

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

META PLATFORMS, INC.,
Petitioner

v.

SITNET, LLC,
Patent Owner

Case Number: IPR2024-00530

SUPPLEMENTAL EXPERT REPORT OF DR. AVIEL D. RUBIN



Aviel D. Rubin

December 3, 2024

TABLE OF CONTENTS

I.	INTRODUCTION.....	2
II.	BACKGROUND AND QUALIFICATIONS.....	2
III.	CLAIM CONSTRUCTION	7
IV.	PERSON OF ORDINARY SKILL IN THE ART (POSITA)	11
V.	OVERVIEW OF THE ALLEGED PRIOR ART	11
	A. Gage	11
	B. Mitchell	13
	C. Shida	15
	D. Sinha	16
VI.	SUMMARY OF PATENTS	16
	A. U.S. Patent No. 9,877,345 (‘345 Patent).....	16
VII.	THE ‘345 CLAIMS ARE VALID OVER THE INSTITUTED GROUNDS AND ART	18
	A. Gage Does Not Teach Or Suggest The Limitations Of The ‘345 Patent Claims	19
	a. <i>Mitchell Does Not Remedy The Deficiencies Of Gage</i>	28
	B. Shida Does Not Teach Or Suggest The Limitations Of The ‘345 Patent Claims	31
	a. <i>Sinha Does Not Remedy The Deficiencies Of Shida</i>	40
VIII.	CONCLUSION	42

I. INTRODUCTION

1. My name is Aviel D. Rubin. I have been retained as an expert witness to provide my independent opinion in regard to the matters at issue in inter partes review of U.S. Patent No. 8,332,454 (“the ‘454 patent”) in IPR2024-00529. I have been retained by Sitnet, LLC (“Sitnet”), the Patent Owner in this proceeding. Petitioner is Meta Platforms Inc. (“Meta” or “Petitioner”).

2. I am being compensated \$925 per hour for my time spent working in connection with this case. My compensation is in no way related to the outcome of this litigation. If called as a witness, I would testify as to the statements and opinions contained in this report.

3. I am not a legal expert and offer no opinions on the law. However, I have been informed by counsel of the various legal standards that apply, and I have applied those standards in arriving at my conclusions.

II. BACKGROUND AND QUALIFICATIONS

4. I have more than 30 years of experience in the fields of computer science and applied cryptography. My professional career has been dedicated to issues relating to software, networks, and computer systems more generally.

5. I received a Bachelor of Science in Computer Science with Honors from the University of Michigan in 1989, a Master of Science in Computer Science and Engineering from the University of Michigan in 1991, and a Ph.D. in Computer

Science and Engineering from the University of Michigan in 1994. My Ph.D. dissertation was titled “Nonmonotonic Cryptographic Protocols” and concerned authentication in long-running network operations.

6. I am a Professor Emeritus in Computer Science at Johns Hopkins University (the “University”). I joined the Computer Science faculty at the University in 2003 and was promoted to full professor with tenure in April 2004. As a member of the faculty, I perform research, teach graduate and undergraduate courses in computer science and related subjects, advise undergraduate and Masters students, and supervise the research of Ph.D. candidates and other students. I have taught courses including Networking, Security and Privacy in Computing, Cryptography, and Advanced Topics in Computer Security. In September 2023, I was appointed Professor Emeritus.

7. I also served as the Technical Director of the University’s Information Security Institute (“ISI”). The ISI is the University’s focal point for research and education in information security, assurance, and privacy. The University, through the ISI’s leadership, has been designated as a Center of Academic Excellence in Information Assurance by the National Security Agency and leading experts in the field.

8. I also have significant industry experience. Since 2011, I have served as the founder and chief scientist of Harbor Labs, a software and networking

consulting firm specializing in data security and privacy. Previously, from 2005 to 2011, I served as the founder and President of Independent Security Evaluators (“ISE”), a computer security consulting firm. In that capacity, I guided ISE through the qualification process to become an independent testing laboratory for Consumer Union, which produces the Consumer Reports magazine. ISE provided consulting services to various companies on potential security flaws and weaknesses in products and systems. These companies included Fortify Software, Verdasys, and Security First Corp. As an independent testing laboratory for Consumer Union, I managed an annual project where we tested popular anti-virus products. Our results were published in Consumer Reports each year for three consecutive years.

9. In addition, I came to the University from AT&T Labs, Secure Systems Research Department, where I spent six years focused on Internet and computer security. Prior to AT&T Labs, I spent two years at Bellcore in its Cryptography and Network Security Research group, also focusing on Internet and computer security issues. I also interned at IBM in 1989. During my time there, I worked on the IBM System/360 family of mainframe computer systems.

10. I am the author or co-author of five books regarding information security issues: Brave New Ballot, Random House, 2006; Firewalls and Internet Security (second edition), Addison Wesley, 2003; White-Hat Security Arsenal,

Addison Wesley, 2001; Peer-to-Peer, O'Reilly, 2001; and Web Security Sourcebook, John Wiley & Sons, 1997.

11. I have received numerous awards for my work and research in the field of computer security, including:

12. In 2020, I received the Distinguished Service Award from the Institute of Electrical and Electronics Engineers (“IEEE”) Computer Society Technical Committee on Security and Privacy;

13. In 2010, I received a Fulbright Scholarship to serve as a Visiting Professor at Tel Aviv University in Israel;

14. In 2009, I received a Google Research Award for my work on securing medical records on smartphones;

15. In 2007, I received the Privacy Enhancing Technologies Award for Outstanding Research for my work on a security analysis of a cryptographically enabled RFID device;

16. In 2004, I was named Baltimorean of the Year by Baltimore Magazine for my work in safeguarding the election process;

17. In 2004, I received the Electronic Frontiers Foundation Pioneer Award; and

18. In 2000, I received the Best Paper Award at the 9th USENIX Security Symposium.

19. I serve, or have served, on several technical and editorial advisory boards. For example, I served on the Editorial and Advisory Board for the International Journal of Information and Computer Security. I also served on the Editorial Board for the Journal of Privacy Technology. In addition, I have been Associate Editor of the IEEE Security and Privacy Magazine and served as Associate Editor of the Association for Computing Machinery's ("ACM") Transactions on Internet Technology. I also served as Associate Editor of the journal Communications of the ACM, and I was an Advisory Board Member of Springer's Information Security and Cryptography Book Series. I also have served in the past as a member of the Defense Advanced Research Projects Agency's Information Science and Technology Study Group, a member of the Government Infosec Science and Technology Study Group of Malicious Code, a member of the AT&T Intellectual Property Review Team, Associate Editor of the Electronic Commerce Research Journal, Co-editor of the Electronic Newsletter of the IEEE Technical Committee on Security and Privacy, a member of the board of directors of the USENIX Association (the leading academic computing systems society), and a member of the editorial board of the Bellcore Security Update Newsletter.

