

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DEPARTMENT OF JUSTICE,
Petitioner,

v.

ENVISIONIT, LLC,
Patent Owner,

CASE NO. TO BE ASSIGNED
PATENT NO. 8,438,221

**PETITION FOR INTER PARTES REVIEW OF
U.S. PATENT NO. 8,438,221
UNDER 35 U.S.C. §§ 311–319 AND 37 C.F.R. § 42.100 *et seq.***

TABLE OF CONTENTS

LIST OF EXHIBITS	III
I. INTRODUCTION	1
II. MANDATORY NOTICES (37 C.F.R. § 42.8(A)(1)).....	1
A. Real Party-In-Interest (37 C.F.R. § 42.8(b)(1)).....	1
B. Related Matters (37 C.F.R. § 42.8(b)(2))	4
C. Lead and Backup Counsel (37 C.F.R. § 42.8(b)(3))	5
D. Service Information (37 C.F.R. § 42.8(b)(4))	6
III. FEES (37 C.F.R. § 42.103).....	6
IV. REQUIREMENTS FOR INTER PARTES REVIEW UNDER 37 C.F.R. § 42.104	6
A. Grounds for Standing (37 C.F.R. § 42.104(a)).....	6
B. Citation of Prior Art.....	7
C. Claims and Statutory Grounds (37 C.F.R. §§ 42.104(b)(1)–(2))	7
D. Person of Ordinary Skill in the Art.....	8
E. Claim Construction (37 C.F.R. § 42.104(b)(3)).....	8
1. “broadcast”	8
F. Unpatentability of the Construed Claims (37 C.F.R. § 42.104(b)(4)) ...	9
G. Supporting Evidence (37 C.F.R. § 42.104(b)(5)).....	10
V. SUMMARY OF THE ’221 PATENT	10
A. Overview of the ’221 Patent.....	10
1. The claim at issue: Claim 19	10
2. The alleged invention of the ’221 Patent	11
B. Prosecution History Summary of the ’221 Patent	11
VI. THERE IS A REASONABLE LIKELIHOOD THAT PETITIONER WILL PREVAIL WITH RESPECT TO AT LEAST ONE CLAIM OF THE ’221 PATENT	13
A. The state of the art on February 12, 2004: broadcasting messages to a geographic region was widely known and well as access control systems for assigning user roles and privileges.....	14

B.	Ground I: Claim 19 of the '221 Patent is obvious over Gundlegård Thesis (Ex. 1013) in view of the 3GPP Standard (Ex. 1019), Sandhu (Ex. 1020), and Rieger (Ex. 1017) in view of Zimmers (Ex. 1018). ...	15
1.	Motivation to Combine Gundlegård with the 3GPP Standard...	29
2.	Motivation to Combine Gundlegård with Sandhu	29
3.	Motivation to Combine Gundlegård with Rieger in View of Zimmers.....	30
C.	Ground II: Claim 19 of the '221 Patent is rendered obvious over Mani (Ex. 1014) in view of the 3GPP Standard (Ex. 1019), Sandhu (Ex. 1020), and Rieger (Ex. 1017) in view of Zimmers (Ex. 1018).	33
1.	Motivation to Combine Mani with the 3GPP Standard	42
2.	Motivation to Combine Mani with Sandhu.....	43
3.	Motivation to Combine Mani with Rieger in View of Zimmers	44
VII.	CONCLUSION	46

LIST OF EXHIBITS

Exhibit	Description
Ex. 1001	U.S. Patent No. 8,438,221
Ex. 1002	U.S. Patent No. 7,693,938
Ex. 1003	U.S. Patent No. 8,103,719
Ex. 1004	U.S. Patent No. 8,438,212
Ex. 1005	U.S. Patent No. 9,136,954
Ex. 1006	File History (excerpts) for U.S. Patent No. 7,693,938
Ex. 1007	File History (excerpts) for U.S. Patent No. 8,103,719
Ex. 1008	File History (excerpts) for U.S. Patent No. 8,438,212
Ex. 1009	File History (excerpts) for U.S. Patent No. 8,438,221
Ex. 1010	File History (excerpts) for U.S. Patent No. 9,136,954
Ex. 1011	Declaration of Randall Snyder
Ex. 1012	CV of Randall Snyder
Ex. 1013	Gundlegård Thesis
Ex. 1014	U.S. Patent Application Publ. No. 2002/0184346 A1 to Mani
Ex. 1015	U.S. Patent Application Publ. No. 2002/0188725 A1 to Mani

Exhibit	Description
Ex. 1016	REPORT AND ORDER AND FURTHER NOTICE OF PROPOSED RULE MAKING (FCC Report No. 94-288) (“FCC Report”)
Ex. 1017	U.S. Patent Application Publ. No. 2002/0103892 A1 to Rieger
Ex. 1018	U.S. Patent No. 6,816,878 to Zimmers
Ex. 1019	3GPP Standard (4.2.0)
Ex. 1020	R. Sandhu et al., “Access Control: Principles and Practice,” IEEE Communications Magazine September 1994, Vol. 32 No. 9, pp. 40-48.
Ex. 1021	Declaration of Amelia Nuss
Ex. 1022	Excerpts from Christensen et al., “Wireless Intelligent Networking” Artech House, Inc., 2001
Ex. 1023	E112 - Wireless Emergency Services Whitepaper, CMG Wireless Data Solutions, November 2001
Ex. 1024	Report of the Ministry of Interior, Finland “Information to the Public – Warning and Alarm System” 2000
Ex. 1025	Wood, M. “Disaster Communications” APCO Institute, Inc., June 1996
Ex. 1026	Excerpts from UNIX System V, RELEASE 4, User’s Guide, UNIX System Laboratories, Inc., Prentice-Hall, Inc. 1990
Ex. 1027	U.S. Patent No. 6,112,075 Weiser
Ex. 1028	3GPP Specification Change Request List

I. INTRODUCTION

U.S. Patent No. 8,438,221 (“the ’221 Patent”) is generally directed toward “message broadcast systems and in particular location-specific message broadcasting aggregator and gateways.” Ex. 1001, ’212 Patent, at 1:19-22. The prior art teaches each and every element (either alone or in combination) recited in claim 19 of the ’221 Patent and, therefore, Petitioner respectfully requests that the Board institute trial proceedings and find the challenged claim invalid under 35 U.S.C. § 103.

II. MANDATORY NOTICES (37 C.F.R. § 42.8(a)(1))

A. Real Party-In-Interest (37 C.F.R. § 42.8(b)(1))

The real party in interest for this petition for Inter Partes Review (“IPR”) is The United States as represented by the Department of Justice and the Department of Homeland Security. International Business Machines Corporation (IBM) was notified in the co-pending Court of Federal Claims action pursuant to Court of Federal Claims Rule 14, giving IBM an opportunity to appear, if it so desired, as a party and to assert whatever interest it may have in that action due to a patent indemnity clause in a procurement contract. *See Cellcast Techs. et al. v. United States*, No. 15-cv-1307, ECF No. 12 (Fed. Cl. March 8, 2016). IBM has since joined the action. However, IBM is not a real party-in-interest here.

The Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,764 (Aug. 14, 2012) explains that “[w]hether a party who is not a named participant in a given proceeding nonetheless constitutes a ‘real party-in-interest’ . . . to that proceeding is a highly fact-dependent question.” *Id.* at 48,759. The determination of whether a non-party is a real party-in-interest involves a consideration of control; “[a] common consideration is whether the non-party exercised or could have exercised control over a party’s participation in a proceeding.” *Id.* Other considerations may include whether a non-party, in conjunction with control, is funding the proceeding and directing the proceeding. *Id.* at 48,759–60.

IBM is not a real party-in-interest here because “[t]he mere existence of an indemnification agreement does not establish that the indemnitor has the opportunity to control an inter partes review.” *Mercedes-Benz USA, LLC v. Proximity Monitoring Innovations LLC*, Case No. IPR2015-00397, slip. op. at 9 (PTAB July 17, 2015) (Paper 18) (determining that the existence of an indemnification agreement was not sufficient to establish that the unnamed parties were real parties-in-interest); *see also Broadcom Corp. v. Telefonaktiebolaget I.M. Ericsson*, IPR2013-00601, slip. op. at 7-11 (PTAB Jan. 24, 2014) (Paper 23) (“Paying for trial expenses pursuant to indemnity normally does not establish privity or control.”); *Wavemarket Inc. v. Locationet Sys. Ltd.*, IPR2014-00199, slip. op. at 5 (PTAB Aug. 11, 2014) (Paper 34); *Apple Inc. v. Achates Reference Publ. Inc.*, IPR2013-00080,

slip. op. at 4-7 (PTAB April 3, 2013) (Paper 18). A petitioner and a non-party's status as codefendants and co-members of a joint defense group is not alone sufficient to render the non-party a real party in interest. Trial Practice Guide, 77 Fed. Reg. at 48,760; *see, e.g., Petroleum Geo-Servs. Inc. v. WesternGeco LLC*, Case IPR2014-00687, slip op. at 16 (PTAB Dec. 15, 2014) (Paper 33) (holding petitioner and non-party's shared interest in invalidating patent at issue, “collaborat[ion] together, and invo[cation of the] common interest privilege with respect to sharing potentially invalidating prior art references” was insufficient to render non-party a real party in interest).

Beyond an arm's length exchange of prior art, IBM and the government have not collaborated in any way on the preparation of this petition. Nor has IBM funded this petition. The filing fees for this petition have been paid from the deposit account of the Department of Homeland Security, which is funded from agency appropriations (which, in turn, of course, originated from taxpayers). No draft or final version of this petition has been exchanged with IBM at any stage. Simply put, the government has no control over IBM, and IBM has exercised no control over the government in any part of the civil action or this proceeding. *Cf. BAE Sys. Info. v. Cheetah Omni, LLC*, IPR2013-00175, Slip. Op. at 5-6 (Paper 15) (PTAB July 3, 2013) (holding that the contractual relationship between the government and its contractor did not constitute a “privy” relationship that would preclude the

contractor from challenging a patent in an Inter Partes Review Proceeding in which the government did not participate).

