US Patent & Trademark Office
Patent Public Search | Text View

United States Patent	12389218
Kind Code	B2
Date of Patent	August 12, 2025
Inventor(s)	Raleigh; Gregory G. et al.

Service selection set publishing to device agent with on-device service selection

Abstract

Disclosed herein are various embodiments for publishing a service offer set to a device agent on an end-user device and for on-device selection of a service. In some embodiments, a network system publishes a service offer set to an end-user device over a wireless access network, receives an offer set user selection from the end-user device, and provisions one or more network functions based on the offer set user selection.

Inventors: **Raleigh; Gregory G. (Incline Village, NV), Lavine; James (Denver, NC), Raissinia; Alireza (Monte Sereno, CA)**

Applicant: **Headwater Research LLC** (Tyler, TX)

Family ID: **1000008747828**

Assignee: **Headwater Research LLC (Tyler, TX)**

Appl. No.: **18/102629**

Filed: **January 27, 2023**

Prior Publication Data

Document Identifier	Publication Date
US 20230179992 A1	Jun. 08, 2023

Related U.S. Application Data

continuation parent-doc US 17093535 20201109 US 11589216 child-doc US 18102629
continuation parent-doc US 16236134 20181228 US 10834577 20201110 child-doc US 17093535
continuation parent-doc US 15416351 20170126 US 10171990 20190101 child-doc US 16236134
continuation parent-doc US 14551809 20141124 US 9572019 20170214 child-doc US 15416351
continuation-in-part parent-doc US 13237827 20110920 US 8832777 20140909 child-doc US

13239321
continuation-in-part parent-doc US 12695019 20100127 US 8275830 20120925 child-doc US 13237827
continuation-in-part parent-doc US 12380780 20090302 US 8839388 20140916 child-doc US 13237827
continuation-in-part parent-doc US 12380778 20090302 US 8321526 20121127 child-doc US 12695019
division parent-doc US 13239321 20110921 US 8898293 20141125 child-doc US 14551809
us-provisional-application US 61472606 20110406
us-provisional-application US 61435564 20110124
us-provisional-application US 61422565 20101213
us-provisional-application US 61422572 20101213
us-provisional-application US 61422574 20101213
us-provisional-application US 61420727 20101207
us-provisional-application US 61418509 20101201
us-provisional-application US 61418507 20101201
us-provisional-application US 61407358 20101027
us-provisional-application US 61389547 20101004
us-provisional-application US 61387247 20100928
us-provisional-application US 61387243 20100928
us-provisional-application US 61385020 20100921
us-provisional-application US 61384456 20100920
us-provisional-application US 61264126 20091124
us-provisional-application US 61270353 20090706
us-provisional-application US 61207739 20090213
us-provisional-application US 61207393 20090210
us-provisional-application US 61206944 20090204
us-provisional-application US 61206354 20090128

Publication Classification

Int. Cl.: **H04W8/24** (20090101); **H04M15/00** (20060101); **H04W8/22** (20090101)

U.S. Cl.:

CPC **H04W8/245** (20130101); **H04M15/41** (20130101); **H04M15/42** (20130101); **H04M15/43** (20130101); **H04M15/44** (20130101); **H04M15/53** (20130101); **H04M15/61** (20130101); **H04M15/80** (20130101); **H04W8/22** (20130101);

Field of Classification Search

CPC: H04W (8/245); H04W (8/22); H04W (4/24); H04W (12/06); H04W (12/08); H04W (8/18); H04M (15/41); H04M (15/42); H04M (15/43); H04M (15/44); H04M (15/53); H04M (15/61); H04M (15/80); H04M (15/58); H04M (15/66); H04M (15/8083); H04M (2215/0188); H04M (15/00); H04M (15/8016); H04L (41/046); H04L (12/1407); H04L (41/5003); H04L (41/5025); H04L (41/0894); H04L (12/1403); H04L (12/14); H04L (41/0816)

USPC: 455/403; 455/418; 455/419

References Cited

U.S. PATENT DOCUMENTS

Patent No.	Issued Date	Patentee Name	U.S. Cl.	CPC
5131020	12/1991	Liebesny et al.	N/A	N/A
5283904	12/1993	Carson et al.	N/A	N/A
5325532	12/1993	Crosswy et al.	N/A	N/A
5572528	12/1995	Shuen	N/A	N/A
5577100	12/1995	McGregor et al.	N/A	N/A
5594777	12/1996	Makkonen et al.	N/A	N/A
5617539	12/1996	Ludwig et al.	N/A	N/A
5630159	12/1996	Zancho	N/A	N/A
5633484	12/1996	Zancho et al.	N/A	N/A
5633868	12/1996	Baldwin et al.	N/A	N/A
5751719	12/1997	Chen et al.	N/A	N/A
5754953	12/1997	Briancon et al.	N/A	N/A
5774532	12/1997	Gottlieb et al.	N/A	N/A
5794142	12/1997	Vanttila et al.	N/A	N/A
5814798	12/1997	Zancho	N/A	N/A
5889477	12/1998	Fastenrath	N/A	N/A
5892900	12/1998	Ginter et al.	N/A	N/A
5903845	12/1998	Buhrmann et al.	N/A	N/A
5915008	12/1998	Dulman	N/A	N/A
5915226	12/1998	Martineau	N/A	N/A
5933778	12/1998	Buhrmann et al.	N/A	N/A
5940472	12/1998	Newman et al.	N/A	N/A
5974439	12/1998	Bollella	N/A	N/A
5983270	12/1998	Abraham et al.	N/A	N/A
5987611	12/1998	Freund	N/A	N/A
6035281	12/1999	Crosskey et al.	N/A	N/A
6038452	12/1999	Strawczynski et al.	N/A	N/A
6038540	12/1999	Krist et al.	N/A	N/A
6047268	12/1999	Bartoli et al.	N/A	N/A
6047270	12/1999	Joao et al.	N/A	N/A
6058434	12/1999	Wilt et al.	N/A	N/A
6061571	12/1999	Tamura	N/A	N/A
6064878	12/1999	Denker et al.	N/A	N/A
6078953	12/1999	Vaid et al.	N/A	N/A
6081591	12/1999	Skoog	N/A	N/A
6098878	12/1999	Dent et al.	N/A	N/A
6104700	12/1999	Haddock et al.	N/A	N/A
6115823	12/1999	Velasco et al.	N/A	N/A
6119933	12/1999	Wong et al.	N/A	N/A
6125391	12/1999	Meltzer et al.	N/A	N/A
6141565	12/1999	Feuerstein et al.	N/A	N/A
6141686	12/1999	Jackowski et al.	N/A	N/A
6148336	12/1999	Thomas et al.	N/A	N/A
6154738	12/1999	Call	N/A	N/A
6157636	12/1999	Voit et al.	N/A	N/A

6185576	12/2000	Mcintosh	N/A	N/A
6198915	12/2000	McGregor et al.	N/A	N/A
6219786	12/2000	Cunningham et al.	N/A	N/A
6223042	12/2000	Raffel	N/A	N/A
6226277	12/2000	Chuah	N/A	N/A
6246870	12/2000	Dent et al.	N/A	N/A
6263055	12/2000	Garland et al.	N/A	N/A
6292828	12/2000	Williams	N/A	N/A
6317584	12/2000	Abu-Amara et al.	N/A	N/A
6370139	12/2001	Redmond	N/A	N/A
6381316	12/2001	Joyce et al.	N/A	N/A
6393014	12/2001	Daly et al.	N/A	N/A
6397259	12/2001	Lincke et al.	N/A	N/A
6401113	12/2001	Lazaridis et al.	N/A	N/A
6418147	12/2001	Wiedeman	N/A	N/A
6438575	12/2001	Khan et al.	N/A	N/A
6445777	12/2001	Clark	N/A	N/A
6449479	12/2001	Sanchez	N/A	N/A
6466984	12/2001	Naveh et al.	N/A	N/A
6477670	12/2001	Ahmadvand	N/A	N/A
6502131	12/2001	Vaid et al.	N/A	N/A
6505114	12/2002	Luciani	N/A	N/A
6510152	12/2002	Gerszberg et al.	N/A	N/A
6522629	12/2002	Anderson, Sr.	N/A	N/A
6526066	12/2002	Weaver	N/A	N/A
6532235	12/2002	Benson et al.	N/A	N/A
6532579	12/2002	Sato et al.	N/A	N/A
6535855	12/2002	Cahill et al.	N/A	N/A
6535949	12/2002	Parker	N/A	N/A
6539082	12/2002	Lowe et al.	N/A	N/A
6542465	12/2002	Wang	N/A	N/A
6542500	12/2002	Gerszberg et al.	N/A	N/A
6542992	12/2002	Peirce et al.	N/A	N/A
6546016	12/2002	Gerszberg et al.	N/A	N/A
6563806	12/2002	Yano et al.	N/A	N/A
6570974	12/2002	Gerszberg et al.	N/A	N/A
6574321	12/2002	Cox et al.	N/A	N/A
6574465	12/2002	Marsh et al.	N/A	N/A
6578076	12/2002	Putzolu	N/A	N/A
6581092	12/2002	Motoyama	N/A	N/A
6591098	12/2002	Shieh et al.	N/A	N/A
6598034	12/2002	Kloth	N/A	N/A
6601040	12/2002	Kolls	N/A	N/A
6603969	12/2002	Vuoristo et al.	N/A	N/A
6603975	12/2002	Inouchi et al.	N/A	N/A
6606744	12/2002	Mikurak	N/A	N/A
6615034	12/2002	Alloune et al.	N/A	N/A
6628934	12/2002	Rosenberg et al.	N/A	N/A
6631122	12/2002	Arunachalam et al.	N/A	N/A
6636721	12/2002	Threadgill et al.	N/A	N/A

6639975	12/2002	O'Neal et al.	N/A	N/A
6640097	12/2002	Corrigan et al.	N/A	N/A
6640334	12/2002	Rasmussen	N/A	N/A
6650887	12/2002	McGregor et al.	N/A	N/A
6651101	12/2002	Gai et al.	N/A	N/A
6654786	12/2002	Fox et al.	N/A	N/A
6654814	12/2002	Britton et al.	N/A	N/A
6658254	12/2002	Purdy et al.	N/A	N/A
6662014	12/2002	Walsh	N/A	N/A
6678516	12/2003	Nordman et al.	N/A	N/A
6683853	12/2003	Kannas et al.	N/A	N/A
6684244	12/2003	Goldman et al.	N/A	N/A
6690918	12/2003	Evans et al.	N/A	N/A
6694362	12/2003	Secor et al.	N/A	N/A
6697821	12/2003	Ziff et al.	N/A	N/A
6704873	12/2003	Underwood	N/A	N/A
6725031	12/2003	Watler et al.	N/A	N/A
6725256	12/2003	Albal et al.	N/A	N/A
6732176	12/2003	Stewart et al.	N/A	N/A
6735206	12/2003	Oki et al.	N/A	N/A
6748195	12/2003	Phillips	N/A	N/A
6748437	12/2003	Mankude et al.	N/A	N/A
6751296	12/2003	Albal et al.	N/A	N/A
6754470	12/2003	Hendrickson et al.	N/A	N/A
6757717	12/2003	Goldstein	N/A	N/A
6760417	12/2003	Wallenius	N/A	N/A
6763000	12/2003	Walsh	N/A	N/A
6763226	12/2003	McZeal, Jr.	N/A	N/A
6765864	12/2003	Natarajan et al.	N/A	N/A
6765925	12/2003	Sawyer et al.	N/A	N/A
6782412	12/2003	Brophy et al.	N/A	N/A
6785889	12/2003	Williams	N/A	N/A
6792461	12/2003	Hericourt	N/A	N/A
6829596	12/2003	Frazee	N/A	N/A
6829696	12/2003	Balmer et al.	N/A	N/A
6839340	12/2004	Voit et al.	N/A	N/A
6842628	12/2004	Arnold et al.	N/A	N/A
6873988	12/2004	Herrmann et al.	N/A	N/A
6876653	12/2004	Ambe et al.	N/A	N/A
6879825	12/2004	Daly	N/A	N/A
6882718	12/2004	Smith	N/A	N/A
6885997	12/2004	Roberts	N/A	N/A
6898654	12/2004	Senior et al.	N/A	N/A
6901440	12/2004	Bimm et al.	N/A	N/A
6920455	12/2004	Weschler	N/A	N/A
6922562	12/2004	Ward et al.	N/A	N/A
6928280	12/2004	Xanthos et al.	N/A	N/A
6934249	12/2004	Bertin et al.	N/A	N/A
6934751	12/2004	Jayapalan et al.	N/A	N/A
6947723	12/2004	Gurnani et al.	N/A	N/A

