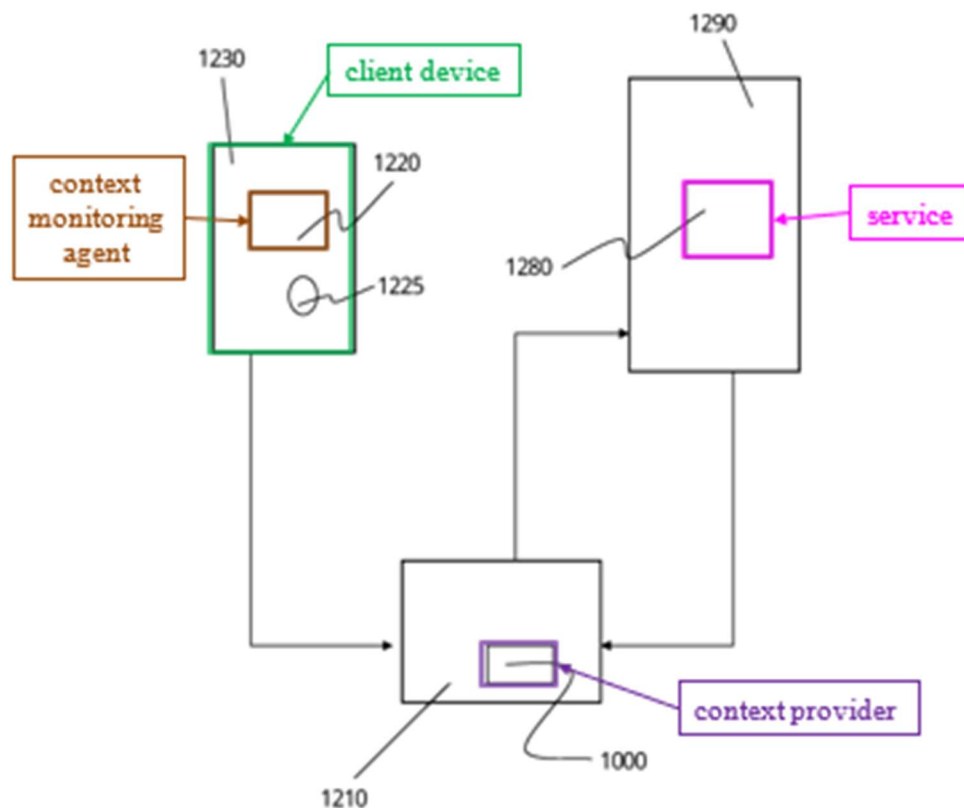


Fig. 1B

Ex-1009, ¶0105, Fig. 1B (annotated).

166. Fig. 1B depicts the arrangement of devices in a typical telework setting: a “client device” (green)—e.g., “an employee’s smart phone or laptop”—remotely accessing a “service” (pink)—e.g., “an organization’s computing resource (say a database or a cloud service account)” —via an undepicted “network.” Ex-1009, ¶0119-20, 0081. The client device connects to the network at the network’s “access point.” *Id.*, ¶¶0140, 0166. This access point can be “a public access point of a restaurant or bar,” as opposed to “an access point operated by [the] organization.”

Id., ¶¶0103-04, 0150-53 (describing a client device connecting to a public access point whose service set identifier (“SSID”) is “:Dragon Bar—Free”).

167. Mishaev taught that, whenever the client device’s user attempts to login and establish a “session” with an organization’s service, the attempt is “redirect[ed]” from the client device to a “context provider”² (purple), and a connection to this context provider is established via, e.g., “an SSL (Secure Sockets Layer)” interchangeably refers to this context provider as an “apparatus 1000.” *Id.*, ¶0126, ¶¶0119-20, ¶¶0186-87, ¶0190. Although Fig. 1B depicts the context provider and service as being physically separate, the context provider may nonetheless be controlled by the organization and implemented as a part of the organization’s service. *See id.*, ¶¶0043-44, ¶0109, ¶0132. In particular, the context provider decides whether to allow or block the client device’s login attempt, place limits on the user’s

² Mishaev interchangeably refers to this context provider as an “apparatus 1000.” Ex-1009, ¶0106. Mishaev also explained that the teachings over each of its other figures apply to Fig. 1B’s depicted context provider/apparatus 1000. *E.g.*, Ex-1009, ¶0100 (“[T]he parts of the apparatus 1000 carry out the steps of the exemplary method illustrated using FIG. 2 hereinbelow....”), ¶¶0185-93 (explaining how the “context provider (i.e., apparatus 1000)” performs the steps illustrated in Fig. 3).

access, and/or take other varying degrees of user-access-related actions “as known in the art” by weighing relevant data requested and received from the client device, including in part: (1) “data on the user,” (2) “data on the device used by the user,” and (3) “data on the network used by the user.” Ex-1009, ¶¶0156-57, ¶0081, ¶¶0187-91.

168. As Mishaev explained, the “data on the user” includes a “username, password, or biometric data provided by the user on the client device.” *Id.*, ¶0098. The context provider uses this data to “authenticate[]” the user and client device using any of the authentication techniques “known in the art.” *Id.*, ¶¶0098-99, ¶¶0123-25.

169. The “data on the device” includes data indicating, e.g., the installation of a “context monitoring agent”³ (brown) on the client device as depicted in Fig. 1B. *Id.*, ¶¶0087-90, ¶0110, ¶0137-39, ¶0259. This data is used in addition to the data on the user when authenticating the user and client device, which “further increases confidence in the security of the established session between the user’s device and

³ Mishaev also referred to the context monitoring agent as a “client application 1220” and explained that its related teachings likewise apply across all figures. Ex-1009, ¶0110, ¶0164, ¶0187, ¶0215.

the service.” *Id.*, ¶¶0123-26 (item numbering omitted). For instance, using the context provider, the organization “download[s] and install[s]” the context monitoring agent onto the client device and uses this installation as a “prerequisite for the remote access” such that, if the client device does not produce a “digital certificate that indicates installation of the context monitoring agent” upon request, then “the user is not allowed access to the [organization’s] service.” *Id.*, ¶0173, ¶¶0187-91.

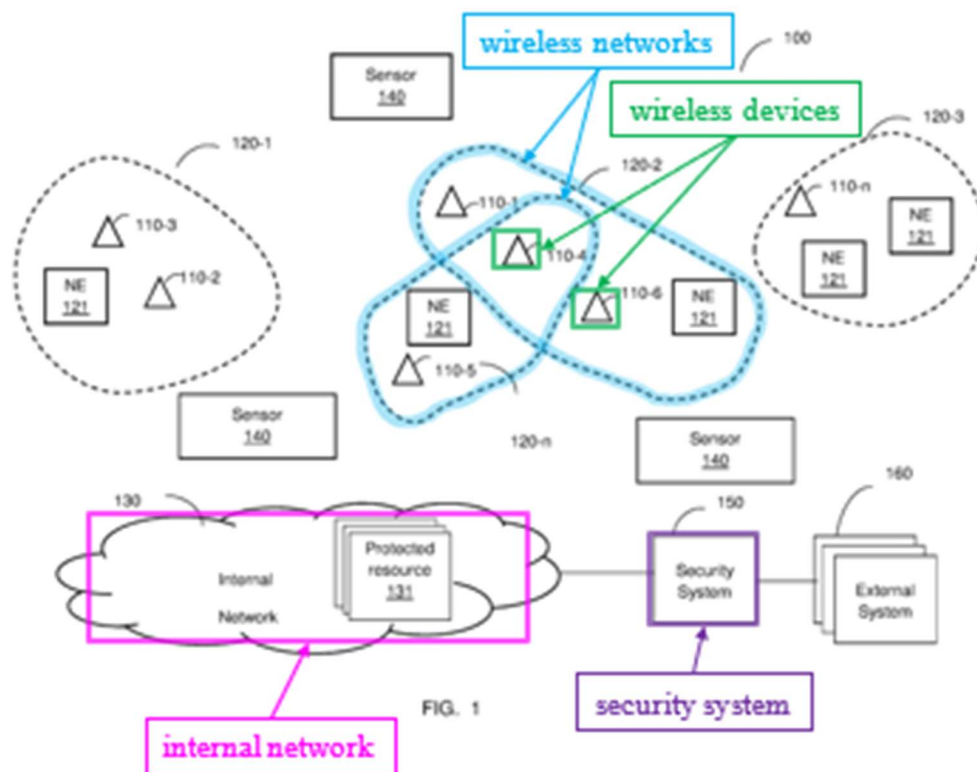
170. Finally, the “data on the network” includes data “identifying the access point that the user’s client device is connected to” as well as other access points. *Id.*, ¶0059, ¶0140. It also include data indicating whether each access point’s network is “malicious” or should otherwise be deemed “risky,” which the client device determines using the discussed context monitoring agent. *Id.*, ¶0059, ¶¶0166-67. Mishaev lists several examples for how this determination on the network’s security is done; however, as Mishaev makes clear, the context monitoring agent can use any technique “as known in the art” to determine the security of the network being used for access. *Id.*, ¶0167.

