

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ERICSSON INC.
Petitioners

v.

KONINKLIJKE KPN NV
Patent Owner

Case No. IPR2023-00525
Patent 10,924,500

**DECLARATION OF DR. JAMES OLIVIER
IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 10,924,500**

Table of Contents

Table of Contents	i
Exhibit List	iii
I. INTRODUCTION	1
II. SUMMARY OF OPINIONS.....	2
III. QUALIFICATIONS AND EXPERIENCE.....	4
A. Education and Work Experience.....	4
B. Compensation.....	8
C. Documents and Other Materials Relied Upon	8
IV. STATEMENT OF LEGAL PRINCIPLES	8
A. Claim Construction.....	8
B. Anticipation	9
C. Obviousness.....	9
V. LEVEL OF ORDINARY SKILL IN THE ART	11
VI. TECHNOLOGY BACKGROUND OF THE '500 Patent.....	14
A. A Brief History of the Evolution of Global System for Mobile Communications ("GSM").....	15
B. The 3rd Generation Partnership Project.....	20
C. Mobility Management	25
D. Tracking Area.....	26
E. Operation of Timers and Sliding Windows	27
VII. OVERVIEW OF THE '500 PATENT.....	29
A. Summary of '500 Patent Subject Matter.....	30
B. Claim Listing.....	32
C. Relevant Prosecution History of Application 14/646,554	32
D. Priority Date	35
E. Claim Construction.....	35
VIII. IDENTIFICATION OF THE PRIOR ART AND SUMMARY OF OPINIONS.....	36

A.	Summary of <i>Eisl</i>	36
IX.	A POSITA’s Reasons to Combine the identified prior art.....	41
A.	<i>Eisl</i> and the Knowledge of a POSITA	41
X.	UNPATENTABILITY OF THE ’500 PATENT CLAIMS	42
A.	Grounds 1-2: Claims 1-3, 5-7 and 9-11 are Unpatentable as Anticipated by <i>Eisl</i> (Ground 1) and Claims 1 – 11 are Obvious in view of <i>Eisl</i> (Ground 2).....	42
1.	Claim 1	42
2.	Claim 2	66
3.	Claim 3	69
4.	Claim 4	71
5.	Claim 5	75
6.	Claim 6	75
7.	Claim 7	77
8.	Claim 8	79
9.	Claim 9	83
10.	Claim 10	84
11.	Claim 11	88
XI.	CONCLUSION	90
XII.	DECLARATION	90

Exhibit List

Exhibit #	Description
EX1001	U.S. Patent No. 10,924,500 to Muller (“the ’500 Patent”)
EX1002	CV of Dr. James Olivier
EX1003	Expert Declaration of Dr. James Olivier
EX1004	International Publication WO2011072719A1 (“ <i>EisI</i> ”)
EX1005	File History of ’500 Patent
EX1006	Claim Listing
EX1007	Report on the Filing or Determination of an Action Regarding a Patent or Trademark
EX1008	Excerpts from Sesia et al., <u>LTE The UMTS Long Term Evolution from Theory to Practice</u> , Second Edition
EX1009	U.S. Patent No. 6,594,241 to Jim Malmlöf (the “’241 Patent”)
EX1010	<i>Flag</i> , <u>A Dictionary of Computing</u> (6th ed. 2008).
EX1011	Frank Muller’s LinkedIn Page
EX1012	Convergence Technologies for 3G Networks – IP, UMTS, EGPRS, and ATM

I, James L. Olivier, Ph.D., hereby declare as follows:

I. INTRODUCTION

1. I am currently a Research Professor and Program Lead for Transformational Technology at the Hunt Institute for Engineering and Humanity, which is part of the Lyle School of Engineering at Southern Methodist University (“SMU”) in Dallas, Texas. The mission of SMU’s Hunt Institute is to partner with leaders in business, academia, and government to develop and scale sustainable and affordable technologies and solutions to the challenges facing people locally and globally.

2. I am also currently an Adjunct Professor in the Telecommunications and Network Engineering Program at SMU’s Graduate School of Electrical Engineering. In addition, I am also the owner of Olivier Consulting, where I provide consulting services for advanced network/product design along with Intellectual Property consulting.

3. I have been engaged by Petitioner to investigate and opine on certain issues relating to U.S. Patent No. 10,924,500 to Muller (EX1001, “the ’500 Patent”).

4. I understand that the ’500 Patent is assigned to Koninklijke KPN N.V. (“KPN”). KPN is also referred to as the “Patent Owner” in this document.

5. In this declaration, I will discuss the technology related to the '500 Patent, including an overview of that technology as it was known at the time of the earliest priority date claimed by the '500 Patent, which I have been informed is November 22, 2012. This overview of the technology provides some of the bases for my opinions with respect to the '500 Patent.

6. This declaration is based on the information currently available to me. To the extent that additional information becomes available, I reserve the right to continue my investigation and study.

7. In forming my opinions, I have relied on information and evidence identified in this declaration, including, without limitation, the '500 Patent, the prosecution history of the '500 Patent, and prior art including the references and other materials mentioned throughout my declaration below. I have also relied on my own experience and expertise in the technologies and systems that were already in use prior to November 22, 2012.

II. SUMMARY OF OPINIONS

8. The '500 patent generally describes “a system for detecting behaviour of a mobile telecommunications device in a telecommunications network.” *See* EX1001, 1:16-18. As I will discuss below in more detail, Claims 1-11 (the “Challenged Claims”) of the '500 Patent were not patentable as of the claimed priority date. *See below* Section X.

9. It is my opinion that Claims 4 and 8 are obvious in light of the prior art discussed below and Claims 1-3, 5-7, and 9-11 are both anticipated and obvious.

10. My declaration is organized as follows: First, in Section III, I discuss my qualifications and background experience. In Section IV, I provide statements regarding the relevant legal principles, as I understand them, that I then apply in later sections. In Section V, I provide an overview of the level of ordinary skill in the art at the time of the alleged invention and then subsequently turn to the relevant technological background at the time of the alleged invention in Section VI. In Section VII, I introduce the '500 Patent, its prosecution history, and its priority date. In Section VIII, I introduce the prior art reference which I use for my opinions in this Declaration—WO 2011/072719 A1 to Eisl ("*Eisl*"). In Section IX, I explain why a POSITA would have been motivated to modify this reference with his or her existing knowledge and why they would have had a reasonable expectation of success in doing so. Finally, in Section X, I walk through Grounds 1 and 2 to show how all the challenged claims of the '500 Patent are invalid as either anticipated or obvious in view of *Eisl*.

III. QUALIFICATIONS AND EXPERIENCE

A. Education and Work Experience

11. I have a Ph.D. from The Ohio State University in Electrical Engineering with minors in Discrete Mathematics, Computer Science, and Microelectronics. I have published papers in the areas of coding theory and multiprocessor computer systems. My CV is attached hereto as EX1002, which shows my education and experience in more detail.

12. I have extensive experience in the design and development of telecommunication systems and have specialized experience in networks and cellular product development.

13. I have developed and designed equipment for cellular networks since I first joined AT&T Bell Laboratories in 1990. From 1990 to 2005 I also designed and implemented a variety of telecommunication systems, including Asynchronous Transfer Mode (“ATM”) based systems for use in cellular networks. ATM is a broadband, packet-switched telecommunications standard defined by the American National Standards Institute (“ANSI”) and the International Telecommunication Union (“ITU”). I also participated in the design and development of AT&T Autoplex Series base stations. I also participated in the design and development of AT&T’s Network Control Points, “NCPs” which were massive network databases containing subscription information for customers. During this time, I first began

my work with telecommunication standards bodies as a contributing member of the ATM Forum.

14. In 1995, I transitioned to the Digital Switch Corporation (“DSC”) Switch Products Division and was the Senior Manager of the ATM systems engineering group developing ATM packet switches for a new generation base station for use by Motorola in their Centralized Base Station Controller, a core part of the second generation cellular network. I also served as DSC’s representative to the ATM Forum. I was one of the first contributors to the wireless standards for the ATM Forum.

15. I next worked at Samsung Telecommunications America from 1996 to 1999 as a Principal Engineer for Samsung’s next generation wireless broadband switching system over the Universal Mobile Telecommunications System (“UMTS”). UMTS is a third-generation (“3G”) broadband standard developed by the 3rd Generation Partnership Project (“3GPP”). My work at Samsung included designing their next generation UMTS cellular switch, which provided both packet and voice services, such as telephony services, wireless services, broadband services, and Internet services. While at Samsung, I also served as Samsung’s North American corporate representative to the ITU, which is the agency of the United Nations responsible for facilitating interconnectivity of information and communication technologies worldwide. The ITU participated in the 3GPP under

the ITU's International Mobile Telecommunications 2000 effort. It was there that I participated in the development of standards for advanced wireless networks.

16. After that, I worked for Marconi Communications from 1999 to 2002, where I was responsible for design and development of a number of systems for the access market, including Digital Subscriber Line ("DSL") modems, along with the design of point-to-point wireless systems. I was also responsible for the servers for the Network Management System for the North American Access product division, which provide service provisioning for DSL customers.

17. I joined Navini Networks in 2002 as a Senior Manager. The Navini system was an entirely packet-based cellular system. I was responsible for layer 2 and layer 3 network protocols for Navini's Wideband Code Division Multiple Access ("WCDMA") wireless base stations and broadband modems. These layers were responsible for packet transmissions for various services over the WCDMA air interface. I also developed servers and databases for network authentication, network services, service provisioning and subscriber management for the Navini's Worldwide Interoperability for Microwave Access 'WiMAX' Network.

18. I have also been the owner of Olivier Consulting since 2003 and have provided consulting services to various companies to develop networking systems and on intellectual property matters, including many such matters relating to cellular technologies specifically.

19. I am currently a Research Professor at the Hunt Institute for Engineering and Humanity, which is part of the Lyle School of Engineering at SMU in Dallas, Texas. Here, I serve as the Program Lead for Transformational Technology. Among the transformational technologies I investigate at the Hunt Institute are Artificial Intelligence, the Internet of Things (“IoT”), and Blockchains.

20. I am also currently an Adjunct Professor in the Telecommunications and Network Engineering Program at SMU’s Graduate School of Electrical Engineering, where I teach Multiprotocol Label Switching (“MPLS”) networked enabled applications. MPLS is a telecommunications routing technique, and one of the MPLS applications I teach is the use of MPLS in advanced cellular networks.

21. Because of my background, training, and experience, I am qualified as an expert to explain the background of the technology encompassed by the ’500 Patent as well as to opine on the validity of the claims of the ’500 Patent in view of the prior art references discussed herein.

22. More details on my education, work experience and technical consulting experience, as well as a list of publications that I have authored or co-authored, are contained in my CV, attached to this Declaration as EX1002.

B. Compensation

23. I am being compensated for the services I am providing in connection with this petition for *inter partes* review of the '500 Patent at the rate of \$650 per hour. The compensation is not contingent upon my performance, the outcome of this *inter partes* review proceeding, or any other proceeding, or any issues involved in or related to the *inter partes* review.

C. Documents and Other Materials Relied Upon

24. The documents on which I rely for the opinions expressed in this declaration are referenced in the Exhibit List above. I also rely on any other references specifically identified in this declaration, in their entirety, even if only portions of these documents are discussed here in an exemplary fashion.

IV. STATEMENT OF LEGAL PRINCIPLES

A. Claim Construction

25. I have been informed that in an IPR proceeding, the challenged claims are generally given their ordinary and customary meaning in view of the specification and the prosecution history as it would have been understood by one of ordinary skill in the art at the time of the alleged invention.

26. I also understand that the claims should be construed consistent with the patent's intrinsic record, which includes the patent itself as well as the patent's prosecution history.

27. Moreover, I understand that extrinsic evidence (including, for example, technical dictionaries and treatises) may shed light on the meaning claim terms would have to one of ordinary skill in the art. I also understand that, where extrinsic evidence conflicts with the intrinsic record, the intrinsic record governs the meaning of claim terms.

28. Further, I understand that conditional language in an apparatus claim does not render the claim indefinite because the structural elements that carry out conditional steps remain present regardless of whether or not the conditions for carrying out the step(s) is (are) met.

B. Anticipation

29. I have been informed that a patent claim is invalid if it is anticipated by prior art. I have been informed that anticipation requires a finding that a single prior art reference discloses each limitation of a claim as the limitations are arranged in the claim. I have been informed that a prior art reference's disclosures may be express or inherent. I have been informed that a limitation is inherently disclosed by a prior art reference if the reference necessarily includes the limitation in question.

C. Obviousness

30. I have also been informed that obviousness is a basis for invalidity of a patent. Specifically, I understand that where a prior art reference discloses less

than all of the limitations of a given patent claim, that patent claim is invalid if the differences between the claimed subject matter and the prior art reference are such that the claimed subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the relevant art.

Obviousness can be based on a single prior art reference or a combination of references that teach all limitations of the claimed invention.

31. I have been informed that a claim is not obvious merely because each limitation was independently known in the prior art. I also have been informed that hindsight reasoning is not an appropriate basis for combining references to form an obviousness combination.

32. I understand that obviousness is not driven by a rigid formula, but is instead a flexible inquiry that reflects the fact that a person of ordinary skill in the art exercising ordinary creativity may find a variety of reasons to combine the teachings of different references. I understand that a non-exclusive list of possible factors that may give a person of ordinary skill in the art a reason to combine references includes any one or more of the following:

- Whether combining elements according to known methods yields predictable results;
- Whether simple substitution of known elements obtains predictable results;

- How use of known techniques improves similar methods in the same way;
- Whether applying known techniques to known methods ready for improvement yields predictable results;
- Whether one can choose from a finite number of identified, predictable solutions, with a reasonable expectation of success;
- How known work in one field of endeavor prompts variations for use in the same field; and
- Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to combine prior art reference teachings to arrive at the claimed invention.

33. I have been informed that obviousness also requires that the combination could have been made with a reasonable expectation of success. I have been informed that absolute predictability is not required; however, at least some degree of predictability is required. I have been informed that predictability is determined at the time the invention was made.

V. LEVEL OF ORDINARY SKILL IN THE ART

34. I understand that the claims and specification of a patent must be read and construed through the eyes of a person of ordinary skill in the art (“POSITA”) at the time of the priority date of the claims.

35. I have also been advised that to determine the appropriate level of a person having ordinary skill in the art, the following factors may be considered: (a)

the types of problems encountered by those working in the field and prior art solutions thereto; (b) the sophistication of the technology in question, and the rapidity with which innovations occur in the field; (c) the educational level of active workers in the field; and (d) the educational level of the inventors.

36. Based on my education and experience, I am familiar with the level of knowledge that a person of ordinary skill would have possessed during the relevant time period.

37. **First**, turning to the types of problems and prior art solutions in the art, the “Field of Invention” to the specification of the ’500 Patent states that the patent “relates to a system for detecting behaviour of a mobile telecommunications device in a telecommunications network.” EX1001, 1:16-18. The “Field of Invention” section further explains that the patent pertains to a problem with mobile devices. *See id.*, 1:32-35 (“Access to the internet exposes devices to malware and malicious applications that may be downloaded, accidentally or onto the mobile device from the internet.”).

38. **Second**, turning to the sophistication of the technology and the rapidity with which innovations occur in the field, the technical specifications that governed the functionality of GSM, UMTS, and LTE networks at the time of the alleged invention required education and experience in cellular communications technology to understand. A person skilled in the art would have been monitoring

these developments. The '500 patent states “[t]elecommunications networks provide radio telecommunication to users of mobile devices, typically according to agreed and standardized radio protocols, for example GSM, UTMS and LTE as would be known by the skilled person.” EX1001, 1:22-25.