B. Related Matters (37 C.F.R. § 42.8(b)(2))

The '221 Patent is currently the subject of litigation against the United States of America in the Court of Federal Claims, captioned *Cellcast Techs. et al. v. United States* (filed November 2, 2015).

Four other patents have been asserted in the same litigation: U.S. Patent Nos. 7,693,938 (“the ‘938 Patent”), 8,103,719 (“the ‘719 Patent”), 8,438,212 (“the ‘212 Patent”), and 9,136,954 (“the ‘954 Patent”). Concurrently with this petition, the United States has also filed IPR petitions against the ‘938, ‘719, ‘212, and ‘954 Patents.

C. Lead and Backup Counsel (37 C.F.R. § 42.8(b)(3))

Lead Counsel	First Back-up Counsel
<p>David M. Ruddy (Reg. No. 53,945) david.ruddy@usdoj.gov <u>Postal Delivery Address</u> Civil Division, Department of Justice 1100 L Street NW, RM 11130 Washington, DC 20530 (use zipcode 20005 for overnight service) T: (202) 353-0517; F:(202) 307-0345</p>	<p>Nathan Grebasch (Reg. No. 48600) Nathan.Grebasch@hq.dhs.gov <u>Postal Delivery Address</u> 245 Murray Lane, Mail Stop 0205 Washington, DC 20528 T: (202) 254-6067</p>
Back-up Counsel	Back-up Counsel
<p>Nathan Cristler (Reg. No. 61736) Nathan.Cristler@fema.dhs.gov <u>Postal Delivery Address</u> Federal Emergency Management Agency, Office of Chief Counsel 500 C Street SW, 8NE Washington, DC 20472 T: (202) 212-1130</p>	<p>Trenton Roche (Reg. No. 61164) Trenton.Roche@hq.dhs.gov <u>Postal Delivery Address</u> 245 Murray Lane, Mail Stop 0205 Washington, DC 20528 T: (202) 254-6067</p>

Back-up Counsel	Back-up Counsel
Lavanya Ratnam (Reg. No. 38277) Lavanya.Ratnam@hq.dhs.gov <u>Postal Delivery Address</u> 245 Murray Lane, Mail Stop 0205 Washington, DC 20528 T: (202) 254-6161	John Fargo (Reg. No. 29,533) john.fargo@usdoj.gov <u>Postal Delivery Address</u> Civil Division, Department of Justice 1100 L Street NW, RM 11116 Washington, DC 20530 T: (202) 514-7223; F:(202) 307-0345

D. Service Information (37 C.F.R. § 42.8(b)(4))

Service information is provided in the designation of lead and back-up counsel above.

III. FEES (37 C.F.R. § 42.103)

The undersigned authorizes the Office to charge all necessary fees to Deposit Account No. 504378 for the fees set forth in 37 C.F.R. § 42.15(a) for this Petition as well as any additional fees that might be due.

IV. REQUIREMENTS FOR INTER PARTES REVIEW UNDER 37 C.F.R. § 42.104

A. Grounds for Standing (37 C.F.R. § 42.104(a))

Pursuant to 37 C.F.R. § 42.104(a), Petitioner certifies that the ‘221 Patent is available for inter partes review and Petitioner is not barred or estopped from

requesting an inter partes review challenging the '221 Patent on the grounds identified in the present petition.

B. Citation of Prior Art

Exhibit	Description	Publication or Filing Date	Availability as Prior Art
Ex. 1013	D. Gunglegard, "Automotive Telematics Services based on Cell Broadcast"	Published at least as early as October 27, 2003 (<i>see</i> Ex. 1021)	35 U.S.C. § 102(a)
Ex. 1014	U.S. Patent Application Publ. No. 2002/0184346 A1 to Mani	Filed May 31, 2001; Published Dec. 5, 2002	35 U.S.C. § 102(a), (b), (e)
Ex. 1015	U.S. Patent Application Publ. No. 2002/0188725 A1 to Mani	Filed May 31, 2001; Published Dec. 12, 2002	35 U.S.C. § 102(a), (b), (e)
Ex. 1017	U.S. Patent Application Publ. No. 2002/0103892 A1 to Rieger	Filed Dec. 26, 2001; Published Aug. 1, 2002	35 U.S.C. § 102(a), (b), (e)
Ex. 1018	U.S. Patent No. 6,816,878 to Zimmers	Filed Feb. 11, 2000;	35 U.S.C. § 102(a), (e)

C. Claims and Statutory Grounds (37 C.F.R. §§ 42.104(b)(1)–(2))

The relief requested by Petitioner is that Claim 19 of the '221 Patent be found unpatentable and cancelled on the following grounds:

Ground	Claims	Basis
I	19	Unpatentable under 35 U.S.C. § 103 over Gundlegård Thesis (Ex. 1013) in view of the 3GPP Standard (Ex. 1019), Sandhu (Ex. 1020), and Rieger (Ex. 1017) in view of Zimmers (Ex. 1018).

Ground	Claims	Basis
II	19	Unpatentable under 35 U.S.C. § 103 over Mani (Ex. 1014) in view of the 3GPP Standard (Ex. 1019), Sandhu (Ex. 1020), and Rieger (Ex. 1017) in view of Zimmers (Ex. 1018).

D. Person of Ordinary Skill in the Art

As explained by Randall Snyder:

a person of ordinary skill in the art relevant to the subject matter of the ‘954 Patent (Ex. 1001) at the time of the invention would have a computer science, engineering, physics, mathematics or other technical degree at the undergraduate level. In addition, I would expect this individual to have at least three to five years of practical cellular network and protocol design and software development experience, along with an understanding of cellular network architecture, standardized protocol specifications and text messaging technologies, all of which was very-well understood by the early 1990s|

Ex. 1011, at ¶ 28.

E. Claim Construction (37 C.F.R. § 42.104(b)(3))

A claim subject to IPR is given its “broadest reasonable construction in light of the specification of the patent in which it appears.” 37 C.F.R. §42.100(b).

1. “broadcast”

Petitioner sets forth and adopts the following construction for the term “broadcast,” used in Claim 19 of the ’221 Patent: “to transmit data for purposes of wide dissemination over a communications network including, but not limited to, cellular carriers, digital private radio systems, private radio systems, internet, wireline telecommunications, satellite, and CATV systems.”

This construction comes directly from the specification, which states “[i]n most cases, the message is transmitted to every known operator offering coverage of the area and may include mobile carriers, digital private radio systems operators, private radio system operators, internet service providers, wireline telecommunication service providers, satellite service providers, CATV operators, etc..” Ex. 1001, 12:49-54. The breadth of transmission means are highlighted in other passages. For example, claims 3 and 5 list a plethora of public and private networks contemplated by the ’221 patent. Ex. 1001, at 26:23-29, 42-48. Indeed, nothing in the specification appears to require electronic communication thereby suggesting the systems and methods could be implemented by hand. Accordingly, a person of ordinary skill in the art would understand the term “broadcast” as used in the claims of the ’221 patent and in light of the specification to mean “to transmit data for purposes of wide dissemination over a communications network including, but not limited to, cellular carriers, digital private radio systems, private radio systems, internet, wireline telecommunications, satellite, and CATV systems.” *See also* Ex. 1011 (Snyder Report), at ¶ 78.

F. Unpatentability of the Construed Claims (37 C.F.R. § 42.104(b)(4))

An explanation of why Claim 19 of the ’221 Patent is unpatentable under the statutory grounds identified above is provided in Section VI, below.

G. Supporting Evidence (37 C.F.R. § 42.104(b)(5))

The exhibit numbers of the supporting evidence relied upon to support the challenge and the relevance of the evidence to the challenge raised, including identifying specific portions of the evidence that support the challenge, are provided below in the form of explanatory text and claim charts. An Exhibit List with the exhibit numbers and a brief description of each exhibit is set forth above.

V. SUMMARY OF THE '221 PATENT

A. Overview of the '221 Patent

The '221 Patent (Ex. 1001), entitled “Message Broadcasting Admission Control System and Method,” issued on April 6, 2010, from U.S. Patent Application No. 11/602,461 (“the '461 Application”). The '221 Patent claims priority under 35 U.S.C. § 119(e) to provisional application No. 60/544,739, filed February 13, 2004 (“the '739 provisional application”).

1. The claim at issue: Claim 19

The claim at issue in this Petition, Claim 19, is directed to a method for delivering broadcast messages. Claim 19 is an independent method claim. The text of the claim is reproduced in the charts below.

2. The alleged invention of the '221 Patent

The '221 patent describes itself as generally directed to “message broadcast systems and in particular location-specific message broadcasting aggregator and gateways.” Ex. 1001, at 1:20-23. The claims are drafted with substantial excess verbiage. Although wordy, none of the claims at issue in this petition specifically recite any particular hardware or software component in delineating the boundaries of the claims. Indeed, the specification repeatedly makes clear that the systems and methods can be implemented on any generic computer. *See, e.g.*, Ex. 1001, at 17:5-6 (“It may be implemented in hardware or software . . . This may be implemented in any possible arrangement including a table, chart, or map.”); *id.* at 18:34-37 (“The Broadcast Agent interacts with the PLBS-SB over a web page, (via a Web Portal); loading of special client software is an [sic] unnecessary. Almost any computer can use PLBS-SB without any modification at all.”); *id.* at 18:52-53 (“may be utilized using any existing or future hardware and/or software platform”). As reflected below, the claims at issue are broadly, albeit awkwardly, drafted without regard to any specific hardware such that they represent nothing more than a routine and predictable combination of well-known elements.