20. I have spoken on information security and electronic privacy issues at more than 50 seminars and symposia. For example, I presented keynote addresses on the topics "Security of Electronic Voting" to Computer Security 2004 Mexico in

Mexico City, Mexico, in May 2004; “Electronic Voting” to the Secure Trusted Systems Consortium 5th Annual Symposium in Washington, D.C., in December 2003; “Security Problems on the Web” to the AT&T EUA Customer Conference in March 2000; and “Security on the Internet” to the AT&T Security Workshop in June 1997. I also presented a talk about hacking devices at the TEDx conference in October 2011 and another TEDx talk on the same topic in September 2015.

21. I am a named inventor on 10 United States patents, including U.S. Patent Nos. 5,638,446 (“Method for the Secure Distribution of Electronic Files in a Distributed Environment”) and 5,809,140 (“Session Key Distribution Using Smart Cards”).

22. A detailed record of my professional qualifications is set forth in the attached Exhibit A, which is my curriculum vitae, including a list of publications, awards, research grants, and professional activities. My curriculum vitae also lists the matters in which I have served as an expert.

III. CLAIM CONSTRUCTION

23. It is my understanding that claim construction is a matter of law and that the claims of a patent define the invention claimed. I understand that an Opinion and Order construing the claims of the ‘345 Patent was issued in *SitNet LLC v. Meta Platforms, Inc.* No. 1:23-cv-06389-AS (S.D.N.Y. July 24, 2024) and that Patent

Owner requested under 37 C.F.R. § 42.100(b) the Board to consider and adopt the District Court's construction.

24. I have adopted those claim constructions during my analysis of the IPR filings, and I have been guided by these constructions in the discussion of the grounds of invalidity.

25. I understand that the Claim Construction Order does not construe every term that appears in the claims of the '345 Patent. For claim terms that the Court and Board have not construed, I have been informed that such terms are to be interpreted based on their plain and ordinary meanings as understood by one of ordinary skill in the art at the time of the invention.

26. I reserve the right to supplement this report if necessary or appropriate, including but not limited to, in the event that any of the claim constructions change.

Claim	District Court Construction
“situational network”	a network created in response to an event or situation
“situation authority”	an entity providing information concerning a situation
“event node”	Needs no construction
“multi-dimensional personal information network (NDSN)”	Relationships between users based on subscription information
“projection of a situational network”	a subset of a situational network
“roll call information”	the status responses and the roll call list
“Caus[e/ing] an automatic redirection of a web browser”	caus[e/ing] a redirection of a web browser application operating on each of the

application operating on each of the devices”	devices without the user’s choosing to go to the redirected page at that time
“Caus[e/ing] an automatic redirection of a web browser application on each of the de vices to a webpage and provid[e/ing] ... at least one of the plurality of advertisements ... for display on the webpage”	caus[ing] an automatic redirection . . . to a webpage” must occur prior to “provid[ing] at least one of the plurality of ad vertisements [. . .] for display on the webpage
“web browser application”	an application that enables users to browse webpages

27. The ‘345 Patent discloses numerous elements that are integral to their respective teachings and innovations. Here, I provide descriptions for several of these elements that are most relevant. Throughout my report, I refer to these elements and refer back to these definitions, which I use as the foundation for my opinions regarding the alleged prior art’s disclosure of the ‘345 Patent claim elements. In my opinion, a POSITA would have understood these elements to have the following definitions at the time of filing for each patent.

28. For any terms below that are covered by claim construction, I have adopted those constructions, and the descriptions below are to provide additional detail. Those that have not been included in claim construction are described in a way that is my opinion of what would be the plain and ordinary definition.

29. **Situation Authority Server (Event Node Server)** – There is a corresponding situation authority server, also referred to as an event node server, for each situation authority. The situation authority server may be connected to a database for storing information related to the situation, or data related to other participants in the situational network.

30. **Trusted Provider** – Source of event/situation information that is provided to a situation network (e.g., news networks, weather networks).

31. **Roll Call List** – A list of users in a situational network, as well as their response to an emergency notification on the status of their safety.

32. **Targeted Marketing** – A marketing strategy that uses profiles constructed about users in order to automatically deliver advertisements to specific users for which they are most relevant. Profiles are constructed on users through the collection of various data such as, but not limited to, demographics, purchase history, location, attended events, interests, hobbies, and more. This is done by platforms without the involvement of the user and without an opt-in by the user for specific events, products, or topics. For example, when a social media user interacting with a specific page or subscribing to events at a specific location receives an advertisement for that event or page as a result of that subscription, it does not constitute targeted marketing.

33. **Social Network (Personal Information Network)** – Traditionally, a social network is a network that consists of individuals who are interconnected by various personal information and social metrics such as interests, location, demographics, community, and more. However, social networks have evolved to also include incorporating businesses, organizations, groups, and other entities into the interconnections of users as their own nodes in the network. As such, these entities can often masquerade in social networks as individual users and appear to users as such.

IV. PERSON OF ORDINARY SKILL IN THE ART (POSITA)

34. A person of ordinary skill in the art (“POSITA”) would have had a bachelor's degree in computer science or electrical engineering or equivalent discipline, and approximately two years of experience in computer networking, database management, or mobile communications. Additional education in a graduate program could substitute for professional experience, and significant accomplishments in an industry environment could substitute for graduate education.

V. OVERVIEW OF THE ALLEGED PRIOR ART

A. Gage

35. Gage teaches “a method for reporting a status indicator using a mobile device during a disaster (§ Abstract). “Specifically, “a disaster response system for

informing concerned parties of a situation status of subscribers, who may have been [a]ffected by a disaster [(e.g., hurricane, flood, fire, tsunami, etc.)] (§ 19).” Subscribers of this system can communicate with each other by a status indicator [(e.g., OK, NEED HELP, and IN CRITICAL NEED.) (§27)], which indicates affected status (by the disaster) of the subscriber (§ 19). The location of a subscriber is obtained through GPS or triangulation within a mobile network (§ 19). Data obtained from subscribers can be aggregated and used for disaster response/relief purposes (§ 21, 31).