39. **Third**, with respect to the educational level of active workers in the field, I personally observed that the individuals that participated in development and implementation of GSM, UMTS, and LTE systems typically had at least a bachelor’s degree in electrical engineering or a related discipline and at least two years of experience working in the cellular communications industry or in academic research in the field of cellular communications.

40. **Fourth**, turning to the educational level of the named inventors, the '500 Patent names one inventor: Frank Muller I am not personally acquainted with this individual, but here is a summary of the information I located from LinkedIn profiles that I reasonably believe to be associated with him:

- Frank Muller’s profile indicates that he started as a Field Service Engineer in in 1990 and moved in network architecture in 2000, by 2012 he had over 12 years’ experience with network architecture, typically in xDSL. EX1011

41. In my opinion, a person of ordinary skill in the art at the time of the alleged invention of the '500 Patent (Nov. 22nd, 2012) would have had a degree in

electrical engineering or a similar discipline, with at least two years of relevant industry or research experience, including designing or implementing network systems. A POSITA would also have familiarity with the wireless standards and protocols relating to subscriber management. This definition is approximate, and more education may substitute for industry experience or vice versa.

42. In addition, in my opinion, while a person of ordinary skill in the art would have some familiarity with such underlying technologies, that familiarity would need only be sufficient to utilize the technology in connection with a broader system and method.

43. Based on my educational and employment background, I am qualified to provide opinions concerning what a POSITA would have known and understood by November 22nd, 2012. Indeed, as reflected in my qualifications above, I am more than qualified as a person of ordinary skill in the art as of the relevant date of the '500 Patent.

VI. TECHNOLOGY BACKGROUND OF THE '500 PATENT

44. I have been asked to provide some context to the technology related to the '500 Patent and the prior art. I understand that the relevant timeframe is

November 22nd, 2012, and below I've provided background on how the various technologies were developed and operating up to that time frame.¹

A. A Brief History of the Evolution of Global System for Mobile Communications ("GSM")

45. The first generation of mobile communications networks, which was retroactively dubbed "1G," dates back to Nippon Telegraph and Telephone's 1979 launch in Tokyo. The United States approved 1G networks for use in or around 1983. This early analog cellular technology was expensive and suffered from a number of drawbacks, including a lack of compatibility between systems, no roaming support between operators, and no encryption. Adoption of this 1G technology began slowly. Many people likely recall the "brick"-sized cell phones that someone that they knew kept in their cars in the late 1980s. Such brick phones, which were something of a novelty item, generally operated on 1G networks.

¹ This technology background is intended to provide an introduction to this technology. My shortened explanations to introduce these concepts for purposes of understanding the claims of the '500 Patent and the prior art discussed in this Declaration are not intended to, and do not, provide a complete explanation of this technology.

46. To overcome these issues, the European Telecommunication Standards Institute (“ETSI”) began developing the Global System for Mobile Communications (“GSM”) standard for second generation mobile networks (“2G”), which first launched in Finland in or around 1991. GSM was standardized in Europe to create an interoperable telecommunications network.

47. GSM used a digital circuit-switched architecture for voice calls, which means that voice channels were established between the “calling” user equipment and the “called” user equipment every time a call was placed. This circuit-switched architecture is described as creating a dedicated digital connection, known as a traffic channel, ‘TCH,’ connecting the two mobile devices during a call. A traffic channel is a designated channel used to carry user data such as voice. EX1012, p. 56 (“Although this is a designated traffic channel consisting of 26 frames, at most only 24 of these are used for TCH user data such as voice.”). 2G GSM also offered standardized traffic channels which carried user data. Digitally encoded voice channels up to 13 Kbit/s and data channels of up to 9.6 kbit/s were offered. Packet data transmission was sent over the data traffic channels, and made use of the Packet Switched Public Data Network, ‘PSPDN’.

48. The 2G GSM Architecture is shown below.

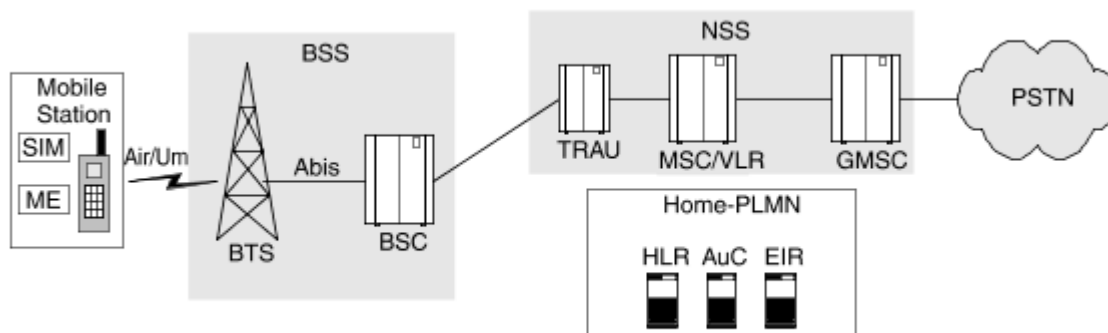


Figure 3.1 GSM general architecture

Id., p. 44.

49. The network entities described in the 2G GSM architecture include the user equipment, known as the Mobile Station (MS), the Base Station Transceivers (BTSs), Base Station Controller (BSC), which make up the radio access network, known as the base station subsystem (BSS). In the core network there is a Transcoder and Rate Adaptation Unit, (TRAU), a Mobile Switching Center (MSC) and Visitor Location Register (VLR), a Home Location Register (HLR), an Authentication Center (AuC) and Equipment Identity Register (EIR). The Home Public Land Mobile Network (PLMN) provide authentication data for the MSC/VLR, so that a visiting MS could register with the visited network. This authentication procedure is shown below. *Id.*, p. 65.

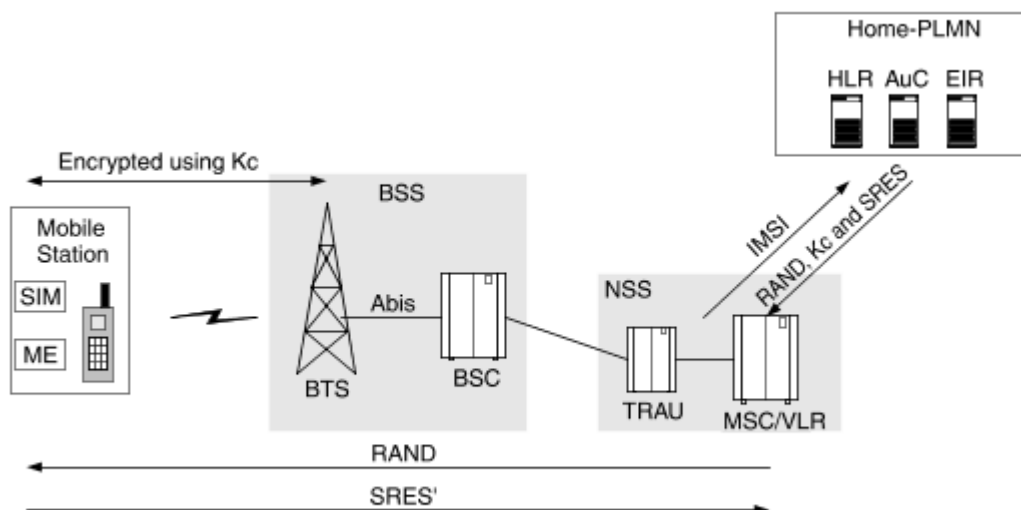


Figure 3.19 GSM authentication

50. The HLR through interaction with the AuC, provides a triplet of data including a security key (Kc), a random number (RAND) and signed response (SRES), based in part on the international mobile subscriber identity (IMSI) stored in the subscriber identity module (SIM) at the MS. The triplet is provided to the MSC/VLR. Thus, since the beginning of 3GPP standards, the authentication procedure made use of the mobile's identity, *e.g.* the IMSI to authenticate the user.

51. From this starting point a planned migration from this second generation to a third generation was planned. The standards groups then specified a migration from the 2G GSM standard to Universal Mobile Telecommunications System (UMTS) via the general packet radio service (GPRS) and enhanced data rates for global evolution (EDGE), as shown in Figure 1.1. *Id.*, p. 4.

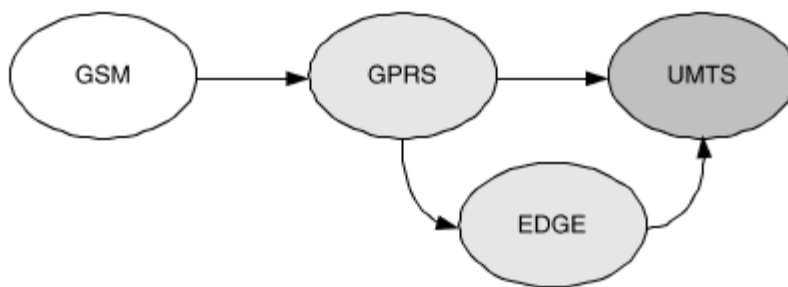


Figure 1.1 GSM evolution to UMTS

52. The GSM standard evolved into the General Packet Radio Packet Service (“GPRS”) standard developed by ETSI, sometimes known as 2.5G, and the Universal Mobile Telecommunications System (“UMTS”) technical specifications developed by the 3rd Generation Partnership Project (“3GPP”). The GPRS extension was an overlay on the existing 2G GSM Architecture and is shown below. *Id.*, p. 266.

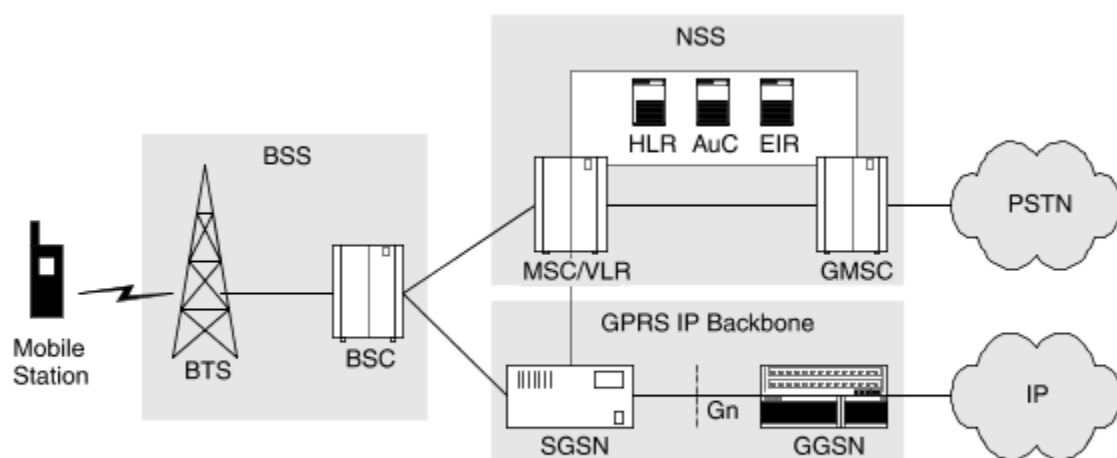


Figure 6.1 GPRS general architecture. Note that there are connections from the MSC and SGSN to the home location, visitor location and equipment identity registers (HLR/VLR/EIR)

53. GPRS introduced a packet-based core network but still uses much of the GSM functionality, including the home location register (HLR), equipment identity register (EIR) and authentication center (AuC) (3G systems also use this GSM functionality). GPRS extension to GSM added new network elements Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN). The SGSN was the connection point between the BSS and the Core Network, and at a high level it provided a similar role for the packet switched network as the MSC/VLR provides to the circuit switched network. *Id.*, pp. 81-82.

B. The 3rd Generation Partnership Project

54. In the late 1990s, the various standards joined to form the 3rd Generation Partnership Project (3GPP). The 3GPP was formed in 1998 with an initial objective of producing technical specifications for a 3G cellular communication system called UMTS. UMTS is a 3G standard that was derived from the 2G GSM standard. For reference, GSM is a 2G standard, UMTS is 3G, and LTE is (generally considered) 4G.

55. UMTS introduced a new air interface and therefore a new Radio Access Network (RAN), known as UMTS Terrestrial Radio Access Network (UTRAN) which contained a wideband BTS known as Node B and a Radio Network Controller (RNC). The first release of the standards for UMTS occurred

in 1999, with the network architecture shown below. As shown below the UMTS RAN was deployed alongside the GSM access network in this release. *Id.*, p. 266.

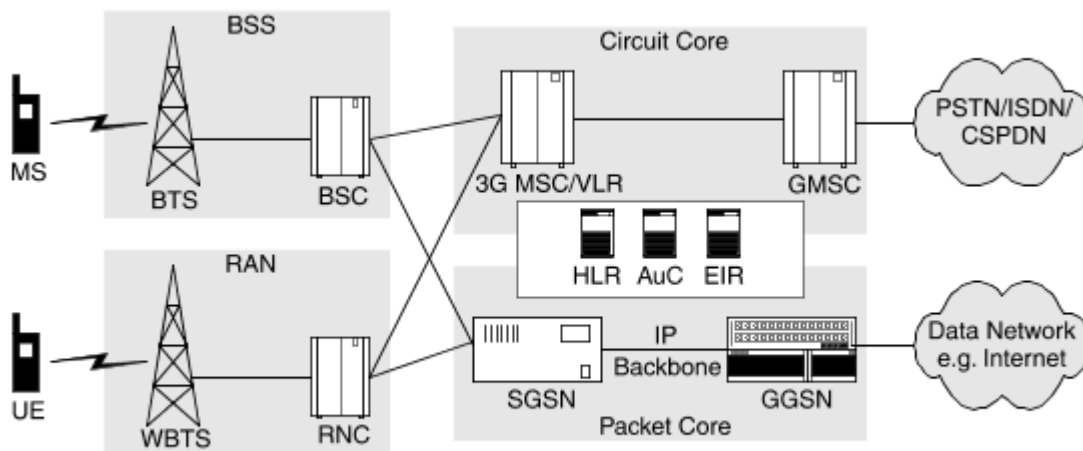


Figure 6.2 UMTS release 99 network

56. The 3GPP initiated the Long Term Evolution (“LTE”) project in or around 2004. The goal of the project was to enhance 3GPP’s radio access architecture. Over the next four years, 3GPP worked to develop the LTE technical specifications, which were first released in December 2008. The UMTS Release 4 architecture is shown below. *Id.*, p. 510.

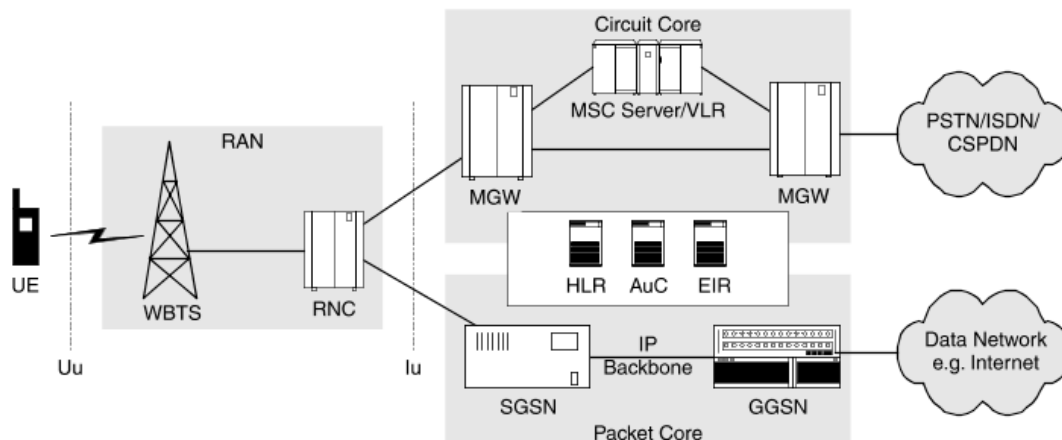


Figure 8.1 Release 4 UMTS architecture

57. UMTS R4 included an iteration of the MSC known as an MSC Server. The MSC Server performed similar functions to the MSC, such as call control for mobile stations and mobility management, which registers the user equipment. The MSC Server also contains the VLR component like the MSC.