171. After this security determination’s result is sent from the context monitoring agent to the context provider, the context provider weighs this with the other data received from the client device to make the discussed decision of, e.g.,

whether to “block or allow the user’s attempt to login into the service,” and/or whether less restrictive user-related-actions should be taken. *Id.*, ¶¶0075-78, ¶0081, ¶0127, ¶¶0156-57, ¶¶0073-74 (explaining how data on an exemplary whitelisted “:CORO-001’ access point” would be signaled by the context monitoring agent as “:Allowable” and access would be granted to the client device accordingly, though limited based on the data on the device indicating a “:Jail Broken” status).

172. Lastly, Mishaev explained that, even after access is granted and the network connection between the client device and the service is established, the context provider “continues to monitor the connection...throughout the time period of the connection,” such as by having the context monitoring agent “repeat[] periodically” the security determination on the network. *Id.*, ¶0192, ¶¶0180-82, ¶0257. “An organization may thus be able to dynamically monitor, condition, and control remote access to [its] services...in a continuous or nearly continuous manner.” *Id.*, ¶0102, ¶0038. For instance, “during the service’[s] use by the user” and weighing “new data on the user, client device, [and] network” received from the client device, the context provider continuously decides whether to “disconnect the user from the service” using, e.g., “SLO (Single Logout),” which ends the session and thus requires a new login by the client device’s user. *Id.*, ¶0038, ¶¶0075-78, ¶¶0100-02, ¶0157, ¶192.

2. Schwartz



174. Figure 1 depicts a teleworking arrangement that, though slightly expanded in comparison to Mishaeu, includes the same devices of a typical teleworking arrangement.

175. Figure 1 depicts several “wireless devices” (green)—e.g., “a laptop, a PC, a smartphone, an Internet of Things (IoT) device,” or any other wireless-capable device. *Id.*, 4:5-11. Each wireless device is connected to one or more “wireless networks” (blue) that may contain other wireless devices, along with network elements (unannotated). *See id.*, 3:50-64, 5:39-44, 6:21-26 (explaining that a wireless network can be a “Wi-Fi network,” which wireless devices can connect to at the network’s “access point”), Figs. 1-2.

176. Using such a wireless network, a wireless device may be able to access a separate “internal network [(pink)] of an organization.” *See id.*, 3:65-4:3 (explaining that the internal network in Fig. 1 can include “protected resources” (unannotated)), 5:47-55 (explaining that a wireless network can connect to an internal network to access its protected resources), 9:27-36 (describing Fig. 3 as depicting such a protected resource being “communicatively coupled via a wireless network” to a wireless device), 5:66-6:11 (explaining that the wireless network can be “not part of,” and thus external to, “the IT infrastructure of the organization”).

177. Further, like Mishaev, Schwartz taught that wireless networks can potentially be “malicious” or otherwise be deemed “vulnerable.” *Compare* Ex-1010, 5:66-6:5, 11:17-27, *with* Ex-1009, ¶0059, ¶0167. And like the context monitoring agent of Mishaev’s client device, Schwartz’s wireless device determines whether the

connected wireless network is vulnerable using a “software application installed on the wireless device,” which Schwartz calls an “agent sensor.” *Compare* Ex-1010, 10:5-7, 4:56-5:15, 9:54-65, 11:4-27, 12:27-53, *with* Ex-1009, ¶¶0059, ¶¶0166-67.

178. Schwartz, however, described certain security determination techniques not discussed in detail in Mishaev, including by determining whether any “malicious devices” or “unknown device[s]” are or have been connected to the wireless network. Ex-1010, 11:4-53, 6:33-7:31, 5:39-6:9, 11:57-59 (explaining that the agent sensor can “probe other wireless devices communicatively connected with the wireless device”). Malicious devices include “unintentionally unsecured devices such as the Amazon Echo® (which automatically records and uploads audio)” and other IoT devices. *Id.*, 11:49-53. Unknown devices are devices not “authorized to access the internal network” as determined by, “e.g., an active directory of the organization” and may likewise include IoT devices. *Id.*, 6:33-7:3, 7:31-36 (explaining difference between an authorized wireless device, such as a “smartphone” or “laptop...of an employee of the organization,” and an “unknown device,” such as a generic “smart-watch”). If the agent sensor determines that a wireless network has been connected to such malicious or unknown devices, then the wireless network may thus be deemed “vulnerable”; otherwise, a wireless network determined as containing only authorized, “legitimate” devices may be

considered “safe” to use. *Id.*, 5:66-6:11, 7:4-42. Other criteria may also be considered, and a specific “risk factor” or “risk score” for the network may be assigned or adjusted accordingly. *See, e.g., id.*, 6:12-32 (“The risk factor is based on, for example, the type of detected vulnerability, the internal resources being accessed, the type of data being exploited, a device type, a connection type, any combination thereof, and so on.”), 8:66-9:10 (describing “low, medium, high” risk factors and scores).

179. Based on the security determination by the agent sensor, a “security system” (purple) of the organization decides—as similar to Mishaev’s context provider—whether and which user-access-related “mitigation actions” should be performed in response to the wireless device’s attempted or existing access to the organization’s internal network. *Compare* Ex-1010, 4:56-5:55, 15:64-16:4, 6:19-32, *with* Ex-1009, ¶¶0075-78, ¶0081, ¶0127, ¶0156-57. *See also* Ex-1010, 9:8-10 (“[A] decision to perform a mitigation action is based on the determined risk score.”). Schwartz taught that these security-based mitigation decisions can be made by the security system and the agent sensor itself “under the control of the security system.” Ex-1010, 4:56-5:22, 9:54-10:4, 13:17-22. For instance, like Mishaev’s context provider and Schwartz’s security system, and indeed as “control[led]” by the latter, Schwartz’s agent sensor can decide—based on a wireless network being

determined as “vulnerable” and its associated “risk factor” or “risk score”—that any “traffic” from the wireless device should be “mitigate[d]” and “block[ed],” that such traffic should be forced to “be transmitted through a secure connection,” that any “active connections” should be “disconnect[ed],” and/or even that the wireless device should be completely “block[ed]...from connecting to [the wireless] network.” *Compare* Ex-1010, 4:56-5:22, 6:12-32, 8:66-9:10, 15:64-16:4, 13:17-37, 9:54-10:4, *with* Ex-1009, ¶¶0127, ¶¶0075-78, ¶¶0137-39. *See also* Ex-1010, 13:27-35 (explaining that the agent sensor can perform “combinations” of these known mitigation actions).

