

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 Numbers: IPR2024-00529,
) IPR2024-00530
)
)
)
)

EXPERT REPORT OF DR. AVIEL D. RUBIN



Aviel D. Rubin

June 13, 2024

TABLE OF CONTENTS

I.	INTRODUCTION	2
II.	QUALIFICATIONS	2
III.	PERSON OF ORDINARY SKILL IN THE ART (POSITA).....	6
IV.	SUMMARY OF PATENTS	6
	A. U.S. Patent No. 9,877,345 (‘345 Patent).....	6
	B. U.S. Patent No. 8,332,454 (454 Patent).....	8
	C. Relevant Definition.....	10
V.	OVERVIEW OF THE ALLEGED PRIOR ART	11
	A. Amidon	11
	B. Wong.....	12
	C. Gogic.....	13
	D. Gage	15
	E. Mitchell.....	16
	F. Shida	16

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 and U.S. Patent No. 9,877,345 (“the 345 patent”) in IPR2024-00530. 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. 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. PERSON OF ORDINARY SKILL IN THE ART (POSITA)

23. In my opinion, a person of ordinary skill in the art at the time of the invention would have a bachelor’s degree in computer science (or an equivalent degree) with at least three years of experience in the field of computer science (or an equivalent). This level of skill is approximate, and more experience would compensate for less formal education, and vice versa.

IV. SUMMARY OF PATENTS

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

24. The 345 Patent 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. 345 Patent, 4: 3-15, 15:4-10.

25. 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. 345 Patent, 23:65-24:23.

26. The situational network can be implemented in a multi-dimensional social network (NDSN) that allows multiple connections between individual nodes. 345 Patent, 6:11-18. Projections of the NDSN take a subset of the connections subject to criteria to create a smaller and more relevant network. 345 Patent, 16:53-57. Nodes within an NDSN can query their neighbors to discover new nodes that meet a criterion to initiate a connection. 345 Patent, 18:18-24. Thus, users within a situational network can identify other users within the situational network to connect with.

27. The 345 Patent discloses a “roll call query” that allows the event node to query the user and receive a response of the status of the user for the given event. 345 Patent, 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. 345 Patent, 25:23-26, 26:51-56. A user can share personal or situational information with other users in the situational network. 345 Patent, 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. 345 Patent, 26:65-27:3.

B. U.S. Patent No. 8,332,454 (454 Patent)

28. The 454 Patent teaches a method of creating a projection of a situational network (SitNet) including creation, by an event node server, an event node in a multi-dimensional personal information network, where the event node corresponds to a situation. 454 Patent, Abstract.

29. A SitNet is created when an occurrence or expected occurrence of an event or situation causes connections (links) to be established between, within, or among a set of participants (*i.e.*, users, groups, entities (454 Patent, 14:33-35)). 454 Patent, 3:60-64. A SitNet allows the participants to interact and exchange information over connections regarding the event or situation. 454 Patent, 3:64-67. A SitNet can be used to efficiently deliver and propagate a message or notification from a single user related to a situation or event to an expanded group of individuals who are directly or indirectly affected by the event or situation. 454 Patent, 29:59-63. Some, or all of the participants included in the SitNet may have no prior connections with each other participants of the situational network. 454 Patent, 4:1-5. The data sent between users may be diverse (*e.g.*, voice, video, text).

30. The participants may include external entities, also called situation authorities that generally are able to aggregate and provide comprehensive information related to the situation. 454 Patent, 4:6-10. Situation authorities include, but are not limited to news organizations, such as news agencies, weather agencies, traffic agencies, emergency relief organizations, and government agencies. 454 Patent, 4:10-17. There is a corresponding situation authority server, also referred to as an event node server, for each situation authority. 454 Patent, 4:17-19. The event node server may be connected to a database for storing information related to an event or participants in a SitNet. 454 Patent, 4:20-23. Event node servers create event nodes based on events and may create multiple event nodes for a single event. 454 Patent, 20:20-21. Additionally, one

event may have multiple event nodes created by different event node servers. 454 Patent, 20: 21-22.