58. LTE introduced a new air interface and therefore a new RAN, known as Enhanced UMTS Terrestrial Radio Access Network (E-UTRAN) which contained a wideband BTS known as eNode B. An LTE network consists of an E-UTRAN and an Evolved Packet Core (EPC) and uses packet-switched transmission for all services. The combination of E-UTRAN and EPC is known as the Evolved Packet System (EPS) and is shown below. EX1008, p. 26.

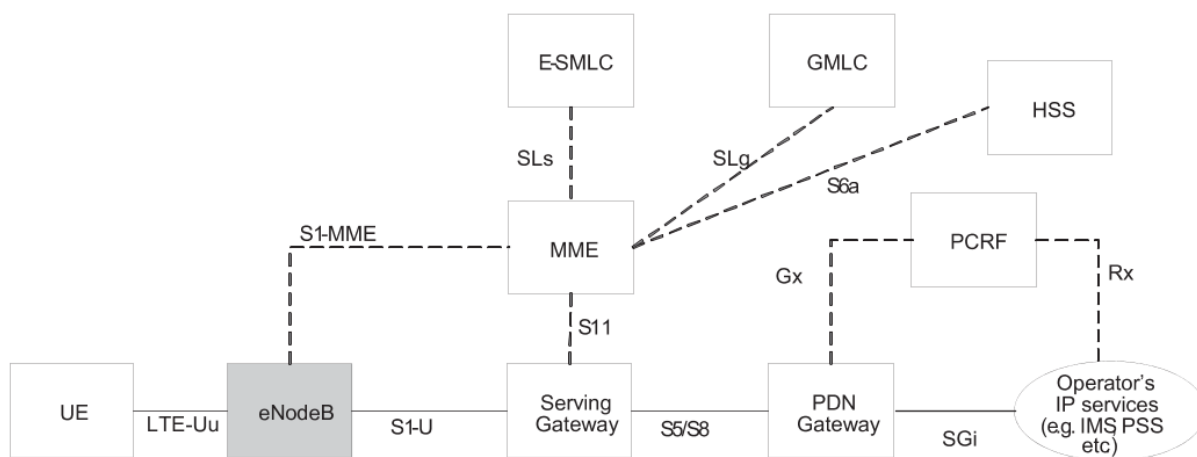


Figure 2.1: The EPS network elements.

59. The access network for LTE, the E-UTRAN, consists of eNodeBs and is shown below. *Id.*, p. 30.

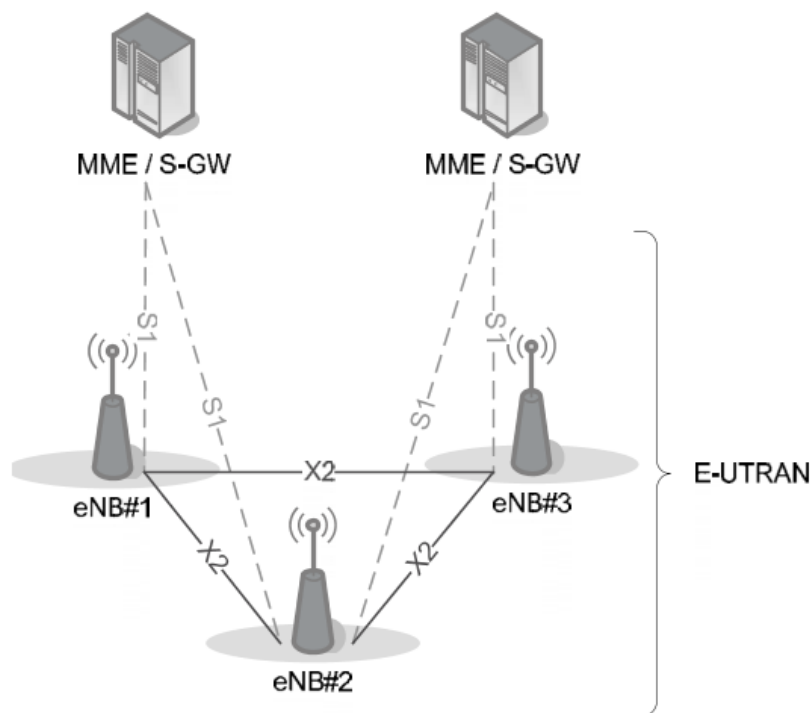


Figure 2.3: Overall E-UTRAN architecture. Reproduced by permission of © 3GPP.

60. The Evolved Packet Core consists of many network elements, but I will concentrate on only four here:

- Mobility Management Entity (“MME”): The MME handles the signaling between the EPC and the user equipment for purposes of mobility (i.e., the user equipment’s current location) and security for E-UTRAN access. The MME is responsible for registration of users to the network.
- Home Subscriber Server (“HSS”): The HSS is a database of user- and subscriber-related information. It also provides mobility management, user authentication, and access authorization data.
- Serving Gateway (“Serving GW” or “SGW”): The Serving GW transports the IP data traffic between the user equipment and the EPC. The Serving GW is the point of interconnect between the radio-side, E-UTRAN, and the EPC. As its name indicates, this gateway serves the UE by routing the incoming and outgoing IP packets.
- Packet Data Network Gateway (“PDN GW” or “PGW”): The PDN GW is another gateway that transports the IP data traffic between the user equipment and the external networks. More specifically, the PDN GW is the interconnection between the EPC and the external IP networks, and it routes packets to and from those external IP networks.

61. The evolution of GSM standardization is summarized in the Figure below. This figure is helpful to understand the role that the radio access technology plays in a user equipment connecting to a network. *Id.*, p. 3.

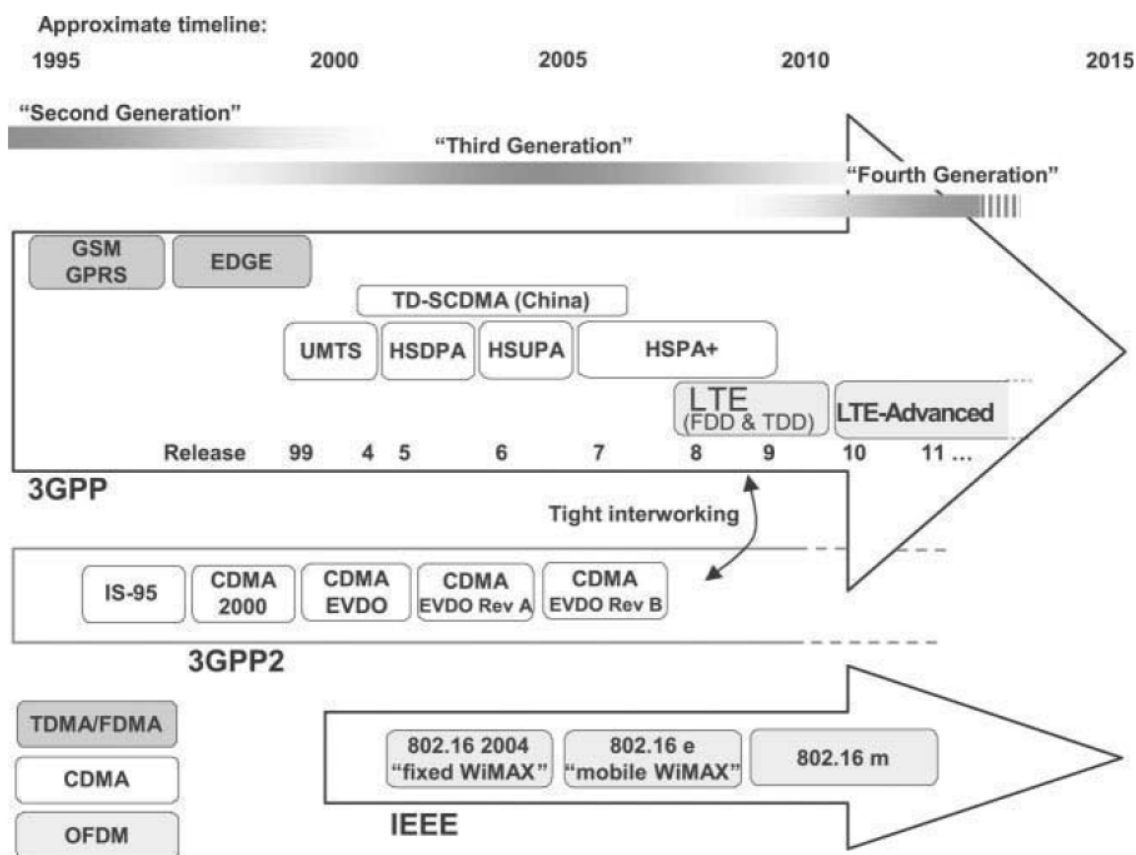


Figure 1.1: Approximate timeline of the mobile communications standards landscape.

C. Mobility Management

62. The mobility management (MM) function is required in networks, such as cellular networks, which allow for device mobility. In order for user equipment to connect to any wireless network, whether packet-switched or circuit-switched, it must first “attach” to the network. GSM, GPRS, UMTS, and LTE have

an attach procedures for their networks which results in the network trying to authenticate the device. EX1001, 3:19-30 (“ As is known by the skilled person, when the mobile device transmits signals to the telecommunications network they are received in a base station and processed into data streams internal to the telecommunications network. For example, if an *attach request is made by a mobile device then the telecommunication network which receives the attach request makes an attempt to authenticate the mobile device*. This results in data streams, or signals, being sent between, for example in the case of a UMTS network, the radio network controller RNC, the mobile switching centre MSC, the Home Location Register HLR, and the Authentication Centre AuC, as would be known by the skilled person.”). As discussed above, a POSITA would understand that authentication in a 3GPP network requires identification. *See above* Section VI.A.

D. Tracking Area

63. In the context of Long-Term Evolution (LTE) cellular networks, a tracking area (TA) is a geographic region in which a mobile device can communicate with a set of base stations. The mobile device periodically sends a tracking area update (TAU) message to the network to inform it of its current location and to request service. The network uses this information to determine which base stations should be used to communicate with the mobile device, and to

manage the device's connection to the network. The size and number of TAs can be configured by the network operator to control network capacity and coverage.

64. When a mobile device enters a new TA, it will send a tracking area update message to the network, which includes the device's current location and the identity of the new TA. The network will then update its records to reflect the device's new location, and will assign the device to the appropriate base stations within the new TA. If the device moves out of the coverage area of the current TA, it will send another TAU message and the network will reassign the device to the appropriate base stations of new TA.

65. The tracking area concept is important in LTE networks because it allows the network to efficiently manage its resources and provide optimal service to mobile devices. By dividing the network into smaller geographic regions, the network can better control capacity and coverage, and can also more accurately track and manage the location of mobile devices. This can help to improve overall network performance and to provide a better experience for mobile users.

E. Operation of Timers and Sliding Windows

66. One example of the use of timers in LTE networks is the tracking area update (TAU) timer. This timer is used to control the frequency at which mobile devices send TAU messages to the network. If a mobile device does not send a

TAU message within the specified time period, the network will consider the device to be inactive and will release its resources.

67. Another example of the use of timers in LTE networks is the session management timer. This timer is used to control the duration of a session between a mobile device and the network. If a mobile device does not send any data or initiate any new sessions within the specified time period, the network will consider the session to be inactive and will release its resources.

68. Windows are also used to monitor for malicious behavior in LTE networks. For example, the network may maintain a window of recently received messages from a mobile device and use it to detect patterns of abnormal behavior. If the network detects that a mobile device is sending an unusual number of messages or requesting an unusual amount of resources, it may flag the device as potentially malicious and take appropriate action, such as blocking its access to the network.

69. Additionally, in order to detect malicious behavior, the network can also use a sliding window mechanism which keeps track of the number of packets sent and acknowledged by the device, allowing the network to detect abnormal patterns of data transmission.

70. U.S. Patent No. 6,594,241 (the “’241 Patent”) describes the operation of sliding time windows. The ’241 patent teaches that a sliding window is

established once a particular event occurs, such as a user connection assigned to a channel. *See* EX1009, 6:20-23 (“**Assuming that the mobile user connection is assigned to a particular type of channel, a sliding window with a predetermined number of time intervals is established.**”). At the end of each time interval, the data stored from the last window position is removed and the most recently data is stored in the first window. *Id.*, 4:41-50 (“The first number of **time intervals may be viewed as a sliding window.** In an example, non-limiting embodiment, the sliding window stores both a channel type and a data amount for each time interval in a memory array. Of course, other parameters may be monitored in the sliding window. **At the end of the next time interval,** data stored in the memory array is shifted so that the channel type and **data amount in the last window position are removed and a most recently determined channel type and data amount are stored in the first window position.**”); *Id.*, 9:39-43. (“The oldest channel type and buffer amount information in time interval T is removed from the sliding window array 90 when channel-type and buffer amount information for the next time interval is stored in the array location associated with T_n .”).

VII. OVERVIEW OF THE '500 PATENT

71. The '500 Patent is titled “System to Detect Behaviour in a Telecommunications Network.” EX1001, Cover. The '500 patent claims priority to a PCT application was filed on Nov. 22, 2013, which claims priority to Patent

Application EP 12193884.9, filed in the European Patent Office on Nov. 22, 2012.

The '500 patent is directed to “[a] system is provided for detecting behaviour of a mobile telecommunications device in a telecommunications network.” *Id.*,

Abstract. The patent has eleven claims: two independent and nine dependent claims. The independent claims largely duplicate each other.

A. Summary of '500 Patent Subject Matter

72. The '500 Patent describes “a system for detecting behavior of a mobile telecommunications device in a telecommunications network.” EX1001, 1:16-18. More specifically, the '500 Patent is directed to the detection of malicious behaviors from mobile devices, such as the excessive use of network resources or invocation of network functions like handovers. The '500 Patent claims a very simple solution to detect this behavior; it merely proposes to *count* signals indicative of the device's behavior, and to register when the count exceeds a threshold. EX1001, 2:8-10 (“The claims describe a system for detecting behaviour of a mobile telecommunications device in a telecommunications network.”); *Id.*, 4:23-30 (“The system as claimed solves the problem by identifying malicious behaviour in a mobile device, but identifying it from within the telecommunications network itself. This is done according to the arrangement of the invention by monitoring the data streams, or transfers of data, which occur in

the network due to the interaction between the network and the mobile. This data is monitored for excessive occurrences of particular signals.”).

73. The ’500 describes how this procedure takes place, by for example counting network signaling messages arriving at the MME. *Id.*, 4:56-62 (“In a particularly advantageous example the **network includes a counter, C, and is arranged to detect a detectable event, X**, which occurs within the network, for example the first instance of an attach, or, the transmission of a request for authentication to the AuC, or, the **arrival of signaling in the MME indicating that a handover has taken place, and starts the counter.**”).