180. In fact, Schwartz disclosed that, although not required, there may even be other devices in a particular teleworking arrangement that can make such mitigation decisions. Ex-1010, 14:49-61, 4:56-67, 13:17-37. In particular, Schwartz disclosed two categories of such other devices: “out-of-band device[s],” such as unannotated “sensors 140” depicted in Fig. 1 above that exist outside of the wireless network containing the wireless device; and in-network (i.e., in-band) devices located within the wireless network, such as those depicted in Fig. 3:

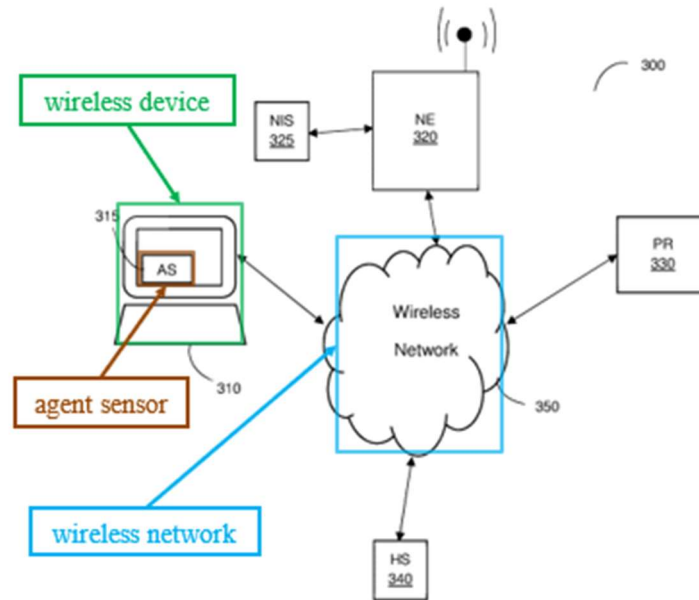


FIG. 3

Ex-1010, 4:23-29, 5:6-22, 9:27-46, 14:49-61, Fig. 3 (annotated); Ex-1017, 350 (explaining difference between “out-of-band” and “in-band” channels).

181. As shown, in addition to the agent sensor (brown) installed on the wireless device (green), the wireless network (blue) also connects to two separate in-band sensors (unannotated): a standalone “hardware sensor 340,” and a network-element-integrated “network infrastructure sensor 325,” each of which can also “independently or collectively” make the mitigation decisions as I discussed. Ex-1010, 14:49-61. However, as Schwartz explained, these other sensors are optional—i.e., a teleworking arrangement need not include such other sensors in order for Schwartz’s teachings to apply. *Id.*, 13:61-14:19.

3. Rationale to Combine Mishaev with Schwartz

182. A POSITA would have found it obvious to modify Mishaev using the teachings of Schwartz as detailed below.

a. A POSITA Would Have Used Schwartz's Security Determinations in Mishaev

183. Mishaev taught that the organization-provided “context monitoring agent” installed on the “client device” determines—both before and continuously after logging in for each session of access with an organization’s “service”—whether the network used for the access is “malicious” or otherwise “risky.” Ex-1009, ¶¶0110, ¶¶0166-67, ¶0081, ¶¶0180-82, ¶0126. To perform such security determinations, the context monitoring agent may use any technique “as known in the art” to achieve this function. *Id.*, ¶0167. Thus, Mishaev contained an explicit suggestion to use known techniques for determining the security of a network.

184. Such applicable, known techniques are described in Schwartz. For instance, Schwartz taught that, in a teleworking arrangement like that described in Mishaev, an “agent sensor” similarly installed on a “wireless device” likewise determines whether a “wireless network” is “malicious” or otherwise “vulnerable,” but it does so more specifically based on criteria such as whether a “malicious” or “unknown device” is also connected. Ex-1010, 9:54-65, 10:5-7, 11:4-59, 5:39-6:9, 6:63-7:53. “Malicious devices” include “unintentionally unsecured devices,”

whereas “unknown devices” are devices that are not “authorized” to access an internal network. *Id.*, 11:49-53, 6:33-7:3. These devices include, for example, IoT devices. *Id.*, 7:31-53, 11:49-53. Other criteria that may be considered include, e.g., “connection type” between the client device and wireless network (e.g., “Wi-Fi,” “Bluetooth®,” “Zigbee”) and “sensitivity” of data being transmitted or accessed (e.g., “sensitive or not sensitive”), which, combined, determine an overall “risk factor” or “risk score” for the wireless network’s vulnerability (e.g., “low, medium, high”). *Id.*, 6:12-32, 4:12-22, 14:62-67, 11:14-40, 8:66-9:10.

185. In my opinion, a POSITA would have been motivated to modify Mishaev’s client device so that it performs known techniques—including those taught in Schwartz—for determining a network’s security, since Mishaev explicitly suggested doing so. Ex-1009, ¶0167. But even without this explicit invitation, a POSITA would have still been motivated to make this modification because Schwartz’s techniques achieve the exact function of determining the security of a network that Mishaev expressly requires. *See id.*, ¶0167; Ex-1010, 11:4-53, 6:33-7:53. And since Schwartz taught performing these techniques in a device otherwise identical to Mishaev’s client device within the same setting of telework, a POSITA would have had no difficulty modifying Mishaev’s client device to perform Schwartz’s techniques as directly taught and would have had a reasonable

expectation of success in doing so. *Compare, e.g.,* Ex-1009, ¶0043, *with* Ex-1010, 4:5-11.

186. Accordingly, to determine the security of a network both before and continuously after logging in for each session of access with an organization's service, Mishaev-Schwartz—specifically, the context monitoring agent installed on the client device taught in Mishaev—determines whether malicious or unknown devices are or have been connected to the network as taught in Schwartz. If any are identified, then the network may be deemed risky; if not, then the network may be determined allowable for use. *Id.* In making such security determinations, the context monitoring agent also considers other factors, including the type of connection with the network and the sensitivity of data being transmitted or accessed by the client device, and assigns or adjusts a risk factor/score of the network accordingly. *Id.*

b. A POSITA Would Have Modified Mishaev's Client Device to Make Mitigation Decisions

187. In my opinion, a POSITA would have found it obvious to further modify Mishaev such that the client device's context monitoring agent also—and not just the context provider—decides whether to take user-access-related mitigation actions based on the discussed security determinations, including whether to block or allow its attempt to access the organization's service over the network, whether

any subsequent traffic over the network is to be transmitted through a secure connection, whether to disconnect or continue any existing access, whether or not its connection with the network should be completely blocked, and whether to perform other known mitigation actions. First, a POSITA would have recognized that, in a teleworking arrangement like in Mishaev's Fig. 1B, the context provider need not be the sole device to decide whether, e.g., the client device's attempted/existing access to the service should be blocked/disconnected or allowed/continued. Rather, as I explain below, a small and known number of other devices could also perform these mitigation actions—and, indeed, the prior art acknowledges as much—such that a POSITA would have found it obvious to try utilizing any such devices for performing the discussed mitigation actions, including a combined use of both the context provider and client device. And second, a POSITA would have sought such an implementation for, e.g., increased security, as I also explain below.

188. First, a POSITA would have recognized, when presented with Mishaev's teleworking arrangement depicted in its Fig. 1B, that there was not just one but, rather, several devices able to make the discussed decisions of, e.g., whether to block the client device's login attempt, logout of any established session between the client device and service, and/or take any other user-access-related actions as

known in the art. *See* Ex-1009, ¶¶0156-57, ¶¶0075-78. As I explained earlier, Mishaev taught that, in its Fig. 1B's teleworking arrangement, after receiving the client device's login attempt and weighing the relevant data on the user, device, and network, the context provider decides whether and which action should be taken regarding the client device's access to the service. *Id.*, ¶¶0119-20, ¶0127, ¶0186-87. Such is similarly taught in Schwartz: that, in the same technological setting of a teleworking arrangement, and based on similar data gathered by the agent sensor, the "security system" decides whether or not to block a wireless device's traffic to an organization's internal network, disconnect any active connection to that internal network, and/or perform other user-access-related "mitigation actions" and "the like." Ex-1010, 15:40-16:4, 6:19-32.