36. If a subscriber is outside of the designated disaster area, they are automatically deemed safe and not in need of assistance (§ 19). Furthermore, “[c]oncerned parties can communicate with the disaster response system to obtain the status indicator and location of queried subscribers (§ 20).” Additionally, if a subscriber within a geographic area of a disaster has not interacted with the system, an “Are You OK” request may be issued to the subscriber periodically (§36), which may lead to a subscriber being listed as “Unknown” (§38).

37. Communications about a disaster area may be handled primarily by resources outside the affected region (§22). Specifically, a series of servers are placed geographically such that any server deemed inaccessible (i.e., within the affected area) may be disabled, and thus forcing all communications through the

other servers (§ 23). Furthermore, specific network resources may be reserved for the system to alleviate any potential congestion (§ 24).

38. The disaster subscriber indicator system may be built upon existing communication technologies (e.g., mobile telephony and push-to-talk, Bluetooth, WIMAX, WiFi, and/or ad hoc networks) (§25, 32). The system is implemented with a user device connected to an established network (§ 26, 33) and runs software allowing the communication of status indicators (§ 27).

B. Mitchell

39. Mitchell teaches “[a] real time automatic headcount system [] configured with a portable transmitter [] operable to output an alert signal which is received by a plurality of receivers [] associated with a crisis-event site” (§ Abstract). More specifically, the defined system operates in response to a crisis coordinator initiating the headcount system upon learning of a crisis (§ 32). This triggers a predefined email/voice notification to be sent to every person associated with the crisis-event site (§ 33). The receivers of the notification are then able to send an acknowledgment of the signal back to the crisis coordinator (§ 34). This response carries personal identification and updates that person as “outside” the crisis site (§ 34). The acknowledged persons no longer receive alert signals (§ 34, 40). Furthermore, a checklist of specific individuals must be present in a database (§ 35, 48). The alert system ends when all persons have checked in with the system (§ 47).

40. If a signal is sent over a network, it is associated with a person's email address and prompts a popup on the receiver's device (§ 36). The response requires manual user intervention to acknowledge and may be in the form of clicking a URL link (§ 37). The receiving user may manually enter further information into the response of the alert signal (§ 38).

41. If the signal is sent over a mobile network, a voice message is required instead of an alert notification (§ 44). The receiving user must then respond to the message (e.g., calling an 800 number and entering a phone number) (§ 44). Alternatively, after receiving the alert in this manner, further activation of the cell phone may send an automatic response with a unique identifier (§ 45).

42. Additionally, an IR, video, or GPS based tracking system is implemented to track persons not currently present at their computers (§ 61). The IR system places scanners around a specific location and tracks users as they enter into the proximity near those scanner locations (§ 62). The video system operates similarly to the IR system, sans IR cameras, and requires an image/video recognition system to track persons (§ 63). The GPS system can track a person's location and requires cellular carrier bandwidth to operate (§ 64). GPS coordinates are transmitted over the cellular network (§ 65).

C. Shida

43. Shida discloses a method of confirming the safety of “subscribers in the disaster occurring region” (Shida Abstract). The object of invention operates on a cellular network as “wireless base station” connects with “wireless terminals” (§ 2) to “transmit a disaster notice” (Shida Abstract). Shida teaches a center server that has an “emergency measure information”, a “regional map,” and a “disaster region subscriber table” (§ 30). The center server is also connected to an “operator terminal [] in facilities such as fire stations and police stations” (§ 30).

44. When a “reporting subscriber inputs disaster information” (§ 32), the carrier server of the reporting subscriber will identify the region the reporting subscriber is in and designate that region a disaster region. The carrier server will then “retrieve[] the regional subscriber table by the disaster occurring region ID, and extracts the subscribers who exist in the disaster occurring region” (§ 37) to transmit the information to the center server. The center server will then store and transmit this data to the operator terminals (§ 38). After the operator receives this information, “the operator judges whether to have to carry out the safety confirmation of the subscribers who exist in the disaster occurring region” (§ 44). The center server then generates notice information, and then “the subscriber terminal of the designated subscriber receives the broadcast notice information from the mobile

communication network system” (§ 46). The subscriber then inputs a “safety confirmation response” (Abstract), which is then relayed to the center server.

D. Sinha

45. Sinha teaches a “business continuity application” that “allows for notifications to be sent to the workforce [] and further provides remote-access to computing resources” (Sinha Abstract). This is “displayed on a computing device [] to an employee of workforce in response to the occurrence of an event”, and the graphic user interface is “stored on a portable memory device” (Claim 18). Thus, Sinha discloses a private message board for workforce employees that a “manager may review, update or otherwise manage the roll call” (§ 124).

VI. SUMMARY OF PATENTS

A. U.S. Patent No. 9,877,345 (‘345 Patent)

46. Patent ‘345 details techniques to exchange and aggregate information relating to an event (e.g., a natural disaster) between a situation authority and user devices identified as affected by the event. The method creates a situational network, shown in Figure 2, in which a situational authority 207 can connect a situational network 3000 of identified users 250 to an event 3011 that is controlled by the situational authority 207. When a situational authority creates a situational network, the users 250 form connections with the event node 3011 through a network 900 and

can form connections with other users connected to the event node (4: 3-15, 15:4-10).

47. Figure 28 shows an example of a situational authority 207 creating an event node 3000 due to the snowstorm 3005. Users 3026 and 3029 discover the situational network by seeking out information on the snowstorm. Users 3027 and 3028 are invited to the situational network by the event node identifying them to be affected by the situation 3005 (23:65-24:23).

48. The situational network can be implemented in a multi-dimensional social network (NDSN) that allows multiple connections between individual nodes (6:11-18). Projections of the NDSN take a subset of the connections subject to criteria to create a smaller and more relevant network (16:53-57). Projection within the NDSN may use affinity attributes between nodes during the creation of the more relevant network. The affinity attributes are compared with a threshold value that determines whether or not nodes within an NDSN are qualified for inclusion in the more relevant network. (17:7-14). This indicates that a projection is capable of creating new relationships withing the NDSN. Specifically, the '345 states that "The affinity attributes between nodes of the NDSN 100 may also be used to determine the set of nodes that form a projection of the NDSN." (17: 7-10) No where is it stated that this system of projection is limited to pre-existing edges within the NDSN. Therefore, the event node is capable of forming new connection not

previously found in the NDSN. Nodes within an NDSN can query their neighbors to discover new nodes that meet a criterion to initiate a connection (18:18-24). Thus, users within a situational network can identify other users within the situational network to connect with.

