

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

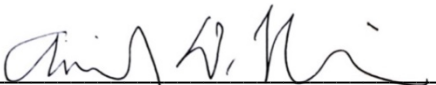
META PLATFORMS, INC.,
Petitioner

v.

SITNET, LLC,
Patent Owner

)
)
)
) Case Numbers: IPR2024-00529
)
)
)
)
)

AMENDED EXPERT REPORT OF DR. AVIEL D. RUBIN



Aviel D. Rubin

December 4, 2024

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	BACKGROUND AND QUALIFICATIONS	1
III.	CLAIM CONSTRUCTION.....	5
IV.	PERSON OF ORDINARY SKILL IN THE ART (POSITA).....	8
V.	OVERVIEW OF THE ALLEGED PRIOR ART	8
	A. AMIDON	8
	B. WONG	10
	C. GOGIC.....	14
VI.	SUMMARY OF PATENT	16
	A. U.S. PATENT NO. 8,332,454 ('454 PATENT)	16
VII.	THE '454 CLAIMS ARE VALID OVER THE INSTITUTED GROUNDS AND ART.....	19
	A. AMIDON DOES NOT TEACH OR SUGGEST THE LIMITATIONS OF THE '454 PATENT CLAIMS.....	19
	B. WONG/GOGIC COMBINATION DOES NOT TEACH OR SUGGEST THE LIMITATIONS OF THE '454 PATENT CLAIMS	26
VIII.	CONCLUSION.....	33

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 application operating on each of the devices”	caus[e/ing] a redirection of a web browser application operating on each of the 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 devices 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 advertisements [. . .] 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.

34. **Node** - A node within a social network is an object that has attributes defining the node. A node can be various types of objects. For example, Meta defines in their Graph API documentation that “a node is an individual object with a unique ID. For example, there are many User node objects, each with a unique ID representing a person on Facebook. Pages, Groups, Posts, Photos, and Comments are just some of the nodes of the Facebook Social Graph.”¹ Thus, in addition to the connections (i.e., edges) of the graph, a node has attributes that contain unique properties about the node.

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

35. 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. AMIDON

36. Amidon teaches a computer-based systems and methods provide additional management options for members of social networks whereby the members can define and participate in conferences, with the extent of the participation and messaging within such conferences based on the structure of the underlying social network(s) (Abstract:1-6). The present

¹ <https://developers.facebook.com/docs/graph-api/overview/>

disclosure also refers to the relay of communicated data over a network such as the Internet but may operate over other network types (e.g., dial-in networks, LANs, WANs, PSTNs, or intranets) (6:11-17). This system primarily involves communications via instant messaging (IM). However, one of ordinary skill in the art will understand that the principles and teachings contained herein are applicable not only to IM systems but any other suitable network-based communication technology (e.g., e-mail, web-based communications, SMS, file and content sharing, audio communications, video communications, etc.) (6:49-57). Furthermore, multiple social networks and/or multiple portions of social networks may be utilized in defining conferences and messaging within conferences (7:65-67).

37. This system includes a messaging server and a social network server. Additionally, this system includes stores (i.e., databases) that maintain information about the status of various aspects of the system. The servers access instructions stored in a database(s), and the instructions configure the servers to provide social network conferencing functionality (8:4-11). Conferencing clients (i.e., one or more computing devices each accessing instructions that configure the client to provide messaging functionality) interface with this system (8:15-16). The social networking and conference functionality may be modularly decoupled or combined in a single application (8:23-35).

38. Key functionality is that all users who wish to participate in the conferencing must be directly connected to a conferencing client, the conferencing system, or a social network (8:45-59). After connection and download of metadata, conference clients may operate with each other in a P2P fashion (20:8-10). The relationships of users in a conference may be defined externally through the underlying social media network (9:9-22). Conferencing relationships may be defined by metadata (e.g., degrees of separation, geographical location, relationships, active/inactive) that

is stored in the social network, calculated dynamically, or given by a user (9:39-67). This metadata is used as direct parameters for the creation of the conference network (10:11-19). These inclusion criteria may span multiple social networks (10:29-31).

39. After the establishment of the conference, message sending may be further restricted to selected participants or widely broadcast to all participants (10:47-51). These message inclusion parameters are handled by the social network servers (10:59-62). The parameters may be used to access cached messages to receive filtered messages (11:29-34). Users may specify any number or combination of rules, preferences, and parameters in defining the extent of conference participation, distribution of messages, and distribution of replies to messages (12:37-40). Inclusion criteria may define different permissions such as viewing, contributing to, or moderating the conference (13:8-17).

40. The system may automatically form a conference including all users currently listening to the same song, music by the same artist, music of the same genre, etc. (14:1-3).