6947985	12/2004	Hegli et al.	N/A	N/A
6952428	12/2004	Necka et al.	N/A	N/A
6957067	12/2004	Iyer et al.	N/A	N/A
6959202	12/2004	Heinonen et al.	N/A	N/A
6959393	12/2004	Hollis et al.	N/A	N/A
6965667	12/2004	Trabandt et al.	N/A	N/A
6965872	12/2004	Grdina	N/A	N/A
6967958	12/2004	Ono et al.	N/A	N/A
6970692	12/2004	Tysor	N/A	N/A
6970927	12/2004	Stewart et al.	N/A	N/A
6982733	12/2005	McNally et al.	N/A	N/A
6983370	12/2005	Eaton et al.	N/A	N/A
6996062	12/2005	Freed et al.	N/A	N/A
6996076	12/2005	Forbes et al.	N/A	N/A
6996393	12/2005	Pyhalammi et al.	N/A	N/A
6998985	12/2005	Reisman et al.	N/A	N/A
7000001	12/2005	Lazaridis	N/A	N/A
7002920	12/2005	Ayyagari et al.	N/A	N/A
7007295	12/2005	Rose et al.	N/A	N/A
7013469	12/2005	Smith et al.	N/A	N/A
7017189	12/2005	DeMello et al.	N/A	N/A
7020781	12/2005	Saw et al.	N/A	N/A
7023909	12/2005	Adams	N/A	N/A
7024200	12/2005	McKenna et al.	N/A	N/A
7024460	12/2005	Koopmas et al.	N/A	N/A
7027055	12/2005	Anderson et al.	N/A	N/A
7027408	12/2005	Nabkel et al.	N/A	N/A
7031733	12/2005	Alminana et al.	N/A	N/A
7032072	12/2005	Quinn et al.	N/A	N/A
7039027	12/2005	Bridgelall	N/A	N/A
7039037	12/2005	Wang et al.	N/A	N/A
7039403	12/2005	Wong	N/A	N/A
7039713	12/2005	Van Gunter et al.	N/A	N/A
7042988	12/2005	Juitt et al.	N/A	N/A
7043225	12/2005	Patel et al.	N/A	N/A
7043226	12/2005	Yamauchi	N/A	N/A
7043268	12/2005	Yukie et al.	N/A	N/A
7047276	12/2005	Liu et al.	N/A	N/A
7058022	12/2005	Carolan et al.	N/A	N/A
7058968	12/2005	Rowland et al.	N/A	N/A
7068600	12/2005	Cain	N/A	N/A
7069248	12/2005	Huber	N/A	N/A
7082422	12/2005	Zirngibl et al.	N/A	N/A
7084775	12/2005	Smith	N/A	N/A
7092696	12/2005	Hosain et al.	N/A	N/A
7095754	12/2005	Benveniste	N/A	N/A
7099943	12/2005	Tondering	N/A	N/A
7102620	12/2005	Harries et al.	N/A	N/A
7110753	12/2005	Campen	N/A	N/A
7113780	12/2005	Mckenna et al.	N/A	N/A

7113997	12/2005	Jayapalan et al.	N/A	N/A
7120133	12/2005	Joo et al.	N/A	N/A
7131578	12/2005	Paschini et al.	N/A	N/A
7133386	12/2005	Holur et al.	N/A	N/A
7133695	12/2005	Beyda	N/A	N/A
7133907	12/2005	Carlson et al.	N/A	N/A
7136361	12/2005	Benveniste	N/A	N/A
7139569	12/2005	Kato	N/A	N/A
7142876	12/2005	Trossen et al.	N/A	N/A
7149229	12/2005	Leung	N/A	N/A
7149521	12/2005	Sundar et al.	N/A	N/A
7151764	12/2005	Heinonen et al.	N/A	N/A
7158792	12/2006	Cook et al.	N/A	N/A
7162237	12/2006	Silver et al.	N/A	N/A
7165040	12/2006	Ehrman et al.	N/A	N/A
7167078	12/2006	Pourchot	N/A	N/A
7171199	12/2006	Rahman	N/A	N/A
7174156	12/2006	Mangal	N/A	N/A
7174174	12/2006	Boris et al.	N/A	N/A
7177919	12/2006	Truong et al.	N/A	N/A
7180855	12/2006	Lin	N/A	N/A
7181017	12/2006	Nagel et al.	N/A	N/A
7191248	12/2006	Chattopadhyay et al.	N/A	N/A
7197321	12/2006	Erskine et al.	N/A	N/A
7200112	12/2006	Sundar et al.	N/A	N/A
7200551	12/2006	Senez	N/A	N/A
7203169	12/2006	Okholm et al.	N/A	N/A
7203721	12/2006	Ben-Efraim et al.	N/A	N/A
7203752	12/2006	Rice et al.	N/A	N/A
7207041	12/2006	Elson et al.	N/A	N/A
7209664	12/2006	McNicol et al.	N/A	N/A
7212491	12/2006	Koga	N/A	N/A
7219123	12/2006	Fiechter et al.	N/A	N/A
7222190	12/2006	Klinker et al.	N/A	N/A
7222304	12/2006	Beaton et al.	N/A	N/A
7224968	12/2006	Dobson et al.	N/A	N/A
7228354	12/2006	Chambliss et al.	N/A	N/A
7236780	12/2006	Benco	N/A	N/A
7242668	12/2006	Kan et al.	N/A	N/A
7242920	12/2006	Morris	N/A	N/A
7245901	12/2006	McGregor et al.	N/A	N/A
7248570	12/2006	Bahl et al.	N/A	N/A
7248868	12/2006	Snyder et al.	N/A	N/A
7251218	12/2006	Jorgensen	N/A	N/A
7260382	12/2006	Lamb et al.	N/A	N/A
7266371	12/2006	Amin et al.	N/A	N/A
7269157	12/2006	Klinker et al.	N/A	N/A
7271765	12/2006	Stilp et al.	N/A	N/A
7272660	12/2006	Powers et al.	N/A	N/A
7280816	12/2006	Fratti et al.	N/A	N/A

7280818	12/2006	Clayton	N/A	N/A
7283561	12/2006	Picher-Dempsey	N/A	N/A
7283963	12/2006	Fitzpatrick et al.	N/A	N/A
7286834	12/2006	Walter	N/A	N/A
7286848	12/2006	Vireday et al.	N/A	N/A
7289489	12/2006	Kung et al.	N/A	N/A
7290283	12/2006	Copeland, III	N/A	N/A
7310424	12/2006	Gehring et al.	N/A	N/A
7313237	12/2006	Bahl et al.	N/A	N/A
7315892	12/2007	Freimuth et al.	N/A	N/A
7317699	12/2007	Godfrey et al.	N/A	N/A
7318050	12/2007	Musgrave	N/A	N/A
7318111	12/2007	Zhao	N/A	N/A
7320029	12/2007	Rinne et al.	N/A	N/A
7320781	12/2007	Lambert et al.	N/A	N/A
7322044	12/2007	Hrastar	N/A	N/A
7324447	12/2007	Morford	N/A	N/A
7325037	12/2007	Lawson	N/A	N/A
7336960	12/2007	Zavalkovsky et al.	N/A	N/A
7340244	12/2007	Osborne et al.	N/A	N/A
7340772	12/2007	Panasyuk et al.	N/A	N/A
7346410	12/2007	Uchiyama	N/A	N/A
7349695	12/2007	Oommen et al.	N/A	N/A
7349698	12/2007	Gallagher et al.	N/A	N/A
7353533	12/2007	Wright et al.	N/A	N/A
7356011	12/2007	Waters et al.	N/A	N/A
7356337	12/2007	Florence	N/A	N/A
7366497	12/2007	Nagata	N/A	N/A
7366654	12/2007	Moore	N/A	N/A
7366934	12/2007	Narayan et al.	N/A	N/A
7369848	12/2007	Jiang	N/A	N/A
7369856	12/2007	Ovadia	N/A	N/A
7373136	12/2007	Watler et al.	N/A	N/A
7373179	12/2007	Stine et al.	N/A	N/A
7379731	12/2007	Natsuno et al.	N/A	N/A
7388950	12/2007	Elsey et al.	N/A	N/A
7389412	12/2007	Sharma et al.	N/A	N/A
7391724	12/2007	Alakoski et al.	N/A	N/A
7395056	12/2007	Petermann	N/A	N/A
7395244	12/2007	Kingsford	N/A	N/A
7401338	12/2007	Bowen et al.	N/A	N/A
7403763	12/2007	Maes	N/A	N/A
7409447	12/2007	Assadzadeh	N/A	N/A
7409569	12/2007	Illowsky et al.	N/A	N/A
7411930	12/2007	Montojo et al.	N/A	N/A
7418253	12/2007	Kavanah	N/A	N/A
7418257	12/2007	Kim	N/A	N/A
7421004	12/2007	Feher	N/A	N/A
7423971	12/2007	Mohaban et al.	N/A	N/A
7428750	12/2007	Dunn et al.	N/A	N/A

7433362	12/2007	Mallya et al.	N/A	N/A
7436816	12/2007	Mehta et al.	N/A	N/A
7440433	12/2007	Rink et al.	N/A	N/A
7444669	12/2007	Bahl et al.	N/A	N/A
7450591	12/2007	Korling et al.	N/A	N/A
7450927	12/2007	Creswell et al.	N/A	N/A
7454191	12/2007	Dawson et al.	N/A	N/A
7457265	12/2007	Julka et al.	N/A	N/A
7457870	12/2007	Lownsbrough et al.	N/A	N/A
7460837	12/2007	Diener	N/A	N/A
7466652	12/2007	Lau et al.	N/A	N/A
7467160	12/2007	Mcintyre	N/A	N/A
7472189	12/2007	Mallya et al.	N/A	N/A
7478420	12/2008	Wright et al.	N/A	N/A
7486185	12/2008	Culpepper et al.	N/A	N/A
7486658	12/2008	Kumar	N/A	N/A
7489918	12/2008	Zhou et al.	N/A	N/A
7493659	12/2008	Wu et al.	N/A	N/A
7496652	12/2008	Pezzutti	N/A	N/A
7499438	12/2008	Hinman et al.	N/A	N/A
7499537	12/2008	Elsey et al.	N/A	N/A
7502672	12/2008	Kolls	N/A	N/A
7505756	12/2008	Bahl	N/A	N/A
7505795	12/2008	Lim et al.	N/A	N/A
7508794	12/2008	Feather et al.	N/A	N/A
7508799	12/2008	Sumner et al.	N/A	N/A
7512128	12/2008	DiMambro et al.	N/A	N/A
7512131	12/2008	Svensson et al.	N/A	N/A
7515608	12/2008	Yuan et al.	N/A	N/A
7515926	12/2008	Bu et al.	N/A	N/A
7516219	12/2008	Moghaddam et al.	N/A	N/A
7522549	12/2008	Karaoguz et al.	N/A	N/A
7522576	12/2008	Du et al.	N/A	N/A
7526541	12/2008	Roese et al.	N/A	N/A
7529204	12/2008	Bourlas et al.	N/A	N/A
7533158	12/2008	Grannan et al.	N/A	N/A
7535880	12/2008	Hinman et al.	N/A	N/A
7536695	12/2008	Alam et al.	N/A	N/A
7539132	12/2008	Werner et al.	N/A	N/A
7539862	12/2008	Edgett et al.	N/A	N/A
7540408	12/2008	Levine et al.	N/A	N/A
7545782	12/2008	Rayment et al.	N/A	N/A
7546460	12/2008	Maes	N/A	N/A
7546629	12/2008	Albert et al.	N/A	N/A
7548875	12/2008	Mikkelsen et al.	N/A	N/A
7548976	12/2008	Bahl et al.	N/A	N/A
7551921	12/2008	Petermann	N/A	N/A
7551922	12/2008	Roskowski et al.	N/A	N/A
7554983	12/2008	Muppala	N/A	N/A
7555757	12/2008	Smith et al.	N/A	N/A

7561899	12/2008	Lee	N/A	N/A
7562213	12/2008	Timms	N/A	N/A
7564799	12/2008	Holland et al.	N/A	N/A
7565141	12/2008	Macaluso	N/A	N/A
7565328	12/2008	Donner	N/A	N/A
7574509	12/2008	Nixon et al.	N/A	N/A
7574731	12/2008	Fascenda	N/A	N/A
7577431	12/2008	Jiang	N/A	N/A
7580356	12/2008	Mishra et al.	N/A	N/A
7580857	12/2008	VanFleet et al.	N/A	N/A
7583964	12/2008	Wong	N/A	N/A
7584298	12/2008	Klinker et al.	N/A	N/A
7585217	12/2008	Lutnick et al.	N/A	N/A
7586871	12/2008	Hamilton et al.	N/A	N/A
7593417	12/2008	Wang et al.	N/A	N/A
7593730	12/2008	Khandelwal et al.	N/A	N/A
7596373	12/2008	Mcgregor et al.	N/A	N/A
7599288	12/2008	Cole et al.	N/A	N/A
7599714	12/2008	Kuzminskiy	N/A	N/A
7602746	12/2008	Calhoun et al.	N/A	N/A
7603710	12/2008	Harvey et al.	N/A	N/A
7606357	12/2008	Daigle	N/A	N/A
7606918	12/2008	Holzman et al.	N/A	N/A
7607041	12/2008	Kraemer et al.	N/A	N/A
7609650	12/2008	Roskowski et al.	N/A	N/A
7609700	12/2008	Mng et al.	N/A	N/A
7610047	12/2008	Hicks, III et al.	N/A	N/A
7610057	12/2008	Bahl et al.	N/A	N/A
7610328	12/2008	Haase et al.	N/A	N/A
7610396	12/2008	Taglienti et al.	N/A	N/A
7612712	12/2008	LaMance et al.	N/A	N/A
7613444	12/2008	Lindqvist et al.	N/A	N/A
7614051	12/2008	Glaum et al.	N/A	N/A
7616962	12/2008	Oswal et al.	N/A	N/A
7617516	12/2008	Huslak et al.	N/A	N/A
7620041	12/2008	Dunn et al.	N/A	N/A
7620065	12/2008	Falardeau	N/A	N/A
7620162	12/2008	Aaron et al.	N/A	N/A
7620383	12/2008	Taglienti et al.	N/A	N/A
7627314	12/2008	Carlson et al.	N/A	N/A
7627600	12/2008	Citron et al.	N/A	N/A
7627767	12/2008	Sherman et al.	N/A	N/A
7627872	12/2008	Hebeler et al.	N/A	N/A
7633438	12/2008	Tysowski	N/A	N/A
7634253	12/2008	Plestid et al.	N/A	N/A
7634388	12/2008	Archer et al.	N/A	N/A
7636574	12/2008	Poosala	N/A	N/A
7636626	12/2008	Oesterling et al.	N/A	N/A
7643411	12/2009	Andreasen et al.	N/A	N/A
7644151	12/2009	Jerrim et al.	N/A	N/A