49. Patent '345 allows the event node to query the user and receive a response of the status of the user for the given event (27:6-9). The user device can send their status to the event node. These responses are aggregated by the situational authority and disseminated throughout the situational network if the user requests to view the aggregated data (25:23-26, 26:51-56). A user can share personal or situational information with other users in the situational network (8:4-5, 27:21-25). The event node can create external portals to provide information on users within the network to external users not connected to the situational network (26:65-27:3).

VII. THE '345 CLAIMS ARE VALID OVER THE INSTITUTED GROUNDS AND ART

50. It is also my opinion that Meta Platforms Inc. has failed to disclose any of the claims in the '345 Patent taking into consideration the alleged prior art. Below I discuss how the alleged prior art, and combinations, do not disclose the claimed invention of the '345 Patent.

A. Gage Does Not Teach Or Suggest The Limitations Of The '345 Patent Claims

51. In my opinion, Gage does not disclose and/or renders obvious the claims of the '345 Patent. The '345 Patent includes several attributes that Gage neither reveals nor would have been obvious to a POSITA.

52. First, the IPR claims Gage's disaster response system comprises a situational network¹. This is incorrect. Gage's disaster response system does not comprise a network created in response to an event or situation. The plain and ordinary meaning of a "network" is an interconnected system of elements that transmits information. The American Heritage Dictionary defines a network as: "a. A group or system of electric components and connecting circuitry designed to function in a specific manner. B. Computers A system of computers interconnected by telephone wires or other means in order to share information. Also called net."²

53. Similarly, PC Mag defines a "network" as: "(1) Any arrangement of elements that are interconnected. See neural network and network database. (2) A system that transmits data between users, which includes the client devices

¹ '345 IPR Petition at pg. 27

² American Heritage Dictionary Entry: network, <https://ahdictionary.com/word/search.html?q=network> (emphasis added).

(computers, tablets and phones) and the network equipment (servers, switches, routers and cables). In wireless systems, antennas replace the cables.”³

54. Each of these definitions specify a “network” as a system of interconnected elements that transmit information or data. Thus, one of the key elements that defines a network are the connections established between the various components or elements present within the network. It is important to note that for this analysis we must consider logical networks rather than just physical networks. In a logical network, the links that connect the different elements or components of the network are logical, as the name would imply, rather than physical. For example, in a social network, the connections between the various users are logical connections such as friendships or group memberships, rather than physical wires connecting each of the members of the social network. These different logical connections (e.g., friends, groups memberships, etc.) can be thought of different connections between the users, similar to having multiple physical connections between elements of a network (e.g., ethernet, Wi-Fi, etc.).

55. With this in mind, the act of creating a network logically must include constructing the interconnection that defines the network. These connections can be created from pre-existing connections or be derived specifically for the new network.

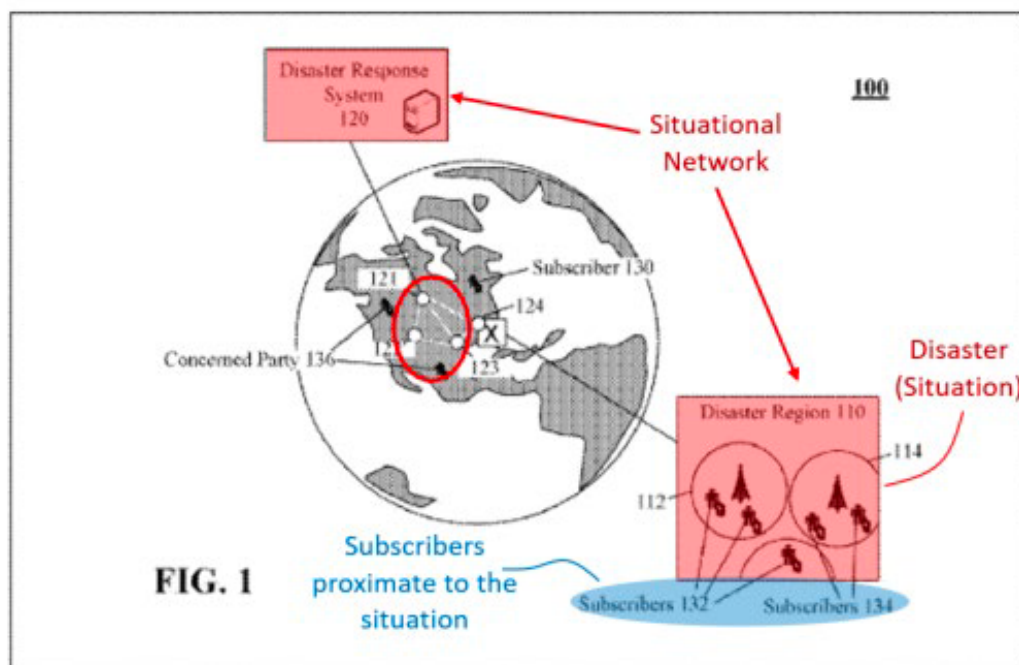
3 Definition of network | PC Mag, <https://www.pcmag.com/encyclopedia/term/network> (emphasis added).

In either case, the logical connections that define a specific network are distinct to that network. In other words, if a pre-existing network were used to define a new network, any changes made to the pre-existing network after the creation of the new network should not necessarily be reflected in the new network. For example, consider a situational network was formed using a pre-existing social network that included a group for a specific local activity. After the situational network was formed, a member of the local activity group left the group, breaking the relationship used to include the user in the situational network. The user's departure from the local activity group should not guarantee removal of the user from the ongoing situational network, since the departure does not guarantee the user is no longer local to and, therefore, impacted by the ongoing situation. Alternatively, users opting out of a situational network should not alter the pre-existing connections used to form the situational network. For example, let us return to our previous example. If a member of the local activity group were to opt out of a situational network, that action should not remove the user from the local activity group. Thus, the two networks must remain distinctly separate from one another after the creation of new network since the logical connections used to create the networks are different, even if one logical network was used to during the creation of another.