B. Prosecution History Summary of the '221 Patent

The '221 Patent was issued from U.S. Patent Application No. 13/311,448 which was filed on December 5, 2011.

On April 24, 2012, the examiner rejected all pending claims on double patenting and obviousness grounds. Ex. 1009, pp. 140-160. The examiner's double patenting rejections were based on either U.S. Patent No. 8,073,903 ("the '903 Patent"), or U.S. Patent No. 7,752,259 ("the '259 Patent). Ex. 1009, pp. 142-145. The remaining claims were rejected on double patenting grounds based on the '903 Patent or the '259 Patent in view of the following additional references: Atkin (U.S. Publication No. 2004/0192258) and Vella (U.S. Publication No. 2004/0103158 to Vella). Ex. 1009, pp. 144-146.

In the same office action, the examiner also rejected all pending claims on separate obviousness grounds. The examiner stated that pending claims 1-8, 12, 15-17, and 19 were obvious over Vella in view of Allport (U.S. Patent No. 6,480,578). Ex. 1009, pp. 146-153. The examiner rejected pending claims 9-11 as obvious over Vella, in view of Allport and Kolsrud (U.S. Publication No. 2004/0203562). Ex. 1009, pp. 153-155. The examiner rejected pending claims 13-14 as obvious over Vella, in view of Allport and Atkin. Ex. 1009, pp. 155-157. The examiner rejected pending claims 18 and 20 as obvious over Vella, in view of Allport and Zimmers (U.S. Publication No. 2005/0013417). Ex. 1009, pp. 157-159.

On October 24, 2012, the applicant responded to the office action. First, the applicant submitted terminal disclaimers over the '903 Patent and the '259 Patent. Ex. 1009, p. 214 ('259 Patent disclaimer), p. 219 ('903 Patent disclaimer). Second,

the applicant amended the claims; in particular, the applicant amended claims 1 and 19 to include the term “geographically defined” in the claims. Ex. 1009, pp. 209, 213. Third, the applicant responded to the examiner’s obviousness rejections by distinguishing the claims from the cited prior art.

On December 11, 2012, the PTO issued a notice of allowance. Ex. 1009, pp. 230-236.

VI. THERE IS A REASONABLE LIKELIHOOD THAT PETITIONER WILL PREVAIL WITH RESPECT TO AT LEAST ONE CLAIM OF THE ’221 PATENT

According to the pre-AIA version of 35 U.S.C. § 103(a), “[a] patent may not be obtained . . . if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious to a [POSITA] to which said subject matter pertains.” In this case, the subject matter of Claim 19 of the ’221 Patent is disclosed, taught, and rendered obvious by the prior art as explained below. As set forth below, the references in Ground I together render obvious claim 19 pursuant to 35 U.S.C. § 103, and the references in Ground II together render obvious claim 19 pursuant to 35 U.S.C. § 103. These Grounds thus provide a reasonable likelihood that the Petitioner will prevail on at least one claim. *See* 35 U.S.C. § 314(a).

A. The state of the art on February 12, 2004: broadcasting messages to a geographic region was widely known and well as access control systems for assigning user roles and privileges

The declaration of Randall Snyder (Ex. 1011) goes into great detail explaining the state of the art on and before February 12, 2004. As set forth in the declaration, it was well known on and before February 12, 2004, to implement a cell broadcast messaging application. As one example, Mr. Snyder points to a telecommunications standard in existence more than one-year before February 12, 2004 and writes that “[t]he 3GPP Standard details the underlying technology required to implement a cell broadcast messaging application. This standard describes and depicts several example applications of the technology including news, sports, weather, finance, etc.” Ex. 1011, at ¶ 53 (relying on Ex. 1019). In addition, Mr. Snyder points to a report from the government of Finland “describing and depicting how cell broadcast messaging technology could be used for a public warning and alarm system.” *Id.* at ¶ 54 (relying on Ex. 1024).

Mr. Snyder then explains that the state of telecommunications applications on and before February 12, 2004, were “implemented with comprehensive functions to record and log the details of transmissions sent from or received by the application.” Ex. 1011, at ¶ 61-63 (relying on Ex. 1013). The use of cell broadcast applications to transmit messages to defined target areas was also well-known, including implementing the application using standard database as a lookup table to associate

cellular coverage with other established geographic boundaries. *See id.* at ¶ 67 (describing examples of lookup tables).

Mr. Snyder then explains that principles of system access control, user roles, and permissions were also very well-known. *See id.* at ¶ 69 (“determining what users are authorized to do based on who they are, was a well-known security technique at least as far back as 1990.”). Mr. Snyder points to a UNIX user manual and an IEEE article, both published nearly a decade or more before the pertinent prior art date. *See* Ex. 1011, at ¶ 69-70 (relying on Ex. 1020 and 1026).

B. Ground I: Claim 19 of the '221 Patent is obvious over Gundlegård Thesis (Ex. 1013) in view of the 3GPP Standard (Ex. 1019), Sandhu (Ex. 1020), and Rieger (Ex. 1017) in view of Zimmers (Ex. 1018).

Gundlegård (Ex. 1013) is a master’s program thesis from the Linköping University in Sweden. As documented by the declaration of Amelia Nuss (Ex. 1021), the thesis was published at least as early as October 27, 2003. Ex. 1021. Gundlegård discloses a cell broadcast system for a number of applications intended for delivering targeted messages to a specific geographic area, including for local warnings (Ex. 1013 at Section 6.5) and weather forecasts and warnings (Ex. 1013 at Section 6.6).

The Office Patent Trial Practice Guide, explains that “[w]here appropriate, claim charts can streamline the process of identifying key features of a claim and comparing those features with specific evidence.” 77 Fed. Reg. 48,756, 48,764

(Aug. 14, 2012). Petitioner submits that Gundlegård in view of 3GPP Standard, Sandhu, and Rieger in view of Zimmers teaches each of the features of the subject claims as set forth in the charts below, which are included in the expert report of Randall Snyder. Ex.1011.

Claim 19	Gundlegård in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers
<p>19[pre]. A method of public service broadcast messaging to a broadcast target area, the method comprising:</p>	<p>Gundlegård discloses a method of public service broadcast messaging to a broadcast target area.</p> <p>Ex. 1013, at 3 ¶ 6 (“Cell Broadcast is a technique within GSM and UMTS to broadcast text messages to one or more cells in the network.”).</p> <p>Ex. 1013, at 5 ¶ 6 (“In order to analyse the effects of an incident warning system based on Cell Broadcast a study of relevant tests and literature within incident warning systems and in-car behaviour has been made.”) (emphasis added).</p> <p>Ex. 1013, at 6 ¶ 6 (“<i>Chapter six</i> contains a short description of the services outside automotive telematics that can be offered with Cell Broadcast.”).</p> <p>Ex. 1013, at 34 ¶ 7 (“Cell Broadcast is also well suited for local warnings outside the scope of road traffic.” Ex. 1013, at 34 ¶ 7.). (emphasis added).</p> <p>The 3GPP Standard, Rieger and Zimmers also disclose a method of public service broadcast messaging to a broadcast target area. Ex. 1019, at Section 2 (“The CBS service is analogous to the Teletex service offered on television, in that like Teletex, it permits a number of unacknowledged general CBS messages to be broadcast to all receivers within a particular region. CBS messages are broadcast to defined geographical areas known as cell broadcast areas. These areas may comprise of one or more cells, or may comprise the entire PLMN. Individual CBS messages will be assigned their own</p>

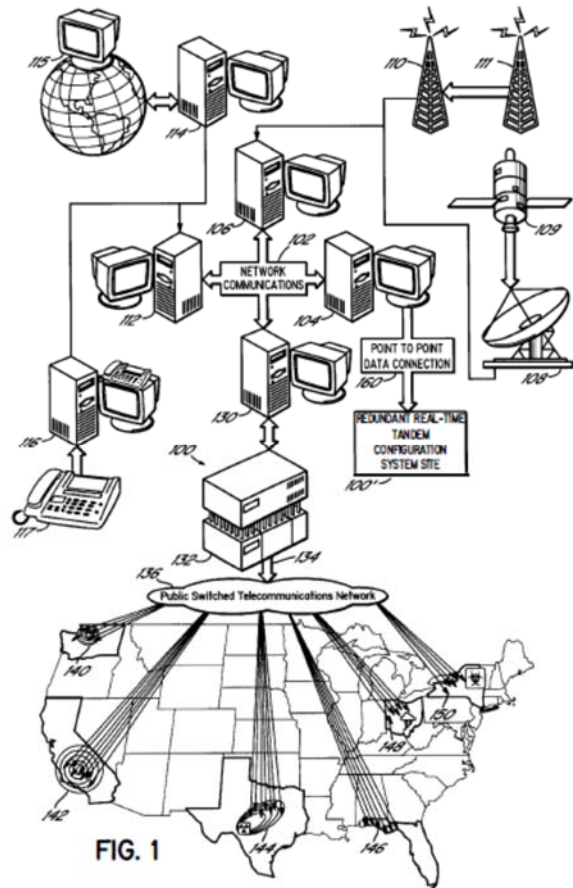
Claim 19	Gundlegård in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers
	<p>geographical coverage areas by mutual agreement between the information provider and the PLMN operator. CBS messages may originate from a number of Cell Broadcast Entities (CBEs), which are connected to the Cell Broadcast Centre. CBS messages are then sent from the CBC to the cells, in accordance with the CBS's coverage requirements.”) (emphases added).</p> <p>Ex. 1017, Abstract (“A communications system to post arbitrary information to any geographical region simply by outlining the region on a map in the system’s user interface and attaching the information to the outlined region is provided.”).</p> <p>Ex. 1018, at 1:5-7 (“The present invention relates to the delivery of emergency information to persons needing to be notified of such information.”).</p> <p>Ex. 1018, at 4:5-15 (“It is ... important that the alert notification system have the ability to pinpoint, calculate and define dynamically all recipients with respect to their notification requirements then systematically notify those individuals (and only those individuals) within those defined geographic locations. The system must provide the notification quickly and accurately, with the ability to track the progress of the notification process and provide scenario resolution status until the notification scenario is completed or until the alert has expired.”)</p>
<p>19[a]. receiving over an input interface a broadcast request including a broadcast agent identification, a geographically defined broadcast target area, and a broadcast message from one of a plurality of coupled</p>	<p>Gundlegård discloses receiving over an input interface a broadcast request from one of a plurality of coupled broadcast agent message origination systems.</p> <p>Ex. 1013, at 7 ¶ 3 (“The content provider has an interface to the Cell Broadcast Entity (CBE) that varies depending on application.”) (emphasis added).</p> <p>Ex. 1013, at 7:</p>