7644267	12/2009	Ylikoski et al.	N/A	N/A
7644414	12/2009	Smith et al.	N/A	N/A
7647047	12/2009	Moghaddam et al.	N/A	N/A
7650137	12/2009	Jobs et al.	N/A	N/A
7653394	12/2009	McMillin	N/A	N/A
7656271	12/2009	Ehrman et al.	N/A	N/A
7657920	12/2009	Arseneau et al.	N/A	N/A
7660419	12/2009	Ho	N/A	N/A
7661124	12/2009	Ramanathan et al.	N/A	N/A
7664494	12/2009	Jiang	N/A	N/A
7668176	12/2009	Chuah	N/A	N/A
7668612	12/2009	Okkonen	N/A	N/A
7668903	12/2009	Edwards et al.	N/A	N/A
7668966	12/2009	Klinker et al.	N/A	N/A
7676673	12/2009	Weller et al.	N/A	N/A
7680086	12/2009	Eglin	N/A	N/A
7681226	12/2009	Kraemer et al.	N/A	N/A
7684370	12/2009	Kezys	N/A	N/A
7685131	12/2009	Batra et al.	N/A	N/A
7685254	12/2009	Pandya	N/A	N/A
7685530	12/2009	Sherrard et al.	N/A	N/A
7688792	12/2009	Babbar et al.	N/A	N/A
7693107	12/2009	De Froment	N/A	N/A
7693720	12/2009	Kennewick et al.	N/A	N/A
7697540	12/2009	Haddad et al.	N/A	N/A
7707320	12/2009	Singhai et al.	N/A	N/A
7710932	12/2009	Muthuswamy et al.	N/A	N/A
7711848	12/2009	Maes	N/A	N/A
7719966	12/2009	Luft et al.	N/A	N/A
7720206	12/2009	Devolites et al.	N/A	N/A
7720464	12/2009	Batta	N/A	N/A
7720505	12/2009	Gopi et al.	N/A	N/A
7720960	12/2009	Pruss et al.	N/A	N/A
7721296	12/2009	Ricagni	N/A	N/A
7724716	12/2009	Fadell	N/A	N/A
7725570	12/2009	Lewis	N/A	N/A
7729326	12/2009	Sekhar	N/A	N/A
7729484	12/2009	Coppage	N/A	N/A
7730123	12/2009	Erickson et al.	N/A	N/A
7734784	12/2009	Araujo et al.	N/A	N/A
7742406	12/2009	Muppala	N/A	N/A
7742961	12/2009	Aaron et al.	N/A	N/A
7743119	12/2009	Friend et al.	N/A	N/A
7746854	12/2009	Ambe et al.	N/A	N/A
7747240	12/2009	Briscoe et al.	N/A	N/A
7747699	12/2009	Prueitt et al.	N/A	N/A
7747730	12/2009	Harlow	N/A	N/A
7752330	12/2009	Olsen et al.	N/A	N/A
7756056	12/2009	Kim et al.	N/A	N/A
7756509	12/2009	Rajagopalan et al.	N/A	N/A

7756534	12/2009	Anupam et al.	N/A	N/A
7756757	12/2009	Oakes, III	N/A	N/A
7757185	12/2009	Paquette et al.	N/A	N/A
7760137	12/2009	Martucci et al.	N/A	N/A
7760711	12/2009	Kung et al.	N/A	N/A
7760861	12/2009	Croak et al.	N/A	N/A
7765294	12/2009	Edwards et al.	N/A	N/A
7769397	12/2009	Funato et al.	N/A	N/A
7770785	12/2009	Jha et al.	N/A	N/A
7774323	12/2009	Helfman	N/A	N/A
7774412	12/2009	Schnepel	N/A	N/A
7774456	12/2009	Lownsbrough et al.	N/A	N/A
7778176	12/2009	Morford	N/A	N/A
7778643	12/2009	Laroia et al.	N/A	N/A
7783754	12/2009	Morford et al.	N/A	N/A
7788386	12/2009	Svensson	N/A	N/A
7788700	12/2009	Feezel et al.	N/A	N/A
7792257	12/2009	Vanier et al.	N/A	N/A
7792538	12/2009	Kozisek	N/A	N/A
7792708	12/2009	Alva	N/A	N/A
7797019	12/2009	Friedmann	N/A	N/A
7797060	12/2009	Grgic et al.	N/A	N/A
7797204	12/2009	Balent	N/A	N/A
7797401	12/2009	Stewart et al.	N/A	N/A
7801523	12/2009	Kenderov	N/A	N/A
7801783	12/2009	Kende et al.	N/A	N/A
7801985	12/2009	Pitkow et al.	N/A	N/A
7802724	12/2009	Nohr	N/A	N/A
7805140	12/2009	Friday et al.	N/A	N/A
7805522	12/2009	Schlüter et al.	N/A	N/A
7805606	12/2009	Birger et al.	N/A	N/A
7809351	12/2009	Panda et al.	N/A	N/A
7809372	12/2009	Rajaniemi	N/A	N/A
7813746	12/2009	Rajkotia	N/A	N/A
7817615	12/2009	Breau et al.	N/A	N/A
7817983	12/2009	Cassett et al.	N/A	N/A
7821985	12/2009	Van Megen et al.	N/A	N/A
7822837	12/2009	Urban et al.	N/A	N/A
7822849	12/2009	Titus	N/A	N/A
7826427	12/2009	Sood et al.	N/A	N/A
7826607	12/2009	De Carvalho Resende et al.	N/A	N/A
7835275	12/2009	Swan et al.	N/A	N/A
7843831	12/2009	Morrill et al.	N/A	N/A
7843843	12/2009	Papp, III et al.	N/A	N/A
7844034	12/2009	Oh et al.	N/A	N/A
7844728	12/2009	Anderson et al.	N/A	N/A
7848768	12/2009	Omori et al.	N/A	N/A
7849161	12/2009	Koch et al.	N/A	N/A
7849170	12/2009	Hargens et al.	N/A	N/A

7849477	12/2009	Cristofalo et al.	N/A	N/A
7853250	12/2009	Harvey et al.	N/A	N/A
7853255	12/2009	Karaoguz et al.	N/A	N/A
7853656	12/2009	Yach et al.	N/A	N/A
7856226	12/2009	Wong et al.	N/A	N/A
7860088	12/2009	Lioy	N/A	N/A
7865182	12/2010	Macaluso	N/A	N/A
7865187	12/2010	Ramer et al.	N/A	N/A
7868778	12/2010	Kenwright	N/A	N/A
7868814	12/2010	Bergman	N/A	N/A
7873001	12/2010	Silver	N/A	N/A
7873344	12/2010	Bowser et al.	N/A	N/A
7873346	12/2010	Petersson et al.	N/A	N/A
7873540	12/2010	Arumugam	N/A	N/A
7873705	12/2010	Kalish	N/A	N/A
7873985	12/2010	Baum	N/A	N/A
7877090	12/2010	Maes	N/A	N/A
7881199	12/2010	Krstulich	N/A	N/A
7881267	12/2010	Crosswy et al.	N/A	N/A
7881697	12/2010	Baker et al.	N/A	N/A
7882029	12/2010	White	N/A	N/A
7882247	12/2010	Sturniolo et al.	N/A	N/A
7882560	12/2010	Kraemer et al.	N/A	N/A
7885644	12/2010	Gallagher et al.	N/A	N/A
7886047	12/2010	Potluri	N/A	N/A
7889384	12/2010	Armentrout et al.	N/A	N/A
7890084	12/2010	Dudziak et al.	N/A	N/A
7890111	12/2010	Bugenhagen	N/A	N/A
7890581	12/2010	Rao et al.	N/A	N/A
7894431	12/2010	Goring et al.	N/A	N/A
7899039	12/2010	Andreasen et al.	N/A	N/A
7899438	12/2010	Baker et al.	N/A	N/A
7903553	12/2010	Liu	N/A	N/A
7907970	12/2010	Park et al.	N/A	N/A
7908358	12/2010	Prasad et al.	N/A	N/A
7911975	12/2010	Droz et al.	N/A	N/A
7912025	12/2010	Pattenden et al.	N/A	N/A
7912056	12/2010	Brassem	N/A	N/A
7916707	12/2010	Fontaine	N/A	N/A
7917130	12/2010	Christensen et al.	N/A	N/A
7920529	12/2010	Mahler et al.	N/A	N/A
7921463	12/2010	Sood et al.	N/A	N/A
7924730	12/2010	McAllister et al.	N/A	N/A
7925740	12/2010	Nath et al.	N/A	N/A
7925778	12/2010	Wijnands et al.	N/A	N/A
7929446	12/2010	Bozarth et al.	N/A	N/A
7929959	12/2010	DeAtley et al.	N/A	N/A
7929960	12/2010	Martin et al.	N/A	N/A
7929973	12/2010	Zavalkovsky et al.	N/A	N/A
7930327	12/2010	Craft et al.	N/A	N/A

7930446	12/2010	Kesselman et al.	N/A	N/A
7930553	12/2010	Satarasinghe et al.	N/A	N/A
7933274	12/2010	Verma et al.	N/A	N/A
7936736	12/2010	Proctor, Jr. et al.	N/A	N/A
7937069	12/2010	Rassam	N/A	N/A
7937450	12/2010	Janik	N/A	N/A
7937470	12/2010	Curley et al.	N/A	N/A
7940685	12/2010	Breslau et al.	N/A	N/A
7940751	12/2010	Hansen	N/A	N/A
7941184	12/2010	Prendergast et al.	N/A	N/A
7944948	12/2010	Chow et al.	N/A	N/A
7945238	12/2010	Baker et al.	N/A	N/A
7945240	12/2010	Klock et al.	N/A	N/A
7945470	12/2010	Cohen et al.	N/A	N/A
7945945	12/2010	Graham et al.	N/A	N/A
7948952	12/2010	Hurtta et al.	N/A	N/A
7948953	12/2010	Melkote et al.	N/A	N/A
7948968	12/2010	Voit et al.	N/A	N/A
7949529	12/2010	Weider et al.	N/A	N/A
7953808	12/2010	Sharp et al.	N/A	N/A
7953877	12/2010	Vemula et al.	N/A	N/A
7957020	12/2010	Mine et al.	N/A	N/A
7957381	12/2010	Clermidy et al.	N/A	N/A
7957511	12/2010	Drudis et al.	N/A	N/A
7958029	12/2010	Bobich et al.	N/A	N/A
7962622	12/2010	Friend et al.	N/A	N/A
7965983	12/2010	Swan et al.	N/A	N/A
7966405	12/2010	Sundaresan et al.	N/A	N/A
7967682	12/2010	Huizinga	N/A	N/A
7969950	12/2010	Iyer et al.	N/A	N/A
7970350	12/2010	Sheynman	N/A	N/A
7970426	12/2010	Poe et al.	N/A	N/A
7974624	12/2010	Gallagher et al.	N/A	N/A
7975184	12/2010	Goff et al.	N/A	N/A
7978627	12/2010	Taylor et al.	N/A	N/A
7978686	12/2010	Goyal et al.	N/A	N/A
7979069	12/2010	Hupp et al.	N/A	N/A
7979889	12/2010	Gladstone et al.	N/A	N/A
7979896	12/2010	McMurtry et al.	N/A	N/A
7984130	12/2010	Bogineni et al.	N/A	N/A
7984511	12/2010	Kocher et al.	N/A	N/A
7986935	12/2010	D'Souza et al.	N/A	N/A
7987449	12/2010	Marolia et al.	N/A	N/A
7987496	12/2010	Bryce et al.	N/A	N/A
7987510	12/2010	Kocher et al.	N/A	N/A
7990049	12/2010	Shioya	N/A	N/A
8000276	12/2010	Scherzer et al.	N/A	N/A
8000318	12/2010	Wiley et al.	N/A	N/A
8000715	12/2010	Melpignano et al.	N/A	N/A
8005009	12/2010	McKee et al.	N/A	N/A

8005459	12/2010	Balsillie	N/A	N/A
8005726	12/2010	Bao	N/A	N/A
8005913	12/2010	Carlander	N/A	N/A
8005988	12/2010	Maes	N/A	N/A
8010080	12/2010	Thenthiruperai et al.	N/A	N/A
8010081	12/2010	Roskowski	N/A	N/A
8010082	12/2010	Sutaria et al.	N/A	N/A
8010623	12/2010	Fitch et al.	N/A	N/A
8010990	12/2010	Ferguson et al.	N/A	N/A
8015133	12/2010	Wu et al.	N/A	N/A
8015234	12/2010	Lum et al.	N/A	N/A
8015249	12/2010	Nayak et al.	N/A	N/A
8019687	12/2010	Wang et al.	N/A	N/A
8019820	12/2010	Son et al.	N/A	N/A
8019846	12/2010	Roelens et al.	N/A	N/A
8019868	12/2010	Rao et al.	N/A	N/A
8019886	12/2010	Harrang et al.	N/A	N/A
8023425	12/2010	Raleigh	N/A	N/A
8024230	12/2010	Zeinfeld et al.	N/A	N/A
8024397	12/2010	Erickson et al.	N/A	N/A
8024424	12/2010	Freimuth et al.	N/A	N/A
8027339	12/2010	Short et al.	N/A	N/A
8028060	12/2010	Wyld et al.	N/A	N/A
8031601	12/2010	Feroz et al.	N/A	N/A
8032168	12/2010	Ikaheimo	N/A	N/A
8032409	12/2010	Mikurak	N/A	N/A
8032899	12/2010	Archer et al.	N/A	N/A
8032920	12/2010	Maes	N/A	N/A
8036387	12/2010	Kudelski et al.	N/A	N/A
8036600	12/2010	Garrett et al.	N/A	N/A
8044792	12/2010	Orr et al.	N/A	N/A
8045973	12/2010	Chambers	N/A	N/A
8046449	12/2010	Yoshiuchi	N/A	N/A
8050275	12/2010	Iyer	N/A	N/A
8050690	12/2010	Neeraj	N/A	N/A
8050705	12/2010	Sicher et al.	N/A	N/A
8054778	12/2010	Polson	N/A	N/A
8059530	12/2010	Cole	N/A	N/A
8060017	12/2010	Schlicht et al.	N/A	N/A
8060463	12/2010	Spiegel	N/A	N/A
8060603	12/2010	Caunter et al.	N/A	N/A
8064418	12/2010	Maki	N/A	N/A
8064896	12/2010	Bell et al.	N/A	N/A
8065365	12/2010	Saxena et al.	N/A	N/A
8068824	12/2010	Shan et al.	N/A	N/A
8068829	12/2010	Lemond et al.	N/A	N/A
8073427	12/2010	Koch et al.	N/A	N/A
8073721	12/2010	Lewis	N/A	N/A
8078140	12/2010	Baker et al.	N/A	N/A
8078163	12/2010	Lemond et al.	N/A	N/A