189. Schwartz, however, additionally taught that the wireless device itself also has the capability to make these same mitigation decisions "under the control of the security system" using the agent sensor and its gathered data. *Id.*, 4:56-5:20. Such disclosure demonstrates that a POSITA would have known—or otherwise garnered from Schwartz—that Mishaev's client device likewise was modifiable to make the same or similar type of user-access-related mitigation decisions as the context provider while under the control of the same. *See, e.g.*, Ex-1005, Fig. F, ¶¶0040-42, (explaining that an "agent" installed in a "Remote/Mobile" device can

“prevent [itself] to establish any network connection” with a “server” based on “its built-in scanner (S)” determining the “security of its own external network connectivity”).

190. In other words, presented with the particular teleworking arrangement depicted in Mishaev’s Fig. 1B, a POSITA would have recognized that Mishaev’s teleworking arrangement could have either the context provider or the client device (as controlled by the context provider) perform the discussed mitigation actions. Either: (1) the context provider could directly decide on the client device’s login attempt and any continuing access as originally done in Mishaev; or (2) the client device, as controlled by the context provider, could decide, e.g., whether any “traffic” from the client device (such as the login attempt and corresponding data on the user, client device, and network to be sent to the context provider) is to be “mitigate[d]” and “block[ed],” whether that traffic should “be transmitted through a secure connection,” whether any “active connection[.]” with the service should be “disconnect[ed],” and/or whether to completely “block[.]” the client device “from connecting to [the] network,” based on whether the network was determined as vulnerable and its assigned risk factor/score as done in Schwartz. Ex-1010, 4:56-5:22, 15:64-16:4, 13:17-37, 9:54-10:4, 6:12-18, 8:66-9:10; Ex-1009, ¶¶0075-78, ¶0127, ¶¶0137-39, ¶¶0192-93.

191. But even further, a POSITA would also have recognized that a third option also existed in Mishaev's Fig. 1B: combining both options (1) and (2) above such that both the context provider and client device make the discussed mitigation decisions. Indeed, Schwartz taught that not just one but multiple devices—including both the security system and the wireless device via its agent sensor—can each make the discussed mitigation decisions in a teleworking arrangement. *See* Ex-1010, 14:49-61, 13:61-14:19, Fig. 1 (depicting a teleworking arrangement with multiple “sensors 140” being controlled by a security system, in addition to the security system itself). But even with the possibility of such combined use, there still remains—particularly in Mishaev's Fig. 1B—only a limited number of different possible implementations that a POSITA could try, such that having both Mishaev's context provider and client device (under the control of the former) decide whether to block or allow the client device's access attempt and/or make other such user-access-related-mitigation decisions would have been not the result of innovation but of ordinary skill and common sense.

192. Second, a POSITA not only could have but would have been motivated to give both the context provider and client device the capability to make the discussed mitigation decisions, as such would have delivered recognizable, known benefits, including improving security coverage. As Schwartz taught, by having

multiple devices and sensors at different network locations making their own mitigation decisions under the control of the security system, a wireless device thus “can be probed and interrogated differently by different sensors...based on [each sensor’s] capabilities,” which thereby expands the security coverage beyond what just one device or sensor alone could achieve. *See* Ex-1010, 12:10-17, 4:56-5:30 (explaining that the security system may perform its mitigation decisions using its own “sensor” that is “integrated,” “installed,” or “embedded in the security system”); Ex-1017, 226 (recommending that organizations adopt a “defense-in-depth approach”—i.e., “strategically allocat[ing] security and privacy controls in the security and privacy architectures so that adversaries must overcome multiple controls to achieve their objective”—because this increases both “the work factor of the adversary” and “the likelihood of detection”). Moreover, as a POSITA would have also recognized, giving mitigation-decision-making capability to both Mishae’s context provider and client device would have also increased reliability by allowing one device to continue making mitigation decisions and provide protection of the organization’s service if the other fails or is taken over by an adversary. *See* Ex-1017, 294 (explaining that defense-in-depth also “allow[s] the system to continue in a secure state even when one mechanism has failed”).

193. Finally, a POSITA would have had a reasonable expectation of success in making these discussed modifications to Mishaev’s client device. As Schwartz taught, the “agent sensor” that makes the discussed mitigation decisions can be “implemented as a software application installed on [a] wireless device” such as “a laptop” or other similar device. Ex-1010, 10:5-17. Mishaev’s client device—being also “a laptop computer, etc.”—would have likewise been easily programmed with such mitigation-decision-making software-functionality, especially given that it already has installed on it an otherwise similar “context monitoring agent” application. *See* Ex-1009, ¶¶0043, ¶¶0110, ¶¶0171-73.

194. Accordingly, in Mishaev-Schwartz, the context monitoring agent of Mishaev’s client device—like Schwartz’s agent sensor—decides whether and which user-access-related mitigation actions should be taken by the context monitoring agent of based on whether the network is determined as vulnerable and the network’s assigned risk factor/score. Such is decided in addition to the context provider making its own mitigation decisions independently.

4. Element-by-Element Analysis

- a. 1[pre], 11[pre], 14[pre]: A method for reducing network threats, the method comprising/A system comprising: one or more processing resources; a non-transitory computer-readable medium couple to one or more processing resources, wherein the non-transitory computer-readable medium has store thereon**

instructions that when executed by one or more processing resources cause the one or more processing resources to/A non-transitory computer-readable storage medium embodying a set of instructions, which when executed by one or more processing resources of a computer system, causes the one or more processing resources to perform a method comprising:

195. If the preamble is limiting, Mishaev-Schwartz includes Mishaev's "client device" that performs the steps I describe below in Sections VII.C.4.b-VII.C.4.g (collectively, 1[pre]'s "method"). The client device is, e.g., "an employee's smart phone or laptop," which a POSITA would have understood as necessarily including at least a general-purpose processor (11[pre]/14[pre]'s "processing resource") and memory storing instructions for the processor to perform to the discussed steps (11[pre]/14[pre]'s "medium" and "instructions"). Ex-1009, ¶¶0132, ¶0043, ¶0110-17 (describing a "context monitoring agent" application being "install[ed]" on the client device); Ex-1001, 11:28-46 (explaining that a "processing resource" includes a general-purpose processor). Such steps allow an organization to control access by the client device to the organization's "service," thereby reducing "threats" and "cyber attacks" on the latter. Ex-1009, ¶¶0023-25; Ex-1010, 1:7-2:27.

196. Accordingly, Mishaev-Schwartz disclosed or rendered obvious these limitations.

b. 1[a], 11[a], 14[a]: receiving, by a processing device, a request to access a known network from a known access device connected through a remote network,

197. Mishaev taught that the client device (“known access device”) connects to a “network” at the network’s “access point” to “remote[ly] access” the organization’s service, which includes the “organization’s computing resource[s] (say a database or a cloud service account)” (“known network”). Ex-1009, ¶¶0119-20, ¶0140, ¶0081, ¶0166; Ex-1001, 7:41-59 (explaining that a “known network” may include “network accessible resource(s)” such as “databases”). The access point can be “a public access point of a restaurant or bar”—in contrast to “an access point operated by [the] organization”—which would thus meet the claimed “remote network.” Ex-1009, ¶¶0103-04; Ex-1001, 3:4-8 (describing a “remote network” as being a network that is “not controlled by the entity that is responsible for the security of the known network”).

198. Before the start of each session with the service, “the user attempts to login” and provides the client device with related data including a “username, password, or biometric data,” any of which meets the claimed “receiving, by a processing device, a request....” Ex-1009, ¶¶0119-20, ¶0098, ¶0126; Ex-1001, 12:57-64 (explaining that “determin[ing] whether a request to access a known

network is received” can be the result of the known access device “detect[ing]” the “preparing [of] an authorization credential”).

199. Lastly, to carry out each of these functions, a POSITA would have understood that the client device—being, e.g., a “laptop”—includes the discussed processor, memory, and any other components needed to perform the functions described hereinbelow (collectively, “processing device”). *See* Ex-1009, ¶¶0132, ¶0043.