B. WONG

41. Wong teaches a method for generating a network of living and non-living entities (living and nonliving users) (§ 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 (§ 21). The network of living and non-living entities is hosted through social networking server(s) that have a connection to a computer network (i.e., the internet, LAN, WAN, etc.) (§ 17, 45). Users interacting with this network of living and non-living entities will have access and a means of communication to the same internet infrastructure as the hosting social network server(s) (§ 17, 44). Furthermore, all data pertaining to the social network can be categorized, sorted, and stored in the same database (§ 36).

42. Users initially gain access to the network of living and non-living entities through a website that prompts registration information (i.e., name, gender, address, birth date, username and password) (§ 18). The user is assigned a node along with a UUID and this node is designated as active (§ 18). There are four preferred main types of nodes (e.g., represent people (living and deceased), places, objects and animals), but the number of main types can be any number (§ 21, 22). Each main node type can have any number of subtypes/designations, and each subtype may have further subtypes (§ 22).

43. There are three designations of nodes: active, potentially-active, and inactive (§ 29). These designations are designated as follows. Active nodes are ones where the node in question was created by the specified (registered) entity (§ 29). Potentially-active nodes are ones whose associated entity is a live person or organization of persons but who have not registered with the system (§ 29). Inactive nodes are ones whose associated user is deceased, or which represents an entity other than a living person or organization of living persons (§ 29). The designation of a node may change where inactive nodes will always be inactive (unless creation errors occurred), potentially-active nodes can become active when the living person associated with the node registers with the social network, and active nodes become inactive when the person associated dies (§ 30, 40).

44. An active node can contain information pertaining to the living individual person that it represents, communication tools, data and files, storage space, network information and tools to edit the network of living and non-living entities (§ 29). A user may edit his/her node in a multitude of ways such as building a network of living and non-living entities, editing a network of living and non-living entities, and communicating with other entities in the social network at large (§ 19).

45. An inactive/potentially-active node can contain information pertaining to the entity that it represents (i.e., a home page, communication tools, data and files, storage space, and tools to allow one or more living individual persons to view, add, edit, or delete information pertaining to the entity) (§ 29, 31, 32). Specifically, an inactive node can also contain communication tools that allow living individual persons to exchange information pertaining to the entity that it represents (§ 31). Furthermore, a potentially-active node can contain invitation tools to invite the entity the node represents to register with the network (thus changing this node to an active node) (§ 32, 40).

46. Regardless of node designation, a user may expand and edit their network of living and non-living entities by adding nodes and links between nodes (i.e., direct links between two adjacent nodes or a chain of links between non-adjacent nodes), editing previous nodes and links, sending/accepting personal network join invitations, communicate with other nodes inside/outside their personal network, edit user permissions to their personal network, share/compare information in their personal network, and use any features of the main social network (§ 42).

47. Each node type/subtype can be linked to any other node of the same node type/subtype, or a different node type/subtype in the same network (§ 23). The type(s) of links which can exist between two nodes depends on the node type/subtype of the nodes to be linked and represents the types of relationships between nodes (§ 23). Links need not be symmetrical (i.e., parental links), but each linkage type represents the actual relationship type that exists between a node and any other node type (§ 23, 24). Nodes can be linked by more than one linkage type (§ 33).

48. Any user (i.e., active node) may create another node (§ 26, 27). First, the user selects a main node type (e.g., person, place, object, or animal) (§ 26). Next, the user selects a node subtype

from a given list, or types an acceptable subtype, and creates further node subtypes as necessary (§ 26). Finally, the user fills out node information (e.g., name, description) (§ 26). After a node is created it may then be linked to existing nodes in the social network by locating that node (i.e., clicking on the node, identifying its unique identifier, or by searching keyword identifiers) and defining a linkage type (§ 27). The linkage type is selected from a list of pre-existing types, or an acceptable type is created (§ 27). A network of living and non-living entities may be created by uploading a file describing the structure such as a GEDCOM file (§ 37).

49. Each node may be viewed by the user or third parties as a web page having features designated by the user it represents (§ 22). However, only a living individual with an active node can view the link, or chain of links, between its node and any other node in the network (§ 34). The network of living and non-living entities can be viewed graphically as a set of nodes connected by their associated linkages, or as a list, and this view may be changed to show different nodes as the root (§ 35).

50. The network of living and non-living entities can be edited by living individual persons who are represented by active nodes within the same network of living and non-living entities or another network or outside the network of living and non-living entities in the system (§ 38). An active node may only be edited by the entity that the node represents, or by another active node (provided permissions are given) (§ 39). Whereas, inactive/potentially-active nodes can be edited by any active node (§ 38, 39). The permissions to edit an active node are defined by the entity that represents that node and any other active node that this edit will affect (§ 40).