74. Claim 1 is representative of the claims of the ’500 Patent and is reproduced below:

1. A system comprising:
 - a telecommunications network configured to identify mobile telecommunications device and comprising a core network and a base station, wherein the base station is configured to receive radio signals from the mobile telecommunications device and further process the radio signals into processed signals and to transmit the processed signals to the core network,wherein the telecommunications network is arranged to count in the core network a number of occurrences of a certain predetermined signal associated with the mobile telecommunications device, the certain predetermined signal representing an interaction

between network devices in the core network for normal processing of signals,
and wherein the telecommunications network is further arranged to register when the number of occurrences of the certain predetermined signal exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network,
wherein the certain predetermined signal indicates handover of the mobile telecommunications device.

EX1001, Claim 1.

B. Claim Listing

75. A full claim listing is included as Exhibit 1006. I will rely on this labeling to streamline my discussion in Section X.

C. Relevant Prosecution History of Application 14/646,554

76. Application 14/646,554, which issued as the '500 Patent, was first filed in the United States under 371(c) on May 21, 2015. EX1005, 1-3. The Examiner issued a first non-final rejection on May 10, 2016. *Id.*, 170-181. The Examiner issued a final rejection on December 13, 2016. *Id.*, 356-368. After the applicant filed an RCE on May 09, 2017, *Id.*, 404-405, the Examiner issued a second non-final rejection on June 27, 2017. *Id.*, 413-425. The Examiner issued a second final rejection on November 29, 2017. *Id.*, 451-463. After the applicant filed a second RCE on May 24, 2018, *Id.*, 498-499, the Examiner issued a third

non-final rejection on October 29, 2018. *Id.*, 507-517. The Examiner issued a third final rejection on July 5, 2019. *Id.*, 557-568. After the applicant filed a third RCE on December 31, 2019, *Id.* 603-604, the Examiner issued a fourth non-final rejection on February 28, 2020. *Id.*, 610-623.

77. *Eisl* was submitted in an IDS on March 27, 2020. The Examiner issued a notice of allowance on October 30, 2020. *Id.*, 736-748. The Examiner did not mark *Eisl* as considered until October 23, 2020, a week after the Examiner and Applicant had reached an agreement to advance prosecution over *Bu* with an Examiner's Amendment. EX1005, at 749-750 (Interview Summary); *Id.* 772-773 (IDS marked by examiner). The examiner's amendment included in the notice of allowance included several changes to the claims. *Id.*, 741-746. For example, Claim 1 was amended as shown below:

Claim 1:

A system comprising:

a telecommunications network configured to identify ~~at least one~~ mobile telecommunications device and comprising a core network and a base station, wherein the base station is configured to receive radio signals from the mobile telecommunications device and further process the radio signals into processed signals and to transmit the processed signals to the core network,

wherein the telecommunications network is arranged to count in the core network a number of occurrences of a certain predetermined signal associated with the mobile telecommunications device, the certain predetermined signal representing an interaction between network devices in the core network for normal processing of signals,

and wherein the telecommunications network is further arranged to register when the number of occurrences of the certain predetermined signal exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network,

wherein the certain predetermined signal indicates handover of the mobile telecommunications device.

Id., 741-742.

78. In particular, the examiner amendment adds a limitation that the predetermined signal that is counted “indicates handover of the mobile telecommunications device.” *Id.* Besides the examiner amendment, the notice of allowance also stated that Applicant’s remarks on “pages 9-16 of the

Arguments/Remarks filed on 7/28/2020” were persuasive and “[t]herefore, the claims [were] allowable over the prior arts of records.” *Id.*, 746.

D. Priority Date

79. The ’500 Patent was filed as a PCT application on November 22, 2013. EX1001, Code 22. The ’500 Patent claims priority on its face to EP12193884 filed November 22, 2012. *Id.*, Code 30. For the purposes of my report, I have assumed a priority date of November 22, 2012.

80. If Patent Owner introduces evidence in this proceeding of an earlier invention date, I reserve the right to offer additional opinions and testimony to respond to such evidence.

E. Claim Construction

81. In my opinion, all of the claim terms in the ’500 Patent should be given their plain and ordinary meaning, as a POSITA would understand them in light of the specification and file history of the ’500 Patent. Except as otherwise noted, I have applied such a plain and ordinary meaning in my analysis of the claims. I reserve the right to offer additional opinions on claim construction in response to arguments that may be made by Patent Owner.

VIII. IDENTIFICATION OF THE PRIOR ART AND SUMMARY OF OPINIONS

82. As explained below, it is my opinion that the following prior art reference discloses or renders obvious all technical features of the Challenged Claims of the '500 Patent, thus rendering them unpatentable:

- **International Application Publication WO 2011/072719 by Eisl (EX1004, “*Eisl*”)**

A. Summary of *Eisl*

83. International Application Publication WO 2011/072719 by *Eisl* is titled “[m]ethod, apparatus and related computer program product for detecting changes to a network connection.” The application was published on June 23, 2011.

84. *Eisl* provides a solution to the same problem recognized by the '500 Patent—detecting malicious activities of a mobile device. *See* EX1004, [007] (“user initiated handover may be triggered by . . . malicious mobile device software”); [009] (“It is noted that such **frequent handover actions** and frequent connections establishment / teardown actions, which may be **initiated by a malicious user or software**, are just example for not needed actions which consume network resources and so reduce network performance.”). [0011] *Eisl* discloses an apparatus and a related computer program product for detecting changes to a network connection. EX1004, [0011] (“In particular, the present

invention provides **a method**, an apparatus and a related computer program product for **detecting changes to a connection** of mobile device(s) to a network.”). Beyond simply detecting and registering a problem, *Eisl* proposes to inhibit the malicious activity. *Id.* [0011] (“If changes to the connection, resulting for example from frequent actions without purpose, are detected **measures may be applied in order to for example inhibit such frequent actions** or inform the user or network operator about it.”).

85. To achieve this solution, *Eisl* teaches that different core network elements involved in changes to connection, such as handover activities, are observed. EX1004 Code 57 (“The **changes to the connection are detected** by checking if **parameters** related to the mobile device, or related to **network elements**, violate defined policy rules. The detection itself is done in a network element, which is preferably a core network element.”). “Examples for **core network elements involved in handover activities** are **Serving GPRS Support Node (SGSN)**, **Gateway GPRS Support Node (GGSN)**, **Mobility Management Entity (MME)**, **Serving Gateway (SGW)** and **Packet Data Network Gateway (PGW)**.” EX1004 [0037]. Network related data related to handovers is received from these core network elements. EX1004 [0079] (“Received **network related data 4-5 may include information related to handover actions**, attach/ detach

actions or PDP context activation/modification/ deactivation actions.”). This network related data is processed into network related parameters.

86. Fig. 4 of *Eisl* goes into detail, where the network related data is used to create network related parameters, which are then used as inputs to the policy rules. *See id.*, Fig. 4. If there is found to be a violation of a policy rules, measures are initiated to such sending a message to the mobile or block its access. *Id.*

87. *Eisl* specifically teaches that network related data including information related to handover actions such as the network area or cells where the action occurred. EX1004 [0079] (“Further on the data may **include information** about the involved one or more mobile devices, **the network area or cell(s) where the actions occurred**, the target and the originating networks involved in the actions (for example in case of handover actions) and other related data (for example the amount of transferred data during a connection).”).

88. Fig. 4 of *Eisl* “illustrates method steps related to the present invention in more detail.” EX1004 [0026]. Fig. 4 is further representative of the disclosure of *Eisl*.

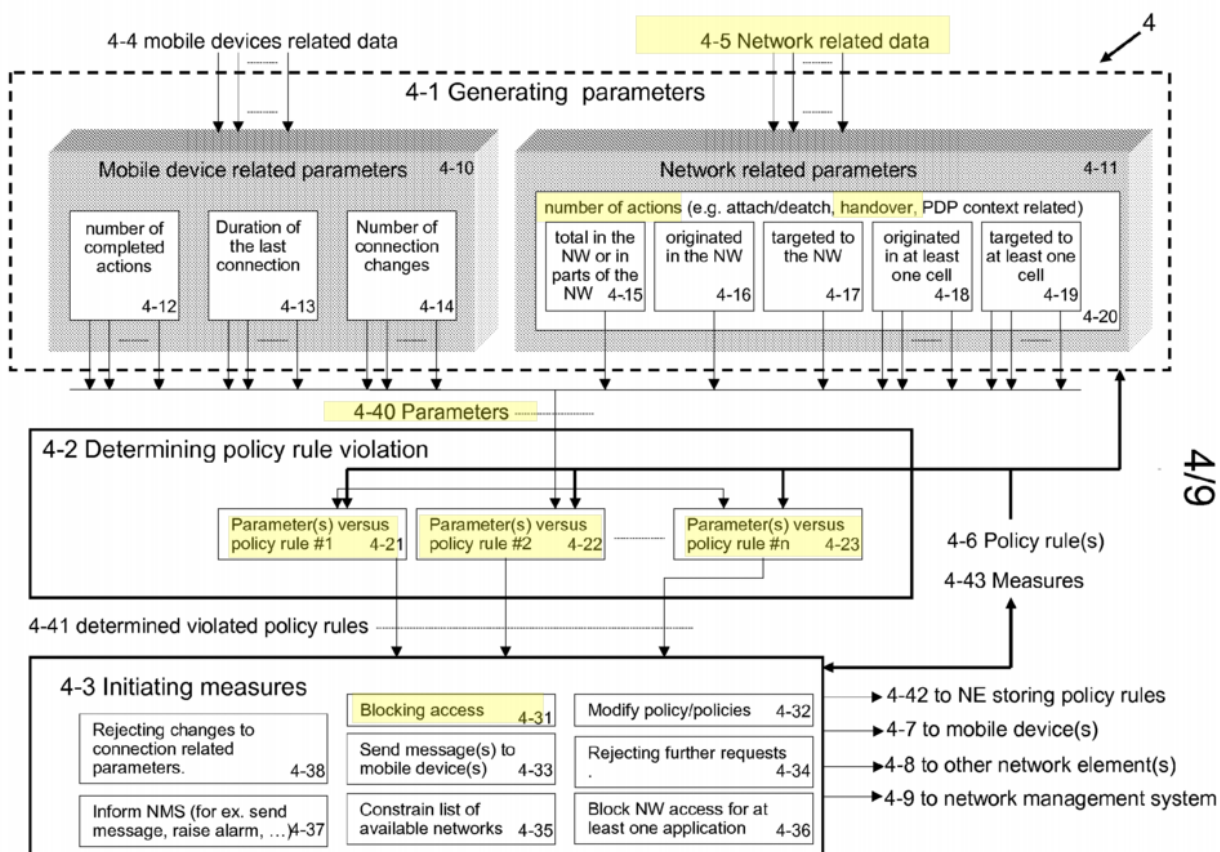


FIG 4

Id., Fig. 4.

89. With reference to Fig. 4, network related data actions (as well as network related parameters) are counted and used as inputs to the policy rules. As seen above, the “number of actions” including handovers are counted, and if the number of actions violate a policy rule, the violation registers specific actions to be taken. EX1004 [0083]-[0084], [0089]-[0090]. If there is found to be a violation of a policy rules, measures are initiated such as sending a message to the mobile or blocking its access.

90. *Eisl* specifically describes that the policy rules shown above may include when a parameter is above a threshold. EX1004, [0085] (“A **policy rule might include one or more thresholds** for one or more parameter. A device may be assumed to violate a policy if one or more of those thresholds are crossed.”). *Eisl* goes on to give a specific example of violating a policy when a number of completed handovers, i.e. a count of, exceeds a threshold in a time window:

Example of a policy rule:

Parameters:

- A = **number of completed handover actions** of mobile one device
- B = Duration of last network connection of the mobile 25 device

Policy rule:

IF ((within TW (**A>5**)) and (B<10s)) THEN policy rule =VIOLATED

TW = time window = e.g. 1 minute

In the above example “5” is the threshold for the number of the completed handover actions and “10s” is the connection time threshold.

EX1004, [0086]-[0087]

91. As seen in the excerpt above, *Eisl* discloses counting the number of handover actions within a single time window, and to register a violation if the number of handover actions is greater than 5 within a single 1-minute time window. It is important to note that after a time window is exceeded, the value of the variable ‘A’ is set to zero, and a new time window is started. This is how

sliding time windows operate. *See above* Section VI.E. If ‘A’ was not reset as the time window slides, then the policy rule could never detect a second occurrence a violation.

IX. A POSITA’S REASONS TO COMBINE THE IDENTIFIED PRIOR ART

A. *Eisl* and the Knowledge of a POSITA

92. As I explain below, in my opinion Claims 1-3, 5-7, and 9-11 of the ’500 Patent are unpatentable because they are anticipated by *Eisl*. However, if the Board finds that any of the these Claims are not anticipated by *Eisl*, it is my opinion that they are nonetheless rendered obvious by *Eisl* in view of the knowledge of a POSITA at the time of the ’500 Patent. In addition to these claims, it is my opinion that Claims 4 and 8 of the ’500 Patent are rendered obvious by *Eisl*. It is my opinion that there are a multitude of reasons why a POSITA would have been motivated to apply certain implementation details to *Eisl* based on a POSITA’s knowledge at the time of the alleged invention and that a POSITA would have had a reasonable expectation of success in applying such details. Thus, in my analysis in Section X, I have provided example motivations that a POSITA would have had for applying specific implementation details to the extent they are not explicitly disclosed in *Eisl*.

X. UNPATENTABILITY OF THE '500 PATENT CLAIMS

A. Grounds 1-2: Claims 1-3, 5-7 and 9-11 are Unpatentable as Anticipated by Eisl (Ground 1) and Claims 1 – 11 are Obvious in view of Eisl (Ground 2)

93. In my opinion, Claims 1-3, 5-7 and 9-11 are anticipated by *Eisl*. Each of the individual claim limitations of the Challenged Claims are taught by *Eisl*. In the event that Claims 1-3, 5-7 and 9-11 are not anticipated by *Eisl*, it is my opinion that they are rendered obvious in view of *Eisl*. It is also my opinion that Claims 4 and 8 are rendered obvious in view of *Eisl*.