8081612	12/2010	Want et al.	N/A	N/A
8085808	12/2010	Brusca et al.	N/A	N/A
8086398	12/2010	Sanchez et al.	N/A	N/A
8086497	12/2010	Oakes, III	N/A	N/A
8086791	12/2010	Caulkins	N/A	N/A
8090359	12/2011	Proctor, Jr. et al.	N/A	N/A
8090361	12/2011	Hagan	N/A	N/A
8090616	12/2011	Proctor, Jr. et al.	N/A	N/A
8091087	12/2011	Ali et al.	N/A	N/A
8094551	12/2011	Huber et al.	N/A	N/A
8095112	12/2011	Chow et al.	N/A	N/A
8095124	12/2011	Balia	N/A	N/A
8095175	12/2011	Todd et al.	N/A	N/A
8095640	12/2011	Guingo et al.	N/A	N/A
8095666	12/2011	Schmidt et al.	N/A	N/A
8098579	12/2011	Ray et al.	N/A	N/A
8099077	12/2011	Chowdhury et al.	N/A	N/A
8099517	12/2011	Jia et al.	N/A	N/A
8102814	12/2011	Rahman et al.	N/A	N/A
8103285	12/2011	Kalhan	N/A	N/A
8104080	12/2011	Burns et al.	N/A	N/A
8107953	12/2011	Zimmerman et al.	N/A	N/A
8108520	12/2011	Ruutu et al.	N/A	N/A
8108680	12/2011	Murray	N/A	N/A
8112435	12/2011	Epstein et al.	N/A	N/A
8116223	12/2011	Tian et al.	N/A	N/A
8116749	12/2011	Proctor, Jr. et al.	N/A	N/A
8116781	12/2011	Chen et al.	N/A	N/A
8121117	12/2011	Amdahl et al.	N/A	N/A
8122128	12/2011	Burke, II et al.	N/A	N/A
8122249	12/2011	Falk et al.	N/A	N/A
8125897	12/2011	Ray et al.	N/A	N/A
8126123	12/2011	Cai et al.	N/A	N/A
8126396	12/2011	Bennett	N/A	N/A
8126476	12/2011	Vardi et al.	N/A	N/A
8126722	12/2011	Robb et al.	N/A	N/A
8130793	12/2011	Edwards et al.	N/A	N/A
8131256	12/2011	Martti et al.	N/A	N/A
8131281	12/2011	Hildner et al.	N/A	N/A
8131301	12/2011	Ahmed et al.	N/A	N/A
8131840	12/2011	Denker	N/A	N/A
8131858	12/2011	Agulnik et al.	N/A	N/A
8132256	12/2011	Bari	N/A	N/A
8134954	12/2011	Godfrey et al.	N/A	N/A
8135388	12/2011	Gailloux et al.	N/A	N/A
8135392	12/2011	Marcellino et al.	N/A	N/A
8135657	12/2011	Kapoor et al.	N/A	N/A
8140690	12/2011	Ly et al.	N/A	N/A
8144591	12/2011	Ghai et al.	N/A	N/A
8144853	12/2011	Aboujaoude et al.	N/A	N/A

8145194	12/2011	Yoshikawa et al.	N/A	N/A
8146142	12/2011	Lortz et al.	N/A	N/A
8149748	12/2011	Bata et al.	N/A	N/A
8149771	12/2011	Khivesara et al.	N/A	N/A
8149823	12/2011	Turcan et al.	N/A	N/A
8150394	12/2011	Bianconi et al.	N/A	N/A
8150431	12/2011	Wolovitz et al.	N/A	N/A
8151205	12/2011	Follmann et al.	N/A	N/A
8152246	12/2011	Miller et al.	N/A	N/A
8155155	12/2011	Chow et al.	N/A	N/A
8155620	12/2011	Wang et al.	N/A	N/A
8155666	12/2011	Alizadeh-Shabdiz	N/A	N/A
8155670	12/2011	Fullam et al.	N/A	N/A
8156206	12/2011	Kiley et al.	N/A	N/A
8159520	12/2011	Dhanoa et al.	N/A	N/A
8160015	12/2011	Rashid et al.	N/A	N/A
8160056	12/2011	Van der Merwe et al.	N/A	N/A
8160554	12/2011	Gosselin et al.	N/A	N/A
8160555	12/2011	Gosselin et al.	N/A	N/A
8160556	12/2011	Gosselin et al.	N/A	N/A
8160598	12/2011	Savoor	N/A	N/A
8165576	12/2011	Raju et al.	N/A	N/A
8166040	12/2011	Brindisi et al.	N/A	N/A
8166554	12/2011	John	N/A	N/A
8170553	12/2011	Bennett	N/A	N/A
8174378	12/2011	Richman et al.	N/A	N/A
8174970	12/2011	Adamczyk et al.	N/A	N/A
8175574	12/2011	Panda et al.	N/A	N/A
8175966	12/2011	Steinberg et al.	N/A	N/A
8180028	12/2011	Falcone et al.	N/A	N/A
8180333	12/2011	Wells et al.	N/A	N/A
8180375	12/2011	Awad	N/A	N/A
8180881	12/2011	Seo et al.	N/A	N/A
8180886	12/2011	Overcash et al.	N/A	N/A
8184530	12/2011	Swan et al.	N/A	N/A
8184590	12/2011	Rosenblatt	N/A	N/A
8185088	12/2011	Klein et al.	N/A	N/A
8185093	12/2011	Jheng et al.	N/A	N/A
8185127	12/2011	Cai et al.	N/A	N/A
8185152	12/2011	Goldner	N/A	N/A
8185158	12/2011	Tamura et al.	N/A	N/A
8190087	12/2011	Fisher et al.	N/A	N/A
8190122	12/2011	Alexander et al.	N/A	N/A
8190675	12/2011	Tribbett	N/A	N/A
8191106	12/2011	Choyi et al.	N/A	N/A
8191116	12/2011	Gazzard	N/A	N/A
8191124	12/2011	Wynn et al.	N/A	N/A
8194549	12/2011	Huber et al.	N/A	N/A
8194553	12/2011	Liang et al.	N/A	N/A
8194572	12/2011	Horvath et al.	N/A	N/A

8194581	12/2011	Schroeder et al.	N/A	N/A
8195093	12/2011	Garrett et al.	N/A	N/A
8195153	12/2011	Frencel et al.	N/A	N/A
8195163	12/2011	Gisby et al.	N/A	N/A
8195661	12/2011	Kalavade	N/A	N/A
8196182	12/2011	Sussland et al.	N/A	N/A
8196199	12/2011	Hrastar et al.	N/A	N/A
8200163	12/2011	Hoffman	N/A	N/A
8200200	12/2011	Belser et al.	N/A	N/A
8200509	12/2011	Kenedy et al.	N/A	N/A
8200775	12/2011	Moore	N/A	N/A
8200818	12/2011	Freund et al.	N/A	N/A
8204190	12/2011	Bang et al.	N/A	N/A
8204505	12/2011	Jin et al.	N/A	N/A
8204794	12/2011	Peng et al.	N/A	N/A
8208788	12/2011	Ando et al.	N/A	N/A
8208919	12/2011	Kotecha	N/A	N/A
8213296	12/2011	Shannon et al.	N/A	N/A
8213363	12/2011	Ying et al.	N/A	N/A
8214536	12/2011	Zhao	N/A	N/A
8214890	12/2011	Kirovski et al.	N/A	N/A
8219134	12/2011	Maharajh et al.	N/A	N/A
8219821	12/2011	Zimmels et al.	N/A	N/A
8223655	12/2011	Heinz et al.	N/A	N/A
8223741	12/2011	Bartlett et al.	N/A	N/A
8224382	12/2011	Bultman	N/A	N/A
8224773	12/2011	Spiegel	N/A	N/A
8228818	12/2011	Chase et al.	N/A	N/A
8229394	12/2011	Karlberg	N/A	N/A
8229914	12/2011	Ramer et al.	N/A	N/A
8230061	12/2011	Hassan et al.	N/A	N/A
8233433	12/2011	Kalhan	N/A	N/A
8233878	12/2011	Gosnell et al.	N/A	N/A
8233883	12/2011	De Froment	N/A	N/A
8233895	12/2011	Tysowski	N/A	N/A
8234583	12/2011	Sloo et al.	N/A	N/A
8238287	12/2011	Gopi et al.	N/A	N/A
8238913	12/2011	Bhattacharyya et al.	N/A	N/A
8239520	12/2011	Grah	N/A	N/A
8242959	12/2011	Mia et al.	N/A	N/A
8244241	12/2011	Montemurro	N/A	N/A
8249601	12/2011	Emberson et al.	N/A	N/A
8254880	12/2011	Aaltonen et al.	N/A	N/A
8254915	12/2011	Kozisek	N/A	N/A
8255515	12/2011	Melman et al.	N/A	N/A
8255534	12/2011	Assadzadeh	N/A	N/A
8255689	12/2011	Kim et al.	N/A	N/A
8259692	12/2011	Bajko	N/A	N/A
8260252	12/2011	Agarwal	N/A	N/A
8264965	12/2011	Dolganow et al.	N/A	N/A

8265004	12/2011	Toutonghi	N/A	N/A
8266249	12/2011	Hu	N/A	N/A
8266269	12/2011	Short et al.	N/A	N/A
8266681	12/2011	Deshpande et al.	N/A	N/A
8270955	12/2011	Ramer et al.	N/A	N/A
8270972	12/2011	Otting et al.	N/A	N/A
8271025	12/2011	Brisebois et al.	N/A	N/A
8271045	12/2011	Parolkar et al.	N/A	N/A
8271049	12/2011	Silver et al.	N/A	N/A
8271992	12/2011	Chatley et al.	N/A	N/A
8275415	12/2011	Huslak	N/A	N/A
8275830	12/2011	Raleigh	N/A	N/A
8279067	12/2011	Berger et al.	N/A	N/A
8279864	12/2011	Wood	N/A	N/A
8280351	12/2011	Ahmed et al.	N/A	N/A
8280354	12/2011	Smith et al.	N/A	N/A
8284740	12/2011	O'Connor	N/A	N/A
8285197	12/2011	Preiss et al.	N/A	N/A
8285249	12/2011	Baker et al.	N/A	N/A
8285992	12/2011	Mathur et al.	N/A	N/A
8290820	12/2011	Plastina et al.	N/A	N/A
8291238	12/2011	Ginter et al.	N/A	N/A
8291439	12/2011	Jethi et al.	N/A	N/A
8296404	12/2011	McDysan et al.	N/A	N/A
8300575	12/2011	Willars	N/A	N/A
8301513	12/2011	Peng et al.	N/A	N/A
8306505	12/2011	Bennett	N/A	N/A
8306518	12/2011	Gailloux	N/A	N/A
8306741	12/2011	Tu	N/A	N/A
8307067	12/2011	Ryan	N/A	N/A
8307095	12/2011	Clark et al.	N/A	N/A
8310943	12/2011	Mehta et al.	N/A	N/A
8315198	12/2011	Corneille et al.	N/A	N/A
8315593	12/2011	Gallant et al.	N/A	N/A
8315594	12/2011	Mauser et al.	N/A	N/A
8315718	12/2011	Caffrey et al.	N/A	N/A
8315999	12/2011	Chatley et al.	N/A	N/A
8320244	12/2011	Muqattash et al.	N/A	N/A
8320902	12/2011	Moring et al.	N/A	N/A
8320949	12/2011	Matta	N/A	N/A
8325638	12/2011	Jin et al.	N/A	N/A
8325906	12/2011	Fullarton et al.	N/A	N/A
8326319	12/2011	Davis	N/A	N/A
8326359	12/2011	Kauffman	N/A	N/A
8326828	12/2011	Zhou et al.	N/A	N/A
8331223	12/2011	Hill et al.	N/A	N/A
8331293	12/2011	Sood	N/A	N/A
8332375	12/2011	Chatley et al.	N/A	N/A
8332517	12/2011	Russell	N/A	N/A
8335161	12/2011	Foottit et al.	N/A	N/A