51. Two separate networks may be merged into one by an entity that has an active node in both of the two respective networks (§ 43). Overlaps between identical entities when merged are handled by a set of questions to define the final node (§ 43).

52. Communication (i.e., notification of updates, alerts, sharing of files and photos, blogs, instant messaging, and comments) is facilitated by the underlying social network infrastructure (§ 44). The sender selects those in the network who can receive or view a particular communication (§44).

C. GOGIC

53. 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 (2:21-24). A group is formed based on location criteria, by sending an invitation request to a plurality of devices (2:27-30). Group membership is decided by each of the plurality of devices based on the inclusion of the location criteria received (2:31-35). Permission to transmit in this group is given to one of the devices in this plurality (2:35-38).

54. Specifically, an invitation to join the ad-hoc group is widely broadcast with criteria for membership (4:30-31). The invitation-recipient communication devices (CDs) determine if they are inclusive of the membership criteria (4:31-32). CDs that are inclusive of the membership criteria respond to the invitation with an acceptance of the invitation (4:33-34). The “floor” or permission to speak is managed by a dispatcher (communication manager/CM) to manage voluminous requests to speak, prioritize speakers, assist disabled speakers, and release speakers who may become unable to relinquish the permission to speak (4:35-39).

55. The process is described for CDMA but can be used with GSM, AMPS, TDMA, Satellite, and others (4:40-44). The process is not limited to wireless communication systems. It can be used with wireline telephones, paging devices, portable or desktop computers, digital cameras, video cameras, etc. (4:45-49). The data transmitted is broad (e.g., audio, video, files, email) (4:50-57) and can be used over many protocols (e.g., internet, wireless) (9:1:4, 9:25-27).

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

57. Exclusive transmission privilege is defined (by the CM) which generally allows only a single user to transmit information to other group members at any given time. The transmission privilege is granted or denied to requesting group members, depending on whether or not the transmission privilege is currently assigned to another group member when the request is received (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” (7:4-6). The CM manages the real-time and administrative operation of groups, including PTT request arbitration (e.g., floor request/grant/deny), maintenance, and distribution of group membership and registration lists, call set-up and tear-down of necessary system and communication resources, as well as overall control of group or net status (7:10-16). The CM maintains a list of defined groups and is designed to be managed remotely by either a communication system service provider, group members, or both, assuming that authorization is provided by the service provider (7:17-20). The CM maintains one or more databases for managing information (e.g., a telephone number, or dial number, associated with the member's CD, a Mobile Identification Number assigned to the CD, the current member's status in the group) pertaining to individual group members as well as to each defined net (8:45-58). The CM can be in many places

in the network (8:39-40). Only authorized personnel are allowed to have access to the dispatcher (CM) (10:1-4).

VI. SUMMARY OF PATENT

A. U.S. PATENT NO. 8,332,454 ('454 PATENT)

58. 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 (Abstract).

59. 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 (14:33-35)) (3:60-64). A SitNet allows the participants to interact and exchange information over connections regarding the event or situation (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 (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 (4:1-5). The data sent between users may be diverse (e.g., voice, video, text).

60. The participants may include external entities, also called situation authorities that generally are able to aggregate and provide comprehensive information related to the situation (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 (4:10-17). There is a corresponding situation authority server, also referred to as an event node server, for each situation authority (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 (4:20-23). Event

node servers create event nodes based on events and may create multiple event nodes for a single event (20:20-21). Additionally, one event may have multiple event nodes created by different event node servers (20: 21-22).

61. 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 (4:25-30). A participant is required to have at least one device but may have any number (4:23-33). These devices may connect to a SitNet automatically via a connection request, or through an invitation to join the SitNet (4:33-35). Connections (i.e., links) between participants may be temporary, or persistent (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) (15:22-25). Furthermore, a SitNet may be created using a diverse set of computer products, software, programming languages, and hardware (31:58 - 32:55).

62. 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 (4:48-58). Furthermore, it is possible to anticipate or pre-form a SitNet based on expected conditions (4:60-61). If the event changes over time (e.g., scope or location), the users included in the SitNet may also change (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 (5:9-

11). Links and event nodes may be temporary (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 (27:35-40).

63. A SitNet may be formed when users involved in a situation or event are determined to be in relatively close geographic positions (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 (5:54-65).

64. 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) (6:30 - 7:52). The NDSN uses multiple dimensions of association to characterize the relationships between users or members (14:36-38). The NDSN permits the user to discover and utilize indirect relationships with other users that are connected, through first-degree users (14:46-48). Each relationship between two nodes (users) in the NDSN may have an attribute of affinity, i.e., trust or alignment (15:52-53).