56. Gages's disaster response system does not include a network created in response to a situation, given that it already exists at the time of the event. This is

obvious given that no new logical connection needs to be created at the time of the situation. Gage's disaster response system, and therefore the logical connections that define it, exist before, during, and after the situation. Furthermore, alterations made to Gage's disaster response system, such as the addition of a subscriber, that occur during event will continue to persist after the event. As described above, alterations made to a distinct situational network should not affect any network used during its creation. For this reason, we can conclude that Gage's disaster response system does not include a network created in response to a situation that will be destroyed once the situation has ended, but is instead a single network that exists before, during, and after the event.

57. The IPR asserts portions of Gage's Fig.1 in red to identify what it believes to be the situational network:



4

What has been identified in the IPR, however, is a server that is in communication with subscribers' mobile devices *before* the system even detects a disaster has occurred. As Gage explains, the disaster response implements a method that “*begin[s]*” in step 305, *where a server can request location information from mobile devices*. Corresponding database entries can be populated using this information. In step 310, *a determination can be made as to whether a disaster has occurred.*⁵ Performing such operations requires utilizing connections with subscribers' devices established *before* the occurrence of the event or situation.

⁴ 345 IPR Petition at pg. 28.

⁵ Gage, ¶ [0036] (emphasis added).

58. Connections established *before* the occurrence of an event or situation are also necessary to “look-up a last known location” and ascertain the “last known activity for the mobile device” when a mobile device is unable to be contacted. When a Gage’s system is unable to contact a subscriber’s mobile device, “the disaster response server can *look-up a last known location* of user and to ascertain whether mobile communications are down in that area. Further, a *last known activity* for the mobile device can be ascertained and compared against disaster related times.”⁶ These operations could only be performed if Gage’s system was connected to subscriber devices *before* the event or situation to receive and store such location data. Thus, Gage’s disaster response system is a network including participant devices formed prior to the occurrence of an event or situation.

59. Furthermore, a situational network can be established in ways that do not fit Gage’s teaching. This is supported by a proximity-based situational network as described in ‘345. These proximity-based situational networks can be formed as “... a result of the occurrence of the event or situation causing the potential members of the SitNet to be within a relatively small geographic area, ...” (5:62-64). ‘345 further discusses that these proximity-based situational networks may also be established without a situation authority or the creation of an event node. In contrast to the teaching found in ‘345, the IPR petition claims that the disaster response

⁶ Gage, ¶ [0010] (emphasis added).

system forms connections with multiple participants including subscriber devices with the system itself. In other words, the disaster response system is a central component of the claims presented in Gage's teaching. However, as '345 teaches, a central component such as that of a disaster response system is not needed for proximity-based situational networks.

60. Indeed '345 gives an example as to how proximity-based situations can be instantiated without said central component. As stated in the patent, a proximity-based situational network "... may be established in response to a request for goods or services..." where "A device associated with an individual broadcasts a message containing a request for goods and/or services" along with positional coordinates. Other close proximity devices may respond to the request for goods or services and establish a connection (creating a situational network). In this example, a situational network is without the need for a centralized component as any device could have sent out the request and any other close-proximity device could have responded. However, in Gage's teachings, the disaster response system acts as a centralized component that queries the subscribers, but subscribers cannot query for each other (like in the case of proximity-based situational networks). This technical functionality is a deficiency that is not addressed in Gage's teachings and as such Gage's disaster response system does not comprise a situational network as stated by the IPR claim.

61. Furthermore, Gage does not form a situational network as described in ‘345. The IPR petition claims that when a disaster is detected, a central server queries the mobile devices of subscribers located near the disaster⁷. This functionality is limiting in light of situational networks. In the ‘345 patent, devices can either automatically connect to the situational network or be given an invitation to connect. That is, a participant’s device in the ‘345 patent can either find an occurrence related to a situational network (e.g., by crawling a social network) or the occurrence related to the situational network can query the participant’s device. Gage does not discuss this bi-directional method of subscribers joining a situation. Rather, a disaster response system supports automatically querying mobile communication devices of subscribers to determine if the subscribers are part of a disaster/occurrence. The bidirectional functionality stated in this paragraph is not discussed in Gages teachings yet is a functionality supported by situational networks. As such, the IPR claims do not meet the definition of a situational network, and disaster response systems do not form situational networks.

62. The IPR further claims that the disaster response system is a situational authority⁸. This is incorrect as a disaster response system lacks flexibility that is supported by a situational authority as described in ‘345. Gage’s teaching shows that

⁷ ‘345 IPR Petition at pg. 26

⁸ ‘345 IPR Petition at pg. 34

disaster response systems are central systems that aggregate status indicators from subscribers and let concerned parties obtain the status information of said subscribers. In the methods discussed by Gage, the disaster response system plays an important role as the centralized form of communication aggregation in the architecture. However, this does not need to be the case for situational authorities as taught by '345. Situational authorities can also be participants in a peer-to-peer network. The distinction between the disaster response system and the situational authority is that a situational authority may "... act[s] as a participant in the peer-to-peer network. While the situation authority may act as an important source of information, it does not act as the central authority or host" (7:5-8). That is, in a situational network, the situational authority can act both as a central authority, in a centralized architecture, or as a regular participant in a peer-to-peer network. The disaster response systems taught by Gage simply do not have this functionality. Given said deficiency, it is my opinion that Gage's teaching of a disaster response system is not a situational authority.

63. Given all of the deficiencies mentioned above, a POSITA would not find it obvious to implement a situational network as discussed in '345 given the teachings in Gage.

64. As such, it is my opinion that Gage does not disclose and/or render obvious the claims of the '345 Patent.

a. Mitchell Does Not Remedy The Deficiencies Of Gage

65. It is my opinion that the combination of the alleged prior arts does not disclose and/or render obvious the claimed invention of the ‘345 patent. Moreover, Mitchell does not remedy the deficiencies identified in Gage.