1. Claim 1

1[p]: “A system comprising:”

94. In my opinion, *Eisl* discloses the preamble of Claim 1. *Eisl* describes a system for detecting and mitigating malicious activity from a mobile device. *See* EX1004, [0007]. *Eisl*'s solution is a system and is described as follows:

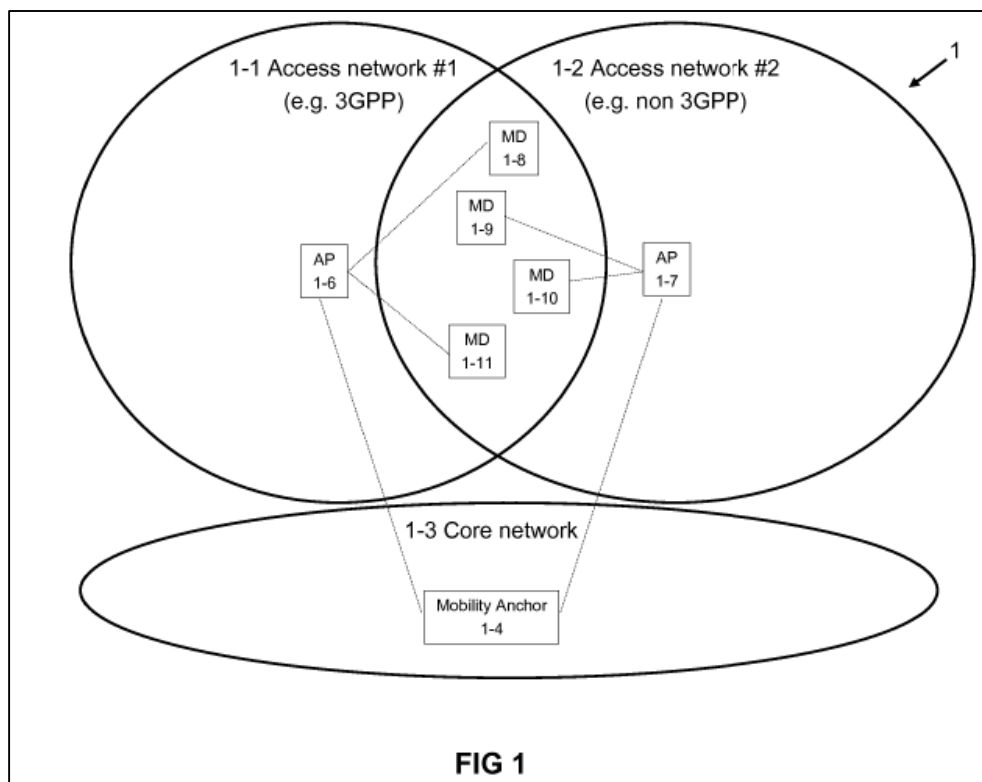
Disclosed is a method, a device and a computer program product for detecting changes to the connection of a device (preferably a mobile device) to a network and for initiating at least one measure when changes are detected. Changes might be caused by malicious users or malicious mobile phone SW in order to perform Denial of Service (DoS) attacks to the network. Those changes could be for example frequent handover actions, frequent attach/detach actions or frequent Packet Data Protocol context activation, deactivation or modification actions initiated by a mobile device or a group of mobile devices. The

changes to the connection are detected by checking if parameters related to the mobile device, or related to network elements, violate defined policy rules. The detection itself is done in a network element, which is preferably a core network element.

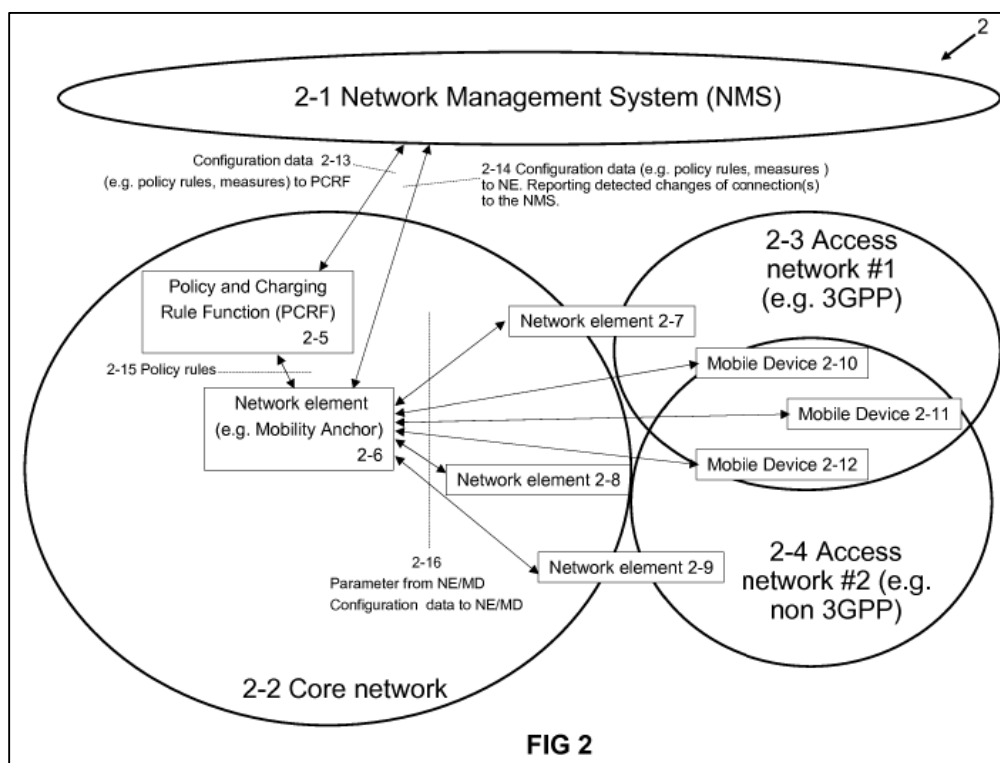
EX1004, Abstract.²

95. *Eisl* specifically discloses example cellular systems in Figures 1 and

2:



² cf. EX1001, 2:23-30 (describing the '500 Patents' solution in similar terms).



EX1004 Figures 1-2; [0023]; [0024]; [0050]-[0052]; [0060]-0063].

96. *Eisl* discloses that its teachings are applicable to multiple embodiments of wireless systems, including GSM, UMTS, LTE, and other well-known wireless systems. *Id.*, [0002] (“Examples of the present invention are applicable, but not limited, to **Global System** for Mobile communication (GSM) networks, Universal Mobile **Telecommunications System** (UMTS) networks, Code Division Multiple Access (CDMA) networks, Worldwide Interoperability for Microwave Access (WIMAX) networks, Wireless Local Area Networks (WLAN) , Long Term Evolution (LTE) and **System** Architecture Evolution (SAE) networks, Cable networks and DSL networks.”).

97. For at least these reasons, a POSITA would have recognized that *Eisl* discloses the preamble (*i.e.*, “a system”).

Claim 1[a]: “a telecommunications network configured to identify mobile telecommunications device and comprising a core network and a base station,”

98. In my opinion, *Eisl* discloses these limitations. First, *Eisl* discloses a telecommunications network that includes a core network and a base station. *Eisl* discloses that its teachings are applicable to a variety of telecommunication networks, including GSM, UMTS, LTE, and others. *See e.g.*, EX1004, [0002] (“ Examples of the present invention are applicable, but not limited, to Global System for Mobile communication (GSM) **networks**, Universal Mobile **Telecommunications** System (UMTS) **networks**, Code Division Multiple Access (CDMA) **networks**, Worldwide Interoperability for Microwave Access (WIMAX) networks, Wireless Local Area Networks (WLAN), Long Term Evolution (LTE) and System Architecture Evolution (SAE) networks, Cable networks and DSL networks.”). Some of these, including GSM, UMTS, and LTE are examples of

well-known telecommunications networks that included a base station and a core network.³

99. *Eisl* describes its system includes access networks. For example, *Eisl*'s Figure 1 illustrates a telecommunication network that includes access networks with access points (APs) connecting mobile devices to a core network.

³ The '500 Patent describes that these networks “provide radio telecommunication to users of mobile devices” and that “GSM, UTMS and LTE would be known by the skilled person.” EX1001, 1:22-25. The '500

Patent also describes that these networks include a core network. *Id.*, 3:54-59 (“In a particularly advantageous embodiment the detection of data [sic] streams is performed *in the core network, and in particular in* the Mobility Management Entity MME if the network is an *LTE network*, in the MSC if it is a *UMTS or GSM network*”).

structure (or data record) including subscriber session related information for an active session (for example **subscribers IP address**, Tunnel end point identifier, **subscriber identifier**, ..."); EX1004, [0056] ("Further on when a mobile device starts for example a GPRS connection, a PDP context will be activated (generated) including parameters related to the GPRS connection between the mobile device and for example a core network element like a SGSN. These parameters related to the GPRS connection may be for example the subscribers IP address, **subscriber identifier** like **International Mobile Subscriber Identity (IMSI)** or Tunnel Endpoint Identifier(s) (TEIDs)....").

102. In addition, Eisl discloses that the mobile device is authenticated by core network functions. *See* EX1004, [0101] ("In next steps 6-12 and 6-13 the mobile device is **authenticated**."); EX1004, [0037] ("Examples of **core network functions** are traffic aggregation, **authentication**...."). After the mobile device has been authenticated, it can attach to the network. *See* EX1004, [00102] ("If **the authentication and authorization** was successful the mobile device triggers a layer 3 **attach action** 6-14."). A POSITA would have understood that in the system taught by *Eisl*, in order to authenticate a mobile in a 3GPP network, its identity must be known. *See above* Section VI.A.

103. *Eisl* also discloses measures taken by the system include blocking a mobile device or sending a message to the mobile device. *See* EX1004, [0090]. A

POSITA would have understood that to implement targeted measures (*i.e.*, blocking or sending a message to a specific mobile device), the system must know the identity of the device.

104. Thus, *Eisl* discloses “a telecommunications network configured to identify mobile telecommunications device and comprising a core network and a base station” as claimed.

105. To the extent that the Patent Owner argues that *Eisl* does not expressly disclose Claim 1[a], *Eisl* renders Claim 1[a] obvious. It would have been obvious for mobile communications device to provide information to the network for the purpose of proving its identity to the network. This is a basic aspect of each of the disclosed cellular networks in *Eisl* (*see* EX1004, [002]); the mobile device is identified by the network in order to accept the requested communication and to allow the network the ability to locate the mobile to receive calls. *See above* Section VI.A. To the extent this implementation detail is not already taught by *Eisl*, a POSITA would have been motivated to modify *Eisl*’s system in this way at least for the purpose of keeping track of mobile telecommunications devices exhibiting abnormal and/or malicious behavior. A POSITA would have had a reasonable expectation of success in implementing *Eisl*’s system in this way because it would merely involve adding well-known functionality to *Eisl*’s system. Thus, *Eisl* at least renders obvious “a telecommunications network configured to

identify mobile telecommunications device and comprising a core network and a base station” as claimed.

Claim 1[b]: “wherein the base station is configured to receive radio signals from the mobile telecommunications device and further process the radio signals into processed signals and to transmit the processed signals to the core network,”

106. In my opinion, *Eisl* discloses these limitations. *Eisl* discloses a base station configured to receive radio signals from a mobile telecommunications device, process them, and transmit them to the core network. For example, as shown in Figure 1 below, *Eisl* describes a system in which mobile devices are connected to the core network via a radio interface with the APs (e.g., base stations).

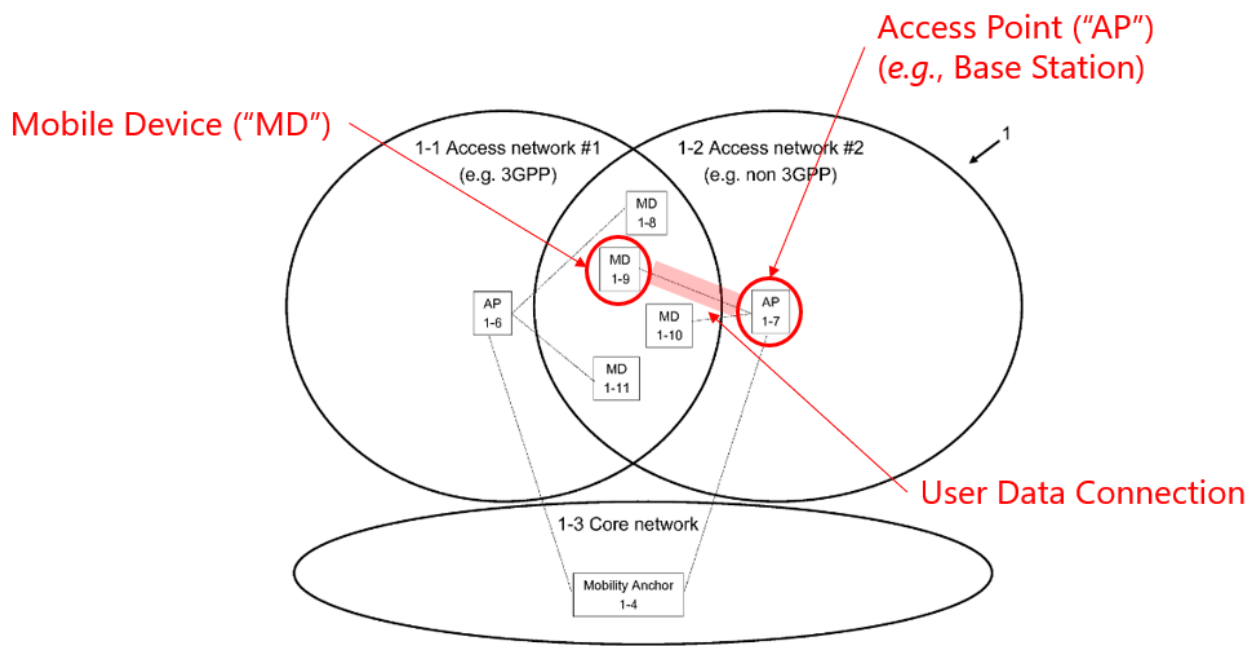


FIG 1

EX1004, Figure 1 (annotated). *see also* EX1004, [0050] (“Fig. 1 shows a high level example network 1 where mobile devices 1-8 to 1-11 are connected via access networks 1-1 and 1-2 to a core network 1-3, ... The shown connections between the network elements refer to user data connections.”); *id.*, [0051] (“Access point 1-6 or 1-7 could be for example a base station....”); *id.*, [0042] (“mobile device (MD) connects to the base station . . . via a radio interface to the wireless network”).

107. Base stations in the cellular networks described by *Eisl* receive radio signals sent from mobile telecommunications devices and process those signals for transmission to the core network.⁴ *See above* Section VI.A; *see also* EX1004 [0037] (“A core network (or network core) is the central part of a telecom network that provides various services to customers who are connected by the access networks.”). The ’500 Patent concedes this was known by a skilled person: EX1001, 3:19-22 (“As is known by the skilled person, when the **mobile device transmits signals to the telecommunications network** they are received in a **base station and processed into data streams internal to the telecommunications**

⁴ *See* EX1004., [0036] (“Access networks of different types could be for example GERAN, UTRAN, E-UTRA, CDMA2000 RAN, WLAN or Wimax (note this is just an example list and might not be complete).”).

network.”). Thus, *Eisl* discloses a “the base station is configured to receive radio signals from the mobile telecommunications device and further process the radio signals into processed signals and to transmit the processed signals to the core network as claimed.

Claim 1[c]: “wherein the telecommunications network is arranged to count in the core network a number of occurrences of a certain predetermined signal associated with the mobile telecommunications device,”

108. In my opinion, *Eisl* discloses these limitations. *Eisl* teaches that an expert determines criteria such as thresholds for network related parameters. These thresholds are used to distinguish normal behavior from abnormal behavior. These thresholds are used to define policy rules which can be used to register when the number of occurrences of the certain predetermined signal exceeds a level indicating acceptable behavior. EX1004 [0047] (“An expert in the art is able to define criteria (for example **thresholds** for mobile device or **network related parameters**) in order to distinguish **normal changes of a connection between a mobile device and a network from abnormal (frequent) changes** caused by for example DOS attacks. **Those criteria (thresholds) can then be used for defining policy rules to detect frequent changes to a connection caused by those frequent (abnormal) actions.** For example a criteria could be the number of connection changes that happened during a specific time window. Within the

description of this patent application the term ‘frequent changes to a connection’ refers to changes caused by abnormal behavior (like for example by DOS attacks).”).

109. Eis1 teaches an example of using a threshold for the number of handover actions in a policy rule:

```
[0086] Example of a policy rule:
20
Parameters:
    • A = number of completed handover actions of mobile one
      device
    • B = Duration of last network connection of the mobile
25      device

Policy rule:
IF ((within TW (A>5)) and (B<10s)) THEN policy_rule =
VIOLATED
30

TW = time window = e.g. 1 minute

[0087] In the above example "5" is the threshold for the
35 number of the completed handover actions and "10s" is the
connection time threshold.
```

EX1004, [0086]-[0087].