31. Participants are connected to the SitNet by devices generally known to those skilled in the art (*i.e.*, cell phones, PDAs, computers, network servers, PVRs, navigation systems, etc.) that enable connection to, from, and through a computer network. 454 Patent, 4:25-30. A participant is required to have at least one device but may have any number. 454 Patent, 4:23-33. These devices may connect to a SitNet automatically via a connection request, or through an invitation to join the SitNet. 454 Patent, 4:33-35. Connections (*i.e.*, links) between participants may be temporary, or persistent. 454 Patent, 4:37-38. These connections may communicate with each other using a wide variety of available hardware and technologies generally known in the art (*e.g.*, TCP/IP over Ethernet or a wireless network). 454 Patent, 15:22-25. Furthermore, a SitNet may be created using a diverse set of computer products, software, programming languages, and hardware. 454 Patent, 31:58 - 32:55.

32. Examples of events (*i.e.*, situations) that might initiate the formation of a SitNet include weather phenomena, such as hurricanes, tornadoes, severe thunderstorms, or winter storms; emergency situations, such as building fires, aircraft crashes, or toxic Substance releases; natural disasters, such as earthquakes, tsunamis, or floods; weather-related activities, such as skiing or Surfing; navigation and/or travel incidents, such as road closures or construction, vehicle accidents, traffic congestion, roadway debris, or air turbulence; and public health crises, such as disease outbreak. 454 Patent, 4:48-58. If the event changes over time (*e.g.*, scope or location), the users included in the SitNet may also change. 454 Patent, 4:63-67, also called a Dynamic SitNet. Additionally, users may be included in a SitNet if they change location and fit the conditions of the SitNet. 454 Patent, 5:9-11. Links and event nodes may be temporary. 454 Patent, 20:32 - 21:22.

Additionally, a SitNet may be used to provide targeted advertisements to users connected based on aggregated user information via a situational authority. 454 Patent, 27:35-40.

33. A SitNet may be formed when users involved in a situation or event are determined to be in relatively close geographic positions. 454 Patent, 5:46-48. Users may join a SitNet without a request/invitation from a situational authority by sharing GPS locations to form a proximity-based SitNet. 454 Patent, 5:54-65.

34. A variety of different architectures may be used to connect the devices of participants in the situational network (*e.g.*, centralized, decentralized, combinations), also referred to as an N-dimensional social network (NDSN). 454 Patent, 6:30 – 7:52. The NDSN uses multiple dimensions of association to characterize the relationships between users or members. 454 Patent, 14:36-38. The NDSN permits the user to discover and utilize indirect relationships with other users that are connected, through first-degree users. 454 Patent, 14:46-48. The NDSN can also provide a 'projected' view of a subset of the members of the NDSN to the user based on a subset of the NDSN's multiple dimensions. 454 Patent, 14:53-55. Each relationship between two users in the NDSN may have an attribute of affinity, *i.e.*, trust or alignment. 454 Patent, 15:52-53.

C. Relevant Definition

35. **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. For example, a “link” could be when users “become friends” or a user subscribes or “likes” a page or “follows” an influencer. 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.