66. First, Mitchell does not address the limitations in Gage’s teachings regarding situational networks. As discussed in ‘345, a situational network can be established using different architectures (e.g., central, peer-to-peer, or a combination thereof). Gage does not meet this definition as discussed above and Mitchell also does not meet the definition as it claims a system comprising “a central processing unit coupled to the transmitter and receivers and operable to transmit the alert and acknowledgment signals, ... “(Mitchell, Claim 1c). In this architecture, there is a transceiver that is able to directly communicate with receiver devices but the receiver devices themselves are not able to directly communicate with each other. In a situational network as discussed by ‘345, the direct communication of participants is possible by using proximity-based situational networks. Given this lack of peer-to-peer functionality, Mitchell’s teaching does not comprise a situational network.

67. Furthermore, the IPR claims that Mitchell and Gage disclose claims 2, 9, 14⁹. This is incorrect. For example, claim 2 in ‘345 discusses “receiving a request from a responsive participant to view the roll call list”. That is, a participant first

⁹ ‘345 IPR Petition at pg. 44

queries an event node in a situational network for a roll call list. In response, an event node can “present[] the roll call list to the responsive participant”, and further the participant may respond to the event node thereby “receiving from the participant an indication of the status of non-responsive participant”. As it relates to Gage’s teachings, subscribers are not given the ability to request a roll call list. The disaster response system, not subscribers, can “mak[e] the status indicator and the location available to a plurality of concerned parties”. Since subscribers do not have the ability to request aggregate information, Gage’s teachings do not meet the claims. Similarly, Mitchell also does not meet the claim language as described in ‘345. In Mitchell’s teachings, receivers of the headcount system do not request the aggregate status of other receivers. Instead, the transmitter in the headcount system “selectively transmit[s] to the receivers associated with persons on the checklist whose status has not been updated in response to a previous alert signal”. In this system, sending the aggregate responses is initiated by the transmitter, not the receiver, since the transmitter has information on statuses (the checklist). As such, it is my opinion that Mitchell also fails to meet the claims of the ‘345 patent.

68. In addition to not addressing the aforementioned deficiencies, combining Gage and Mitchell would not be compatible with the functionality discussed by the ‘345 patent. The ‘345 patent discusses situational networks in the context of a situation (e.g., weather phenomenon, emergency situations) with

participants being determined to be in proximity to the geographical location of the situation. In such cases, a situational network may have an event node (representing the situation) that can query for participant devices (e.g., PIAs) to request to join the situational network, or participant devices can search (e.g., by crawling the social network) for the event node and request to join the situational network.

69. Converse to the ‘345 teachings mentioned above, Mitchell’s teachings are motivated by a business continuity plan in response to a crisis event. In such an event, businesses may need to evacuate the area around the crisis event, and to do that, the businesses would need to have a headcount of people that may be present such as employees, visitors, or contractors. To that end, claim 1 in Mitchell’s teachings discusses a “... central processing unit being operable to update a status of the person as accounted for on a checklist...”. The limitation noted by the claim is that there exists a checklist already made for participants that must be known beforehand. In ‘345, however, this list of participants can be dynamically altered (e.g., by participants searching for the event node and requesting to join the situational network). This dynamic nature of the teachings in ‘345 are not represented by Mitchell yet is beneficial in a crisis event.

70. For example, emergency responders may need to help evacuate an area where flooding has occurred. Using a situational network can help represent a more accurate roll call list even without knowing a full list of participants that are

physically in the flood zone (e.g., people who happen to be near the flooding event). As mentioned above, a roll call list can be dynamically established with new participants by having the event node related to the flooding situation send requests to join the situational network and/or participants searching for the event node related to the flooding. The dynamic nature of the situational network can let the people who happened to be near the flooding event search for the situational network and be placed in a roll call list such that emergency responders can act accordingly. During the same event, however, using Mitchell's teachings would only provide information related to the people present in the predefined checklist, thereby missing other people near the flooding event and causing emergency responders to not have accurate roll call information.

71. Given the limitations of Mitchell's teachings, it is therefore my opinion that Mitchell combined with Gage does not disclose and/or render obvious the claims of the '345 patent.

B. Shida Does Not Teach Or Suggest The Limitations Of The '345 Patent Claims

72. In my opinion, Shida fails to disclose and/or render obvious the claims as discussed in '345. The '345 Patent's teaching are unique to its disclosures, the likes of which would not have been obvious to a POSITA, regardless of taking Shida's teachings into consideration.

73. First, and foremost, the alleged prior art operates only within a cellular network as a “wireless base station” connects with “wireless terminals” (§ 0002) where a wireless terminal is “a cellular phone or PHS (Personal Handyphone System) equipment” (§ 0027). In Patent ‘345, users are connected to the situational network by “using devices 402 such as cell phones, PDA's, personal computers, network servers,[] or other devices generally known to [] enable connection to, from and through the computer network 900” (4:36-40), and the computer network 900 can be “implemented with a wide variety of hardware platforms” (14:1-2) such as “Ethernet [] and wireless [] networking technologies” (14:3-5). Therefore, the ‘345 Patent is network agnostic and introduces novel art. Thus, in my opinion, Shida does not disclose any of the claims as it operates on a limited network architecture.

74. Shida does not disclose an event node. An event node “propagates up-to-date information on the situation to PIAs of the NDSN connected to that event node” (7:63-65), and as stated above, the “event itself may also be associated with a node on the SitNet, known as the event node for the SitNet” (7:44-46). Thus, an event node provides information on the situation and status of the users to each user. Shida does not provide mechanisms for updating subscribers on the state of the situation. Further, the reporting subscriber submits an “input disaster information and own subscriber ID” (§0033), which the central server stores in column 205 of its database (§0039). Shida’s central server uses the reporting subscriber’s ID to

index the situation that occurs. Therefore, if multiple reporting subscribers report on the same disaster, then the central server would denote each as a separate situation. Further, multiple event nodes can exist within a situational network (7:65-67). Thus, Shida's central server cannot act as an event node within the situational network, as Shida does not permit multiple center servers associated with the same situation. Even if the central server could create event nodes or situational networks, which I do not say, the central server could not create multiple event nodes associated with the situational network.

75. Further, Shida does not disclose a situational authority. Although the IPR states that a central server is a situational authority, a central server is not a situational authority, as a situational authority can act as a peer within the network (7:5-9), which Shida's central server cannot do. Further, the situation authority determines which users to solicit with a roll-call list by geographic proximity (Claim 8). Shida explains that the operator of terminal 7, not the central server, receives "the information of the map" (§ 0043), and "the operator judges whether to have to carry out the safety confirmation of the subscriber" (§ 0044). Thus, the central server cannot act as a situational authority. Finally, Shida does not account for multiple situations happening concurrently, which a situational authority can handle by creating new event nodes within a situational network (7:66-67).