65. A SitNet also provides 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 (14:53-55). Specifically, a projection may be formed using the geographic location from a plurality of devices in the NDSN (29:46-50) and the nodes that represent these devices are linked (22:2-5). The nodes in this formed projection communicate about an event, or situation, thus forming a situational network (14:53-58).

VII. THE '454 CLAIMS ARE VALID OVER THE INSTITUTED GROUNDS AND ART

66. It is also my opinion that Meta Platforms Inc. has failed to disclose and/or render obvious any of the '454 Patent claims in light of all alleged prior art. Here, I discuss how the alleged prior art and combinations do not disclose the claimed invention of the '454 Patent.

A. AMIDON DOES NOT TEACH OR SUGGEST THE LIMITATIONS OF THE '454 PATENT CLAIMS

67. In my opinion, Amidon fails to disclose and/or render obvious the claims of the '454 Patent. There are several unique attributes taught by the '454 Patent that are not disclosed by Amidon, nor would such disclosures have been made obvious to a POSITA.

68. Firstly, Amidon does not disclose an event node. An “event node” as described in the '454 Patent is a node in an N-dimensional social network (NDSN) that corresponds to an event. The node is created by an authority/event node server, and it is disclosed that “an event node server ... configured to ... transmit an invitation to establish a link with the event node server to the device corresponding to each node in the projection”. This provides the technical solution of incorporating into a social graph the concept of transmitting an invitation to establish a link with the event node server to the devices corresponding to each node in the projection (situational network) formed in step (b). As such, the event node taught by the '454 Patent operates as a member of a social network, that communicates with a situation authority/event node server.

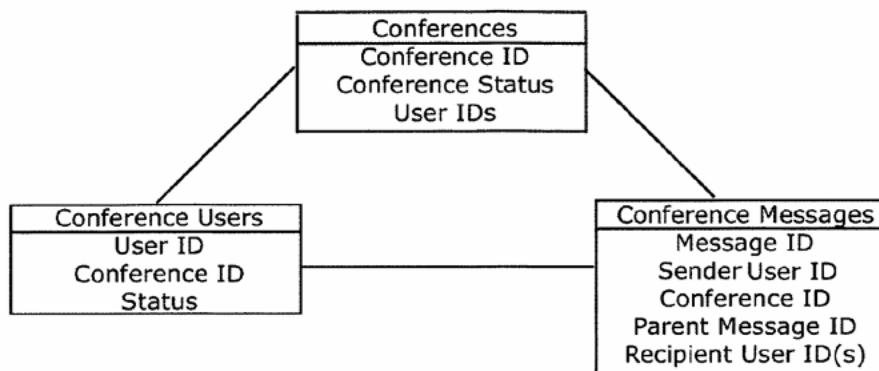
69. A node within a social network is an object that has attributes defining the node. A node can be various types of objects. For example, Meta defines in their Graph API documentation that “a node is an individual object with a unique ID. For example, there are many User node objects, each with a unique ID representing a person on Facebook. Pages, Groups, Posts, Photos,

and Comments are just some of the nodes of the Facebook Social Graph.”² Thus, in addition to the connections (i.e., edges) of the graph, a node has attributes that contain unique properties about the node. The '454 Patent defines “The situation or event itself may also be associated with a node on the SitNet, known as the event node” (7:44-46). Additionally, the 454 Patent, states that “Each node is capable of communicating in a peer-to-peer fashion with other nodes in the NDSN, and thus is a user’s point of connection to the NDSN, providing a user with access to information that can be obtained from other users of the NDSN with whom the user has a relationship.” (15:1-4). Given that an event node “propagates up-to-date information on the situation” and that “each node is capable of communicating in a peer-to-peer fashion with other nodes,” an event node must be a node with an NDSN that communicates information regarding the event in a peer-to-peer fashion with other nodes of a NDSN situational net. Thus, the event node is a node within the NDSN and cannot constitute a social network. The event node cannot facilitate the creation of other nodes. The resulting edges created between event nodes and other nodes within the social network are facilitated by the social network the event node exists in. Furthermore, the event node corresponds to an event and as such, would have the unique properties that define the event.

70. Amidon does not define an event node. A conference as shown in Figure 3 does not have the dynamic connections formed within the network. Figure 3 in Amidon clearly defined as "illustrat[ing] a plurality of exemplary data structures suitable for use in defining and tracking social network conferences". However, petitioner insists that this figure demonstrates that Amidon's conference is a situation network because the conference describes an event node. As stated above, the event node must contain the attributes of the event, which a conference cannot

2 <https://developers.facebook.com/docs/graph-api/overview/>

do. Further, a conference is defined by the American Heritage Dictionary as “a. A meeting for consultation or discussion. b. An exchange of views”.³ This does not define or suggest an NDSN.