8339991	12/2011	Biswas et al.	N/A	N/A
8340625	12/2011	Johnson et al.	N/A	N/A
8340628	12/2011	Taylor et al.	N/A	N/A
8340644	12/2011	Sigmund et al.	N/A	N/A
8340678	12/2011	Pandey	N/A	N/A
8340718	12/2011	Colonna et al.	N/A	N/A
8346023	12/2012	Lin	N/A	N/A
8346210	12/2012	Balsan et al.	N/A	N/A
8346225	12/2012	Raleigh	N/A	N/A
8346923	12/2012	Rowles et al.	N/A	N/A
8347104	12/2012	Pathiyal	N/A	N/A
8347362	12/2012	Cai et al.	N/A	N/A
8347378	12/2012	Merkin et al.	N/A	N/A
8350700	12/2012	Fast et al.	N/A	N/A
8351592	12/2012	Freeny, Jr. et al.	N/A	N/A
8351898	12/2012	Raleigh	N/A	N/A
8352360	12/2012	De Judicibus et al.	N/A	N/A
8352630	12/2012	Hart	N/A	N/A
8352980	12/2012	Howcroft	N/A	N/A
8353001	12/2012	Herrod	N/A	N/A
8355570	12/2012	Karsanbhai et al.	N/A	N/A
8355696	12/2012	Olding et al.	N/A	N/A
8356336	12/2012	Johnston et al.	N/A	N/A
8358638	12/2012	Scherzer et al.	N/A	N/A
8358975	12/2012	Bahl et al.	N/A	N/A
8363658	12/2012	Delker et al.	N/A	N/A
8363799	12/2012	Gruchala et al.	N/A	N/A
8364089	12/2012	Phillips	N/A	N/A
8364806	12/2012	Short et al.	N/A	N/A
8369274	12/2012	Sawai	N/A	N/A
8370477	12/2012	Short et al.	N/A	N/A
8370483	12/2012	Choong et al.	N/A	N/A
8374090	12/2012	Morrill et al.	N/A	N/A
8374102	12/2012	Luft et al.	N/A	N/A
8374592	12/2012	Proctor, Jr. et al.	N/A	N/A
8375128	12/2012	Tofighbakhsh et al.	N/A	N/A
8375136	12/2012	Roman et al.	N/A	N/A
8379847	12/2012	Bell et al.	N/A	N/A
8380247	12/2012	Engstrom	N/A	N/A
8380804	12/2012	Jain et al.	N/A	N/A
8381127	12/2012	Singh et al.	N/A	N/A
8385199	12/2012	Coward et al.	N/A	N/A
8385896	12/2012	Proctor, Jr. et al.	N/A	N/A
8385964	12/2012	Haney	N/A	N/A
8385975	12/2012	Forutanpour et al.	N/A	N/A
8386386	12/2012	Zhu	N/A	N/A
8391262	12/2012	Maki et al.	N/A	N/A
8391834	12/2012	Raleigh	N/A	N/A
8392982	12/2012	Harris et al.	N/A	N/A
8396458	12/2012	Raleigh	N/A	N/A

8396929	12/2012	Helfman et al.	N/A	N/A
8397083	12/2012	Sussland et al.	N/A	N/A
8401906	12/2012	Ruckart	N/A	N/A
8401968	12/2012	Schattauer et al.	N/A	N/A
8402165	12/2012	Deu-Ngoc et al.	N/A	N/A
8402540	12/2012	Kapoor et al.	N/A	N/A
8406427	12/2012	Chand et al.	N/A	N/A
8406736	12/2012	Das et al.	N/A	N/A
8406756	12/2012	Reeves et al.	N/A	N/A
8407345	12/2012	Lim	N/A	N/A
8407472	12/2012	Hao et al.	N/A	N/A
8407763	12/2012	Weller et al.	N/A	N/A
8411587	12/2012	Curtis et al.	N/A	N/A
8411691	12/2012	Aggarwal	N/A	N/A
8412798	12/2012	Wang	N/A	N/A
8413172	12/2012	Sng	N/A	N/A
8413245	12/2012	Kraemer et al.	N/A	N/A
8417234	12/2012	Sanding et al.	N/A	N/A
8418168	12/2012	Tyhurst et al.	N/A	N/A
8422988	12/2012	Keshav	N/A	N/A
8423016	12/2012	Buckley et al.	N/A	N/A
8429403	12/2012	Moret et al.	N/A	N/A
8437734	12/2012	Ray et al.	N/A	N/A
8441955	12/2012	Wilkinson et al.	N/A	N/A
8442015	12/2012	Behzad et al.	N/A	N/A
8442507	12/2012	Duggal et al.	N/A	N/A
8443390	12/2012	Lo et al.	N/A	N/A
8446831	12/2012	Kwan et al.	N/A	N/A
8447324	12/2012	Shuman et al.	N/A	N/A
8447607	12/2012	Weider et al.	N/A	N/A
8447980	12/2012	Godfrey et al.	N/A	N/A
8448015	12/2012	Gerhart	N/A	N/A
8452858	12/2012	Wu et al.	N/A	N/A
8457603	12/2012	El-Kadri et al.	N/A	N/A
8457609	12/2012	Tyhurst et al.	N/A	N/A
8461958	12/2012	Saenz et al.	N/A	N/A
8463194	12/2012	Erlenback et al.	N/A	N/A
8463232	12/2012	Tuli et al.	N/A	N/A
8468337	12/2012	Gaur et al.	N/A	N/A
8472371	12/2012	Bari et al.	N/A	N/A
8477778	12/2012	Lehmann, Jr. et al.	N/A	N/A
8478840	12/2012	Skutela et al.	N/A	N/A
8483057	12/2012	Cuervo	N/A	N/A
8483135	12/2012	Cai et al.	N/A	N/A
8483694	12/2012	Lewis et al.	N/A	N/A
8484327	12/2012	Werner et al.	N/A	N/A
8484568	12/2012	Rados et al.	N/A	N/A
8488597	12/2012	Nie et al.	N/A	N/A
8489110	12/2012	Frank et al.	N/A	N/A
8489720	12/2012	Morford et al.	N/A	N/A

8494559	12/2012	Malmi	N/A	N/A
8495181	12/2012	Venkatraman et al.	N/A	N/A
8495207	12/2012	Lee	N/A	N/A
8495227	12/2012	Kaminsky et al.	N/A	N/A
8495360	12/2012	Falk et al.	N/A	N/A
8495700	12/2012	Shahbazi	N/A	N/A
8495743	12/2012	Kraemer et al.	N/A	N/A
8499087	12/2012	Hu	N/A	N/A
RE44412	12/2012	Naqvi et al.	N/A	N/A
8500533	12/2012	Lutnick et al.	N/A	N/A
8503358	12/2012	Hanson et al.	N/A	N/A
8503455	12/2012	Heikens	N/A	N/A
8504032	12/2012	Lott et al.	N/A	N/A
8504574	12/2012	Dvorak et al.	N/A	N/A
8504687	12/2012	Maffione et al.	N/A	N/A
8504690	12/2012	Shah et al.	N/A	N/A
8504729	12/2012	Pezzutti	N/A	N/A
8505073	12/2012	Taglienti et al.	N/A	N/A
8509082	12/2012	Heinz et al.	N/A	N/A
8510743	12/2012	Hackborn et al.	N/A	N/A
8510804	12/2012	Bonn et al.	N/A	N/A
8514927	12/2012	Sundararajan et al.	N/A	N/A
8516552	12/2012	Raleigh	N/A	N/A
8520589	12/2012	Bhatt et al.	N/A	N/A
8520595	12/2012	Yadav et al.	N/A	N/A
8521110	12/2012	Rofougaran	N/A	N/A
8521775	12/2012	Poh et al.	N/A	N/A
8522039	12/2012	Hyndman et al.	N/A	N/A
8522249	12/2012	Beaule	N/A	N/A
8522337	12/2012	Adusumilli et al.	N/A	N/A
8523547	12/2012	Pekrul	N/A	N/A
8526329	12/2012	Mahany et al.	N/A	N/A
8526350	12/2012	Xue et al.	N/A	N/A
8527013	12/2012	Guba et al.	N/A	N/A
8527410	12/2012	Markki et al.	N/A	N/A
8527662	12/2012	Biswas et al.	N/A	N/A
8528068	12/2012	Weglein et al.	N/A	N/A
8531954	12/2012	McNaughton et al.	N/A	N/A
8531995	12/2012	Khan et al.	N/A	N/A
8532610	12/2012	Manning Cassett et al.	N/A	N/A
8533341	12/2012	Aguirre et al.	N/A	N/A
8533775	12/2012	Alcorn et al.	N/A	N/A
8535160	12/2012	Lutnick et al.	N/A	N/A
8538394	12/2012	Zimmerman et al.	N/A	N/A
8538421	12/2012	Brisebois et al.	N/A	N/A
8538458	12/2012	Haney	N/A	N/A
8539544	12/2012	Garimella et al.	N/A	N/A
8539561	12/2012	Gupta et al.	N/A	N/A
8543265	12/2012	Ekhaguere et al.	N/A	N/A
8543814	12/2012	Laitinen et al.	N/A	N/A

8544105	12/2012	Mclean et al.	N/A	N/A
8548427	12/2012	Chow et al.	N/A	N/A
8548428	12/2012	Raleigh	N/A	N/A
8549173	12/2012	Wu et al.	N/A	N/A
8549588	12/2012	Wynn et al.	N/A	N/A
8554876	12/2012	Winsor	N/A	N/A
8559369	12/2012	Barkan	N/A	N/A
8561138	12/2012	Rothman et al.	N/A	N/A
8565746	12/2012	Hoffman	N/A	N/A
8565766	12/2012	Scherzer et al.	N/A	N/A
8566236	12/2012	Busch	N/A	N/A
8571474	12/2012	Chavez et al.	N/A	N/A
8571501	12/2012	Miller et al.	N/A	N/A
8571598	12/2012	Valavi	N/A	N/A
8571993	12/2012	Kocher et al.	N/A	N/A
8572117	12/2012	Rappaport	N/A	N/A
8572256	12/2012	Babbar	N/A	N/A
8583499	12/2012	De Judicibus et al.	N/A	N/A
8584226	12/2012	Kudla et al.	N/A	N/A
8588240	12/2012	Ramankutty et al.	N/A	N/A
8589541	12/2012	Raleigh et al.	N/A	N/A
8589955	12/2012	Roundtree et al.	N/A	N/A
8594626	12/2012	Woodson et al.	N/A	N/A
8594665	12/2012	Anschutz	N/A	N/A
8595186	12/2012	Mandyam et al.	N/A	N/A
8600850	12/2012	Zabawskyj et al.	N/A	N/A
8600895	12/2012	Felsher	N/A	N/A
8601125	12/2012	Huang et al.	N/A	N/A
8605691	12/2012	Soomro et al.	N/A	N/A
8609911	12/2012	Nicholas et al.	N/A	N/A
8611919	12/2012	Barnes, Jr.	N/A	N/A
8615507	12/2012	Varadarajulu et al.	N/A	N/A
8619735	12/2012	Montemurro et al.	N/A	N/A
8620257	12/2012	Qiu et al.	N/A	N/A
8620281	12/2012	Gosselin et al.	N/A	N/A
8621056	12/2012	Coussemaeker et al.	N/A	N/A
8630314	12/2013	York	N/A	N/A
8630630	12/2013	Raleigh	N/A	N/A
8630925	12/2013	Bystrom et al.	N/A	N/A
8631428	12/2013	Scott et al.	N/A	N/A
8634425	12/2013	Gorti et al.	N/A	N/A
8635164	12/2013	Rosenhaft et al.	N/A	N/A
8635335	12/2013	Raleigh et al.	N/A	N/A
8639215	12/2013	McGregor et al.	N/A	N/A
8644702	12/2013	Kalajan	N/A	N/A
8644813	12/2013	Gailloux et al.	N/A	N/A
8645518	12/2013	David	N/A	N/A
8654952	12/2013	Wang et al.	N/A	N/A
8655357	12/2013	Gazzard et al.	N/A	N/A
8656472	12/2013	McMurtry et al.	N/A	N/A

8660853	12/2013	Robb et al.	N/A	N/A
8666395	12/2013	Silver	N/A	N/A
8667542	12/2013	Bertz et al.	N/A	N/A
8670334	12/2013	Keohane et al.	N/A	N/A
8670752	12/2013	Fan et al.	N/A	N/A
8675507	12/2013	Raleigh	N/A	N/A
8675852	12/2013	Maes	N/A	N/A
8676682	12/2013	Kalliola	N/A	N/A
8676925	12/2013	Liu et al.	N/A	N/A
8688671	12/2013	Ramer et al.	N/A	N/A
8688784	12/2013	Zabawskyj et al.	N/A	N/A
8693323	12/2013	McDysan	N/A	N/A
8694772	12/2013	Kao et al.	N/A	N/A
8699355	12/2013	Macias	N/A	N/A
8700729	12/2013	Dua	N/A	N/A
8701015	12/2013	Bonnat	N/A	N/A
8701080	12/2013	Tripathi	N/A	N/A
8705361	12/2013	Venkataraman et al.	N/A	N/A
8706863	12/2013	Fadell	N/A	N/A
8713535	12/2013	Malhotra et al.	N/A	N/A
8713641	12/2013	Pagan et al.	N/A	N/A
8713667	12/2013	Kalibjian et al.	N/A	N/A
8719397	12/2013	Levi et al.	N/A	N/A
8719423	12/2013	Wyld	N/A	N/A
8724486	12/2013	Seto et al.	N/A	N/A
8725700	12/2013	Rappaport	N/A	N/A
8725899	12/2013	Short et al.	N/A	N/A
8730842	12/2013	Collins et al.	N/A	N/A
8731519	12/2013	Flynn et al.	N/A	N/A
8732808	12/2013	Sewall et al.	N/A	N/A
8738860	12/2013	Griffin et al.	N/A	N/A
8739035	12/2013	Trethewey	N/A	N/A
8742694	12/2013	Bora et al.	N/A	N/A
8744339	12/2013	Halfmann et al.	N/A	N/A
8761711	12/2013	Grignani et al.	N/A	N/A
8761809	12/2013	Faith et al.	N/A	N/A
8768312	12/2013	Deuel et al.	N/A	N/A
8775233	12/2013	Lybrook et al.	N/A	N/A
8780857	12/2013	Balasubramanian et al.	N/A	N/A
8787249	12/2013	Giaretta et al.	N/A	N/A
8792857	12/2013	Cai et al.	N/A	N/A
8793304	12/2013	Lu et al.	N/A	N/A
8793758	12/2013	Raleigh et al.	N/A	N/A
8798610	12/2013	Prakash et al.	N/A	N/A
8799440	12/2013	Zhou et al.	N/A	N/A
8804517	12/2013	Oerton	N/A	N/A
8804695	12/2013	Branam	N/A	N/A
8811338	12/2013	Jin et al.	N/A	N/A
8811991	12/2013	Jain et al.	N/A	N/A