Claim 19	Gundlegård in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers
broadcast agent message origination systems;	<div data-bbox="597 296 1442 590" data-label="Diagram"> <pre> graph LR CP[Content Provider] --- CBE1[CBE] CBE2[CBE] --- CBC[CBC] CBC --- BSC1[BSC/RNC] CBC --- BSC2[BSC/RNC] BSC1 --- BTS1[BTS] BSC2 --- BTS2[BTS] BTS1 --- MT1[MT] BTS1 --- MT2[MT] BTS1 --- MT3[MT] BTS2 --- MT4[MT] BTS2 --- MT5[MT] BTS2 --- MT6[MT] MT1 --- EC[End customer] MT2 --- EC MT3 --- EC MT4 --- EC MT5 --- EC MT6 --- EC </pre> <p>Figure 3. Overview of the nodes used in Cell Broadcast.</p> </div> <p data-bbox="586 615 1435 741">Ex. 1013, at 28 ¶ 1 (“A developed automotive telematics system based on Cell Broadcast can have an information flow as shown in Figure 16.”).</p> <p data-bbox="586 762 894 804">Ex. 1013, Figure 16:</p> <div data-bbox="597 821 1442 1461" data-label="Diagram"> <pre> graph LR TRISS[TRISS] --> CBS((Cell Broadcast System)) FCD[FCD] --> CBS GSM[Information from GSM-network] --> CBS MR[Manual report] --> CBS IF[Integrated functions] --> CBS CBS --> TM[Text message] CBS --> GSM_mod[GSM-module connected to integrated telematic system] CBS --> MM[Multimedia message] </pre> </div> <p data-bbox="586 1486 1435 1745">Ex. 1013, at 8 ¶ 2 (“The CBE is a client from where it is possible to send Cell Broadcast messages. The client is usually implemented in a PC and connected to the CBC via Internet. The appearance of the CBE interface is fully dependent on the application.”) (emphasis added).</p> <p data-bbox="586 1766 1386 1843">Gundlegård also discloses that the received broadcast request includes a broadcast agent identification, a</p>

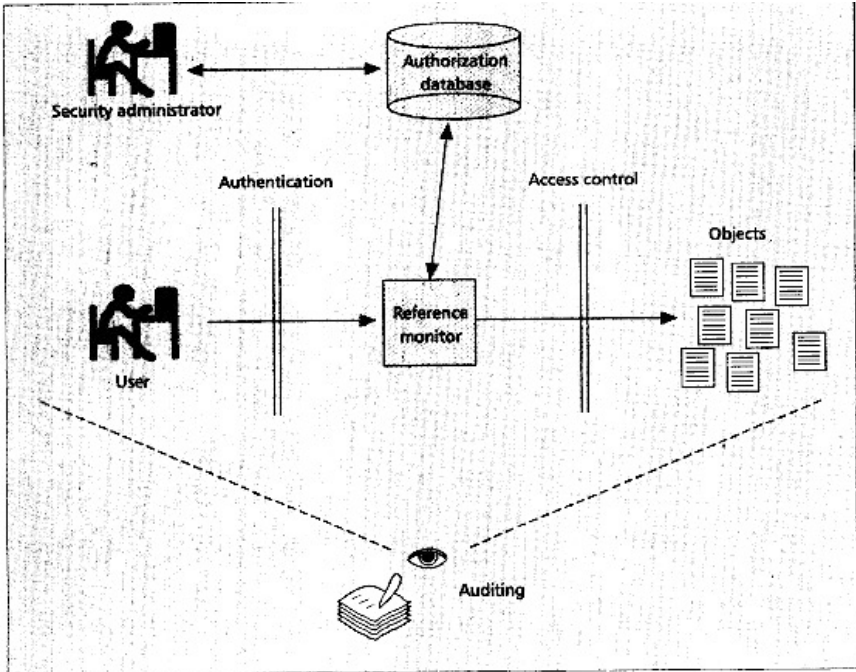
Claim 19	Gundlegård in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers												
	<p>geographically defined broadcast target area, and a broadcast message.</p> <p>Ex. 1013, at 8 ¶ 2 (“Some applications will demand a specially developed interface to be implemented. Many applications can, however, be handled with a map interface where the broadcasting area can be defined and inputs for duration, frequency and message are available.”) (emphases added).</p> <p>Ex. 1013, at 7 ¶ 2 (“You can choose to send a Cell Broadcast message to the whole network or specify the cells you want to send it to. The message is sent to all mobile terminals in idle mode in the specified area.”).</p> <p>Ex. 1013, Table 3:</p> <table data-bbox="634 940 1403 1276"> <tr> <th>Octet(s)</th><th>Field</th></tr> <tr> <td>1</td><td>Message type</td></tr> <tr> <td>2-3</td><td>Message ID</td></tr> <tr> <td>4-5</td><td>Serial number</td></tr> <tr> <td>6</td><td>Data coding scheme</td></tr> <tr> <td>7-1252</td><td>CB data</td></tr> </table> <p><i>Table 3. Cell Broadcast message format in UMTS.⁵</i></p> <p>Ex. 1013, at 11 ¶ 6 (“For a Cell Broadcast message <i>Message ID</i>, <i>Serial number</i> and <i>Data coding scheme</i> are the same as in GSM (see section 2.7.1). The CB data is the content of the message.”) (emphasis added).</p> <p>Ex. 1013, at 10 ¶ 5 (“The Message Identifier defines the source (e.g. “Restaurant Jade Garden”) The serial number identifies a particular Cell Broadcast message with the same message identifier, the geographical scope of the message (cell wide, location area wide, or PLMN wide) and the display mode.”) (emphasis added).</p>	Octet(s)	Field	1	Message type	2-3	Message ID	4-5	Serial number	6	Data coding scheme	7-1252	CB data
Octet(s)	Field												
1	Message type												
2-3	Message ID												
4-5	Serial number												
6	Data coding scheme												
7-1252	CB data												


<p>Claim 19</p>	<p>Gundlegård in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers</p>
	<p>The 3GPP Standard discloses a broadcast request including a broadcast agent identification, a geographically defined broadcast target area, and a broadcast message.</p> <p>For example, Ex. 1019, at Sections 9.3-9.4 describe message parameters including a broadcast message originator identifier (<i>e.g.</i>, the message identifier) and a broadcast target area (<i>e.g.</i>, a cell-list or as part of the serial number parameter).</p> <p>Rieger also discloses receiving over an input interface a broadcast request from one of a plurality of coupled broadcast agent message origination systems.</p> <p>Ex. 1017, Figure 1:</p> <p style="text-align: center;">FIG. 1</p> <p>Ex. 1017, at [0073] (“A user interface 117 is also included with the communication server 111. The user interface 117 processes user transactions, and</p>

Claim 19	Gundlegård in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers
	<p>dynamically composes HTML responses containing maps and other graphical elements (such as icons, photos, and the like), drawing in part upon the communications server's 111 map manager 121. The user interface 117 permits users to interact with the communications system's maps via zoom, pan, and drawing primitives").</p> <p>Rieger also discloses that the received broadcast request includes a broadcast agent identification, a geographically defined broadcast target area, and a broadcast message.</p> <p>Ex. 1017, at [0003] ("[T]he target user community for a posting is defined in terms of geographical coordinates, e.g., by a bounded region on a map.").</p> <p>Ex. 1017, at [0077] ("Each posting is comprised of an identification tag that describes who has posted it, when it was posted, what its posting category is, and other such factual information about its origin.").</p> <p>Ex. 1017, at [0078] ("Postings are further defined by an information component, which is the content of the posting.").</p> <p>Ex. 1017, at [0079] ("Each posting is also provided with a 'broadcast' descriptor, which identifies the posting's geographical target region(s).").</p> <p>Zimmers also discloses receiving over an input interface a broadcast request from one of a plurality of coupled broadcast agent message origination systems.</p> <p>Ex. 1018 at 11:12-18 ("[A]lert conditions may also be identified by individuals Authorized individuals may include") (emphases added).</p> <p>Ex. 1018, at Figure 1:</p>

Claim 19	Gundlegård in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers
	 <p data-bbox="812 1134 893 1176">FIG. 1</p> <p data-bbox="584 1218 1429 1354">Ex. 1018, at 19:21-24 (“[A] user connects to a web server 114, typically using a hypertext transfer protocol (HTTP) application.”).</p> <p data-bbox="584 1365 1429 1543">Zimmers also discloses that the received broadcast request includes a broadcast agent identification, a geographically defined broadcast target area, and a broadcast message.</p> <p data-bbox="584 1554 1429 1890">Ex. 1018, at 19:24-44 (“[W]eb server 114 receives an Internet protocol (IP) address for the user from the Internet connection. ... [T]he user is prompted to enter a login identifier and password via a hypertext markup language (HTML) form, otherwise known as a world wide web-based form. ... If the connection is allowed ... web server 114 determines the notification text that the user is permitted to create. ... [T]he user is prompted</p>