71. In contradiction to what the petitioner claims, an event node cannot act as the social network as it exists within the NDSN. This directly contradicts Amidon itself. In fact, Figure 3 from '864 most closely resembles the logical schema found associated with a relational database. As defined in the American Heritage Dictionary, a schema as a plan, outline, or model.⁴ This implies that a database schema is the plan, outline, or model used to create the database. This matches the definition for database schema given by IBM, one of the original⁵ and still primary companies⁶ in the database space, which defines database schema as:

72. "A database schema defines how data is organized within a relational database; this is inclusive of logical constraints such as, table names, fields, data types and the relationships between these entities."

73. Figure 3 in Amidon defines three tables, "Conference Users", "Conferences", and "Conferences Messages" with their respective fields within the architecture of a relational

3 <https://ahdictionary.com/word/search.html?q=conference>

4 <https://ahdictionary.com/word/search.html?q=schema>

5 <https://www.ibm.com/docs/en/zos-basic-skills?topic=now-history-ims-beginnings-nasa>

6 <https://6sense.com/tech/relational-databases/db2-market-share>

database. For example, the "Conferences" table contains the fields "Conference ID", "Conference Status", and "User IDs". The relationships denoted between the different tables are defined as the shared fields between the tables (i.e. foreign keys). For instance, the table "Conferences" has relationships with the table "Conference Users" on the shared fields "Conference ID" and "User ID(s)". Likewise, each "Conference Message" record within the database includes a shared "conference ID" field, or foreign key, relating it to a specific conference. Also, each "Conference Message" within the database has shared "User ID" field (foreign key) relating it to a specific conference user that either received or sent the message. The relationships established by the shared fields are shown in the architecture depicted by Amidon's Fig. 3 as the lines connecting the various records. As such, Amidon does not define an NDSN, but instead discloses that a conference is a database entry containing a list of users relating the conference to the various user records, but does not disclose or suggest objects with attributes defining them. Furthermore, Amidon does not disclose peer-to-peer connections between nodes that are required for nodes within NDSN by '454 Patent. The conferencing disclosed by Amidon uses the centralized relational database as discussed above.

74. The disclosures of Amidon do not describe such an event node. As previously discussed, Amidon discloses a messaging platform that connects social media users based on specific interests and topics and allows for connection to relevant advertisements based on that interest. The IPR petition claims each chatroom and the underlying databases described in Amidon is the event node⁷, however, this is not an event node but simply a multi-party chatroom. The IPR petition also claims that the chatroom can have a specific event as the subject that the chatroom was created on, but this is not sufficient in showing that it is an "event node" like is described in

⁷ '454 IPR Petition at pg. 29

the '454 Patent. As discussed above, the chatroom itself is not a node in a situational network and is not generated by a situation authority/event node server.

75. The failure of the chatroom described in Amidon to disclose the event node taught in the '454 Patent is also not remedied by the ability of advertisers and businesses to have access to the chatroom with the ability to provide advertisements. The event node is a node in a social network that is part of the generated situational network, analogous to a user. As a result, the situational authority and any business or advertiser that is part of the situational network appears to the user as such. An example of this is how advertisers on popular social media platforms like Facebook and Instagram advertise to users in ways that make it appear similar to content created by actual users. However, Amidon's disclosures are not this, and advertisements are provided via traditional mechanisms in the chatroom. Thus, this further demonstrates that the chatroom is not an event node in a situational network.

76. Further evidence that Amidon does not describe an event node server is demonstrated in the IPR petition's failure to map Amidon to Claim 1.3⁸. The IPR petition claims that Amidon teaches the transmission of invitations to join a social network conference is the same as the '454 Patent's "transmitting and invitation ... to the devices corresponding to each node in the projection formed in step (b)."⁹ However, as previously demonstrated above, a social network conference is not an event node, as a chatroom is not a node in the network. Moreover, accepting an invite to a chatroom is not establishing a link in a social media network, as would occur when a "link" is created between two nodes in the social network. For example, a "link" could be when users "become friends" or a user subscribes or "likes" a page. Joining a chatroom as disclosed by

⁸ '454 IPR Petition at pg. 24

⁹ '454 IPR Petition at pg. 24

Amidon (i.e., not an event node or a node in a social network) is not creating a link between an event node and/or event node server with a situational network or grouping of users.

77. The IPR petition also argues the link is there because there could be multiple social networking services involved in a chatroom. However, this does not remedy the deficiencies of Amidon. In the event that users across multiple social media platforms are connected in a chatroom, this still does not establish social media links between users and the chatroom. This is actually further evidence that the chatroom is not an event node, as this shows the chatroom is not a node in a social network, but instead is an application built on top of multiple social networks.