200. Accordingly, Mishaev-Schwartz disclosed or rendered obvious these limitations.

- c. **1[b], 11[b], 14[b]: wherein the known network is a private network that authorizes credentials associated with the known access device, and the remote network is external to the known network;**

201. Mishaev taught that the organization implements a “context provider” as part of its service to “control[] the user’s remote access.” Ex-1009, ¶¶0119-20, 0043-44, 0132. In particular, the context provider decides whether to block or allow the client device’s attempt to access to the service and whether to perform other known user-access-related actions by weighing data it receives from the client device, including in part “data on the user” and “data on the device used by the user.” *Id.*, ¶¶0081, ¶0119.

202. The “data on the user” includes the “username, password, or biometric data provided earlier by the user on the client device” I discussed above. *Id.*, ¶¶0098. The “data on the device” includes data that indicates, e.g., whether an organization-provided “context monitoring agent” application is installed on the client device. *Id.*, ¶¶0087-90, ¶¶0173, ¶¶0259. As part of making the discussed user-access-related decisions, the context provider uses both data types to “authenticate[]” the user and client device, and thus either of such data from the client device meets the claimed “credentials associated with access device.” *Id.*, ¶¶0098-99, ¶¶0123-27.

203. As I noted, Mishaev taught that the context provider may be used by a specific organization and implemented as a part of its service. *Id.*, ¶¶0043-44, ¶¶0109, ¶¶0132. In such a scenario, the context provider—by being part of the organization’s service—thus forms part of a “known network [that] is a private network that authorizes” said credentials as claimed. *See id.*, ¶¶0043-44, ¶¶0132, ¶¶0123 (describing the aforementioned authentication as being part of an “authorization process”).

204. Lastly, as I discussed, the client-device-connected access point may be “public,” in contrast to being “operated by [the] organization.” *Id.*, ¶¶0103-04. Such a public access point would thus meet a “remote network [that] is external to the known network” as claimed. *See* Ex-1001, 3:4-10 (defining “remote network” as “a

network that includes one or more elements that are: not known to, not governed by, and/or not controlled by the entity that is responsible for the known network”).

205. Accordingly, Mishaev-Schwartz disclosed or rendered obvious these limitations.

- d. 1[c], 11[c], 14[c]: scanning, by the processing device of the known access device, the remote network through which access to the known network is to be established, wherein the scanning is configured to identify an unsecure network element on the remote network;**

206. Mishaev taught that the discussed user-access-related decisions additionally weigh “data on the network used by the user,” including data indicating whether the discussed public access point’s network is “malicious” or otherwise “risky.” Ex-1009, ¶¶0081, ¶0059, ¶¶0166-67. To determine such security of this network, Mishaev’s client device has installed on it a “context monitoring agent” application, which Mishaev-Schwartz, as I discussed above in Section VII.C.3.a, utilizes known network-security-determination techniques, including those taught in Schwartz. *See id.*, ¶0167.

207. Specifically, the context monitoring agent determines, among other criteria, whether a “malicious” or “unknown device” is connected to the network being used to access the organization’s service. *See* Ex-1010, 9:54-65, 10:5-7, 11:4-59, 5:39-6:9, 6:63-7:53; *supra* Section VII.C.3.a. Either device meets the claimed

“unsecure network element on the remote network”: “malicious devices” include “unintentionally *unsecured* devices,” whereas “unknown devices” are not “authorized” by, “e.g., an active directory of the organization.” *See* Ex-1010, 11:49-53 (emphasis added), 6:33-7:3; Ex-1001, 13:32-43 (explaining that “unsecure network elements” may be elements “not considered acceptably secure” as “designated by a network administration of the known network”). If the context monitoring agent identifies any of these devices, then the network may be deemed risky; if not, then the network may be deemed allowable. *See* Ex-1010, 5:39-6:9, 7:31-53, 11:4-53; *supra* Section VII.C.3.a. And by determining whether such devices are on the network, the client device thus performs the claimed “scanning.” Ex-1010, 13:38-55 (referring to the discussed security determinations as “vulnerability *scans*” (emphasis added)).

208. Accordingly, Mishaev-Schwartz disclosed or rendered obvious these limitations.

- e. **1[d], 11[d], 14[d]: based at least in part on identifying at least one unsecure network element on the remote network, denying, by the processing device, access to the known network; and**

209. Mishaev taught that the client device’s login attempt for accessing the service may be “block[ed]” by the context provider, and that other known user-access-related actions may be taken, if the network of an access point—including

the above-discussed public access point—is deemed risky. *See* Ex-1009, ¶¶0119-20, ¶0081, ¶¶0156-57, ¶¶0166-67, ¶0150-53 (describing a client device’s access via a public “:Dragon Bar—Free” access point as “requir[ing] further clearance” due to being unknown to the organization), ¶0104 (explaining that a client device’s user “can no longer access” certain documents stored in the organization’s service if “the user switches to a public access point”). As I explained above, in Mishaev-Schwartz, such security determinations and resulting “mitigation actions” are performed by the context monitoring agent of Mishaev’s client device as well—ranging from “mitigat[ing]” and “blocking” any traffic, such as the client device’s login attempt and corresponding data on the user, device, and network, to completely blocking any connection to the network—based on the network being deemed vulnerable and the associated risk factor or score as taught in Schwartz. *See supra* Section VII.C.3. Accordingly, in Mishaev-Schwartz, the client device’s context monitoring agent “blocks” the client device’s login attempt and corresponding data from being sent to the context provider—thus denying any access to the organization’s service—if it identifies, e.g., that malicious or unknown devices are on the network, thereby meeting 1[d], 11[d], and 14[d]. *See* Ex-1010, 9:54-10:7, 5:39-6:9, 6:63-7:53, 11:4-59; Ex-1009, ¶¶0150-53; *supra* Section VII.C.3.

210. Accordingly, Mishaev-Schwartz disclosed or rendered obvious these limitations.

- f. **1[e], 11[e], 14[e]: based at least in part upon on failure to identify any unsecure network element on the remote network, requesting a grant of access from the known network to the processing device.**

211. On the other hand, Mishaev taught that, if the network—including the above-discussed public access point’s network—is instead determined to be allowable, then the context provider may refrain from taking any user-access-related actions by “allowing...the user’s login attempt,” so long as other criteria do not indicate otherwise. Ex-1009, ¶¶0119-20, ¶0104, ¶¶0073-74 (explaining that, by connecting to a “:CORO-001’ access point” deemed “:Allowable’,” access to the service may be granted, albeit limited based on the client device’s “:Jail Broken” status). And again, as I explained above, in Mishaev-Schwartz, these security determinations and user-access-related/mitigation decisions are made by both Mishaev’s context provider and client device. *See supra* Section VII.C.3.

212. For instance, like the context provider, the client device’s context monitoring agent may refrain from taking mitigating actions and thus “allow[]” the transmission of traffic—including the client device’s login attempt and corresponding data—if only authorized and “legitimate” devices are connected to the network and no other potential network vulnerability exists (the claimed “based

at least in part upon on failure to identify any unsecure network element on the remote network, requesting...”). (See Ex-1010, 5:66-6:11, 7:4-42, 4:56-67, 15:60-16:4; Ex-1009, ¶¶0119-20; *supra* Section VII.C.3.) This login attempt is then “redirect[ed]” to the context provider, which thereafter makes its own user-access-related decision on the login attempt by weighing the received data on the user, device, and network (the login attempt and corresponding data each thus being a “request [of] a grant of access from the known network to the processing device” as claimed). See Ex-1009, ¶¶0186-87, 0119-20; *supra* Section VII.C.3; Ex-1001, 8:67-9:3 (explaining that the known access device can present an “authorization credential” to the known network “as part of requesting access”); *supra* Section VII.C.4.c (explaining how data on the user and client device sent to the context provider are indeed such “credentials”).

213. Further, Mishaev taught that, by “redirect[ing]” the login attempt to the context provider in this manner, a connection from the client device to the context provider is established via, e.g., “an SSL (Secure Sockets Layer) connection and handshake.” Ex-1009, ¶¶0119-20, ¶¶0186-87. A POSITA would have understood that, in establishing such an SSL connection, the client device and context provider necessarily would have initially exchanged “SSL handshake” connection-setup messages beforehand, which likewise meets the claimed “requesting a grant of

access.” *See, e.g.*, Ex-1013, ¶¶0006-28 (explaining the exchange of “CLIENT-HELLO,” “SERVER-HELLO,” and other messages needed for establishing an SSL connection).