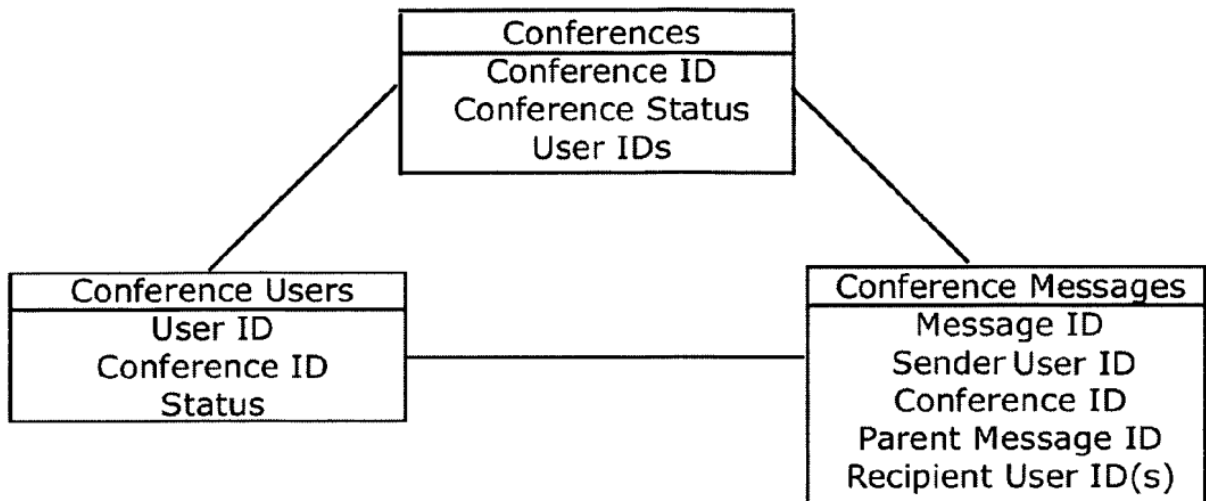
V. OVERVIEW OF THE ALLEGED PRIOR ART

A. *Amidon*

36. Amidon teaches computer-based systems and methods that provide management options for members of a network whereby the members can define and participate in conferences, with the extent of the participation and messaging within such conferences is based on the structure of the underlying network(s). (Amidon, Abstract). However, Amidon fails to teach an “event node” and an “event node server.”

37. Firstly, Amidon does not disclose an event node. An “event node” as described in the 454 Patent is a node in a personal information network that corresponds to an event. 454 Patent, Abstract. Even if one were to consider the Petitioner’s view that the node is in a “situational network,” the node is still created by an event node server. *Id.* An invitation is transmitted to establish a link with the event node server to the device corresponding to each node in the projection.” *Id.* As such, the event node taught by the 454 Patent operates as a member of a social network by being included within the social network and appearing analogous to a user.

38. The disclosures of Amidon do not describe such an event node nor an event node server. In order for an event node to appear analogous to a user within the social network conferences disclosed by Amidon, it would have to participate in the social network conference. Yet, the data structures defining and tracking a network presented in FIG. 3 of Amidon fail to include an event or situation.



Amidon, FIG. 3. Likewise, the depictions of the network conferencing group presented in FIGS. 4 and 5 only include users. For there to be an event node, and consequently an event node server, the conferences data structure would have to include an event or situation that manifest itself as a node analogous to the user within the network conference depicted in FIGS. 4 and 5. As neither is shown, Amidon unmistakably fails to disclose an event node server hosting an event node.

B. Wong

39. Wong teaches a method for generating a network of living and non-living entities Wong, Abstract. A user can be defined as a node (*e.g.*, people (living and deceased), places, objects, and animals), and the connection (links) between nodes constitutes the network. Wong ¶ 21. The network of these entities is hosted through server(s) that have a connection to a computer network (*i.e.*, the internet, LAN, WAN, etc.). Wong ¶¶ 17, 45. Users interacting with this network will have access and a means of communication to the same internet infrastructure as the hosting server(s). Wong ¶¶ 17, 44.

40. However, Wong fails to teach an “event node server.” By its very name, an “event node server” would be a server that hosts an “event node” on a personal information network

corresponding to the event or situation. Even if one were to consider the Petitioner’s view that the node is in a “situational network,” these “event nodes” are not discussed in Wong. Again, Wong teaches a node is a person, place, animal, or object – not an event or situation. Therefore, Wong fails to disclose an event node server hosting an event node.

C. Gogic

41. Gogic teaches a system, method, and media for providing group communication services to an ad-hoc group formed according to the vicinity with other users of communication devices in a communication system. Gogic, 2:21-24.