78. In addition to not disclosing an event node, Amidon does not teach a situation authority/event node server. The IPR petition claims the event node server is Amidon's social network itself¹⁰, but this does not meet the language disclosed in the '454 Patent. The situation authority is a party that may act as a peer or central authority depending on the architecture of the network chosen. The server of the situation authority is for establishing an event node for communication to users in a situational network. The '454 Patent also states that the situation authority is not required to be involved in the process of creating a situational network¹¹. Thus, this demonstrates that the entire network described in Amidon cannot be the situation authority or the situation authority/event node server, due to it being required for creating the chatroom in Amidon.

79. The IPR petition also states that Claim 2 is disclosed by Amidon where a user is able to be a situational authority as a user can be an organization¹². However, this still fails to demonstrate a situation authority and/or a situation authority/event node server disclosed by

¹⁰ '454 IPR Petition at pg. 19

¹¹ '454 Patent at ¶¶ 5:53-55

¹² '454 IPR Petition at pg. 45

Amidon. Regardless of the ability of an organization to act as a user in a chatroom, this still does not show how an organization would fulfill the tasks of a situation authority disclosed in the '454 Patent such as facilitating the formation of a peer-to-peer network or the selection of users through a projection to receive an automatic invitation based on information that associates them with a situation.

80. In addition, an organization acting as a user does not create an event node as there is no event node disclosed by Amidon. Even if an event node was disclosed by Amidon, which it is not, there is no evidence that a user or organization acting as a user would be able to create one and use it for the facilitation of communication between end users.

81. Further, the network described in Amidon is different from the situational network claimed in the '454 Patent. The IPR petition describes the users connected to a chatroom as the situation network¹³. Unlike the situational network disclosed in the '454 Patent, the chatrooms described in Amidon are not situation specific. While a chatroom can be created for an event in addition to topics of interest and other social network criteria, the chatroom will live on after a "situation" has occurred. More specifically, when an event ends, the chat does not have to be closed and can continue indefinitely. That is not possible in the disclosures of the '454 Patent, as the situational network is only created temporarily while the situation is occurring and relevant.

82. As further evidence, the IPR states that the content of the chatrooms is not relevant and only the subject for which they are founded is¹⁴. However, this still demonstrates that the situational network does not have to pertain to a specific situation. As such, the information that is conveyed in the chats created on "situations" does not have to be about the situation because it

¹³ '454 IPR Petition at pg. 15

¹⁴ '454 IPR Petition at pgs. 32, 47

is an open messaging platform. This is not an uncommon occurrence and is commonly seen in practice where chats formed on specific topics can become unrelated or off-topic.

83. Amidon also does not disclose the use of targeted advertisements, as is described in the '454 Patent. The IPR petition suggests that because a specific organization can be a part of a chatroom based on the subject for which it was created, the organization is thus capable of targeted marketing to users¹⁵. However, this is not targeted marketing in the way that is done by social media. As previously explained, targeted marketing is accomplished by building profiles of users through various means (e.g., interactions with content on social media, purchase history, demographics, etc.) to provide advertisements to the users for which they are most relevant. This is not what is done in Amidon. Users opt in to a subject or event and a chatroom is created based on it that an advertiser may also be a part of. This is not targeted marketing as a user is actively choosing to associate with an advertiser. In targeted marketing, the advertiser is locating the user without their direct involvement with a specific event or product. Thus, Amidon does not disclose the use of targeted marketing.

84. Therefore, it is my opinion that Amidon does not disclose and/or render obvious any of the Claims of the '454 Patent.

B. WONG/GOGIC COMBINATION DOES NOT TEACH OR SUGGEST THE LIMITATIONS OF THE '454 PATENT CLAIMS

85. It is my opinion that Gogic in combination with Wong also does not disclose and/or render obvious the limitations of the '454 Patent. The reasoning for this is provided here.

86. First, a POSITA would not have been motivated to combine Gogic with Wong as such combination would have been technically infeasible. The disclosures of Gogic are a method

¹⁵ '454 IPR Petition at pg. 49

and apparatus for forming an ad-hoc location-based multicast group. This is accomplished via leveraging signaling protocols used in telecommunications networks. Specifically, the teachings provided in Gogic are presented with respect to CDMA networks (one of the two most widely deployed 2G cellular technology standards). Gogic also describes that though it is presented with respect to CDMA networks, its teachings can also be applicable to GSM systems (the other widely deployed 2G cellular technology standard), AMPS systems (widely deployed 1G cellular technology standard that was entirely analog), TDMA systems (includes GSM and various other wireless communication technologies), and satellite communication systems. Gogic at ¶ 4:40-46. All of the listed technologies are wireless network technologies. At the time of invention, and in accordance with the technologies listed, these wireless technologies incorporated traditional wireless communication technologies such as circuit-switched networking and traditional telecommunication signaling protocols (e.g., SS7). Moreover, with respect to AMPS, the network technology was entirely analog.