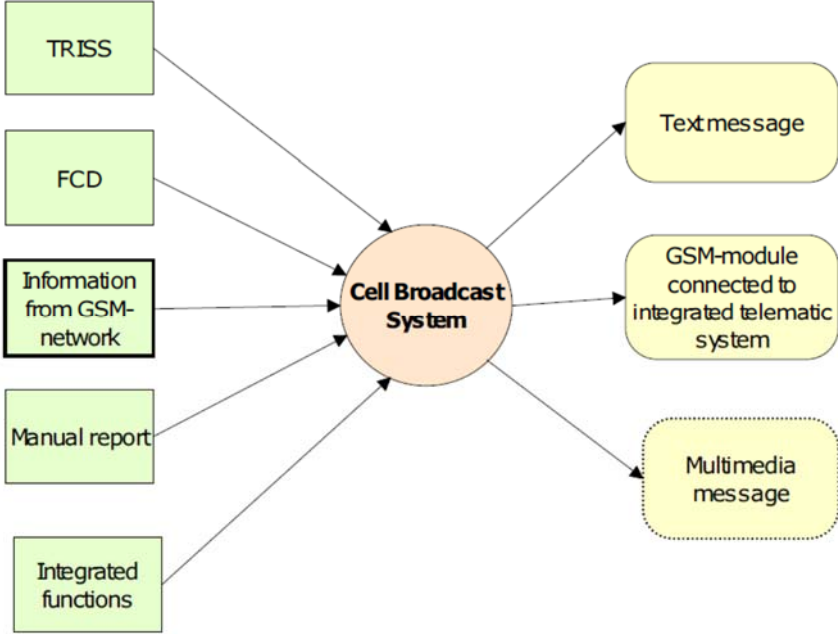
Claim 19	Gundlegård in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers
	again, using the web based form, for a notification type. . . . [A]dditional web based forms are used to prompt the user for relevant information for the notification, such as geographic information”).
<p>19[b]. storing a geographically defined broadcast message jurisdiction for a broadcasting agent;</p>	<p>Gundlegård does not expressly disclose this element.</p> <p>Rieger discloses the complete “storing” element.</p> <p>Ex. 1017, at [0081] (“Administrators of the communications system 100 can restrict the nature of postings created by any particular user by defining geographic regions into which the user is either authorized or unauthorized to post. Authorized regions can be assigned optional passwords and posting category restrictions that further narrow the user’s posting privileges in those regions. These controls would, for example, permit system administrators to grant specific privileges to a regional authority to create postings of particular categories, e.g., Governmental/Traffic, Governmental/Weather, to particular regions, while excluding all other users from posting those categories to the regions.”). Ex. 1017, at [0082] (“The communications server 111 is also comprised of a user accounts manager 125. The user accounts manager 125 stores and retrieves user account information on demand from the user interface 117.”).</p> <p>Ex. 1017, at [0083] (“In an embodiment, user account information is maintained in a database.”).</p> <p>Ex. 1017, at [0184-85] (“3.9.1 User Account Types ... In an embodiment, communications system 200 classifies users by account types, which are defined by subscription packages. Each account type grants or denies access to various system features and resources, defines usage level limits. . . . Posting region size and distance, and ping regions and weekly ping hit counts are examples</p>

Claim 19	Gundlegård in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers
	<p>of system usage limits that are imposed by the various account types.”) (emphasis added).</p> <p>Sandhu discloses storing authorization settings in a database as part of any common access control system.</p> <p>Ex. 1020, at 40 (“Access control is concerned with limiting the activity of legitimate users. It is enforced by a reference monitor which mediates every attempted access by a user (or program executing on behalf of that user) to objects in the system. The reference monitor consults an authorization database in order to determine if the user attempting to do an operation is actually authorized to perform that operation.”) (emphasis added).</p> <p>Ex. 1020, Figure 1:</p>  <p>The diagram illustrates an access control system. At the top left, a 'Security administrator' (represented by a person at a desk) is connected to an 'Authorization database' (represented by a cylinder) via a double-headed arrow. Below the administrator, a 'User' (represented by a person at a desk) is shown. An arrow labeled 'Authentication' points from the User to a 'Reference monitor' (represented by a rectangle). Another arrow labeled 'Access control' points from the Reference monitor to a group of 'Objects' (represented by several document icons). The Reference monitor is also connected to the Authorization database. At the bottom, an 'Auditing' component (represented by an eye icon over a stack of papers) is connected to the User, Reference monitor, and Objects by dashed lines.</p> <p>Ex. 1020, at 41-42 (“The subject-object distinction is basic to access control. Subjects initiate actions or operations on objects. These actions are permitted or denied in accord with the authorizations established in the system.”) (emphasis added).</p>

Claim 19	Gundlegård in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers
<p>19[c]. verifying an authority of the broadcast agent identification including an authority of the originating broadcast agent to send the broadcast message to the broadcast target area by comparing the stored geographically defined broadcast message jurisdiction for the originating broadcast agent with the broadcast target area associated with the broadcast message in the broadcast request; and</p>	<p>Gundlegård does not expressly disclose this element completely. But it does teach the importance of a verification step by disclosing a network that handles “authentication” and acknowledges that messages may be successful or unsuccessful.</p> <p>Ex. 1013, at 2 ¶ 9 (“The GSM and UMTS networks consist of a core network (CN) and a base system. The core network includes nodes that handle e.g. authentication, subscriber information, and switching.”) (emphasis added).</p> <p>Ex. 1013, at 3 ¶ 5 (“The support system contains the Cell Broadcast Centre (CBC) and Cell Broadcast Entities (CBEs) for every sender of Cell Broadcast messages.”) (emphasis added).</p> <p>Ex. 1013, at 9 ¶ 3 (“It [BSC/RNC] is also responsible for scheduling the messages on the Cell Broadcast Channel (CBCH) and giving feedback to the CBC about successful or unsuccessful commands.”) (emphasis added).</p> <p>Ex. 1013, Figure 7 (annotation added):</p>  <p>Figure 7. Information flow for Write-replace command in GSM Cell Broadcast system.⁵</p>

Claim 19	Gundlegård in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers
	<p>The 3GPP Standard also discloses the importance of a verification step by disclosing a standard that requires message validation.</p> <p>Ex. 1019 at Section 9.3.16 (listing error messages that result from invalid broadcast message records).</p> <p>Rieger discloses this element in its entirety.</p> <p>Ex. 1017, at [0081] (“Administrators of the communications system 100 can restrict the nature of postings created by any particular user by defining geographic regions into which the user is either authorized or unauthorized to post. Authorized regions can be assigned optional passwords and posting category restrictions that further narrow the user’s posting privileges in those regions. These controls would, for example, permit system administrators to grant specific privileges to a regional authority to create postings of particular categories, e.g., Governmental/Traffic, Governmental/Weather, to particular regions, while excluding all other users from posting those categories to the regions.”).</p> <p>Zimmers provides an example of how limiting the geographical scope of weather alerts can reduce the “cry wolf” syndrome resulting from overbroad emergency broadcasts. <i>See</i> Ex. 1018, at 2:49-63.</p> <p>Zimmers also discloses two stages: authentication followed by verifying a broadcast message request as a function of the authority of the originating broadcast agent to send the broadcast message to the broadcast target based on certain parameters in the broadcast message request.</p> <p>Ex. 1018 at 19:35-40 (“if the connection is allowed, then in step 492 web server 114 determines the notification text that the user is permitted to create. . . . The provided notification type is then evaluated in step 496 to</p>

Claim 19	Gundlegård in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers
	<p>determine if it is a type allowed by the server for the user.”) (emphases added).</p> <p>And, Sandhu discloses that a basic principle of any access control system is that stored information for an originating user is compared with information associated with the user’s request.</p> <p>Ex. 1020 at 44 (“Discretionary protection policies govern the access of users to the information on the basis of the user’s identity and authorizations (or rules) that specify, for each user (or group of users) and each object in the system, the access modes (e.g., read, write, or execute) the user is allowed on the object. Each request of a user to access an object is checked against the specified authorizations. If there exists an authorization stating that the user can access the object in the specific mode, the access is granted, otherwise it is denied.”) (emphasis added).</p>
<p>19[d]. transmitting the broadcast message over an output interface to one or more coupled broadcast message networks providing broadcast message alerting service to at least a portion of the broadcast target area.</p>	<p>Gundlegård discloses transmitting the broadcast message over an output interface to one or more coupled broadcast message networks providing broadcast message alerting service to at least a portion of the broadcast target area.</p> <p>Ex. 1013, at 8 ¶ 2 (“The CBE is a client from where it is possible to send Cell Broadcast messages.”) (emphasis added).</p> <p>Ex. 1013, Figure 16:</p>

Claim 19	Gundlegård in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers
	 <p data-bbox="586 951 1422 1077">Ex. 1013 at 34 ¶ 8 (“The fact that messages can be sent to the whole country or just to one cell is also important for these kinds of warnings.”) (emphasis added).</p> <p data-bbox="586 1098 1422 1266">Ex. 1013 at 16 ¶ 1 (“The BSC is responsible for queuing, repetition and transmission of the messages, but the BTS can indicate overflow or underflow on the Cell Broadcast channel.”) (emphasis added).</p> <p data-bbox="586 1287 1295 1329">The 3GPP Standard also discloses this element:</p> <p data-bbox="586 1350 1438 1864">Ex. 1019 at 7 ¶ 10 (“CBS messages are broadcast to defined geographical areas known as cell broadcast areas. These areas may comprise of one or more cells, or may comprise the entire PLMN. Individual CBS messages will be assigned their own geographical coverage areas by mutual agreement between the information provider and the PLMN operator. CBS messages may originate from a number of Cell Broadcast Entities (CBEs), which are connected to the Cell Broadcast Centre. CBS messages are then sent from the CBC to the cells, in accordance with the CBS's coverage requirements.”) (emphasis added).</p>

1. Motivation to Combine Gundlegård with the 3GPP Standard

Gundlegård (Ex. 1013) does disclose message parameters, *see, e.g.*, Ex. 1023 (Table 3), however, Ex. 1013 does not describe in detail the specific message formatting for the use of a combined broadcast agent identification, a geographically defined broadcast target area, and a broadcast message as recited in claims 1 and 17. As explained by Randall Snyder, “Gundlegård discloses a number of potential applications, from the content provider and network provider’s points of view, of the 3GPP cell broadcast messaging standard (Ex 1019).” Ex. 1011, at ¶ 95; *see also id.* (“Gundlegård explicitly draws on the 3GPP Standard, for example, by citing it as reference number 5 in the bibliography”). Snyder explains that the very purpose of such a protocol standard is for their adoption and use in the field by ordinary artisans in order to be relied upon in day to day use as what is well-known. *See id.* at ¶ 97 (“a person of ordinary skill in the art would rely on the applicable standard specifications—that’s why they’re developed.”). Accordingly, a POSITA would be motivated to combine the 3GPP standard reflected in Ex. 1019 to implement a geographically targeted broadcast as disclosed in Gundlegård (Ex. 1013).