110. Eis1 describes the use of policy rules which may be implemented in the core network, to detect abnormal behavior of mobile telecommunications devices—including embodiments where the system counts instances of connection

changes and/or handover actions by generating parameters from data indicating the connection changes and/or handover actions (*i.e.*, predetermined signals) associated with the mobile device and compares them to a threshold. *See* EX1004, [0038] (“**Policy rules** might be used to . . . **to detect abnormal situation[s]**. . . .”); [0038] (stating policy rules “can be stored and implemented basically in any network element **in the core** or access **network**.”); [0076] (“Received mobile device related data 4-4 may be for example **indications of a performed or planned handover . . .**”); [0077] (“**parameters like for example the number of completed actions 4-12 (for example **handover actions** . . .), . . . and the number of connection changes 4-14 of a mobile device** to a network are generated.”); (“Further on the parameters might be generated for a defined time window, which means that only **events falling into the sliding time window are counted**”); *see also* EX1004, [0079]-[0080].

111. Figure 4 shows that the network device data (*i.e.*, signals) is used to generate network related parameters (4-10) including the number of completed actions (4-20) such as handovers, which are used for determining if policy rules are violated (4-2):

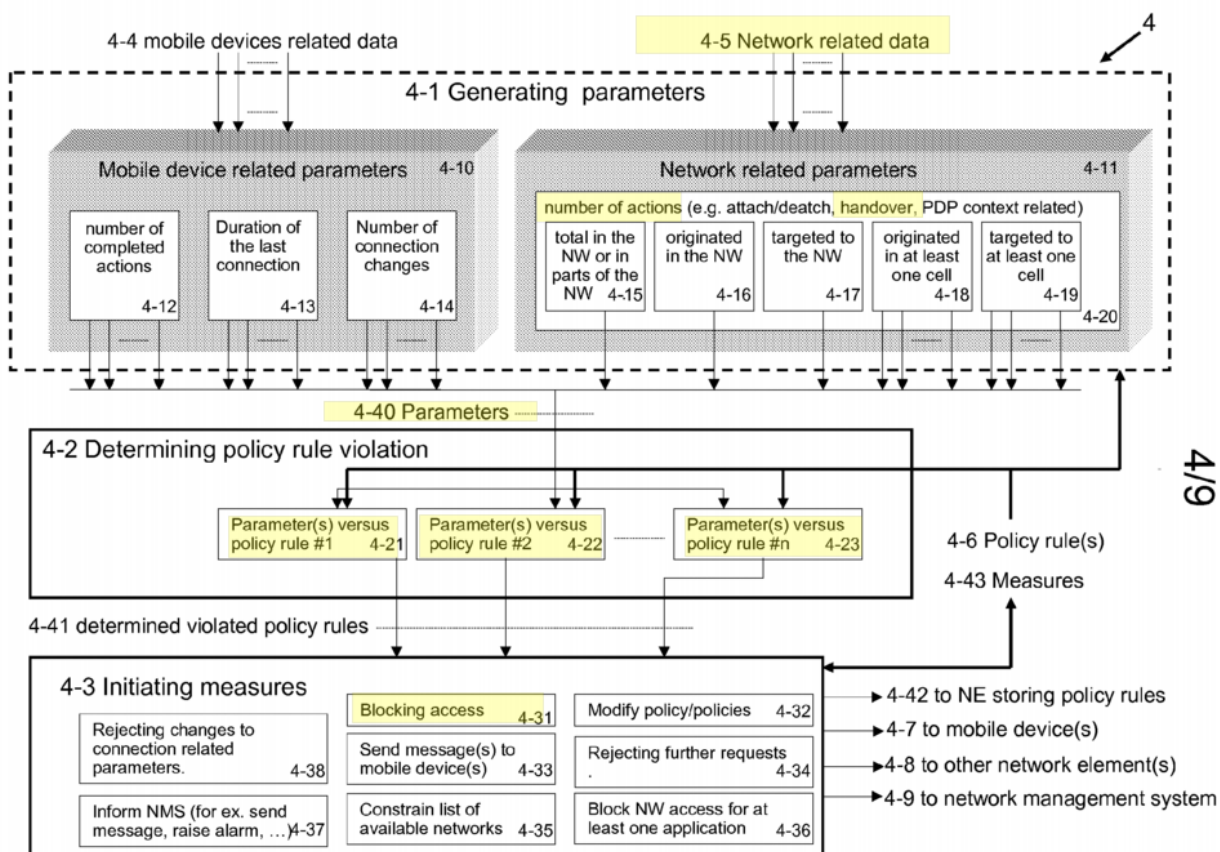


FIG 4

Id., Figure 4 (annotated).

112. As seen above, the number of signals indicating “the number of actions” are counted to create a parameter, and if the number of these actions violate a policy rule, the violation registers specific actions to be taken (4-3). *See* EX1004, [0083]-[0084]; [0089]-[0090]. *EisI* specifically explains that Network related data related to handovers is received from these core network elements. EX1004, [0079] (“Received **network related data 4-5** may include information **related to handover** actions, attach/ detach actions or PDP context

activation/modification/ deactivation actions.”). If there is found to be a violation of a policy rules (4-2), the “result of the different policy rule checks 4-21 to 4-23 may be transferred to the initiating measures step 4-3.” EX1004, [0089]. Within step 4-3, measures are initiated such as sending a message to the mobile device or blocking its access (4-33 and 4-31 respectively). EX1004, Figure 4; [0090]-[0091].

113. *Eisl* specifically explains that the “number” of completed actions or connection changes are determined because they are “counted.” EX1004, [0078] (“Further on the parameters might be generated for a defined time window, which means that only *events falling into the sliding time window are counted*.”). Thus, *Eisl* discloses that “the telecommunications network is arranged to count in the core network a number of occurrences of a certain predetermined signal associated with the mobile telecommunications device” as claimed.

114. To the extent that the Patent Owner contends that “counting” is not explicitly disclosed by *Eisl*, counting is an implementation detail that would have been obvious to a POSITA at the time of the ’500 Patent. A POSITA would have been motivated to use counting to generate the number of, for example, signals indicating completed actions to reliably generate that parameter. Other methods such as estimating the number of signals indicating an action would be less reliable and introduce unnecessary complication. A POSITA would further have had a reasonable expectation of success in generating the number of actions through

counting signals indicating associated actions because counting is a routine and well-known practice. Further, a POSITA would have understood that counting would have been the most obvious and natural way to arrive at a “number” of performed or planned events such as handovers. *See* EX1004, [0077] (“The mobile device related data is processed in the ‘mobile device related parameters’ sub-step 4-10, and parameters like for example **the number of completed actions 4-12 (for example handover actions,⁵ attach/detach actions, PDP context activation/modification/ deactivation actions**), the duration of the last connection of a mobile device to a network 4-13 and **the number of connection changes 4-14 of a mobile device** to a network are generated.”); *id.*, [0079] (“Generated network related parameters may be the **number of completed actions 4-20** for the total network or parts of the network 4-15, **number** of actions originated in the network or in parts of the network 4-16, **number** of actions targeted to the network or at least to parts of the network 4-17, **number** of actions originated in one cell of the network 4-18 or number of actions targeted to one cell of the network 4-19.”).

⁵ Notably, a later claim element identifies a “signal indicat[ing] handover of the mobile telecommunications device” as the “predetermined signal” in Claim 1. *See* EX1001, Claim 1.

Claim 1[d]: “the certain predetermined signal representing an interaction between network devices in the core network for normal processing of signals,”

115. *Eisl* discloses these limitations. *Eisl* teaches monitoring signals in the core network that indicate/represent normal behavior (such as handover of mobile telecommunications devices). *Eisl* teaches that a handover is a normal process for shifting a mobile device from one base station to another. EX1004, [0040] (“A handover action means the shifting of a mobile device connection from one base station or access point to another one.”).

116. *Eisl* teaches that signals are monitored for abnormal frequency, which according to *Eisl*, represent abnormal or malicious behavior. EX1004, [0047] (“**Frequent** handover, **frequent** attach or detach or **frequent** PDP context activation, modification or deactivation actions mean in the context of this application **abnormal frequent actions** caused by for example a malicious user or malicious software performing a DOS attack to the network. Such actions will cause ‘**frequent**’ changes to a connection between a mobile device and a network.”). *Eisl* teaches that “only malicious **frequent** changes to mobile device connections are detected and inhibited, **while still allowing normal actions like normal handover, attach/detach or PDP context.**” *Id.*, [0021]; *see id.*, [0047] (An expert in the art is able to define criteria (for example thresholds for mobile device or network related parameters) **in order to distinguish normal changes of a**

connection between a mobile device and a network from abnormal (frequent) changes caused by for example DOS attacks. Those criteria (thresholds) can then be used for defining policy rules to detect frequent changes to a connection caused by those frequent (abnormal) actions.”). The ’500 Patent similarly describes an example where the signals used to determine “excessive attaches” are likewise normally processed:

“FIG. 2 shows a flow diagram of an embodiment of the invention suitable for detecting excessive attaches of a mobile device to a telecommunications network. In an advantageous embodiment a device attaches 201 to the network at time $t_{sub.1}$ through a base station and the network registers the attach, identifies the mobile device and begins authentication procedures. In parallel with the normal processing of the attach request the network performs the following steps.”

EX1001, 7:24-30.

117. The ’500 Patent goes on to explain additional steps for “detecting excessive attaches” including counting attach requests. EX1001, 7:30-54. Thus, the signals that *Eisl* counts to generate parameters used to determine whether a policy rule has been violated represent normal processing of signals.

118. Thus, *Eisl* discloses that “the certain predetermined signal represent[s] an interaction between network devices in the core network for normal processing of signals” as claimed.

Claim 1[e]: “and wherein the telecommunications network is further arranged to register when the number of occurrences of the certain predetermined signal exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network,”

119. In my opinion, *Eisl* discloses these limitations. *Eisl* teaches that its policy rules may include a threshold of counted parameters to distinguish normal behavior from abnormal behavior. *Eisl* states:

Frequent handover, frequent attach or detach or frequent PDP context activation, modification or deactivation actions mean in the context of this application abnormal frequent actions caused by for example a malicious user or malicious software performing a DOS attack to the network. Such actions will cause “frequent” changes to a connection between a mobile device and a network. An expert in the art is able to define criteria (for example **thresholds for mobile device** or network related parameters) in order to distinguish **normal changes of a connection between a mobile device and a network from abnormal (frequent) changes** caused by for example DOS attacks. **Those criteria (thresholds) can then be used for defining policy rules to detect frequent changes to a connection caused by those frequent (abnormal) actions.** For example a criteria could be the number of connection changes that happened during a specific time window. Within the description of this patent application the term “frequent changes to a connection” refers to changes caused by abnormal behavior (like for example by DOS attacks).

EX1004, [0047].

120. *Eisl* specifically describes that the policy rules shown in Figure 4 may include a threshold related to handover actions. EX1004, [0085] (“A policy rule might include one or more **thresholds for one or more parameter**. A device may be assumed to violate a **policy if one or more of those thresholds** are crossed.”). *Eisl* goes on to give an example of violating a policy rule when a number of completed handovers exceeds a threshold:

Example of a policy rule:

Parameters:

- A = number of completed handover actions of mobile one device
- B = Duration of last network connection of the mobile 25 device

Policy rule:

IF ((within TW (A>5)) and (B<10s)) THEN policy rule =VIOLATED

TW = time window = e.g. 1 minute

In the above example “5” is the threshold for the number of the completed handover actions and “10s” is the connection time threshold.

EX1004, [0086]-[0087].

121. As seen in the excerpt above, *Eisl* discloses counting the number of handover actions within a time window and registering a violation if the number of handover actions is greater than 5 within a 1-minute time window. In this example, “5” is the number of occurrences of the certain predetermined signal within the 1-minute window that exceeds a level indicating acceptable behavior of the mobile

telecommunications device in the telecommunications network, and thus results in the system registering that the policy rule is “VIOLATED.” *See id.*, [0086].

122. Additionally, it would have been understood by a POSITA that the system of *Eisl*, when implemented as a “computer program” (*see* EX1004, [0019]), would register the violation by setting a variable or flag associated with the policy rule to “VIOLATED.” The example in paragraph [0086] of *Eisl* would have been understood to be pseudo-code, which would teach a POSITA to implement a computer program with the following conditional statement “IF ((within TW (A>5)) and (3<10s)) THEN policy rule =VIOLATED.” The POSITA would have readily understood this pseudocode to describe setting a variable in memory associated with the “policy rule” to the value “VIOLATED.” This would have been understood by a POSITA to be registering the violation in a computer memory.

123. As a result of the system registers the violation of a policy rule (*e.g.*, when a count of handovers actions is above a threshold), in Element 4-2 and outputs the determined violated policy rules to Element 4-3 of Figure 4:

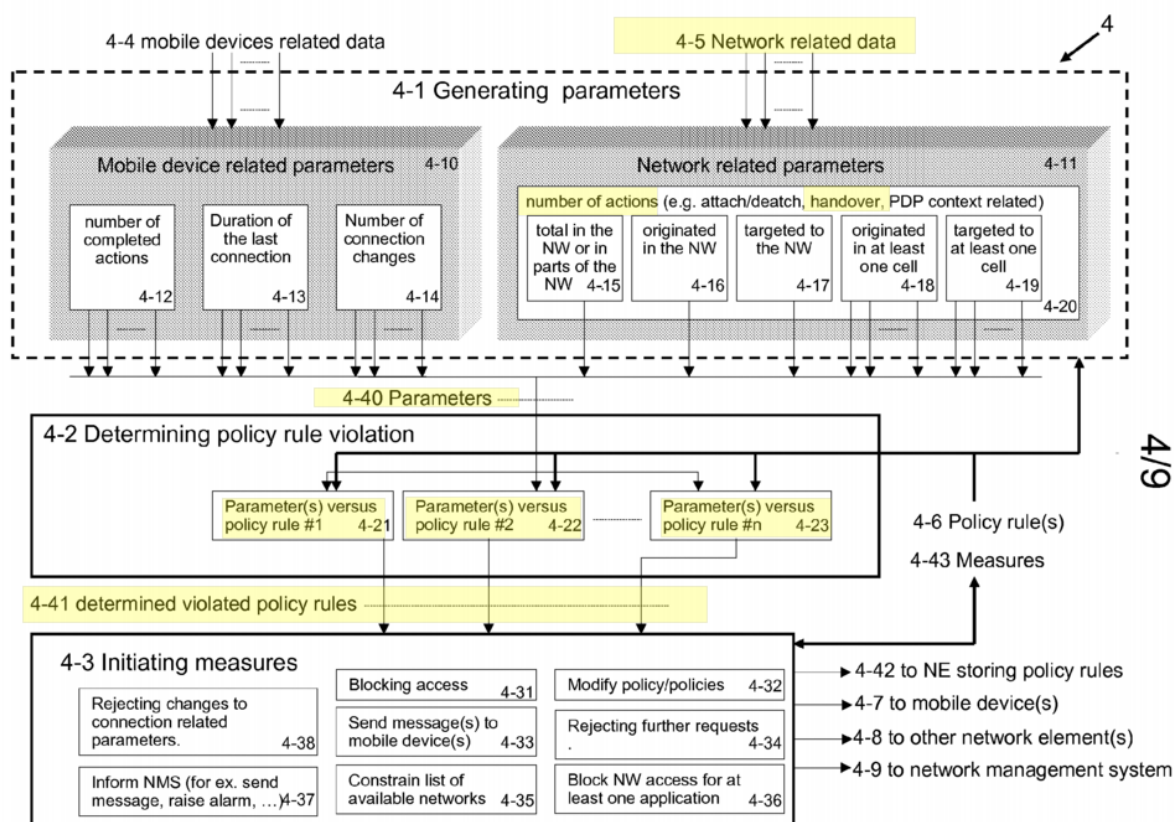


FIG 4

EX1004, Figure 4 (annotated).