87. Though Gogic claims that devices used in IP-based packet-switched networking environments (e.g., desktop computers) can be incorporated into the network, it would be entirely unclear to a POSITA from the patent disclosures how that would be accomplished and what role the device would play. Gogic requires that location criteria be used to determine which devices have access to ad-hoc networks but does not explicitly define "location criteria". However, from the descriptions and figures provided in Gogic it would suggest that location is determined via technologies specific to wireless networks and telecommunications, such as via mobility management (e.g., which base station a device is connected to in a network). The claims also reflect the requirement of telecommunication technologies such as leveraging a paging channel and/or an emergency communication channel. This, in addition to all independent claims requiring

a "group of a plurality of wireless communication devices", would suggest that devices used in IP-based packet-switched networking environments would not have the same role. Further, even if devices used in IP-based packet-switched networking environments did have the same role, it would not be clear to a POSITA how such a device would be able to participate in the network analogous to the wireless communication devices and/or how location criteria would be obtained without leveraging wireless network technologies.

88. Despite Wong claiming that the patent teachings can be applied to "mobile telephones" (Wong at ¶17, ¶42), the devices are required to have access via the same computer network. These two paragraphs in Wong are the only mention of cellular network technologies in the patent and provide no details on how to incorporate "mobile telephones", which cellular network technologies are supported, and how they could be incorporated into the teachings. Additionally, the claims of the patent do not have any mention of "mobile telephones" or any wireless/cellular communication network outside of a traditional computing device using Wi-Fi. Thus, it would have been entirely unclear to a POSITA from a technical perspective how to incorporate a cellular-connected mobile device into Wong's teachings.

89. Even in the case where a POSITA is familiar with the GPRS cellular technology, this would not remedy the lack of motivation to combine Gogic and Wong from a technical perspective. The General Packet Radio Service (GPRS) was an upgrade to traditional 2G GSM networks that allowed for packet-based communication and began being deployed in 2000¹⁶. While revolutionary, the use of GPRS at the time of invention was limited due to the user perception regarding the high costs¹⁷. In addition, the bandwidth of GPRS was limited even at the

¹⁶ <https://www.techtarget.com/searchmobilecomputing/definition/GPRS>

¹⁷ <https://www.lightreading.com/business-management/commentary-cut-those-crazy-gprs-prices-https://www.lightreading.com/business-management/reports-slams-gprs-prices>

time of both patents' invention, including the enhanced version of GPRS called EDGE. Additionally, while GPRS does allow for communication between traditional cellular technologies and the IP-based Internet, this alone would still not remedy the lack of information regarding how to incorporate IP-based devices into Gogic and cellular/wireless devices into Wong.

90. Further, a POSITA would have understood that the social network described in Wong would not be possible to be added to Gogic. This is because IP-based network access via cellular network-connected devices was both limited and costly at the time of invention. While the use of social media by a non-smartphone (also called feature phones) could have been achieved from a technical standpoint with the use of GPRS, this would not have seen much, if any, use due to usability issues. Meta's own expert admitted that in the relevant time period, it was only theoretically possible to use a social network from a feature phone and was not regularly done. As such, the use of social networking by feature phones at the time of invention would have been entirely nonobvious to a POSITA.

91. In addition, Gogic supports various wireless networking technologies including AMPS which did not have support for cellular to IP-based communication and could not be achieved due to the analog nature of AMPS¹⁸. Thus, the support by Gogic for wireless technologies that do not have any means of communicating with IP-based networks would further indicate to a POSITA that the combination of Gogic and Wong would be technically infeasible, regardless of prerequisite knowledge of GRPS.

92. First, Wong does not teach an Event Node as described by the '454 Patent. When a node is created its "main type" is selected (e.g., person, place, animal, object) as a preliminary

¹⁸ C. Peeters, Developing End-To-End Security Solutions For Redirection Attacks in Legacy Telecommunications Infrastructure (Dissertation), University of Florida Publishing, 2022

step. Wong states “While four main node types are preferred, the number of main node types may be greater or less.” It is however implied that this list of types is static after the initial creation of the network as there is no language such as “the user selects a node sub-type from a menu provided for that node type, or by entering an acceptable sub-type” as there are four sub-types¹⁹. An event does not fit any of the default categories of Wong and would be unable to be created after network creation.