76. Shida does not define a situational network. A situational network is a multi-dimensional social network that allows users, situational authorities, and external users to interact and discover each other (4:41-43, 6:31-33, 7:34-36). The IPR points out that Shida “does not enable direct communication between subscribers or other users.” Shida does not allow subscriber devices to discover operator devices or other subscriber devices. Thus, Shida’s center server does not create a situational network. Further, a situational network can be dynamic and allow for new users to be discovered and users to be disconnected from the situational network (5:39-45). Shida does not teach a dynamic network as only subscribers to Shida’s service can be discovered by the central server. This relationship is not reciprocal in Shida’s claims, whereas an “event node may be discovered by a user” (20:28-29). Further, a situational network does not require a situational authority for users to interact with each other (5:65-67), and in the case that a situational authority becomes unavailable, the situational network “can still allow vital situation information to be exchanged between users” (7:21-22). Even if the central server is a situational authority, which it is not, Shida requires the central server, as the IPR states, “the connections are formed by coupling participant devices to a central server.” As such, if the central server becomes unavailable, connections between all users are lost. Therefore, Shida does not form a situational network.

77. Furthermore, Shida's network is not created in response to an event or situation. The plain and ordinary meaning of a "network" is an interconnected system of elements that transmits information. The American Heritage Dictionary defines a network as: "a. A group or system of electric components and connecting circuitry designed to function in a specific manner. b. Computers A system of computers interconnected by telephone wires or other means in order to share information. Also called net." ¹⁰

78. Similarly, PC Mag defines a "network" as: "(1) Any arrangement of elements that are interconnected. See neural network and network database. (2) A system that transmits data between users, which includes the client devices (computers, tablets and phones) and the network equipment (servers, switches, routers and cables). In wireless systems, antennas replace the cables." ¹¹

79. Each of these definitions specify a "network" as a system of interconnected elements that transmit information or data. Thus, one of the key elements that defines a network are the connections established between the various components or elements present within the network. It is important to note that for this analysis we must consider logical networks rather than just physical networks.

10 American Heritage Dictionary Entry: network, <https://ahdictionary.com/word/search.html?q=network> (emphasis added).

11 Definition of network | PC Mag, <https://www.pcmag.com/encyclopedia/term/network> (emphasis added).

In a logical network, the links that connect the different elements or components of the network are logical, as the name would imply, rather than physical. For example, in a social network, the connections between the various users are logical connections such as friendships or group memberships, rather than physical wires connecting each of the members of the social network. These different logical connections (e.g., friends, groups memberships, etc.) can be thought of different connections between the users, similar to having multiple physical connections between elements of a network (e.g., ethernet, Wi-Fi, etc.).

80. With this in mind, the act of creating a network logically must include constructing the interconnection that defines the network. These connections can be created from pre-existing connections or be derived specifically for the new network. In either case, the logical connections that define a specific network are distinct to that network. In other words, if a pre-existing network were used to define a new network, any changes made to the pre-existing network after the creation of the new network should not necessarily be reflected in the new network. For example, consider a situational network was formed using a pre-existing social network that included a group for a specific local activity. After the situational network was formed, a member of the local activity group left the group, breaking the relationship used to include the user in the situational network. The user's departure from the local activity group should not guarantee removal of the user from the ongoing

situational network, since the departure does not guarantee the user is no longer local to and, therefore, impacted by the ongoing situation. Alternatively, users opting out of a situational network should not alter the pre-existing connections used to form the situational network. For example, let us return to our previous example. If a member of the local activity group were to opt out of a situational network, that action should not remove the user from the local activity group. Thus, the two networks must remain distinctly separate from one another after the creation of new network since the logical connections used to create the networks are different, even if one logical network was used to during the creation of another. Shida's network is not created in response to a situation, given that it already exists at the time of the event. This is obvious given that no new logical connection needs to be created at the time of the situation. Shida's network, and therefore the logical connections that define it, exist before, during, and after the situation. For instance, Shida notes a subscriber's "terminals carry out the wireless communication with two or more base stations, and the signal from the base station that receives the signal with the highest reliability may be finally adopted."¹² Shida's system tracks the location of a user based on the base station providing the most reliable signal. "Whenever the subscriber terminal changes its existing region, the carrier server 9 updates the

¹² Shida, ¶ [0028].

regional subscriber table.”¹³ Performing the operation of updating tables in response to a subscriber terminals communication with different base stations requires the subscribers’ devices be connected to the system *prior to* an event or situation.

81. The tracking of users prior to the occurrence of the event of situation is confirmed by the manner in which Shida’s system determines the location of a situation or event – shown in Fig. 2, reproduced below.