124. Within step 4-3, after the system registers a violation, measures are initiated such as sending a message to the mobile, or block its access (4-31, 4-33).

EX1004, (Fig. 4); [0090]-[0091], as by crossing the threshold in a policy rule indicates exceeding a level of acceptable behavior by the mobile telecommunications device. As described by *Eisl*:

“The **measure(s)** a network element involved in the action(s) causing the frequent changes to a connection 4-8 (for example to a base station or base station controller for **blocking mobile device** access to the

network 4-31), a network 30 element storing the policy rules 4-42 (for example the PCRF in fig 2 or the network element performing the determining step 4-2 if the policy rules are stored there), a network management system (NMS) 4-9 or to at least one mobile device 4-7 (for example **sending a message to the mobile device(s)**). If coordinated frequent actions of a group of mobile devices are detected then also the measure(s) may be initiated or applied for/to the whole group of mobile devices.”

EX1004, [0090]; *see also* [0091] (additional measures described).

125. Thus, *Eisl* discloses “wherein the telecommunications network is further arranged to register when the number of occurrences of the certain predetermined signal exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network” as claimed.

126. To the extent that the Patent Owner contends that “registering” is not explicitly disclosed by *Eisl*, it is an implementation detail that would have been obvious to a POSITA at the time of the ’500 Patent. A POSITA would have been motivated to register when the number of occurrences of a signal indicated abnormal or malicious behavior to become aware of or store that the count exceeded a threshold (*i.e.*, a violation took place) to better initiate measures. For example, by registering when a violation took place, the system could implement measure immediately or wait for a future

connection by the offending mobile telecommunications device. *See* EX1004, [00101] (“If a **frequent change to the connection of the mobile device has been recognized earlier** (for example a DoS attack which caused frequent attach/detach actions) the HSS/AAA server may be aware about it (the HSS/AAA server might have been informed about it via measure 4-8 of fig 4) . The HSS/AAA server may then reject the request at this stage (not shown) or inform the mobile device about it (not shown).”) A POSITA would further have had a reasonable expectation of success registering when the number of occurrences of a signal indicated abnormal or malicious behavior because it merely involves the fundamental and well-known technique of storing information. Thus, *Eisl* at least renders obvious “wherein the telecommunications network is further arranged to register when the number of occurrences of the certain predetermined signal exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network” as claimed.

Claim 1[f]: “wherein the certain predetermined signal indicates handover of the mobile telecommunications device.”

127. In my opinion, *Eisl* teaches this limitation. *Eisl* discloses using certain predetermined signals indicating handover of the mobile telecommunications device to determine the behavior of the same. *See* Claims 1[a]-1[e] discussed

above. For example, *Eisl* teaches that a certain type of network related data is counted and these signals indicate handover actions. EX1004, [0079] (“Received **network related data 4-5** may include information **related to handover actions**, attach/ detach actions or PDP context activation/modification/ deactivation actions.”). *Eisl* also discloses that these signals may be counted for a time window. [0078] (“Further on the parameters might be generated for a defined time window, which means that only **events falling into the sliding time window are counted**”). Thus, *Eisl* discloses “wherein the certain predetermined signal indicates handover of the mobile telecommunications device” as claimed.

2. Claim 2

Claim 2[a]: “The system according to claim 1, wherein the telecommunications network is arranged to count in the core network the number of occurrences of the certain predetermined signal by counting a number of times occurrence of the certain predetermined signal is detected when the number of occurrences exceed a predetermined temporal rate,”

128. In my opinion *Eisl* discloses that generated parameters are used to determine the frequency of the number of events of handover actions, which includes determining whether the number of events exceeds a threshold within a specific time window (*i.e.*, a temporal rate). EX1004, [0072] (“Further on the parameters may include a time dimension, which means that the **parameters are generated for data or events falling into a specific time window.**”); EX1004,

[0073] (“A time dimension (**which might be part of the policy rule**) **may be taken into account when doing the evaluation** (note, this is optional for step 3-2).”). A POSITA would have understood that counting the number of actions within a specific one-minute time window is equivalent to a temporal rate (*e.g.*, number of events per minute).

129. *Eisl* provides an example policy rule determining whether the number of occurrences of handover action exceeds a predetermined temporal rate (*i.e.* a rate determined in the policy rule):

Example of a policy rule:

Parameters:

- A = number of completed handover actions of mobile one device
- B = Duration of last network connection of the mobile 25 device

Policy rule:

IF ((within TW (A>5)) and (B<10s)) THEN policy rule =VIOLATED

TW = time window = *e.g.* 1 minute

EX1004, [0086].

130. In the above example the number of occurrences that would exceed the predetermined temporal rate is 5 handover actions per minute. *Id.* If the number of handovers exceeds rate of 5 over 1 minute, the policy rule is violated.

131. *Eisl* further discloses that the number of occurrences of the predetermined signal, for example a handover action, may be counted when the

policy rule is violated. *See* EX1004, [0089] (“In addition information about which policy rule is violated, **which threshold** are when crossed **and how much it is exceeded** might be transferred in 4-41 together with the result(s) from the policy rule check to step 4-3.”). Thus, *Eisl* discloses “wherein the telecommunications network is arranged to count in the core network the number of occurrences of the certain predetermined signal by counting a number of times occurrence of the certain predetermined signal is detected when the number of occurrences exceed a predetermined temporal rate” as claimed. As discussed with respect to Claim 1[c] and incorporated herein by reference, to the extent “counting” is not explicitly disclosed by *Eisl*, counting is an implementation detail that would have been obvious to a POSITA at the time of the ’500 Patent. *See* Section X.A.1.Claim 1[c].

Claim 2[b]: “and wherein the telecommunications network is further arranged to register when the number of times the occurrence of the certain predetermined signal detected exceeds a predetermined threshold.”

132. In my opinion, *Eisl* teaches this limitation. *Eisl* discloses registering when the number of times the occurrence of the certain predetermined signal detected exceeds a predetermined threshold.

133. As discussed with respect to Claim 1[e] above (explaining that the network is arranged to register when the predetermined signal detected exceeds a predetermined threshold), *Eisl* discloses “register[ing] when the number of times

the occurrence of the certain predetermined signal detected exceeds a predetermined threshold” as claimed at least for the reasons stated above. *See above* Section X.A.1.Claim 1[e].

3. Claim 3

“The system according to claim 2, wherein the telecommunications network is arranged to count the number of occurrences of the certain predetermined signal when a time between a detected occurrence and a previously detected occurrence is within a predetermined time interval.”

134. In my opinion *Eisl* discloses counting instances of events that fall within a sliding time window. EX1004, [0078] (“Further on the parameters might be generated for defined time window, which means that only **events falling into the sliding time window are counted.**”). A POSITA would have understood that the time between each occurrence of these events must be within the window to be counted, including the detected event and the previously counted event(s). For example, in the policy rule below each handover action within the predetermined time window of 1 minute is counted to determine if there is a violation.

Example of a policy rule:

Parameters:

- A = number of completed handover actions of mobile one device
- B = Duration of last network connection of the mobile device

Policy rule:

IF ((within TW ($A > 5$)) and ($B < 10s$)) THEN policy rule = VIOLATED

TW = time window = e.g. 1 minute

EX1004, [0086].

135. In other words, *Eisl* teaches counting network data indicating the number of occurrences of completed handover actions (*i.e.*, the certain predetermined signal) when an occurrence of a completed handover action (*i.e.*, a detected occurrence) and at least one previously detected completed handover action (*i.e.*, a previously detected occurrence) fall within a sliding time window (*i.e.*, the time between the occurrences is within a predetermined time window). For example the variable ‘A’ in the policy rule above counts number of completed handover actions of mobile one device in a one-minute sliding time window.

136. These occurrences could be consecutive, but there may be additional occurrences between the detected occurrence and previously detected occurrence recited in the claim depending on the length of the sliding time window. For example by way of illustration: in the policy rule illustrated above, the time window is one minute. If the “detected occurrence” happens at time 0s, and the claimed “previously detected occurrence” happens at time 58 seconds ago, ‘A’ would equal 2 and *Eisl*’s policy rule counts both and the claim language is satisfied because the time between occurrences is within the “predetermined time interval” of one minute. *Id.* However, if occurrences happened at 0s, -5s, -34s, -51s, and -

58s, each of these occurrences would also be counted by *Eisl*'s policy rules and the claim language would still be satisfied because the time between the “detected occurrence” at 0s and the claimed “previously detected occurrence” at 58 seconds ago is still within the predetermined time interval of one minute. Thus, *Eisl* discloses “wherein the telecommunications network is arranged to count the number of occurrences of the certain predetermined signal when a time between a detected occurrence and a previously detected occurrence is within a predetermined time interval” as claimed. As discussed with respect to Claim 1[c] and incorporated herein by reference, to the extent “counting” is not explicitly disclosed by *Eisl*, counting is an implementation detail that would have been obvious to a POSITA at the time of the '500 Patent. *See* Section X.A.1.Claim 1[c].

4. Claim 4

Claim 4[a]: “The system according to claim 3, wherein the telecommunications network includes a counter and a timer,”

137. *In my opinion Eisl* renders these limitations obvious. As explained above with respect to at least Claim 1, 2, and 3, when generating parameters *Eisl* teaches counting the number of, for example, signals (in the form of network data) indicating handover actions that fall within a time window. *See* EX1004, [0086] (showing an example policy rule based on a **number** of handover actions and a timer); *see also* Section X.A.1-3. A POSITA would understand a counter is would

be used count the number signals indicating handover. Also, as previously explained, *Eisl* teaches that parameters may be generated for a sliding time window. *See* Section X.A.3; *see also id.*, [0078] (“Further on the parameters might be generated for defined time window, which means that **only events falling into the sliding time window are counted.**”). A POSITA would understand that a timer would be used to implement a time window. However, to the extent that the Patent Owner contends that a counter and a timer are not explicitly disclosed by *Eisl*, inclusion of counter and timer is an implementation detail that would have been obvious to a POSITA at the time of the ’500 Patent.

138. A POSITA would have been motivated to include a counter and a timer when implementing *Eisl*’s parameter generation and policy rules to efficiently implement the same. For example, *Eisl*’s parameter generation generates the number of certain activities by processing mobile or network related data (*i.e.*, signals); a counter provides an efficient mechanism to do this. Likewise, *Eisl*’s policy rules involve comparing the number of actions within a time window; a timer provides an efficient mechanism for measuring time. A POSITA would further have had a reasonable expectation of success in implementing a counter and a timer because they are fundamental and well-known techniques of measuring the number of things and measuring time respectively. Thus, *Eisl* at least renders

obvious “wherein the telecommunications network includes a counter and a timer” as claimed.

Claim 4[b]: “and wherein the telecommunications network is arranged to start the counter upon detection of the occurrence and further to start the timer,”

139. In my opinion, *Eisl* renders these limitations obvious. It would have been obvious to start counting and to start the sliding time window at the first occurrence of a monitored event/parameter for a particular mobile telecommunications device. A POSITA seeking to implement *Eisl*’s sliding time window, would have needed to start the sliding time window based on an occurrence of some event. The most natural event to start the time window on would have been the occurrence of a first event that the system began counting. To do otherwise would waste system resources such as timers when they are not needed.

140. Thus, to the extent this implementation detail is not already explicitly taught by *Eisl*, a POSITA would have been motivated to modify *Eisl* in this way to save processing resources. A POSITA would recognize it is unnecessary to spend processing resources counting the occurrences of an event in a given time window until the first event occurs. A POSITA would have had a reasonable expectation of success in implementing *Eisl*’s policy rules in this way because it would merely involve adding an additional condition—starting the counting and sliding time

window on first occurrence of an event—to an existing policy rule. Thus, *Eisl* at least renders obvious “wherein the telecommunications network is arranged to start the counter upon detection of the occurrence and further to start the timer” as claimed.

Claim 4[c]: “and wherein the telecommunications network is further arranged to increase the counter by one unit if a following occurrence is within the predetermined time interval as measured by the timer.”

141. In my opinion *Eisl* renders these limitations obvious. As explained above with respect to at least Claim 1, 2, and 3, implementation of *Eisl*’s policy rules involves counting the number of, for example, handover actions within the predetermined time window of, for example, 1 minute. EX1004, [0086], [0078], [0089]; *see also* Section X.A.1-3. For example, the variable ‘A’ described above, counts by 1 unit in the time window. EX1004, [0086]. A POSITA would have understood as a matter of basic mathematics that the counter would be incremented by one each time an instance of the action being counted occurred. Increasing a count by one is the most rudimentary and well-understood form of counting. Thus, *Eisl* renders obvious “wherein the telecommunications network is further arranged to increase the counter by one unit if a following occurrence is within the predetermined time interval as measured by the timer” as claimed.

142. *Eisl* renders Claim 4[c] obvious. A POSITA seeking to implement *Eisl*'s counting functionality would have had to go out of his way to implement a system incrementing a count by anything other than 1 occurrence. A POSITA would have been motivated to use this implementation detail to maintain simplicity and avoid undue effort due to setting up another counting system. A POSITA would have had a reasonable expectation of success because incrementing by 1 is the most rudimentary and routine form of counting known in the art.

5. Claim 5

“The system according to claim 1, wherein the telecommunications network is further configured to detect when the number of occurrences of the certain predetermined signal exceeds a predetermined rate.”

143. In my opinion, *Eisl* discloses these limitations. *See* Section X.A.2.Claim 2[a].

6. Claim 6

Claim 6[a]: “The system according to claim 5, wherein the telecommunications network includes a counter and a timer,”

144. In my opinion, *Eisl* discloses these limitations. *See* Section X.A.4.Claim 4[a].

Claim 6[b]: “and wherein the telecommunications network is arranged to start the counter upon detection of the occurrence and further to start the timer,”

145. In my opinion, *Eisl* discloses these limitations. See Section

X.A.4.Claim 4[b].

Claim 6[c]: “and wherein the telecommunications network is further arranged to calculate a rate as a ratio of a counted number of detected occurrences to time as measured by the timer.”

146. In my opinion, *Eisl* discloses these limitations. A POSITA would have understood that that counting the number of actions within a time window is equivalent to a rate. *See* Section X.A.2.Claim 2[a]. *Eisl* provides an example policy rule determining whether the number of occurrences of handover action exceeds a predetermined temporal rate (*i.e.* a rate determined in the policy rule):

Example of a policy rule:

Parameters:

- A = number of completed handover actions of mobile one device
- B = Duration of last network connection of the mobile device

Policy rule:

IF ((within TW (A>5)) and (3<10s)) THEN policy rule =VIOLATED

TW = time window = e.g. 1 minute.

EX1004, [0086].

147. In the above example, the variable ‘A’ counts the number of handovers in a time window of 1 minute. Therefore, the value of ‘A’ is a rate, as it is a ratio of a counted number of detected occurrences to time as measured by the timer, *e.g.* 1 minute. Thus, *Eisl* discloses “wherein the telecommunications

network is further arranged to calculate a rate as a ratio of a counted number of detected occurrences to time as measured by the timer,” as claimed.

7. Claim 7

“The system according to claim 1, wherein the telecommunications network is arranged to register when the number of occurrences of the certain predetermined signal exceeds the level for acceptable behaviour by setting a flag and/or starting a back off.”