8812525	12/2013	Taylor, III	N/A	N/A
8818394	12/2013	Bienas et al.	N/A	N/A
8819253	12/2013	Simeloff et al.	N/A	N/A
8825109	12/2013	Montemurro et al.	N/A	N/A
8826411	12/2013	Moen et al.	N/A	N/A
8831561	12/2013	Sutaria et al.	N/A	N/A
8837322	12/2013	Venkataramanan et al.	N/A	N/A
8838686	12/2013	Getchius	N/A	N/A
8838752	12/2013	Lor et al.	N/A	N/A
8839388	12/2013	Raleigh	N/A	N/A
8843849	12/2013	Neil et al.	N/A	N/A
8845415	12/2013	Lutnick et al.	N/A	N/A
8849262	12/2013	Desai et al.	N/A	N/A
8849297	12/2013	Balasubramanian	N/A	N/A
8855620	12/2013	Sievers et al.	N/A	N/A
8856015	12/2013	Mesaros	N/A	N/A
8862751	12/2013	Faccin et al.	N/A	N/A
8863111	12/2013	Selitser et al.	N/A	N/A
8868725	12/2013	Samba	N/A	N/A
8868727	12/2013	Yumerefendi et al.	N/A	N/A
8875042	12/2013	LeJeune et al.	N/A	N/A
8880047	12/2013	Konicek et al.	N/A	N/A
8886261	12/2013	Aerrabotu	N/A	N/A
8891483	12/2013	Connelly et al.	N/A	N/A
8891524	12/2013	Chandrapal	N/A	N/A
8898748	12/2013	Burks et al.	N/A	N/A
8908516	12/2013	Tzamaloukas et al.	N/A	N/A
8909211	12/2013	Huq et al.	N/A	N/A
8914783	12/2013	Van Camp	N/A	N/A
8924469	12/2013	Raleigh et al.	N/A	N/A
8929374	12/2014	Tönsing et al.	N/A	N/A
8930238	12/2014	Coffman et al.	N/A	N/A
8930551	12/2014	Pandya et al.	N/A	N/A
8943551	12/2014	Ganapathy et al.	N/A	N/A
8948198	12/2014	Nee et al.	N/A	N/A
8948726	12/2014	Smith et al.	N/A	N/A
8949382	12/2014	Cornett et al.	N/A	N/A
8949591	12/2014	Ovsiannikov	N/A	N/A
8949597	12/2014	Reeves et al.	N/A	N/A
8955038	12/2014	Nicodemus et al.	N/A	N/A
8966018	12/2014	Bugwadia et al.	N/A	N/A
8971841	12/2014	Menezes et al.	N/A	N/A
8971912	12/2014	Chou et al.	N/A	N/A
8977284	12/2014	Reed	N/A	N/A
8995952	12/2014	Baker et al.	N/A	N/A
9002342	12/2014	Tenhunen et al.	N/A	N/A
9008653	12/2014	Sparks et al.	N/A	N/A
9009309	12/2014	Krzanowski et al.	N/A	N/A
9014059	12/2014	Richardson et al.	N/A	N/A
9014973	12/2014	Ruckart	N/A	N/A

9015331	12/2014	Lai et al.	N/A	N/A
9020467	12/2014	Zhang et al.	N/A	N/A
9026100	12/2014	Castro et al.	N/A	N/A
9030934	12/2014	Shah et al.	N/A	N/A
9032427	12/2014	Gallant et al.	N/A	N/A
9049010	12/2014	Jueneman et al.	N/A	N/A
9064275	12/2014	Lu et al.	N/A	N/A
9105031	12/2014	Shen et al.	N/A	N/A
9106414	12/2014	Laves	N/A	N/A
9107053	12/2014	Davis et al.	N/A	N/A
9111088	12/2014	Ghai et al.	N/A	N/A
9135037	12/2014	Petrescu-Prahova et al.	N/A	N/A
9137286	12/2014	Yuan	N/A	N/A
9137744	12/2014	Scherzer et al.	N/A	N/A
9143933	12/2014	Ikeda et al.	N/A	N/A
9158579	12/2014	Robles	N/A	N/A
9172553	12/2014	Dawes et al.	N/A	N/A
9173090	12/2014	Tuchman et al.	N/A	N/A
9177455	12/2014	Remer	N/A	N/A
9183524	12/2014	Carter	N/A	N/A
9204282	12/2014	Raleigh	N/A	N/A
9225847	12/2014	Daymond et al.	N/A	N/A
9252977	12/2015	Levi et al.	N/A	N/A
9262370	12/2015	Hofstaedter et al.	N/A	N/A
9265003	12/2015	Zhao et al.	N/A	N/A
9277433	12/2015	Raleigh et al.	N/A	N/A
9277445	12/2015	Raleigh et al.	N/A	N/A
9282460	12/2015	Souissi	N/A	N/A
9286469	12/2015	Kraemer et al.	N/A	N/A
9286604	12/2015	Aabye et al.	N/A	N/A
9288276	12/2015	Adamczyk et al.	N/A	N/A
9313196	12/2015	Pritchard, Jr.	N/A	N/A
9313708	12/2015	Nam et al.	N/A	N/A
9325737	12/2015	Gutowski et al.	N/A	N/A
9326173	12/2015	Luft	N/A	N/A
9344557	12/2015	Gruchala et al.	N/A	N/A
9350842	12/2015	Swanburg et al.	N/A	N/A
9363285	12/2015	Kitamura	N/A	N/A
9367680	12/2015	Mahaffey et al.	N/A	N/A
9402254	12/2015	Kneckt et al.	N/A	N/A
9408070	12/2015	Altbaum	N/A	N/A
9413546	12/2015	Meier et al.	N/A	N/A
9418381	12/2015	Ahuja et al.	N/A	N/A
9419867	12/2015	Okholm et al.	N/A	N/A
9436805	12/2015	Kravets	N/A	N/A
9438642	12/2015	Alberth, Jr. et al.	N/A	N/A
9479917	12/2015	Gota et al.	N/A	N/A
9491199	12/2015	Raleigh et al.	N/A	N/A
9497563	12/2015	Hornung et al.	N/A	N/A

9501803	12/2015	Bilac et al.	N/A	N/A
9516456	12/2015	Stephens et al.	N/A	N/A
9525992	12/2015	Rao et al.	N/A	N/A
9534861	12/2016	Kellgren	N/A	N/A
9544397	12/2016	Raleigh et al.	N/A	N/A
9557889	12/2016	Raleigh et al.	N/A	N/A
9560108	12/2016	Salkintzis	N/A	N/A
9585088	12/2016	Hanson et al.	N/A	N/A
9589117	12/2016	Ali et al.	N/A	N/A
9609459	12/2016	Raleigh	N/A	N/A
9609510	12/2016	Raleigh et al.	N/A	N/A
9609544	12/2016	Raleigh et al.	N/A	N/A
9615192	12/2016	Raleigh	N/A	N/A
9634850	12/2016	Taft et al.	N/A	N/A
9642004	12/2016	Wang et al.	N/A	N/A
9648022	12/2016	Peterka et al.	N/A	N/A
9673996	12/2016	Upadhyay et al.	N/A	N/A
9680658	12/2016	Goel et al.	N/A	N/A
9681003	12/2016	Kim et al.	N/A	N/A
9691082	12/2016	Burnett et al.	N/A	N/A
9712331	12/2016	Poh et al.	N/A	N/A
9712443	12/2016	Phaal	N/A	N/A
9712476	12/2016	Boynton et al.	N/A	N/A
9749899	12/2016	Raleigh et al.	N/A	N/A
9755842	12/2016	Raleigh et al.	N/A	N/A
9766873	12/2016	Steigleder	N/A	N/A
9852426	12/2016	Bacastow	N/A	N/A
9923790	12/2017	Patel et al.	N/A	N/A
9942796	12/2017	Raleigh	N/A	N/A
9954975	12/2017	Raleigh et al.	N/A	N/A
9986413	12/2017	Raleigh	N/A	N/A
10002332	12/2017	Spong	N/A	N/A
10021251	12/2017	Aaron et al.	N/A	N/A
10021463	12/2017	Qiu et al.	N/A	N/A
10024948	12/2017	Ganick et al.	N/A	N/A
10034220	12/2017	Silver	N/A	N/A
10057775	12/2017	Raleigh et al.	N/A	N/A
10171681	12/2018	Raleigh et al.	N/A	N/A
10171988	12/2018	Raleigh et al.	N/A	N/A
10171990	12/2018	Raleigh et al.	N/A	N/A
10178554	12/2018	Pawar et al.	N/A	N/A
10237773	12/2018	Raleigh et al.	N/A	N/A
10248996	12/2018	Raleigh	N/A	N/A
10264138	12/2018	Raleigh et al.	N/A	N/A
10285025	12/2018	Baker et al.	N/A	N/A
10321515	12/2018	Shen et al.	N/A	N/A
10326800	12/2018	Raleigh et al.	N/A	N/A
10368214	12/2018	Macaluso	N/A	N/A
10395216	12/2018	Coffing	N/A	N/A
10410184	12/2018	Green et al.	N/A	N/A

10462627	12/2018	Raleigh et al.	N/A	N/A
10492102	12/2018	Raleigh et al.	N/A	N/A
10521781	12/2018	Singfield	N/A	N/A
10523726	12/2018	Pantos et al.	N/A	N/A
10536983	12/2019	Raleigh et al.	N/A	N/A
10567930	12/2019	Silver	N/A	N/A
10582375	12/2019	Raleigh	N/A	N/A
10616818	12/2019	Silver	N/A	N/A
10771980	12/2019	Raleigh et al.	N/A	N/A
10779177	12/2019	Raleigh	N/A	N/A
10783581	12/2019	Raleigh	N/A	N/A
10798252	12/2019	Raleigh et al.	N/A	N/A
10798254	12/2019	Raleigh et al.	N/A	N/A
10798558	12/2019	Raleigh et al.	N/A	N/A
10834577	12/2019	Raleigh et al.	N/A	N/A
10841839	12/2019	Raleigh et al.	N/A	N/A
11206516	12/2020	Baker et al.	N/A	N/A
11271629	12/2021	Um et al.	N/A	N/A
11271961	12/2021	Berger et al.	N/A	N/A
2001/0048738	12/2000	Baniak et al.	N/A	N/A
2001/0053694	12/2000	Igarashi et al.	N/A	N/A
2002/0013844	12/2001	Garrett et al.	N/A	N/A
2002/0022472	12/2001	Watler et al.	N/A	N/A
2002/0022483	12/2001	Thompson et al.	N/A	N/A
2002/0049074	12/2001	Eisinger et al.	N/A	N/A
2002/0085516	12/2001	Bridgelall	N/A	N/A
2002/0099848	12/2001	Lee	N/A	N/A
2002/0116338	12/2001	Gonthier et al.	N/A	N/A
2002/0120370	12/2001	Parupudi et al.	N/A	N/A
2002/0120540	12/2001	Kende et al.	N/A	N/A
2002/0131397	12/2001	Patel et al.	N/A	N/A
2002/0131404	12/2001	Mehta et al.	N/A	N/A
2002/0138599	12/2001	Dilman et al.	N/A	N/A
2002/0138601	12/2001	Piponius et al.	N/A	N/A
2002/0152319	12/2001	Amin et al.	N/A	N/A
2002/0154751	12/2001	Thompson et al.	N/A	N/A
2002/0161601	12/2001	Nauer et al.	N/A	N/A
2002/0164983	12/2001	Raviv et al.	N/A	N/A
2002/0176377	12/2001	Hamilton	N/A	N/A
2002/0188732	12/2001	Buckman et al.	N/A	N/A
2002/0191573	12/2001	Whitehill et al.	N/A	N/A
2002/0199001	12/2001	Wenocur et al.	N/A	N/A
2003/0004937	12/2002	Salmenkaita et al.	N/A	N/A
2003/0005112	12/2002	Krautkremer	N/A	N/A
2003/0013434	12/2002	Rosenberg et al.	N/A	N/A
2003/0018524	12/2002	Fishman et al.	N/A	N/A
2003/0028623	12/2002	Hennessey et al.	N/A	N/A
2003/0046396	12/2002	Richter et al.	N/A	N/A
2003/0050070	12/2002	Mashinsky et al.	N/A	N/A
2003/0050837	12/2002	Kim	N/A	N/A