214. Lastly, Mishaev-Schwartz performs both “identifying at least one unsecure network element on the remote network[and] denying...” and 1[d]/11[d]/14[d]’s “fail[ing] to identify any unsecure network element on the remote network[and] requesting...” over two different login/logout sessions, like the ’902 patent. For example, the ’902 patent’s Fig. 2 is a flowchart showing “a method in accordance with various embodiments.” Ex-1001, 12:55-57. Block 214 depicts a binary choice: “whether any unsecure network elements are included in the remote network.” *Id.*, 13:52-55, Fig. 2. From there, it branches into two paths: one for “[w]here no unsecure network elements are included,” corresponding to 1[e]; the other for “where it is determined that unsecure network elements are included,” corresponding to 1[d]. Ex-1001, Fig. 2. *Compare* Ex-1001, 13:55-14:34, *with* Ex-1001, claim 1[d]-[e]. Both branches then remain separate, reconverging only after the method returns to the beginning login step of “determin[ing] whether a request to access a known network is received” corresponding to 1[a] for a new login/logout loop to begin. *See* Ex-1001, 12:57-64, Fig. 2, claims 1[a]/11[a]/14[a]. Indeed, before reconverging, both branches terminate with either no session being

established or an existing session being disconnected. Ex-1001, 14:7-23, 14:26-34, Fig. 2. The '902 patent's other figures are similar. *See* Ex-1001, Figs. 3-6.

215. Like the '902 patent, Mishaev-Schwartz performs both claimed steps over two sessions. For instance, after a session is established from the client device's login attempt described herein under 1[e]/11[e]/14[e], the client device may subsequently “disconnect[] [the] active connection” due to, e.g., a newly connected malicious or unknown device as I describe below in Section VII.C.4.o. *See* Ex-1009, ¶¶0157-58 (describing the context provider similarly forcing a “SLO (Single Logout)”); *supra* Section VII.C.3.b. Should a new login be attempted thereafter over the same network, such corresponding traffic from the client device would then be “mitigate[d]” and “block[ed]” by the context monitoring agent—at least until the malicious or unknown device is disconnected in, e.g., a third session—and thus satisfy 1[d]/11[d]/14[d] for the reasons I explained above in Section VII.C.4.e. Moreover, it would have been obvious to reattempt login after either the discussed logout or blocking of access, given such login is required for each access to the service. *E.g.*, Ex-1009, ¶0120. And a POSITA would not have expected a user whose access was denied or terminated to simply give up. The user of, e.g., an “employee's smart phone or laptop” who is logged out does not stop needing to work; the employee would, sooner or later, attempt to log in again to carry out his

or her job duties. *See, e.g.*, Ex-1009, ¶¶132-33. A POSITA would have found such a renewed attempt to be a matter of common sense.

216. Accordingly, Mishaev-Schwartz disclosed or rendered obvious these limitations.

- g. 1[f], 11[f], 14[f]: wherein mitigating a security issue of the unsecure network element includes starting, by the processing device, a virtual private network application, and wherein requesting the grant of access from the known network to the processing device is done over a virtual private network.**

217. In addition to the “mitigat[ing]” and “block[ing]” of the traffic discussed above and in Section VII.C.4.e, the context monitoring agent in Mishaev-Schwartz may also perform additional mitigation actions based on the connected malicious or unknown device and other relevant criteria, as described above in Section VII.C.3.b. As I discussed, this includes forcing such traffic to “be transmitted through a secure connection” as taught in Schwartz. Ex-1010, 13:27-37; *supra* Section VII.C.3.b.

218. Schwartz provided no further details about this “secure connection” nor restricts it to any one type of secure connection. In my opinion, such is to be expected, given that the establishment of secure connections and even very specific types of such connections is well known. In particular, as used in Schwartz, the term

“secure connection” would have been understood by a POSITA as including the conventional and well-established secure virtual private network (VPN) connection.

219. For instance, Durbin—filed three years earlier than Schwartz—acknowledged that wireless networks pose particular security issues. *Compare, e.g.*, Ex-1011, ¶0001 (“Generally, public wireless networks are unsecured and the user of such unsecured network is at a risk of getting hacked and lo[osing critical or important information.”), *with* Ex-1010, 1:22-27 (“The ever-increasing utilization of wireless devices and wireless networks poses a real threat to any organization, due to vulnerabilities of such devices[,],” including “interception or interference.”). Like Schwartz, Durbin identified the identical solution of “establish[ing] a **secure connection** on public wireless networks” while also further highlighting this as having been a known “area of interest” in the relevant field. Ex-1011, ¶0001 (emphasis added). Durbin then explained that, “[i]n particular,” this comprises “using advanced techniques such as secure **Virtual Private Network (VPN) connections**,” which “provide secure communication within public wireless networks” between, e.g., a “mobile device” and “information sensitive service center.” *Id.*, ¶0001 (emphasis added), ¶0026. Durbin thus not only explicitly defined VPN connections as a type of “secure connection” but described one such VPN connection as carrying out the exact function assigned to Schwartz’s secure

connection: providing the connection through which a device's traffic is transmitted. *Compare* Ex-1011, ¶0001, ¶0026, with Ex-1010, 13:27-37, 9:65-10:4 (explaining that the agent sensor's available mitigation actions include "initiating a secured communication protocol for transmitting information to and from the wireless device").

220. Other contemporaneous references further confirm that Schwartz's usage and description of a "secure connection" would have been understood as including VPN connections. *E.g.*, Ex-1015, 15 (explaining that a VPN provides "a secure remote access connection (tunnel) between a client device and the VPN gateway"); Ex-1016, 7 (defining a VPN as "provid[ing] a secure communications mechanism for data and control information transmitted between computers or networks"); Ex-1019, ¶0005, ¶¶0028-29 (describing an exemplary "secure connection" that routes network traffic to and from an endpoint device, over the Internet, and to and from a "VPN server"). Given such recognition in the art, a POSITA would have thus understood that, in Mishaev-Schwartz, the discussed transmitting of client-device traffic "through a secure connection" would have included, specifically, the context monitoring agent forcing said traffic "to be transmitted through a [VPN] connection" based on the aforementioned security determinations.

221. Forcing traffic through a VPN meets “wherein mitigating a security issue of the unsecure network element includes starting, by the processing device, a virtual private network application.” As the ’902 patent clarifies, such “starting” of a VPN “application” is met when a “VPN application is installed and running on the known access device and network traffic is being routed via the VPN application.” Ex-1001, 16:16-20, 17:39-43, Fig. 5. Mishaev-Schwartz’s client device meets both conditions. As Mishaev taught, the client device’s context monitoring agent is indeed a “client *application*.” Ex-1009, ¶0110 (emphasis added).

222. Again, that context monitoring agent in Mishaev-Schwartz forces the client device’s “traffic to be transmitted through a [VPN] connection.” Moreover, by forcing particularly the previously “mitigate[d]” and “block[ed]” login attempt and corresponding data from above and in Section VII.C.4.e to be transmitted through the VPN connection, the claimed “wherein requesting the grant of access...is done over a virtual private network” is likewise met.

223. Lastly, as I noted above in Section VII.C.3, whether and which mitigation actions should be taken by the context monitoring agent—including the discussed forced-transmitting of traffic “through a secured,” or VPN, “connection”—is decided in Mishaev-Schwartz based not only on whether a “malicious” or “unknown device” is connected to the network but also other criteria,

including, e.g., “connection type” to the network and “sensitivity” of data being transmitted or accessed, which, combined, determine the network’s overall risk factor/score. *See* Ex-1010, 6:12-32, 14:62-67, 11:14-40, 8:66-9:10. Thus, even when no “malicious” or “unknown” device is connected to the network, any login attempt and corresponding data that would otherwise be “allow[ed]” to be transmitted from the client device—e.g., as described above in Section VII.C.4.f—may nonetheless be forced “to be transmitted through a [VPN] connection” if such and other mitigation actions are so warranted, as based on other risk-factor/score considerations and criteria.