148. In my opinion, *Eisl* discloses these limitations. *Eisl* discloses checking whether its defined policy rules are violated in order to detect frequent changes of the connection. *See e.g.*, EX1004, [0066]. As discussed above with respect to Claim 1[e], it would have been understood that the system of *Eisl* would register the violation by setting a variable (*i.e.*, flag) associated with the policy rule to VIOLATED.⁶ *See* EX1004, [0086]; *See also* Section X.A.1.Claim 1[e].

149. *Eisl* further discloses that if frequent changes are detected (*i.e.* a policy rule is violated), this can be reported as an alarm, which is another form of a “flag.” *See e.g.*, EX1004, [0066]. (“If frequent changes are detected this might be

⁶ *See* EX1010 (giving the definition of flag as “[a] variable whose value indicates the attainment of some designated state or condition by an item of equipment or a program. The flag is subsequently used as a basis for conditional branching and similar decision processes.”)

reported to the NMS 2-1 (for example **in form of an alarm** or performance data information which will be fetched from the NMS 2-1).”). A POSITA would have understood that an alarm is a variable (*i.e.*, a flag) that indicates the state of the policy rule violation. *Eisl* describes raising an alarm as an example of a possible measure that can be taken during its “initiating measures” step once frequent changes to a connection are detected. *See* EX1004, [0091] (“Possible measures may ... informing the network management system (NMS) 4-37 (for example by raising an alarm or providing status information which can be read by the NMS)....”).

150. *Eisl* also discloses that the system registers when the number of occurrences of the certain predetermined signal exceeds the level for acceptable behavior by starting a back off timer. For example, when the network registers a violation has occurred, it initiates remedial measures as disclosed in Figure 4 (element 4-3) and as explained above for Claim 1. EX1004 Figure 4, [0090], [0091]. *Eisl* explains that a time window may be applied to these measures, stating that “time window for applying the measure(s) might be defined, thus for example the blocking of network access for one or more mobile devices might be limited to a certain time.” The ’500 Patent similarly describes its back off timer: “starting a back off timer to stop the mobile device from making another connection request within a certain time period.” EX1001, 5:66-6:1. Thus, a POSITA would have

understood that blocking network access for a limited amount of certain time discloses implementing and starting a backoff timer.

151. Thus, *Eisl* discloses “wherein the telecommunications network is arranged to register when the number of occurrences of the certain predetermined signal exceeds the level for acceptable behaviour by setting a flag and/or starting a back off time” as claimed.

8. Claim 8

Claim 8[a]: “The system according to claim 1, wherein the telecommunications network is further arranged to monitor a tracking area of the mobile telecommunications device”

152. In my opinion, *Eisl* renders these limitations obvious. A POSITA would have recognized that a “tracking area” merely refers to a group of one or more cells within a cellular system. Indeed, the ’500 Patent describes using tracking area to determine when the mobile device is moving between parts of the network. *See* EX1001, 5:41-44 (“The network maintains a record of the tracking area of the mobile device and also an indication of when the tracking area changes. This allows the network to know when device is moving.”). Moreover, it was well known to a POSITA that cellular systems needed to monitor the tracking area of a mobile device to locate that device within the network. As discussed with respect to Claim 1, *Eisl* discloses that its teachings are applicable to a variety of telecommunication networks, including GSM, UMTS, WiMAX, CDMA, WLAN,

LTE, and others. *See e.g.*, EX1004, [002]. These are examples of well-known telecommunications networks that monitor the tracking area (or equivalent) of a mobile telecommunications device. Eisl teaches specifically monitoring groups of cells which a POSITA would understand to incorporate a tracking area. EX1004, [0072]. (“The generated parameters may be specific parameters for a dedicated mobile device, for a group of mobile devices, for the whole network or for a part of the network (for example one or more cells of the network.)”).

153. Thus, to the extent that the Patent Owner contends that *Eisl* does not explicitly disclose “wherein the telecommunications network is further arranged to monitor a tracking area of the mobile telecommunications device”, it would have been obvious for a POSITA to modify Eisl to monitor a tracking area. *Eisl* discloses network parameters can be based on parts of a network, including a group of cells. EX1004, [0072]. (“The generated parameters may be specific parameters for a dedicated mobile device, for a group of mobile devices, for the whole network or for a part of the network (for example one or **more cells of the network.**)”). It would have been obvious for a POSITA to make this parameter relating a group of cells a tracking area, so that the system could monitor the mobile behavior in a tracking area. Thus, *Eisl* renders obvious “The system according to claim 1, wherein the telecommunications network is further arranged to monitor a tracking area of the mobile telecommunications device” as claimed.

Claim 8[b]: “and to register the number of occurrences of the certain predetermined signal only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area.”

154. In my opinion, *Eisl* renders these limitations obvious. *Eisl* teaches that its policy rules can be based on *parts* of the network, which a POSITA would understand to include tracking areas comprising sets of cells. *See* EX1004, [0038] (“A policy rule in the context of this application is a rule which might be applied to a whole network, *parts of a network*, one or more network elements, one or more mobile devices or one or more mobile subscribers.”). *Eisl* goes on to explain that different policies may apply to different *areas*, and that within *one area*, one or more criteria might be used within a policy rule:

“Different policy rules might apply for different areas or groups (for example for detecting frequent changes of a connection of a single mobile device or of a group of mobile devices, or for detecting frequent changes of one or more connections in a network or in parts of a network or might be related to a combination of those. Within one area or group one or more criteria . . . might be used within one policy rule.”

EX1004, [0084].

155. It would have been apparent that a particular mobile device’s activities would only be counted when the mobile device’s tracking area coincided with the area to which the policy rule is applied. If the mobile device moved outside of the tracking area to which the policy applies, the POSITA would have

understood that the mobile device's activities would no longer be applied against the policy rule for that area. The '500 Patent specifically describes that a "particularly advantageous embodiment of the invention would be performed in the MME of the Network." EX1001, 8:9-10. MME's are used to manage mobility within one or more tracking area(s). *Eisl* also describes that its policy rules can be implemented in an MME. *See* EX1004, [0068] ("The mobility anchor 1 . . . is just a preferred network element for detecting frequent changes of the connection of at least one mobile device to the network); *see also id.*, [0037] ("Examples for core network elements involved in handover activities are Serving GPRS Support Node (SGSN), Gateway GPRS Support Node (GGSN), Mobility Management Entity (MME), Serving Gateway (SGW) and Packet Data Network Gateway (PGW)."). Given *Eisl*'s disclosure of monitoring parts of the network including sets of cells, and its disclosure of using an MME, it would have been natural for the POSITA to select one or more tracking areas managed by the MME to monitor. It would have been obvious for the POSITA to make monitoring selectively enabled within parts of the network, including in one or more tracking areas. If the user selected one tracking area to monitor, the monitoring of a mobile telecommunications would cease if the mobile telecommunications device leaves the tracking area. A POSITA would have been motivated to do so to conserve and precisely target processing resources (*e.g.*, targeting the portions of the network from which the malicious

behavior is originating). A POSITA would have had a reasonable likelihood of success in implementing this because it merely involves applying *Eisl*'s teachings to an existing and well-known division of the cells in the network.

156. Thus, *Eisl* renders obvious “to register the number of occurrences of the certain predetermined signal only when the monitoring of tracking area shows that the mobile telecommunications device remains within a single tracking area” as claimed.

9. Claim 9

“The system according to claim 1, wherein the telecommunications network is arranged to count the number of occurrences of the certain predetermined signal in a Mobility Management Entity or Serving Gateway Support Node or Mobile Switching Center of the telecommunications network.”

157. In my opinion, *Eisl* discloses these limitations. *Eisl* teaches that policy rules may be implemented in any core network element, and that the preferred network element is the mobility anchor (another name for the claimed mobility management entity). *See* EX1004, [0068] (“The mobility anchor 1. . . is just a preferred network element for detecting frequent changes of the connection of at least one mobile device to the network); [0038] (“Policy rules can be stored and implemented basically in any network element in the core or access network.”). *Eisl* also teaches that Mobility Management Entity or Serving Gateway Support Node are part of the network elements in the core network. EX1004 [0037]

(“Examples for core network elements involved in handover activities are **Serving GPRS Support Node (SGSN)**, Gateway GPRS Support Node (GGSN), **Mobility Management Entity (MME)**, Serving Gateway (SGW) and Packet Data Network Gateway (PGW).”). Thus, *Eisl* discloses “wherein the telecommunications network is arranged to count the number of occurrences of the certain predetermined signal in a Mobility Management Entity or Serving Gateway Support Node or Mobile Switching Center of the telecommunications network” as claimed.

10. Claim 10

Claim 10[p]: “The system according to claim 1, wherein the telecommunications network is further configured to:”

158. In my opinion, *Eisl* discloses these limitations. *See above* Section X.A.1.

Claim 10[a]: “identify at least one additional mobile telecommunications device,”

159. In my opinion, *Eisl* discloses these limitations. As explained with respect to at least Claim 1[a], *Eisl* describes a telecommunications network configured to identify a mobile telecommunications device. *See above* Section X.A.1.Claim 1[a]. *Eisl* further teaches that its system applies to mobile devices (*plural*). *See* EX1004, [0011] (“In consideration of the above, it is an object of the present invention to overcome the above mentioned problem of possible changes to a connection of device(s) (preferable **mobile devices**) to a network caused by for

example a malicious user or mobile device.”); EX1004 [0090] (“If coordinated frequent actions of a **group of mobile devices** are detected then also the measure(s) may be initiated or applied for/to the **whole group of mobile devices.**”). Thus, *Eisl* discloses a telecommunications network configured to “identify at least one additional mobile telecommunications device” as claimed.

Claim 10[b]: “receive radio signals from the at least one additional mobile telecommunications device and to process these radio signals into processed signals and to transmit the processed signals to the core network,”

160. In my opinion, *Eisl* discloses these limitations. As explained with respect to at least Claim 1[b], *Eisl* discloses base stations that receives radio signals from a mobile telecommunications device, process them, and transmit them to the core network. *See above* Section X.A.1.Claim 1[b]. *Eisl* further teaches that its system applies to mobile devices (**plural**). *See* EX1004, [0011]; [0090]. Thus, *Eisl* discloses a telecommunications network configured to “receive radio signals from the at least one additional mobile telecommunications device and to process these radio signals into processed signals and to transmit the processed signals to the core network” as claimed.

Claim 10[c]: “count in the core network a number of occurrences of a certain predetermined signal associated with the at least one additional mobile telecommunications device, the certain predetermined processed signal representing an interaction between network devices for normal processing of signals”

161. In my opinion, *Eisl* discloses these limitations. As explained with respect to at least Claim 1[c] and 1[d], *Eisl* discloses policy rules used to detect abnormal behavior of mobile devices which may be implemented in the core network, and the predetermined signal representing an interaction between network devices for normal processing of signals. *See* Claim 1[c] and Claim 1[d]. *Eisl* further teaches that its system applies to mobile devices (*plural*). *See above* Section X.A.1.Claim 1[a] and Claim 1[b].

Claim 10[d]: “register when the number of occurrences of a certain predetermined signal associated with the at least one additional mobile telecommunications device exceeds a level indicating acceptable behaviour of the at least one additional mobile telecommunications device within the telecommunications network,”

162. In my opinion, *Eisl* discloses these limitations. As explained with respect to at least Claim 1[d], *Eisl* discloses monitoring signals for abnormal behavior that are signals that are normally processed in the core network. *See above* Section X.A.1.Claim 1[d]. *Eisl* further teaches that its system applies to mobile devices (*plural*). *See* EX1004, [0011]; [0090]. Thus, *Eisl* discloses a telecommunications network configured to “register when the number of occurrences of a certain predetermined signal associated with the at least one additional mobile telecommunications device exceeds a level indicating acceptable

behaviour of the at least one additional mobile telecommunications device within the telecommunications network” as claimed.

Claim 10[e]: “wherein the telecommunications network is further arranged to aggregate registered data of the mobile telecommunications device and the at least one additional mobile telecommunications device,”

163. In my opinion, Eisl discloses these limitations. *Eisl* discloses that the generated parameters evaluated with its policy rules may include parameters for a group of mobile devices (*i.e.* a mobile telecommunications device and the at least one additional mobile telecommunications device). *See* EX1004, [0072] (“The generated parameters may be specific parameters ... ***for a group of mobile devices....***”); EX1004, [0078] (“Mobile device related parameters 4-10 might be generated for a single mobile device or a group of mobile device.”). *Eisl* likewise discloses that both policy rules and measure initiated for policy rule violations may be applied to groups of mobile devices. *See id.*, [0084] (“Different policy rules might apply for different areas or groups (for example for detecting frequent changes of a connection of a single mobile device ***or of a group of mobile devices....***”); EX1004, [0090] (“If coordinated frequent actions of a group of mobile devices are detected then also the measure(s) may be initiated or applied for/to ***the whole group of mobile devices.***”). Thus, *Eisl* discloses “wherein the telecommunications network is further arranged to aggregate registered data of the

mobile telecommunications device and the at least one additional mobile telecommunications device” as claimed.

Claim 10[f]: “and wherein the certain predetermined signal associated with the at least one additional mobile telecommunications device indicates handover of the at least one additional mobile telecommunications device.”

164. In my opinion, *Eisl* discloses these limitations. As explained with respect to at least Claim 1[f], *Eisl* discloses using handover actions to determine the behavior of the mobile telecommunications device. See above Section X.A.1.Claim 1[f].

11. Claim 11

Claim 11[pre]: “A method for detecting behaviour of a mobile telecommunications device in a telecommunications network comprising a core network, the telecommunications network including a base station, the method comprising:”

165. In my opinion, *Eisl* discloses these limitations. *See above* Section X.A.1.Claim 1[a].

Claim 11[a]: “at the base station, receiving radio signals from the mobile telecommunications device, and processing the radio signals into processed signals and transmitting the processed signals to the core network;”

166. In my opinion, *Eisl* discloses these limitations. *See above* Section X.A.1.Claim 1[b].

Claim 11[b]: “in the telecommunications network, identifying the mobile telecommunications device;”

167. In my opinion, *Eisl* discloses these limitations. *See above* Section

X.A.1.Claim 1[a].

Claim 11[c]: “the telecommunications network counting, in the core network, a number of occurrences of a certain predetermined signal associated with the mobile telecommunications device,”

168. In my opinion, *Eisl* discloses these limitations. *See above* Section

X.A.1.Claim 1[c].

Claim 11[d]: “the certain predetermined signal representing an interaction between network devices in the core network for normal processing of signals; and”

169. In my opinion, *Eisl* discloses these limitations. *See above* Section

X.A.1.Claim 1[d].

Claim 11[e]: “registering when the number of occurrences of the certain predetermined signal exceeds a level indicating acceptable behaviour of the mobile telecommunications device in the telecommunications network,”

170. In my opinion, *Eisl* discloses these limitations. *See above* Section

X.A.1.Claim 1[e].

Claim 11[f]: “wherein the certain predetermined signal indicates handover of the mobile telecommunications device.”

171. In my opinion, *Eisl* discloses these limitations. *See above* Section

X.A.1.Claim 1[f].

XI. CONCLUSION

172. In my opinion the '500 Patent does not claim a novel or non-obvious invention. For all of the reasons explained above, *Eisl* renders Claims 1-3, 5-7 and 9-11 anticipated, in addition, each of these claims are rendered obvious by *Eisl* in view of the knowledge of a POSITA. Additionally, Claims 4 and 8 are rendered obvious by *Eisl* in view of the knowledge of a POSITA.

XII. DECLARATION

173. I hereby declare that all the statements made in this Declaration are of my own knowledge and true; that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. § 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Executed in Dallas, Texas on February 22nd, 2023.

/James Olivier/

James Olivier