2. Motivation to Combine Gundlegård with Sandhu

Snyder notes that Gundlegård discloses a number of business models “based on which party would be charged for the service[.]” Ex. 1011, at ¶ 98 (citing to Ex. 1013, Section 2.10 at 13). Snyder then explains that “the problem of allocating costs

as suggested in Gundlegård would require an access, authorization and auditing scheme.” Ex. 1011, at ¶ 98. Sandhu teaches well known applications of access control, implementing user roles, which, it discloses, as preferably being coupled with auditing. *See* Ex. 1020. Snyder further explains that “auditing procedures do not just assist in ensuring security; they are required for competent commercial operations, such as billing, accounting, auditing, marketing, engineering and other reasons. To audit the system for such reasons, data must be recorded and logged such that the audit function can analyze that data.” Ex. 1011, ¶ 101. Accordingly, it would have been obvious to a POSITA to apply the teaching of Sandhu to the system of Gundlegård to “to maintain system security, facilitating billing) to solve a common problem (*e.g.*, maintaining system security and facilitating billing).” Ex. 1011, ¶ 100.

3. Motivation to Combine Gundlegård with Rieger in View of Zimmers

Claim element 1(b) recites in part: “the broadcast message management system storing a broadcast message jurisdiction authority for each broadcast agent[.]” In addition, Claim element 1(e) recites in part: “verifying the broadcast message request to provide a verified broadcast message . . . the verifying ensuring the stored broadcast message jurisdiction of the originating broadcast agent includes the broadcast target area of each broadcast message request.” Similarly, claim element 17(b) recites a “storing” of a jurisdiction authority and claim element 17(c)

provides a “verifying.” Thus, together these elements in independent claims 1 and 17 recite storing a “jurisdiction authority” of the agent as well as a check (i.e., a verification) of the preexisting stored geographic privilege or authorization parameters associated with the originating agent.

Gundlegård clearly discloses an application whereby messages are delivered to a target area. Gundlegård does not expressly disclose a storing a *geographic jurisdiction* for a broadcasting agent. Nor does Gundlegård expressly disclose a verification that specifically restricts the geographic scope of a broadcast message based on the sender’s authority. Zimmers (Ex. 1018) provides an example of how limiting the geographical scope of weather alerts can reduce the “cry wolf” syndrome resulting from overbroad emergency broadcasts. *See* Ex. 1018, at 2:49-63. Specifically, Zimmers provides that:

Perhaps the most pernicious problem is that weather broadcasts must cover a relatively large area and so many of the alert signals transmitted by those broadcasts will be irrelevant to a large percentage of the listening population. ... This results in the situation not unlike the fable of the Boy Who Cried Wolf in which citizens decide that the warnings are not normally relevant, and either ignore them or turn their NWS receiver off.

Ex. 1018, at 2:49-62. This is one of the “safety considerations” relied on by Randall Snyder in support of his opinion relying on the teaching of Zimmers. *See* Ex. 1011, at ¶ 101. Snyder further explains that there are commercial reasons to police limitations on the broadcast area of a message. *See* Ex. 1011, at ¶ 102 (“[f]rom a

commercial or financial perspective, cost recovery and commercial fees may be based on the number of messages broadcast, the broadcast area, the particular cost to connect to cellular networks to broadcast the message, etc.”). Rieger (Ex. 1017) expressly discloses a message transmission system that “teaches restricting message distribution based on two criteria: (1) the message category and (2) the applicable geographic region.” (Ex. 1011, at ¶104); *see also id.* at ¶ 103 (citing to Ex. 1017, at ¶ 81)). Thus, Snyder notes that there are obvious safety and financial benefits in implementing a system as taught by Rieger and Zimmers to “prohibit[] a user from posting messages beyond a geographic area authorized for that user.” Ex. 1011, at ¶ 105.

Thus analysis is further supported by additional content in Zimmers (Ex. 1018), wherein there are disclosed two (2) stages of security in an emergency message transmission system: namely, “(1) user authentication and (2) user privileges.” Ex. 1011, at ¶ 106 (relying on, *inter alia*, FIG. 4D of Zimmers, Ex. 1018). Thus, additional motivation to combine is generated by the aforementioned content in Zimmers. Snyder explains that “Gundlegård discloses the capability to enable charging for different users of a cell broadcast messaging system. Thus, a user who is granted privileges to broadcast a particular message type can only be charged for sending that message type if the system knows who that user is.” Ex. 1011, at ¶ 107. Accordingly, a POSITA would be motivated to combine the

geographic restriction disclosed in Rieger (Ex. 1017) with the system of Gundlegård to restrict emergency messages to their proper target as taught by Zimmers (Ex. 1018).

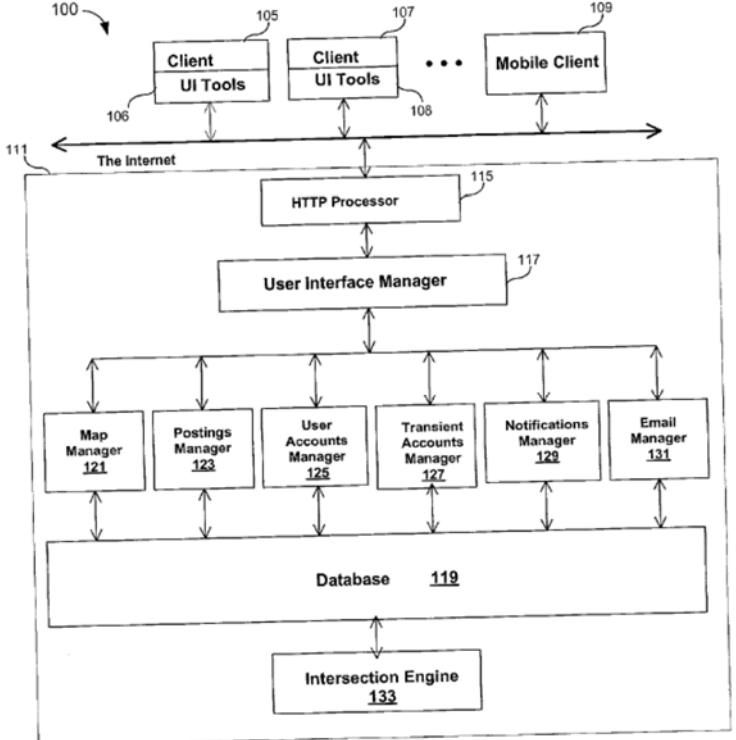
C. Ground II: Claim 19 of the '221 Patent is rendered obvious over Mani (Ex. 1014) in view of the 3GPP Standard (Ex. 1019), Sandhu (Ex. 1020), and Rieger (Ex. 1017) in view of Zimmers (Ex. 1018).

Mani (Ex. 1014) “is directed to an emergency notification and override service in a multimedia-capable next-generation network.” Ex. 1014, at ¶ 3. FIG. 5 of Mani depicts an exemplary service network including a plurality of participants capable of sending and receiving messages via the network, such as, for example, subscribers 508, an authorized agency 511, and an authorized user 513. Ex. 1014, at FIG. 5. Mani makes clear that messages are sent based upon the privilege or authorization level of the sender, and that there must be successful user verification before emergency messages are sent. Ex. 1014, at FIG. 9 (items 902 and 904). Mani also teaches that emergency messages can be sent to a specific geographic target area. Ex. 1014, at FIG. 10 (item 1004).

The Office Patent Trial Practice Guide, explains that “[w]here appropriate, claim charts can streamline the process of identifying key features of a claim and comparing those features with specific evidence.” 77 Fed. Reg. 48,756, 48,764 (Aug. 14, 2012). Petitioner submits that Mani in view of 3GPP Standard, Sandhu, and Rieger in view of Zimmers teaches each of the features of the subject claims as

set forth in the charts below, which are included in the expert report of Randall Snyder. Ex.1011.