224. Accordingly, Mishaev-Schwartz disclosed or rendered obvious these limitations.

- h. 2, 12: ...wherein access by the processing device to the known network is granted upon a combination of the requesting a grant of access from the known network to the processing device and a correct authorization credential presented by the processing device to the known network.**

225. As I explained above in Section VII.C.4.f, the client device in Mishaev-Schwartz transmits various data to the context provider that, in doing so, meets the claimed “requesting a grant of access”: allowing the login attempt and sending corresponding data on the user, device, and network to the context provider; and as part of establishing the SSL connection with the context provider. Thereafter, the

context provider then performs its own mitigation decisions and, if none are taken, “authenticates” the user and client device using such received data (each of which thus meets the claimed “authorization credential”). Ex-1009, ¶¶0098-99, ¶¶0123-27; *supra* Section VII.C.4.c. Access to the service may be granted based on such data being satisfactory to the context provider, which thus meets the remaining requirements of claims 2 and 12. *See, e.g.*, Ex-1009, ¶0201, ¶¶0259-60 (explaining that the data on the device includes “a digital certificate that indicates installation of” the context monitoring agent, which may be “used as a prerequisite for the remote access”), ¶0098, ¶¶0205-06 (explaining that the context provider may “authenticate[]” the “data on the user,” which ultimately “authorizes...the user’s access to the service”).

226. Accordingly, Mishaev-Schwartz disclosed or rendered obvious these claims.

i. 3, 13: ...wherein the unsecure network element is an Internet of Things (IoT) device.

227. Schwartz explained that the discussed malicious and unknown devices may include IoT devices, such as a “smart-watch” and “Amazon Echo®.” Ex-1010, 7:31-53, 11:49-53, 4:5-11.

228. Accordingly, Mishaev-Schwartz disclosed or rendered obvious these claims.

j. 4: ...wherein administration of the processing device and the known network is controlled by a common administration entity.

229. As I explained above in Section VII.C.3.b, in Mishaev-Schwartz, the client device performs mitigation decisions under the control of the context provider. *See* Ex-1009, ¶0173 (explaining that the context monitoring agent may be “downloaded and installed on the client device...by...[a] part of” the context provider). Further, as I explained above in Section VII.C.4.c, the organization may implement the context provider as part of its service. Thus, the administration of both the client device and service are controlled by the organization and therefore “by a common administration entity.”

230. Accordingly, Mishaev-Schwartz disclosed or rendered obvious this claim.

k. 5, 15: ...wherein administration of the processing device and the known network is controlled by a common administration entity.

231. Schwartz taught that the known mitigation actions taken after a wireless network is deemed risky may include not only those discussed above in Section VII.C.4.e but also “generating an alert.” *See* Schwartz, claim 7 (claiming both of such blocking and alerting being performed by a sensor), 6:19-32 (explaining that the security system can also perform the alerting “upon detection of a vulnerable wireless network”). Indeed, other references confirm that such blocking-and-

alerting—including alerting, specifically, the client device’s user—was conventional and well-known. *See, e.g.*, Ex-1005, ¶0006 (explaining that, if a “client device” determines that its “network connection” to a “server” has a “vulnerability,” then “the client device can notify [its] user” and also “prevent[]” the network connection), ¶¶0040-42. In Mishaev-Schwartz, the client device performs such known mitigation actions as I explained above in Section VII.C.4.b, thereby meeting claims 5 and 15. Indeed, a POSITA would have been motivated to implement such known alerting after mitigating and blocking the login attempt discussed above in Section VII.C.4.e, because doing so would allow the user to know that such blocking occurred and to then reattempt login as I explained above in Section VII.C.4.f.

232. Accordingly, Mishaev-Schwartz disclosed or rendered obvious these claims.

- I. **6[a], 6[b], 16[a], 16[b]: ...mitigating a security issue of the unsecure network element; and based at least in part upon mitigating the security issue of the unsecure network element, requesting a grant of access from the known network to the processing device.**

233. As I explained in 1[f]/11[f]/14[f], “mitigating a security issue of the unsecure network element”—as also recited in 6[a]/16[a]—includes “starting, by the processing device, a virtual private network application.” And as I explained above in Section VII.C.4.g, such is performed—and thus 6[a]/16[a] is met—by Mishaev-

Schwartz. The '902 patent's Fig. 5 depicts an embodiment in which establishing and routing traffic through a VPN connection serves as the sole "mitigating" condition "to cure the identified unsecure network element(s)." *See* Ex-1001, 17:22-49, Figs. 3, 5. Similarly, Mishaev-Schwartz's transmission of the login attempt and corresponding data that were previously mitigated and blocked as I explained above in Section VII.C.4.g meets 6[b]/16[b] for the same reasons explained therein. *See* Ex-1001, 17:22-49, Figs. 3, 5.

234. Accordingly, Mishaev-Schwartz disclosed or rendered obvious these claims.

- m. **7: ...upon identifying an unsecure network element on the remote network while using the network connection between the processing device and the known network disconnecting, by the processing device, the processing device from the known network.**

235. As I explained above in Sections VII.C.4.g-VII.C.4.h, after transmitting the previously mitigated and blocked login attempt and corresponding data "through [the] secured"—i.e., VPN—"connection," access to the service in Mishaev-Schwartz may thereafter be granted. However, even after such access is granted and a session is established, as I explained above in Section VII.C.3.a, the client device's context monitoring agent nonetheless makes continuous security determinations, including not only by identifying even newer connections by malicious or unknown

devices with the network but also by continuously considering, e.g., the “connection type[s]” with the network and the “sensitivity” of data being transmitted or accessed by the client device, and adjusting the network’s risk factor/score accordingly. *See* Ex-1010, 6:12-32, 14:62-67, 8:66-9:10, 16:12-19 (“[N]ew data collected from network sensors may be iteratively or continuously analyzed to detected wireless connections and devices, thereby allowing for constant monitoring of the network to detect potential vulnerabilities.”); *infra* Section VII.C.4.n.

236. Moreover, in Mishaev-Schwartz, further mitigation actions may be taken based on such continuous security determinations. *See supra* Section VII.C.3.b. Such mitigation actions again include, as I also explained above in Section VII.C.3.b, completely “block[ing]” the Mishaev-Schwartz client device “from connecting to [the] network.” *See* Ex-1010, 9:54-10:4. And even more mitigation actions are available, including “establishing a containment network” and “forc[ing]” any device, including the client device, to “connect to the established containment network.” *See id.*, 13:17-35.

237. Thus, even after establishing a VPN connection as I explained above in Section VII.C.4.g and being granted subsequent access to the network accordingly, if for instance “the transmission of sensitive information is detected over the wireless network,” then the corresponding change to the network’s risk factor/score may thus

cause the client device's context monitoring agent to, e.g., force the client device into a containment network, thus meeting claim 7. *See* Ex-1010., 7:65-8:4, 8:66-9:10, 13:17-35; *supra* Section VII.C.3.b; Ex-1014, 111 (asserting infringement of claim 7 based similarly on an purported "segmenting or isolating/quarantining [of] devices").

238. Alternatively, should the client device be completely "block[ed]...from connecting to [the] network," a POSITA would have recognized the obvious next step to be to reattempt access to the service but using a different network, thereby also meeting claim 7. Indeed, Mishaev acknowledged that there exist networks predetermined by the organization as safe and thus allowable. *E.g.*, Ex-1009, ¶¶0073-74 (explaining that a "':CORO-001' access point" may be determined as "':Allowable'" due to it being "on a white list of allowable access points predefined in advance by an administrator of the" context provider). Having been blocked from accessing the previously discussed network, a POSITA would have been motivated to connect to such other, allowable networks—including, particularly, the user of an "employee's smart phone or laptop" that I mentioned previously in Section VII.C.4.f—since access would thereafter be established.