93. If an Event Node were taught by Wong, which clearly is not the case, then the node type would necessarily be an inactive node due to not being a living person²⁰. To edit an inactive node in the network requires an active node (i.e., a living person who is registered with the network). Additionally, this active account must have sufficient permissions to edit nodes and links between specific nodes. This permission is defined as “permission for a living individual person... represented by an active node to edit a linkage[node] in the network... can be defined by living individual persons... who will be affected by the edit²¹.” An editing definition like this means that editing a specific node or linkage requires major permissions from many users in the network. Therefore, permissions could feasibly limit the removal of a created node or the links between nodes. Thus, if the situation was temporary, the node may not be temporary itself.

94. The ‘454 patent teaches of a temporally limited (i.e., temporary) situational network²². Furthermore, ‘454 teaches of a shifting situational network (e.g., scope or event location change) which requires dynamically altering the links of event nodes in the situational network to both potentially remove current nodes and/or add new nodes²³. This dynamic nature of a situational

¹⁹ Wong patent at ¶ 26

²⁰ ‘454 patent at ¶ 29

²¹ Wong patent at ¶ 40

²² ‘454 patent at 20:32-34 | 4:37-39

²³ ‘454 patent at 5:1-11

network contrasts with the semi-permanent nature of the network architecture of Wong as described above. This is a key feature of the '454 Patent and a stark differentiation between Wong/Gogic and the '454 patent.

95. Wong does not teach of a “Situational Authority” as described in '454. Any active user is free to create a new node (regardless of type) in the architecture defined by Wong, which is a contradiction to the definition of a “Situational Authority.” Abuse of event creation may exist with the structure of Wong when applied to “Situational Authorities.” For example, using the IPR petition’s suggested Wong/Gogic combination, any individual may masquerade as a Situational Authority and propagate disinformation about emergency events. Gogic teaches of a “Dispatcher” which is only accessible by authorized personnel, but there are still no checks and balances to this Dispatcher as described²⁴ when used in a network as taught by Wong, which creates the same abuse potential as in Wong alone. Thus, Gogic does not remedy the deficiency of Wong not providing a Situational Authority.

96. Furthermore, Gogic teaches a communication manager (CM) which is responsible for granting transmission privileges to communication devices (CD) in the network²⁵. This CM is responsible for the arbitration of communication within an ad-hoc network and may request or deny communication privileges for any and all CDs²⁶. The scheme devised by Gogic only works when the underlying network supports the ability to block unidirectional/bidirectional communication between linked nodes at will, which Wong simply does not implement. At best, the combination of Wong/Gogic would need to remove links between nodes to stop communication, but this then means that the disconnected node will not receive any of the desired

²⁴ Gogic patent at 10:1-4

²⁵ Gogic patent at 7:7-10

²⁶ Gogic patent at 7:1-6

situational communication, which is fundamentally counter to the desired outcome. Due to this Wong and Gogic are incompatible at a structural level, as described by both patents.

97. The IPR petition states that Wong suggests an “Event Node Server”, as a server for hosting the social network infrastructure²⁷, yet this statement is contradictory to the definition of an “Event Node Server” (i.e. a corresponding event node server for each situation authority)²⁸.

98. Neither Wong alone, Gogic alone, nor the combination of Wong/Gogic disclose or teach the use of targeted advertising within any network. Most critically, the alleged prior arts do not teach targeted advertisements within a situational network as described in the ‘454 patent.

99. A core feature of ‘454 is “a projection of nodes... formed using geographic location...” and this is key to forming an appropriate projection of nodes. The IPR argues a combination of the Wong network structure with Gogic group formation logic. Therefore, a strict requirement is that geographic location be recorded in the node information of every node in the network, which is also noted in the IPR petition²⁹. However, Wong does not impose or teach this strict requirement of geographic information in the nodes. Wong teaches that node information is loose and at the discretion of the creator and while a suggested field of information is an entity's address, there is no means of forcing that information to be filled³⁰. Furthermore, since this information is user-filled, there is a potential of inaccuracy and mistakes, or simply incorrect information entered. It is feasible for a user of a network as described in Wong to be a college student who lists his/her main address as the location of the school they attend but may be home at a different location for summer break. In this scenario, the location information entered for the

²⁷ ‘454 IPR Petition at pg. 54

²⁸ ‘454 Patent 4:17-19

²⁹ IPR petition 2024-00529 at page 68

³⁰ Wong patent at ¶ 18

college student is incorrect over the summer break period. More critically, since the group formation design of Gogic would be built upon the network architecture of Wong, Gogic does not remedy the deficiency of Wong³¹.

100. Therefore, it is my opinion that neither Wong nor Gogic nor the combination of Wong/Gogic discloses and/or renders obvious any of the claims of the '454 Patent.

VIII. CONCLUSION

101. 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.

102. 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.

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



Aviel D. Rubin

³¹ Gogic patent at 4:40-56