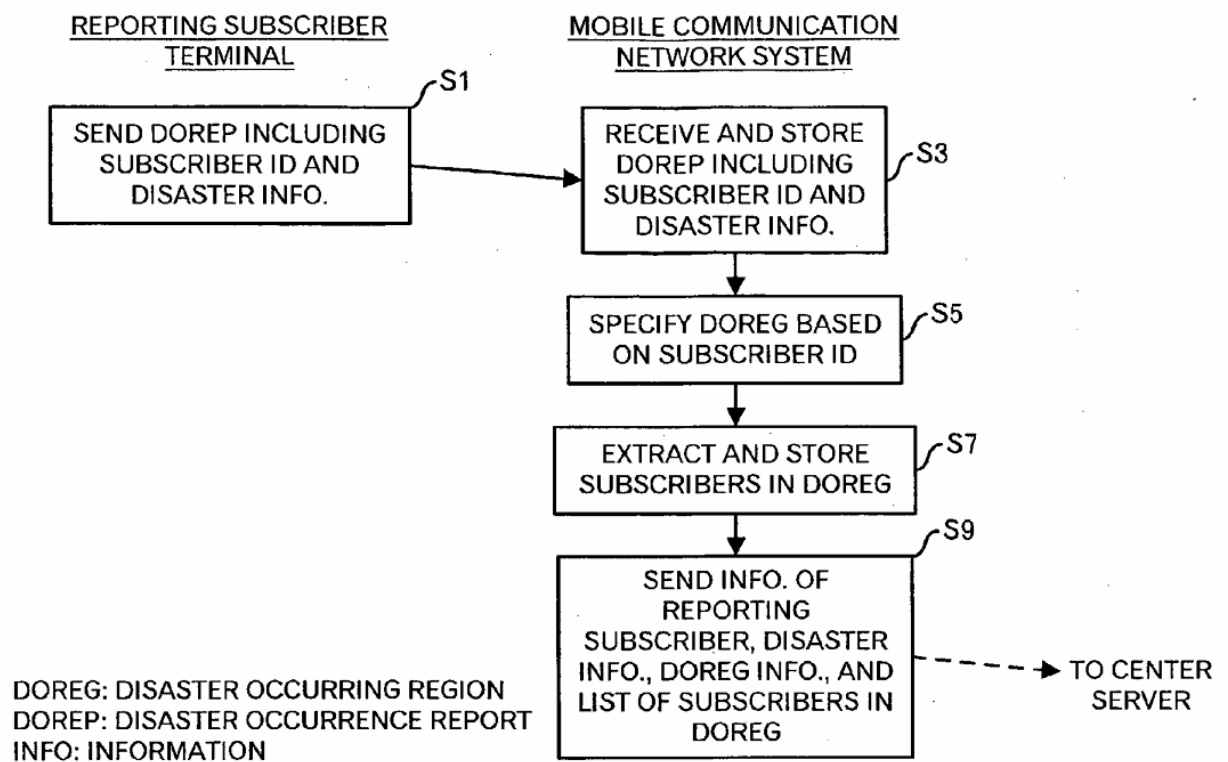


FIG.2

82. At S1 with a “reporting subscriber terminal 53 generates the disaster occurrence report including the input disaster information and own subscriber ID,

¹³ Shida ¶ [0036].

and transmits it (step S1).”¹⁴ Next, “the carrier server 9 receives the disaster occurrence report including the Subscriber ID and disaster information from the reporting subscriber terminal 53, it temporarily stores the report in the Storage device (step S3).”¹⁵ After receiving and storing the report, “the carrier *server 9 retrieves the regional subscriber table* stored in the regional subscriber table storage unit 91 *by the received subscriber ID, and specifies the disaster occurring region* (step S5).”¹⁶ Thus, by looking up the location of a reporting user in a regional subscriber table Shida’s system determines a location of an event or situation. Accordingly, Shida’s system utilizes constant tracking of user to determine the location of an event or situation. This necessitates the user devices are connected to the system prior to the occurrence of an event or situation. Thus, Shida’s system is a network including participant devices formed prior to the occurrence of an event or situation.

83. Furthermore, alterations made to Shida’s network, such as the addition of a subscriber, that occur during event will continue to persist after the event. As described above, alterations made to a distinct situational network should not affect any network used during its creation. For this reason, we can conclude that Shida’s network is not a network created in response to a situation that will be destroyed

¹⁴ Shida, ¶ [0033].

¹⁵ Shida, ¶ [0033].

¹⁶ Shida, ¶ [0034] (emphasis added).

once the situation has ended, but is instead a single network that exists before, during, and after the event. For the reasons stated above, Shida does not form a situational network or authority.

84. Thus, it is my opinion that Shida does not disclose and/or render obvious any of the claims of the '345 Patent.

a. Sinha Does Not Remedy The Deficiencies Of Shida

85. It is my opinion that the alleged prior art, Sinha, does not remedy the deficiencies of Shida. Therefore, the alleged prior arts do not disclose and/or render obvious the claims of the '345 Patent alone and/or in combination with one another.

86. As stated above, the Shida does not form a situational network, situational authority, or an event node. As such, it is also my opinion that Sinha cannot remedy the deficiencies of Shida. Furthermore, combining Sinha with Shida does not render obvious any of the claims of the '345 Patent.

87. Both Sinha and Shida assume that the participants in the network are known to the business continuity application (Sinha) and the central server (Shida). Furthermore, the discovery of new users or new users discovering their systems is not allowed by either Sinha or Shida. As such, neither patent alone nor in combination with one another can fulfill an operation of a situational network disclosed in '345. Fundamentally, Sinha and Shida assume all users are known to a

central server, but ‘345 allows both the situational authority and the user to “discover each other” (8:3).

88. The IPR states that combining Shida and Sinha would allow the central server to create a “message board and roll call to Shida’s subscribers in the disaster area, as well as to concerned parties, such as friends and families of the subscribers, in accordance with Sinha’s teachings.” Sinha does not create a public messaging board but a message board “to an employee of the workforce” (Sinha: Claim 18). Further, this message board is “created by a program stored on a portable memory device” (Sinha: Claim 18). Sinha in no way teaches a public message board concerned parties can access. A POSITA would recognize that expanding Shida’s central server using Sinha’s private application would not create a public message board. Thus, Sinha does not render claims 4 and 16 obvious.

89. The IPR wrongly conveys that managers are responsive participants who can view the roll call list and respond on behalf of non-responsive users. The IPR fails to recognize that a manager is a subset of users, thus, not all users can request the roll call list and respond to non-responsive users. For example, consider if no manager is affected by the situation. Then, no responsive participants can “request [] to view the roll call list [and] indicat[e] the status of non-responsive participants” (‘345: Claim 2). Thus, Sinha does not teach claims 2, 9, and 14.

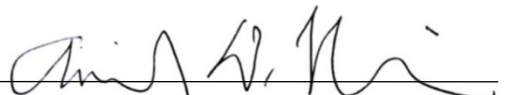
90. For the reasons, stated above, the alleged prior arts do not disclose and/or render obvious the teachings of Patent '345.

VIII. CONCLUSION

91. My analysis of the materials produced in this investigation is ongoing and I will continue to review any new material as it is provided. This declaration represents only those opinions I have formed to date on the topics addressed herein. I reserve the right to revise, supplement, and/or amend my opinions stated herein based on new information and on my continuing analysis of the materials already provided. In that connection, I reserve the right to address any evidence that Defendants provide for the above-described issues and to otherwise address issues raised in Defendants' expert reports.

92. I am a U.S. citizen, a resident of the United States, over 18 years of age, and mentally competent to make this declaration. I have personal knowledge of the facts stated in this declaration and could testify competently to them if asked to do so.

93. Executed this 3rd day of December 2024 in Annapolis, MD.


Aviel D. Rubin