42. The participants of an ad-hoc communication group are shown in FIG. 4, reproduced below.

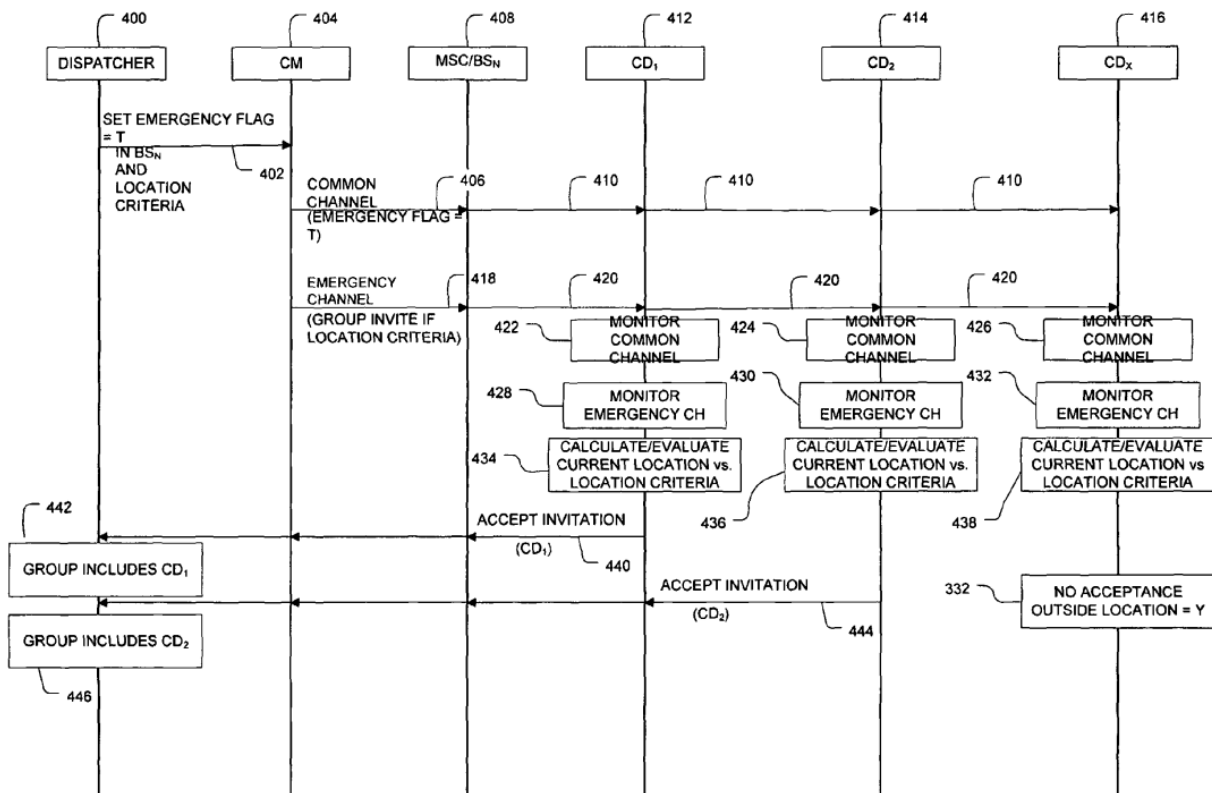


FIG. 4

43. Some of the depicted participants are communication devices (CD), which are generally terrestrial wireless telephones capable of converting media, typically human speech, into data packets suitable for transmission over a data network. Gogic, 6:38-40. Communication devices typically comprise an antenna, a display, keys, a speaker, an earpiece, and an optional push-to-talk (PTT) switch. Gogic, 6:41-42. CDs further include conventional transmitters and receivers for compatible interaction in the wireless communication system. Gogic, 6:48-50.

44. Another participant is communication manager (CM) that defines exclusive transmission privilege which generally allows only a single user to transmit information to other group members at any given time via a CD. The transmission privilege is granted or denied to requesting group members, depending on whether the transmission privilege is currently assigned to another group member when the request is received. Gogic, 6:60-66. The CM defines schemes to evaluate factors such as priority levels assigned to each CD in determining whether a requesting group member is granted the transmission privilege or “floor.” Gogic, 7:4-6.

45. A third participant is a mobile switching station (MSC) for processing data packets and is thus a packet switch for routing data packets in accordance with IP protocols. Gogic, 8:14-20. The MSC thus provides the infrastructure permitting communication amongst the participants.