239. Accordingly, Mishaev-Schwartz disclosed or rendered obvious this claim.

- n. **8[a], 8[b], 17[a], 17[b]: ...using, by the processing device, a network connection between the processing device and the known network; and while using the network connection between the processing device and the known network, scanning, by the processing device, the remote network through which access to the known network is established, wherein the scanning is configured to identify an unsecure network.**

240. Mishaev explained that, even after the attempted (or reattempted) access to the service has been granted (8[a]/17[a]’s “using, by the processing device, a network connection...”), *see supra* Section VII.C.4.h, the context provider may require the client device to “repeat[] periodically” the discussed security determination on the network. Ex-1009, ¶¶0180-82, ¶0192, ¶0257. And in Mishaev-Schwartz as I explained above in Section VII.C.3.a, this includes continuously determining, e.g., whether malicious or unknown devices are connected to the network as taught in Schwartz—i.e., 8[b]/17[b]’s “scanning...” as I explained above in Section VII.C.4.d. *See* Ex-1010, 16:12-19.

241. Accordingly, Mishaev-Schwartz disclosed or rendered obvious these claims.

- o. **9, 18: ...upon identifying an unsecure network element on the remote network while using the network connection between the processing device and the**

known network disconnecting, by the processing device, the processing device from the known network.

242. Mishaev and Schwartz teach that such continuous security determinations can be used to decide whether to perform mitigation actions during the existing access, including “disconnecting [the] active connection[.]” (the claimed “disconnecting...the processing device from the known network”) if “new data” from the security determinations detect, e.g., a “newly connected” malicious or unknown device (the claimed “upon identifying...”) or other “potential vulnerabilities.” Ex-1010, 13:17-35, 15:37-16:19, 3:39-49, 6:19-26; Ex-1009, ¶¶0075-78, ¶¶0100-02. And as I explained VII.C.3.b, the client device itself makes such a mitigation decision in Mishaev-Schwartz as taught in Schwartz (the claimed “disconnecting, by the processing device”). *See id.*, 13:17-35, 15:37-16.

243. Accordingly, Mishaev-Schwartz disclosed or rendered obvious these claims.

- p. **10: ...upon disconnecting the processing device from the known network by the processing device, providing a message to a user of the processing device requesting the user to access the known network via another remote network.**

244. Schwartz taught that “generating an alert” can also be performed together with the discussed “disconnecting [of the] active connection,” both of which are known mitigation actions. *See* Ex-1010, claim 7, 13:27-35. Indeed, other

references confirm that such disconnecting-and-alerting—including alerting, specifically, the client device’s user—was conventional and well-known. *See, e.g.*, Ex-1005, ¶0006 (explaining that, if a “client device” determines that its “network connection” to a “server” has a “vulnerability,” then “the client device can notify [its] user” and also “cancel[]” the network connection), ¶¶0040-42. And again, in Mishaev-Schwartz, the client device performs such known mitigation actions as I explained above in Section VII.C.3.b, thereby meeting claim 10. Indeed, a POSITA would have been motivated to have the client device alert its user after performing the disconnecting for similar reasons as I explained above in Section VII.C.4.k with respect to blocking the initial access attempt.

245. Accordingly, Mishaev-Schwartz disclosed or rendered obvious this claim.

D. Ground 4: Mishaev with Schwartz and Durbin Renders Claims 1-18 Obvious

246. In my opinion, and to the extent that Mishaev-Schwartz in Ground 3 does not disclose 1[f]/11[f]/14[f], Durbin in combination with Mishaev and Schwartz disclosed or rendered obvious Claims 1-18.

1. Durbin

247. Durbin explained that, “[g]enerally, public wireless networks are unsecured and the user of such unsecured network is at a risk of getting hacked and

lo[]sing critical or important information.” Ex-1011, ¶0001. As Durbin acknowledged, “establish[ing] a secure connection on public wireless networks” has been an “area of interest” and including, “[i]n particular,...using advanced techniques such as secure Virtual Private Network (VPN) connections.” *Id.* Such VPN connections “provide secure communication within public wireless networks,” thus allowing, e.g., a “mobile device” to transmit “sensitive information” to an “information sensitive service center” through “an unsecured public wireless network such as from a cyber café,” while preventing a “promiscuous” device (“e.g., device of a hacker in the café”) from “monitor[ing] and gather[ing] the sensitive information.” *Id.*, ¶0026, ¶0024, ¶0049, ¶0037.

248. Durbin explained that however these VPN connections may have to be set up “manually, which is technically complex and time consuming.” *Id.*, ¶0001. Durbin thus proposed “[a]n approach for automatically securing a public wireless network.” *Id.*, Abstract. In particular, an “application” installed on the mobile device “scan[s] for nearby access points” and determines whether they are to be “trusted.” *Id.*, ¶¶0040-42. If none may be trusted, “then the application transmits a command to a VPN data center and/or VPN service provider to automatically establish the VPN connection for the mobile device.” *Id.*, ¶0041. As such, when the mobile device “tr[ies] to establish a connection to the information sensitive

service center”—i.e., any entity that “may manipulate and/or store sensitive information”—through any such access point’s likewise “untrusted network,” a VPN connection is “automatically” established between the device and service center. *Id.*, ¶0026, ¶0021, ¶0039.

2. Rationale to Combine Mishaev and Schwartz with Durbin

249. A POSITA would have been motivated to include forcing the device’s “traffic to be transmitted through a [VPN] connection” as an available mitigation action in Mishaev-Schwartz.

250. This exact use of a VPN connection is taught in Durbin. Indeed, Schwartz taught that, through mitigation actions, agent sensors installed on wireless devices can “mitigate potential vulnerabilities,” including those arising from “vulnerable networks,” by, e.g., “initiating a secured communication protocol for transmitting information to and from the wireless device.” Ex-1010, 3:29-49, 4:56-5:15, 9:54-10:4. Durbin’s VPN connection does exactly that: it provides mobile devices with “secure communication” through an otherwise “untrusted network”—as “automatically” established by a likewise device-installed “application”—thereby allowing even “sensitive information” to be transmitted by that device through the network. Ex-1011, ¶0026, ¶0021, ¶0039.

251. And since, aside from the terminology of “secured” over “VPN,” Durbin’s teachings otherwise align with Schwartz’s in both function and even implementation, a POSITA would have been motivated utilize Durbin’s VPN connection as one of Schwartz’s mitigation actions as proposed, and would have had no difficulty in doing so. Indeed, notwithstanding such overlap, a POSITA would have been motivated to utilize Durbin’s VPN connection given its improvements to security and ease of functionality as I discussed.

252. Accordingly, in Mishaev-Schwartz-Durbin, Mishaev-Schwartz is modified such that one of the mitigation actions utilized by the client device’s context monitoring agent includes establishing a VPN connection for the transmission of traffic to and from the client device through a network as taught in Durbin.

3. Analysis

253. As I explained in Ground 3, Mishaev-Schwartz renders all challenged claims obvious, including, in part, because the context monitoring agent of Mishaev’s client device starts a VPN application as one of its mitigation actions. *See, e.g., supra* Section VII.C.4.g. As I explained above in Section VII.D.2, this does not change in Mishaev-Schwartz-Durbin. Mishaev-Schwartz-Durbin therefore

operates identically to Mishaev-Schwartz and, thus, renders all challenged claims obvious for the same reasons I explained above in Section VII.C.

VIII. CONCLUSION

254. For the reasons set forth above, it is my opinion that claims 1-18 of the '902 patent would have been obvious to a POSITA at the time of the alleged invention in view of the above grounds.

Declaration of M. Franz ISO Petition for
Inter Partes Review Of U.S. Pat. No. 11,916,902

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

256. This declaration was executed in Munich, Germany on October 15, 2026.

A handwritten signature in black ink, appearing to read "Michael Franz", is positioned above a horizontal line.

Michael Franz