2003/0060189	12/2002	Minear et al.	N/A	N/A
2003/0084321	12/2002	Tarquini et al.	N/A	N/A
2003/0088671	12/2002	Klinker et al.	N/A	N/A
2003/0133408	12/2002	Cheng et al.	N/A	N/A
2003/0134650	12/2002	Sundar et al.	N/A	N/A
2003/0159030	12/2002	Evans	N/A	N/A
2003/0161265	12/2002	Cao et al.	N/A	N/A
2003/0171112	12/2002	Lupper et al.	N/A	N/A
2003/0182420	12/2002	Jones et al.	N/A	N/A
2003/0182435	12/2002	Redlich et al.	N/A	N/A
2003/0184793	12/2002	Pineau	N/A	N/A
2003/0188006	12/2002	Bard	N/A	N/A
2003/0188117	12/2002	Yoshino et al.	N/A	N/A
2003/0191646	12/2002	D'Avello et al.	N/A	N/A
2003/0206533	12/2002	Charas	N/A	N/A
2003/0220984	12/2002	Jones et al.	N/A	N/A
2003/0224781	12/2002	Milford et al.	N/A	N/A
2003/0229900	12/2002	Reisman	N/A	N/A
2003/0233332	12/2002	Keeler et al.	N/A	N/A
2003/0236745	12/2002	Hartsell et al.	N/A	N/A
2004/0019539	12/2003	Raman et al.	N/A	N/A
2004/0019564	12/2003	Goldthwaite et al.	N/A	N/A
2004/0021697	12/2003	Beaton et al.	N/A	N/A
2004/0024756	12/2003	Rickard	N/A	N/A
2004/0030705	12/2003	Bowman-Amuah	N/A	N/A
2004/0039792	12/2003	Nakanishi	N/A	N/A
2004/0044623	12/2003	Wake et al.	N/A	N/A
2004/0047358	12/2003	Chen et al.	N/A	N/A
2004/0054779	12/2003	Takeshima et al.	N/A	N/A
2004/0073672	12/2003	Fascenda	N/A	N/A
2004/0082346	12/2003	Skytt et al.	N/A	N/A
2004/0098610	12/2003	Hrastar	N/A	N/A
2004/0098715	12/2003	Aghera et al.	N/A	N/A
2004/0102182	12/2003	Reith et al.	N/A	N/A
2004/0103193	12/2003	Pandya et al.	N/A	N/A
2004/0107360	12/2003	Herrmann et al.	N/A	N/A
2004/0114553	12/2003	Jiang et al.	N/A	N/A
2004/0116140	12/2003	Babbar et al.	N/A	N/A
2004/0123153	12/2003	Wright et al.	N/A	N/A
2004/0127200	12/2003	Shaw et al.	N/A	N/A
2004/0127208	12/2003	Nair et al.	N/A	N/A
2004/0127256	12/2003	Goldthwaite et al.	N/A	N/A
2004/0132427	12/2003	Lee et al.	N/A	N/A
2004/0133668	12/2003	Nicholas, III	N/A	N/A
2004/0137890	12/2003	Kalke	N/A	N/A
2004/0165596	12/2003	Garcia et al.	N/A	N/A
2004/0167958	12/2003	Stewart et al.	N/A	N/A
2004/0168052	12/2003	Clisham et al.	N/A	N/A
2004/0170191	12/2003	Guo et al.	N/A	N/A
2004/0176104	12/2003	Arcens	N/A	N/A

2004/0198331	12/2003	Coward et al.	N/A	N/A
2004/0203755	12/2003	Brunet et al.	N/A	N/A
2004/0203833	12/2003	Rathunde et al.	N/A	N/A
2004/0224668	12/2003	Shell et al.	N/A	N/A
2004/0225561	12/2003	Hertzberg et al.	N/A	N/A
2004/0225898	12/2003	Frost et al.	N/A	N/A
2004/0236547	12/2003	Rappaport et al.	N/A	N/A
2004/0243680	12/2003	Mayer	N/A	N/A
2004/0243992	12/2003	Gustafson et al.	N/A	N/A
2004/0249918	12/2003	Sunshine	N/A	N/A
2004/0255145	12/2003	Chow	N/A	N/A
2004/0259534	12/2003	Chaudhari et al.	N/A	N/A
2004/0260766	12/2003	Barros et al.	N/A	N/A
2004/0267872	12/2003	Serdy et al.	N/A	N/A
2004/0268351	12/2003	Mogensen et al.	N/A	N/A
2005/0007993	12/2004	Chambers et al.	N/A	N/A
2005/0009499	12/2004	Koster	N/A	N/A
2005/0021995	12/2004	Lal et al.	N/A	N/A
2005/0037740	12/2004	Smith et al.	N/A	N/A
2005/0041617	12/2004	Huotari et al.	N/A	N/A
2005/0048950	12/2004	Morper	N/A	N/A
2005/0055291	12/2004	Bevente et al.	N/A	N/A
2005/0055309	12/2004	Williams et al.	N/A	N/A
2005/0055595	12/2004	Frazer et al.	N/A	N/A
2005/0060266	12/2004	Demello et al.	N/A	N/A
2005/0060525	12/2004	Schwartz et al.	N/A	N/A
2005/0075115	12/2004	Corneille et al.	N/A	N/A
2005/0079863	12/2004	Macaluso	455/414.3	H04M 15/80
2005/0091505	12/2004	Riley et al.	N/A	N/A
2005/0096024	12/2004	Bicker et al.	N/A	N/A
2005/0097516	12/2004	Donnelly et al.	N/A	N/A
2005/0107091	12/2004	Vannithamby et al.	N/A	N/A
2005/0108075	12/2004	Douglis et al.	N/A	N/A
2005/0111463	12/2004	Leung et al.	N/A	N/A
2005/0128967	12/2004	Scobbie	N/A	N/A
2005/0135264	12/2004	Popoff et al.	N/A	N/A
2005/0163320	12/2004	Brown et al.	N/A	N/A
2005/0166043	12/2004	Zhang et al.	N/A	N/A
2005/0177515	12/2004	Kalavade et al.	N/A	N/A
2005/0183143	12/2004	Anderholm et al.	N/A	N/A
2005/0186948	12/2004	Gallagher et al.	N/A	N/A
2005/0198377	12/2004	Ferguson et al.	N/A	N/A
2005/0216421	12/2004	Barry et al.	N/A	N/A
2005/0226178	12/2004	Forand et al.	N/A	N/A
2005/0228985	12/2004	Ylikoski et al.	N/A	N/A
2005/0238046	12/2004	Hassan et al.	N/A	N/A
2005/0239447	12/2004	Holzman et al.	N/A	N/A
2005/0245241	12/2004	Durand et al.	N/A	N/A
2005/0246282	12/2004	Naslund et al.	N/A	N/A

2005/0250508	12/2004	Guo et al.	N/A	N/A
2005/0250536	12/2004	Deng et al.	N/A	N/A
2005/0254435	12/2004	Moakley et al.	N/A	N/A
2005/0266825	12/2004	Clayton	N/A	N/A
2005/0266880	12/2004	Gupta	N/A	N/A
2005/0286476	12/2004	Crosswy et al.	N/A	N/A
2006/0014519	12/2005	Marsh et al.	N/A	N/A
2006/0019632	12/2005	Cunningham et al.	N/A	N/A
2006/0020787	12/2005	Choyi et al.	N/A	N/A
2006/0026679	12/2005	Zakas	N/A	N/A
2006/0030306	12/2005	Kuhn	N/A	N/A
2006/0034256	12/2005	Addagatla et al.	N/A	N/A
2006/0035631	12/2005	White et al.	N/A	N/A
2006/0039354	12/2005	Rao et al.	N/A	N/A
2006/0039364	12/2005	Wright	N/A	N/A
2006/0040642	12/2005	Boris et al.	N/A	N/A
2006/0045245	12/2005	Aaron et al.	N/A	N/A
2006/0048223	12/2005	Lee et al.	N/A	N/A
2006/0068796	12/2005	Millen et al.	N/A	N/A
2006/0072451	12/2005	Ross	N/A	N/A
2006/0072550	12/2005	Davis et al.	N/A	N/A
2006/0072646	12/2005	Feher	N/A	N/A
2006/0075506	12/2005	Sanda et al.	N/A	N/A
2006/0085543	12/2005	Hrastar et al.	N/A	N/A
2006/0093107	12/2005	Chien	N/A	N/A
2006/0095517	12/2005	O'Connor et al.	N/A	N/A
2006/0098627	12/2005	Karaoguz et al.	N/A	N/A
2006/0099970	12/2005	Morgan et al.	N/A	N/A
2006/0101507	12/2005	Camenisch	N/A	N/A
2006/0112016	12/2005	Ishibashi	N/A	N/A
2006/0114821	12/2005	Willey et al.	N/A	N/A
2006/0114832	12/2005	Hamilton et al.	N/A	N/A
2006/0126562	12/2005	Liu	N/A	N/A
2006/0135144	12/2005	Jothipragasam	N/A	N/A
2006/0136882	12/2005	Noonan et al.	N/A	N/A
2006/0143066	12/2005	Calabria	N/A	N/A
2006/0143098	12/2005	Lazaridis	N/A	N/A
2006/0153122	12/2005	Hinman et al.	N/A	N/A
2006/0156398	12/2005	Ross et al.	N/A	N/A
2006/0160536	12/2005	Chou	N/A	N/A
2006/0165060	12/2005	Dua	N/A	N/A
2006/0168128	12/2005	Sistla et al.	N/A	N/A
2006/0173959	12/2005	Mckelvie et al.	N/A	N/A
2006/0174035	12/2005	Tufail	N/A	N/A
2006/0178917	12/2005	Merriam et al.	N/A	N/A
2006/0178918	12/2005	Mikurak	N/A	N/A
2006/0178943	12/2005	Rollinson et al.	N/A	N/A
2006/0182137	12/2005	Zhou et al.	N/A	N/A
2006/0183461	12/2005	Pearce	N/A	N/A
2006/0183462	12/2005	Kolehmainen	N/A	N/A

2006/0190314	12/2005	Hernandez	N/A	N/A
2006/0190987	12/2005	Ohta et al.	N/A	N/A
2006/0193280	12/2005	Lee et al.	N/A	N/A
2006/0199608	12/2005	Dunn et al.	N/A	N/A
2006/0200663	12/2005	Thornton	N/A	N/A
2006/0206709	12/2005	Labrou et al.	N/A	N/A
2006/0206904	12/2005	Watkins et al.	N/A	N/A
2006/0218395	12/2005	Maes	N/A	N/A
2006/0221829	12/2005	Holmstrom et al.	N/A	N/A
2006/0233108	12/2005	Krishnan	N/A	N/A
2006/0233166	12/2005	Bou-Diab et al.	N/A	N/A
2006/0236095	12/2005	Smith et al.	N/A	N/A
2006/0242685	12/2005	Heard et al.	N/A	N/A
2006/0258341	12/2005	Miller et al.	N/A	N/A
2006/0274706	12/2005	Chen et al.	N/A	N/A
2006/0277590	12/2005	Limont et al.	N/A	N/A
2006/0291419	12/2005	McConnell et al.	N/A	N/A
2006/0291477	12/2005	Croak et al.	N/A	N/A
2007/0005795	12/2006	Gonzalez	N/A	N/A
2007/0010248	12/2006	Dravida et al.	N/A	N/A
2007/0019670	12/2006	Falardeau	N/A	N/A
2007/0022289	12/2006	Alt et al.	N/A	N/A
2007/0025301	12/2006	Petersson et al.	N/A	N/A
2007/0033194	12/2006	Srinivas et al.	N/A	N/A
2007/0033197	12/2006	Scherzer et al.	N/A	N/A
2007/0035390	12/2006	Thomas et al.	N/A	N/A
2007/0036312	12/2006	Cai et al.	N/A	N/A
2007/0038763	12/2006	Oestvall	N/A	N/A
2007/0055694	12/2006	Ruge et al.	N/A	N/A
2007/0060200	12/2006	Boris et al.	N/A	N/A
2007/0061243	12/2006	Ramer et al.	N/A	N/A
2007/0061800	12/2006	Cheng et al.	N/A	N/A
2007/0061878	12/2006	Hagiu et al.	N/A	N/A
2007/0073899	12/2006	Judge et al.	N/A	N/A
2007/0076616	12/2006	Ngo et al.	N/A	N/A
2007/0093243	12/2006	Kapadekar et al.	N/A	N/A
2007/0100981	12/2006	Adamczyk et al.	N/A	N/A
2007/0101426	12/2006	Lee et al.	N/A	N/A
2007/0104126	12/2006	Calhoun et al.	N/A	N/A
2007/0104169	12/2006	Polson	N/A	N/A
2007/0109983	12/2006	Shankar et al.	N/A	N/A
2007/0111740	12/2006	Wandel	N/A	N/A
2007/0124077	12/2006	Hedlund	N/A	N/A
2007/0130283	12/2006	Klein et al.	N/A	N/A
2007/0130315	12/2006	Friend et al.	N/A	N/A
2007/0140113	12/2006	Gemelos	N/A	N/A
2007/0140145	12/2006	Kumar et al.	N/A	N/A
2007/0140275	12/2006	Bowman et al.	N/A	N/A
2007/0143824	12/2006	Shahbazi	N/A	N/A
2007/0147317	12/2006	Smith et al.	N/A	N/A