46. The final participant is the dispatcher that organizes the ad-hoc communication group by initiating the group and managing its membership. Gogic, 10:19-25 and 11:6-9.

47. None of the participants correspond to an event or situation that is analogous to a user, indicating the ad-hoc communication group lacks an event node and corresponding event node server.

D. Gage

48. Gage teaches “a method for reporting a status indicator using a mobile device during a disaster. Gage, 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.” Gage ¶ 19. However, Gage’s disaster response system does not comprise a situational network. A situational network is a type of social network, and a POSITA would not recognize Gage’s disaster response system as a social network. As previously stated, in a social network, individuals are interconnected by various personal information and social metrics. However, the only networks Gage discloses are “network 250” and “network 252” that comprise “hardware/software/and firmware necessary to convey digital content encoded within carrier waves.” Gage ¶ 33. These networks do not represent a social network but rather merely provide components that establish data and telephony telecommunication networks. While a social networking service may require the use of a telecommunications network for access, that sort of access network should not be confused with the social network itself, as the Petition has done.

49. Further, Gage fails to teach the connections of a situational network being formed *when* an event or situation occurs. Gage teaches that the connections with “subscribers” in the disaster response system are established *prior to* an occurrence or expected occurrence of an event. For example, Gage details that “when a disaster is detected, mobile devices of **subscribers** can be queried for location and wireless connectivity by a centrally located disaster response system.” Gage ¶ 9 (emphasis added). Subscribing to Gage’s disaster response system requires establishing a connection with the disaster response system *prior to* the occurrence or expected occurrence of an event or situation. This established connection is formed for an indefinite time *prior to* the occurrence or expected occurrence of an event or situation, not *when* the event or situation occurs.

E. Mitchell

50. 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.” Mitchell, Abstract. More specifically, the defined system operates in response to a crisis coordinator initiating the headcount system upon learning of a crisis. Mitchell ¶ 32. This triggers a predefined email/voice notification to be sent to every person associated with the crisis-event site. Mitchell ¶ 33. The receivers of the notification are then able to send an acknowledgement of the signal back to the crisis coordinator. Mitchell ¶ 34. This response carries personal identification and updates that person as “outside” the crisis site. Mitchell ¶ 34. The acknowledged persons no longer receive alert signals. Mitchell ¶¶ 34, 40. Furthermore, a checklist of specific individuals must be present in a database. Mitchell ¶¶ 35, 48. The alert system ends when all persons have checked in with the system. Mitchell ¶¶ 47.

51. Mitchell is applied in the Petition in combination with Gage; however, Mitchell fails to cure the deficiencies found in Gage. Specifically, Mitchell provides no disclosure of a “situational network” and fails to disclose the connections of a situational network being formed *when* an event or situation occur.

F. Shida

52. Shida discloses a method of confirming the safety of “subscribers in the disaster occurring region.” Shida, Abstract. The system utilizes base stations, a carrier server, and computer network that collectively form a mobile communication network system to establish data and cellular communication channels. Shida ¶¶ 27, 29. Shida teaches a center server that has a “emergency measure information,” a “regional map,” and a “disaster region subscriber table.”

Shida ¶ 30. The center server is also connected to an “operator terminal [] in facilities such as fire stations and police stations.” Shida ¶ 30.

53. Shida thus discloses the use of computer network 1 and a mobile communication network. The connections forming the networks, as such, would be data and/or cellular channels. This is completely different from, as detailed *supra*, the connections forming a *social network*, which are links representing the personal information and social metrics that interconnect users of the social networking service, such as “friendship,” “work colleague,” “classmate,” “likes,” and “follows.” While a social networking service would require the use of a telecommunications network for *access*, that sort of access network should not be confused with the social network itself, as the Petition has done. Accordingly, Shida fails to disclose a “situational network” as defined in the specification and claimed.

54. In addition to confusing the connections used to access a “situational network” with those used to form a “situational network,” Petitioner has not demonstrated that the connections are formed at the required time. The connections formed between Shida’s center server and “subscribers” are formed *prior to* the occurrence or expected occurrence of an event or situation, not *when* the event or situation occurs.