Claim 19	Mani in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers
19[pre] . A method of public service broadcast messaging to a broadcast target area, the method comprising:	Ex. 1014, at ¶ 60 (“the present invention advantageously provides an enhanced emergency message notification service... .”); <i>See also</i> Ex. 1014, at ¶ 59 (“the emergency message may be transmitted in broadcast mode to the target serving area (step 1004).”).
19[a] . receiving over an input interface a broadcast request including a broadcast agent identification, a geographically defined broadcast target area, and a broadcast message from one of a plurality of coupled broadcast agent message origination systems;	<p>Ex. 1014, at ¶ 39 (“A multimedia node or network element 504 is operable to serve a plurality of subscribers, e.g., subscriber 508A operating a multimedia IT device 506A for originating and/or terminating calls.”).</p> <p>Broadcast request...</p> <p>Ex. 1014, at ¶ 54 (“The incoming emergency message may preferably include parametric information comprised of, for example, emergency type, magnitude of the emergency, target area to be served, geographic area information relating to the message originator (i.e., authorized entity), and the like.”); <i>See also</i> Ex. 1015 (incorporated by reference), ¶ 39 (disclosing the use of originator identification information including password and loginID information.”).</p> <p>Ex. 1019 goes into great detail describing the message parameters, including message type, message ID (for source), and geographic area. See Ex. 1019, Sections 9.3-9.4 (describing message parameters including a broadcast message originator identifier (<i>e.g.</i>, the message identifier) and a broadcast target area (<i>e.g.</i>, a cell-list or as part of the serial number parameter).</p> <p>Rieger also discloses receiving over an input interface a broadcast request from one of a plurality of coupled broadcast agent message origination systems.</p>

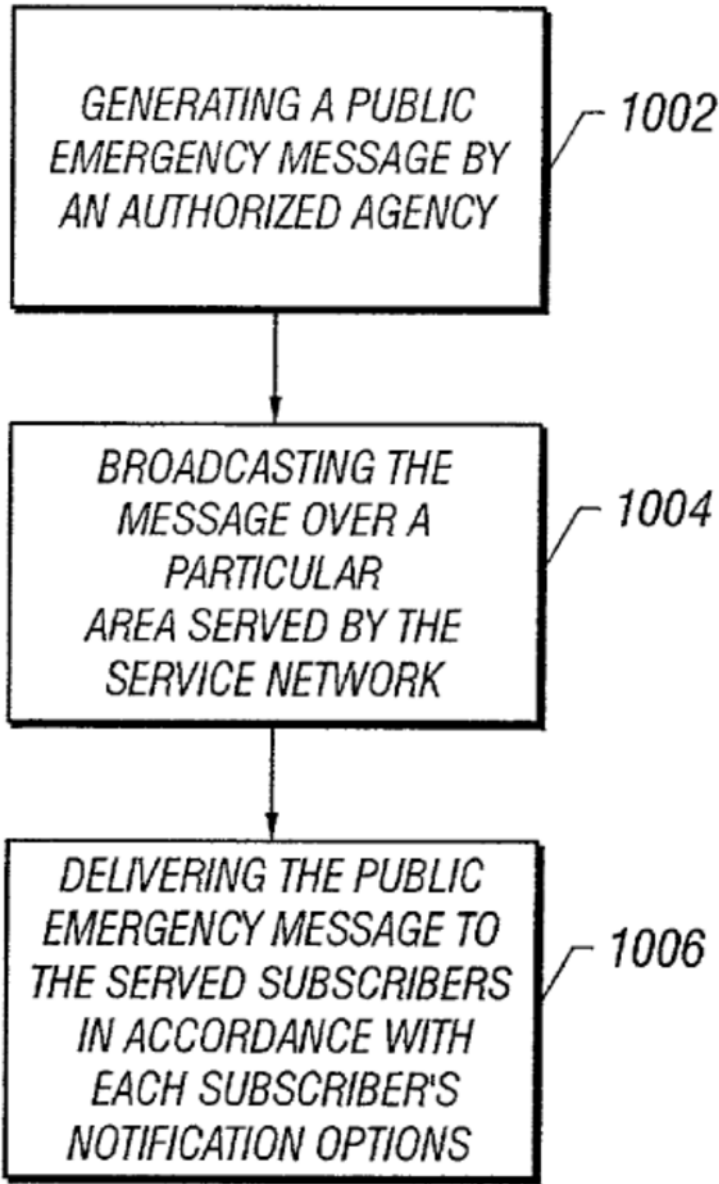
<p>Claim 19</p>	<p>Mani in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers</p>
	<p>Ex. 1017, Figure 1:</p>  <p style="text-align: center;">FIG. 1</p> <p>Ex. 1017, at [0073] (“A user interface 117 is also included with the communication server 111. The user interface 117 processes user transactions, and dynamically composes HTML responses containing maps and other graphical elements (such as icons, photos, and the like), drawing in part upon the communications server’s 111 map manager 121. The user interface 117 permits users to interact with the communications system’s maps via zoom, pan, and drawing primitives ...”).</p> <p>Rieger also discloses that the received broadcast request includes a broadcast agent identification, a geographically defined broadcast target area, and a broadcast message.</p>

Claim 19	Mani in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers
	<p>Ex. 1017, at [0003] (“[T]he target user community for a posting is defined in terms of geographical coordinates, e.g., by a bounded region on a map.”).</p> <p>Ex. 1017, at [0077] (“Each posting is comprised of an identification tag that describes who has posted it, when it was posted, what its posting category is, and other such factual information about its origin.”).</p> <p>Ex. 1017, at [0078] (“Postings are further defined by an information component, which is the content of the posting.”).</p> <p>Ex. 1017, at [0079] (“Each posting is also provided with a ‘broadcast’ descriptor, which identifies the posting’s geographical target region(s).”).</p>
<p>19[b]. storing a geographically defined broadcast message jurisdiction for a broadcasting agent;</p>	<p>Mani does not expressly disclose storing geographic jurisdiction for a broadcasting agent.</p> <p>Rieger (Ex. 1017) discloses this feature. <i>See</i> Ex. 1017, at ¶ 81 (“Administrators of the communications system 100 can restrict the nature of postings created by any particular user by defining geographic regions into which the user is either authorized or unauthorized to post. Authorized regions can be assigned optional passwords and posting category restrictions that further narrow the user’s posting privileges in those regions. These controls would, for example, permit system administrators to grant specific privileges to a regional authority to create postings of particular categories, e.g., Governmental/Traffic, Governmental/Weather, to particular regions, while excluding all other users from posting those categories to the regions.”); <i>see also</i> Ex. 1017, at ¶¶ 184-185 (explaining the use of the system for different user account types for sending messages to different jurisdictions: “Posting region size and distance are examples of system usage limits that are imposed by the various account types.”).</p>

Claim 19	Mani in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers
	<p>Sandhu discloses storing authorization settings in a database as part of any common access control system.</p> <p>Ex. 1020, at 40 (“Access control is concerned with limiting the activity of legitimate users. It is enforced by a reference monitor which mediates every attempted access by a user (or program executing on behalf of that user) to objects in the system. The reference monitor consults an authorization database in order to determine if the user attempting to do an operation is actually authorized to perform that operation.”) (emphasis added).</p>
<p>19[c]. verifying an authority of the broadcast agent identification including an authority of the originating broadcast agent to send the broadcast message to the broadcast target area <u>by comparing</u> the stored geographically defined broadcast message jurisdiction for the originating broadcast agent with the broadcast target area associated with the broadcast message in the broadcast request; and</p>	<p>Rieger (Ex. 1017) in view of Zimmers (Ex. 1018) disclose this feature and motivation for providing it.</p> <p><i>See</i> Ex. 1017, at ¶ 81 (“Administrators of the communications system 100 can restrict the nature of postings created by any particular user by defining geographic regions into which the user is either authorized or unauthorized to post. Authorized regions can be assigned optional passwords and posting category restrictions that further narrow the user’s posting privileges in those regions. These controls would, for example, permit system administrators to grant specific privileges to a regional authority to create postings of particular categories, e.g., Governmental/Traffic, Governmental/Weather, to particular regions, while excluding all other users from posting those categories to the regions.”).</p> <p>Ex. 1018 (Zimmers) provides an example of how limiting the geographical scope of weather alerts can reduce the “cry wolf” syndrome resulting from overbroad emergency broadcasts. <i>See</i> Ex. 1018, at 2:49-63.</p> <p>Ex. 1020 (Sandhu) also explains a background description of basic authorization and auditing concepts well-known in the art.</p>

Claim 19	<p>Mani in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers</p>
	<p>“Access control is concerned with limiting the activity of legitimate users. It is enforced by a reference monitor which mediates every attempted access by a user (or program executing on behalf of that user) to objects in the system. The reference monitor consults an authorization database in order to determine if the user attempting to do an operation is actually authorized to perform that operation.” Ex. 1020, at 40.</p> <div data-bbox="589 669 1443 1339" data-label="Diagram"> <pre> graph TD SA[Security administrator] <--> AD[(Authorization database)] U[User] -- Authentication --> RM[Reference monitor] RM <--> AD RM -- Access control --> O[Objects] A[Auditing] -.-> U A -.-> O </pre> </div> <p>“Access control assumes that authentication of the user has been successfully verified prior to enforcement of access control via a reference monitor.” Ex. 1020, at 40.</p> <p>“Discretionary protection policies govern the access of users to the information on the basis of the user’s identity and authorizations (or rules) that specify, for each user (or group of users) and each object in the system, the access modes (e.g., read, write, or execute) the user is allowed on the object. Each request of a user to access an object is checked against the specified authorizations. If there exists an authorization stating that the user can</p>

Claim 19	Mani in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers
	<p>access the object in the specific mode, the access is granted, otherwise it is denied.” Ex. 1020, at 44 (emphasis added).</p> <p>Thus, Sandhu, Rieger and Zimmers disclose storing a defined jurisdictional area for a message sender, and setting a user restriction wherein a request to broadcast a message “is checked against the specified authorizations” as taught by Sandhu and Rieger to verify the sender’s authority.</p>

Claim 19	Mani in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers
<p>19[d]. transmitting the broadcast message over an output interface to one or more coupled broadcast message networks providing broadcast message alerting service to at least a portion of the broadcast target area.</p>	 <pre> graph TD 1002[GENERATING A PUBLIC EMERGENCY MESSAGE BY AN AUTHORIZED AGENCY] --> 1004[BROADCASTING THE MESSAGE OVER A PARTICULAR AREA SERVED BY THE SERVICE NETWORK] 1004 --> 1006[DELIVERING THE PUBLIC EMERGENCY MESSAGE TO THE SERVED SUBSCRIBERS IN ACCORDANCE WITH EACH SUBSCRIBER'S NOTIFICATION OPTIONS] </pre> <p style="text-align: center;">FIG. 10</p> <p>Mani explains that notifications can be distributed across multiple networks. “It should be appreciated by those skilled in the art upon reference hereto that in one embodiment, the network 502 may be comprised of a</p>

Claim 19	Mani in View of the 3GPP Standard, Sandhu and Rieger in View of Zimmers
	<p>combination of various PSN and CSN portions and their hybrids, including local and inter-carrier network portions. A multimedia node or network element 504 is operable to serve a plurality of subscribers, e.g., subscriber 508A operating a multimedia IT device 506A for originating and/or terminating calls ... it should be recognized that the softswitch functionality may also be provided as part of the serving multimedia node 504. A call treatment server 512 is provided as an application server node coupled to the network 502, wherein suitable multimedia service logic 513 is provided for querying a subscriber emergency notification profile database. Again, as alluded to hereinabove, it should be apparent that the functionality of the call treatment server node 512 may be distributed or embedded, depending upon the service architecture and application layering.” (Ex. 1014, ¶¶ 39-40.)</p> <p>The 3GPP Standard also discloses this element:</p> <p>Ex. 1019, at 7 ¶ 10 (“CBS messages are broadcast to defined geographical areas known as cell broadcast areas. These areas may comprise of one or more cells, or may comprise the entire PLMN. Individual CBS messages will be assigned their own geographical coverage areas by mutual agreement between the information provider and the PLMN operator. CBS messages may originate from a number of Cell Broadcast Entities (CBEs), which are connected to the Cell Broadcast Centre. CBS messages are then sent from the CBC to the cells, in accordance with the CBS's coverage requirements.”) (emphasis added).</p>

1. Motivation to Combine Mani with the 3GPP Standard

Mani does not expressly disclose the use of “a broadcast agent identification” as recited in claim elements 1(d) and 17(a). As reflected in the chart above, the system of Mani is disclosed as utilizing, in part, the Public Land Mobile Network (PLMN) for wireless telephony, *see* Ex. 1014 at 3, ¶ 34, and transmitting a message in broadcast mode to the target serving area. *See, e.g., id. at* ¶ 59. A POSITA would have knowledge of the Cell Broadcast implementing specifications to bring about message delivery “in broadcast mode.” The expert report of Randall Snyder provides that a POSITA “would naturally choose the 3GPP Standard, which was written to enable the development of cell broadcast messaging applications.” Ex. 1011, at ¶ 108; *see also id.* (writing that a POSITA “would understand that a standard message formatting protocol would be necessary to implement Mani.”). The use of the term PLMN in Mani would be known to a POSITA “to designate a particular cellular network.” *Id.* at ¶ 109. Mr. Snyder explains that, because Mani discloses transmission over multiple networks, a POSITA would make use of the 3GPP standard in order to broadcast to multiple networks, including multiple PLMNs. *Id.* at ¶ 110. Accordingly, a POSITA would be motivated to combine the 3GPP standard reflected in Ex. 1019 to implement a geographically targeted broadcast as disclosed in Mani (Ex. 1014).

2. Motivation to Combine Mani with Sandhu

Claim element 1(e) recites in part: “verifying the broadcast message request to provide a verified broadcast message . . . the verifying ensuring the stored broadcast message jurisdiction of the originating broadcast agent includes the broadcast target area of each broadcast message request.” Claim element 17(c) provides a similar “verifying.” Thus, the claim elements recite a check (i.e., a verification) of the preexisting privilege or authorization parameters associated with an originating agent. Although Mani does teach the concept of different users having different privilege and authorization levels, *see* Ex. 1014, at ¶ 55, Mani does not expressly disclose how to implement user roles to manage and maintain the different disclosed *privilege and authorization levels* in implementing its system.

As explained by Mr. Snyder, “[a] person of ordinary skill in the art would understand that implementing user roles and the administrative functions taught by Mani would involve the teachings of Sandhu, which provides a comprehensive background description of basic authorization and auditing concepts well-known in the art.” Ex. 1011, at ¶ 113. Sandhu discloses, for example, that “[e]ach request of a user to access an object **is checked against the specified authorizations**. If there exists an authorization stating that the user can access the object in the specific mode, the access is granted, otherwise it is denied.” Ex. 1020, Page 44 (emphasis added). These concepts were well-known and implementing them with Mani would be “a

predictable use of known techniques to achieve expected results in messaging applications (*e.g.*, to maintain system security, facilitating billing) to solve a common problem (*e.g.*, maintaining system security and facilitating billing).” Ex. 1011, at ¶ 115.

3. Motivation to Combine Mani with Rieger in View of Zimmers

Claim element 1(b) recites in part: “the broadcast message management system storing a broadcast message jurisdiction authority for each broadcast agent[.]” In addition, Claim element 1(e) recites in part: “verifying the broadcast message request to provide a verified broadcast message . . . the verifying ensuring the stored broadcast message jurisdiction of the originating broadcast agent includes the broadcast target area of each broadcast message request.” Similarly, claim element 17(b) recites a “storing” of a jurisdiction authority and claim element 17(c) provides a “verifying.” Thus, together these elements in independent claims 1 and 17 recite storing a “jurisdiction authority” of the agent as well as a check (*i.e.*, a verification) of the preexisting stored geographic privilege or authorization parameters associated with the originating agent. Mani discloses that “the emergency message may be transmitted in broadcast mode to the target serving area (step 1004).” Ex. 1014, ¶ 59. However, Mani does not expressly disclose a storing a *geographic jurisdiction* for a broadcasting agent. Nor does Mani expressly disclose a verification that specifically restricts the geographic scope of a broadcast

message based on the sender's authority.

Zimmers (Ex. 1018) provides an example of how limiting the geographical scope of weather alerts can reduce the "cry wolf" syndrome resulting from overbroad emergency broadcasts. *See* Ex. 1018, at 2:49-63. Specifically, Zimmers provides that:

Perhaps the most pernicious problem is that weather broadcasts must cover a relatively large area and so many of the alert signals transmitted by those broadcasts will be irrelevant to a large percentage of the listening population. ... This results in the situation not unlike the fable of the Boy Who Cried Wolf in which citizens decide that the warnings are not normally relevant, and either ignore them or turn their NWS receiver off.

Ex. 1018, at 2:49-62. This is one of the "safety considerations" relied on by Randall Snyder in support of his opinion relying on the teaching of Zimmers. *See* Ex. 1011, at ¶ 117. Snyder further explains that there are commercial reasons to police limitations on the broadcast area of a message. *See* Ex. 1011, at ¶118 ("[f]rom a commercial or financial perspective, cost recovery and commercial fees may be based on the number of messages broadcast, the broadcast area, the particular cost to connect to cellular networks to broadcast the message, etc."). Rieger expressly discloses a message transmission system that "teaches restricting message distribution based on two criteria: (1) the message category and (2) the applicable geographic region." (Ex. 1011, at ¶120); *see also id.* at ¶ 119 (citing to Ex. 1017, at ¶81)).

Thus, there are known safety and commercial reasons supporting a basis to combine the solution applied by Rieger based on the safety focused motivation in Zimmers (Ex. 1018) and the financial motivation explained by Snyder (Ex. 1011, at ¶ 118). Accordingly, a POSITA would be motivated to combine the geographic restriction disclosed in Rieger (Ex. 1017) with the system of Mani to restrict emergency messages to their proper target as taught by Zimmers (Ex. 1018). *See Perfect Web Technologies, Inc. v. InfoUSA, Inc.*, 587 F.3d 1324, 1329 (Fed. Cir. 2009) (“any need or problem known in the field of endeavor at the time of invention and addressed by the patent” can support a basis for combining references).

VII. CONCLUSION

Petitioner respectfully requests that this Petition be granted and Claim 19 of the '221 Patent be found unpatentable.

Department of Justice
Washington, DC 20530
Telephone: (202) 353-0517

November 1, 2016

/David M. Ruddy/
DAVID M. RUDDY
Reg. No. 53,945
Trial Attorney
Commercial Litigation Branch
Civil Division

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(d) (2016), I hereby certify that, this petition contains no more than 14,000 words, as recorded in the document statistics for this document in Microsoft Word 2013, which provides the following information:

Typeface: Times New Roman, proportionally spaced, 14 point

Word Count: 9,493 (excluding the parts of the petition exempted by 37 C.F.R. § 42.24(a), *i.e.*, a table of contents, a table of authorities, mandatory notices under §42.8, a certificate of service or word count, or appendix of exhibits or claim listing.)

/ David M. Ruddy/
DAVID M. RUDDY
Reg. No. 53,945
Trial Attorney
Commercial Litigation Branch
Civil Division
Department of Justice
Washington, DC 20530
Telephone: (202) 353-0517

November 1, 2016

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 42.6 and 42.105, I hereby certify that on this 1st day of November 2016, the foregoing Petition for *Inter Partes* Review of U.S. Patent No. 8,438,221 under 35 U.S.C. §§ 311-319 and 37 C.F.R. § 42.100 *et seq.*, together with Petitioner's Exhibits Nos. [1001 to 1028], was served by FedEx, a means at least as fast and reliable as Priority Mail Express®, on the following correspondence address of record for patent owner:

Polster, Lieder, Woodruff & Lucchesi, L.C.
Attn: David Howard
12412 Powerscourt Dr. Suite 200
St. Louis, MO 63131-3615
(314) 238-2400

In addition, service is also made at the following “address known to the petitioner as likely to effect service” pursuant to 37 C.F.R. § 42.105(a):

Peter J. Chassman
REED SMITH
811 Main Street, Suite 1700
Houston, TX 77002-6110
(713) 469-3885

November 1, 2016

/David Ruddy/