2007/0147324	12/2006	McGary	N/A	N/A
2007/0149252	12/2006	Jobs et al.	N/A	N/A
2007/0155365	12/2006	Kim et al.	N/A	N/A
2007/0157203	12/2006	Lim	N/A	N/A
2007/0165630	12/2006	Rasanen et al.	N/A	N/A
2007/0168499	12/2006	Chu	N/A	N/A
2007/0171856	12/2006	Bruce et al.	N/A	N/A
2007/0173283	12/2006	Livet et al.	N/A	N/A
2007/0174490	12/2006	Choi et al.	N/A	N/A
2007/0191006	12/2006	Carpenter	N/A	N/A
2007/0192460	12/2006	Choi et al.	N/A	N/A
2007/0198656	12/2006	Mazzaferri et al.	N/A	N/A
2007/0201502	12/2006	Abramson	N/A	N/A
2007/0213054	12/2006	Han	N/A	N/A
2007/0220251	12/2006	Rosenberg et al.	N/A	N/A
2007/0226225	12/2006	Yiu et al.	N/A	N/A
2007/0226775	12/2006	Andreasen et al.	N/A	N/A
2007/0234402	12/2006	Khosravi et al.	N/A	N/A
2007/0242619	12/2006	Murakami et al.	N/A	N/A
2007/0242659	12/2006	Cantu et al.	N/A	N/A
2007/0243862	12/2006	Coskun et al.	N/A	N/A
2007/0244965	12/2006	Dowling	N/A	N/A
2007/0248100	12/2006	Zuberi et al.	N/A	N/A
2007/0254646	12/2006	Sokondar	N/A	N/A
2007/0254675	12/2006	Zorlu Ozer et al.	N/A	N/A
2007/0255769	12/2006	Agrawal et al.	N/A	N/A
2007/0255797	12/2006	Dunn et al.	N/A	N/A
2007/0255848	12/2006	Sewall et al.	N/A	N/A
2007/0255942	12/2006	Weller et al.	N/A	N/A
2007/0256128	12/2006	Jung et al.	N/A	N/A
2007/0257767	12/2006	Beeson	N/A	N/A
2007/0259656	12/2006	Jeong	N/A	N/A
2007/0259673	12/2006	Willars et al.	N/A	N/A
2007/0263558	12/2006	Salomone	N/A	N/A
2007/0265003	12/2006	Kezys et al.	N/A	N/A
2007/0266422	12/2006	Germano et al.	N/A	N/A
2007/0271598	12/2006	Chen et al.	N/A	N/A
2007/0274327	12/2006	Kaarela et al.	N/A	N/A
2007/0280453	12/2006	Kelley	N/A	N/A
2007/0282896	12/2006	Wydroug et al.	N/A	N/A
2007/0293191	12/2006	Mir et al.	N/A	N/A
2007/0294395	12/2006	Strub et al.	N/A	N/A
2007/0294410	12/2006	Pandya et al.	N/A	N/A
2007/0297378	12/2006	Poyhonen et al.	N/A	N/A
2007/0298764	12/2006	Clayton	N/A	N/A
2007/0299965	12/2006	Nieh et al.	N/A	N/A
2007/0300252	12/2006	Acharya et al.	N/A	N/A
2008/0005285	12/2007	Robinson et al.	N/A	N/A
2008/0005561	12/2007	Brown et al.	N/A	N/A
2008/0010379	12/2007	Zhao	N/A	N/A

2008/0010452	12/2007	Holtzman et al.	N/A	N/A
2008/0018494	12/2007	Waite et al.	N/A	N/A
2008/0020738	12/2007	Ho et al.	N/A	N/A
2008/0022354	12/2007	Grewal et al.	N/A	N/A
2008/0025230	12/2007	Patel et al.	N/A	N/A
2008/0032715	12/2007	Jia et al.	N/A	N/A
2008/0034063	12/2007	Yee	N/A	N/A
2008/0034419	12/2007	Mullick et al.	N/A	N/A
2008/0039102	12/2007	Sewall et al.	N/A	N/A
2008/0046965	12/2007	Wright et al.	N/A	N/A
2008/0049630	12/2007	Kozisek et al.	N/A	N/A
2008/0050715	12/2007	Golczewski et al.	N/A	N/A
2008/0051076	12/2007	O'Shaughnessy et al.	N/A	N/A
2008/0052387	12/2007	Heinz et al.	N/A	N/A
2008/0056273	12/2007	Pelletier et al.	N/A	N/A
2008/0057894	12/2007	Aleksic et al.	N/A	N/A
2008/0059474	12/2007	Lim	N/A	N/A
2008/0059743	12/2007	Bychkov et al.	N/A	N/A
2008/0060066	12/2007	Wynn et al.	N/A	N/A
2008/0062900	12/2007	Rao	N/A	N/A
2008/0064367	12/2007	Nath et al.	N/A	N/A
2008/0066149	12/2007	Lim	N/A	N/A
2008/0066150	12/2007	Lim	N/A	N/A
2008/0066181	12/2007	Haveson et al.	N/A	N/A
2008/0070550	12/2007	Hose	N/A	N/A
2008/0077705	12/2007	Li et al.	N/A	N/A
2008/0080457	12/2007	Cole	N/A	N/A
2008/0080458	12/2007	Cole	N/A	N/A
2008/0081606	12/2007	Cole	N/A	N/A
2008/0082643	12/2007	Storrie et al.	N/A	N/A
2008/0083013	12/2007	Soliman et al.	N/A	N/A
2008/0085707	12/2007	Fadell	N/A	N/A
2008/0089295	12/2007	Keeler et al.	N/A	N/A
2008/0089303	12/2007	Wirtanen et al.	N/A	N/A
2008/0095339	12/2007	Elliott et al.	N/A	N/A
2008/0096559	12/2007	Phillips et al.	N/A	N/A
2008/0098062	12/2007	Balia	N/A	N/A
2008/0101291	12/2007	Jiang et al.	N/A	N/A
2008/0101293	12/2007	Woo	N/A	N/A
2008/0109679	12/2007	Wright et al.	N/A	N/A
2008/0120129	12/2007	Seubert et al.	N/A	N/A
2008/0120174	12/2007	Li	N/A	N/A
2008/0120668	12/2007	Yau	N/A	N/A
2008/0120688	12/2007	Qiu et al.	N/A	N/A
2008/0124330	12/2007	Nakano et al.	N/A	N/A
2008/0125079	12/2007	O'Neil et al.	N/A	N/A
2008/0126287	12/2007	Cox et al.	N/A	N/A
2008/0127304	12/2007	Ginter et al.	N/A	N/A
2008/0130534	12/2007	Tomioka	N/A	N/A
2008/0130656	12/2007	Kim et al.	N/A	N/A

2008/0132201	12/2007	Karlberg	N/A	N/A
2008/0132268	12/2007	Choi-Grogan et al.	N/A	N/A
2008/0134330	12/2007	Kapoor et al.	N/A	N/A
2008/0139210	12/2007	Gisby et al.	N/A	N/A
2008/0146268	12/2007	Gandhi et al.	N/A	N/A
2008/0147454	12/2007	Walker et al.	N/A	N/A
2008/0148402	12/2007	Bogineni et al.	N/A	N/A
2008/0160958	12/2007	Abichandani et al.	N/A	N/A
2008/0161041	12/2007	Pernu	N/A	N/A
2008/0162637	12/2007	Adamczyk et al.	N/A	N/A
2008/0162704	12/2007	Poplett et al.	N/A	N/A
2008/0164304	12/2007	Narasimhan et al.	N/A	N/A
2008/0166993	12/2007	Gautier et al.	N/A	N/A
2008/0167027	12/2007	Gautier et al.	N/A	N/A
2008/0167033	12/2007	Beckers	N/A	N/A
2008/0168275	12/2007	DeAtley et al.	N/A	N/A
2008/0168523	12/2007	Ansari et al.	N/A	N/A
2008/0177998	12/2007	Apsangi et al.	N/A	N/A
2008/0178300	12/2007	Brown et al.	N/A	N/A
2008/0181117	12/2007	Acke et al.	N/A	N/A
2008/0181208	12/2007	Maes	N/A	N/A
2008/0183811	12/2007	Kotras et al.	N/A	N/A
2008/0183812	12/2007	Paul et al.	N/A	N/A
2008/0184127	12/2007	Rafey et al.	N/A	N/A
2008/0189760	12/2007	Rosenberg et al.	N/A	N/A
2008/0201266	12/2007	Chua et al.	N/A	N/A
2008/0207167	12/2007	Bugenhagen	N/A	N/A
2008/0212470	12/2007	Castaneda et al.	N/A	N/A
2008/0212751	12/2007	Chung	N/A	N/A
2008/0219268	12/2007	Dennison	N/A	N/A
2008/0221951	12/2007	Stanforth et al.	N/A	N/A
2008/0222692	12/2007	Andersson et al.	N/A	N/A
2008/0225748	12/2007	Khemani et al.	N/A	N/A
2008/0229385	12/2007	Feder et al.	N/A	N/A
2008/0229388	12/2007	Maes	N/A	N/A
2008/0235511	12/2007	O'Brien et al.	N/A	N/A
2008/0240373	12/2007	Wilhelm	N/A	N/A
2008/0242290	12/2007	Bhatia et al.	N/A	N/A
2008/0250053	12/2007	Aaltonen et al.	N/A	N/A
2008/0256593	12/2007	Mnberg et al.	N/A	N/A
2008/0259924	12/2007	Gooch et al.	N/A	N/A
2008/0262798	12/2007	Kim et al.	N/A	N/A
2008/0263348	12/2007	Zaltsman et al.	N/A	N/A
2008/0268813	12/2007	Maes	N/A	N/A
2008/0270212	12/2007	Blight et al.	N/A	N/A
2008/0279216	12/2007	Sharif-Ahmadi et al.	N/A	N/A
2008/0280656	12/2007	Gonikberg et al.	N/A	N/A
2008/0282319	12/2007	Fontijn et al.	N/A	N/A
2008/0291872	12/2007	Henriksson	N/A	N/A
2008/0293395	12/2007	Mathews et al.	N/A	N/A

2008/0298230	12/2007	Luft et al.	N/A	N/A
2008/0305793	12/2007	Gallagher et al.	N/A	N/A
2008/0311885	12/2007	Dawson et al.	N/A	N/A
2008/0311897	12/2007	Segal	N/A	N/A
2008/0313315	12/2007	Karaoguz et al.	N/A	N/A
2008/0313730	12/2007	Iftimie et al.	N/A	N/A
2008/0316923	12/2007	Fedders et al.	N/A	N/A
2008/0316983	12/2007	Daigle	N/A	N/A
2008/0318547	12/2007	Ballou et al.	N/A	N/A
2008/0318550	12/2007	DeAtley	N/A	N/A
2008/0319879	12/2007	Carroll et al.	N/A	N/A
2008/0320497	12/2007	Tarkoma et al.	N/A	N/A
2009/0005000	12/2008	Baker et al.	N/A	N/A
2009/0005005	12/2008	Forstall et al.	N/A	N/A
2009/0006116	12/2008	Baker et al.	N/A	N/A
2009/0006200	12/2008	Baker et al.	N/A	N/A
2009/0006229	12/2008	Sweeney et al.	N/A	N/A
2009/0013157	12/2008	Beaule	N/A	N/A
2009/0016310	12/2008	Rasal	N/A	N/A
2009/0017809	12/2008	Jethi et al.	N/A	N/A
2009/0019022	12/2008	Schallert et al.	N/A	N/A
2009/0036111	12/2008	Danford et al.	N/A	N/A
2009/0042536	12/2008	Bernard et al.	N/A	N/A
2009/0044185	12/2008	Krivopaltsev	N/A	N/A
2009/0046707	12/2008	Smires et al.	N/A	N/A
2009/0046723	12/2008	Rahman et al.	N/A	N/A
2009/0047989	12/2008	Harmon et al.	N/A	N/A
2009/0048913	12/2008	Shenfield et al.	N/A	N/A
2009/0049156	12/2008	Aronsson et al.	N/A	N/A
2009/0049518	12/2008	Roman et al.	N/A	N/A
2009/0054030	12/2008	Golds	N/A	N/A
2009/0054061	12/2008	Dawson et al.	N/A	N/A
2009/0065571	12/2008	Jain	N/A	N/A
2009/0066999	12/2008	Ito	N/A	N/A
2009/0067372	12/2008	Shah et al.	N/A	N/A
2009/0068984	12/2008	Burnett	N/A	N/A
2009/0070379	12/2008	Rappaport	N/A	N/A
2009/0077622	12/2008	Baum et al.	N/A	N/A
2009/0079699	12/2008	Sun	N/A	N/A
2009/0093247	12/2008	Srinivasan	N/A	N/A
2009/0109898	12/2008	Adams et al.	N/A	N/A
2009/0113514	12/2008	Hu	N/A	N/A
2009/0119773	12/2008	D'Amore et al.	N/A	N/A
2009/0125619	12/2008	Antani	N/A	N/A
2009/0132860	12/2008	Liu et al.	N/A	N/A
2009/0149154	12/2008	Bhasin et al.	N/A	N/A
2009/0154348	12/2008	Newman	N/A	N/A
2009/0157792	12/2008	Fiatal	N/A	N/A
2009/0163173	12/2008	Williams	N/A	N/A
2009/0170554	12/2008	Want et al.	N/A	N/A

2009/0172077	12/2008	Roxburgh et al.	N/A	N/A
2009/0180391	12/2008	Petersen et al.	N/A	N/A
2009/0181662	12/2008	Fleischman et al.	N/A	N/A
2009/0197585	12/2008	Aaron	N/A	N/A
2009/0197612	12/2008	Kiiskinen	N/A	N/A
2009/0203352	12/2008	Fordon et al.	N/A	N/A
2009/0207817	12/2008	Montemurro et al.	N/A	N/A
2009/0210537	12/2008	Irwin et al.	N/A	N/A
2009/0217065	12/2008	Araujo, Jr.	N/A	N/A
2009/0217364	12/2008	Salmela et al.	N/A	N/A
2009/0219170	12/2008	Clark et al.	N/A	N/A
2009/0248883	12/2008	Suryanarayana et al.	N/A	N/A
2009/0254857	12/2008	Romine et al.	N/A	N/A
2009/0257379	12/2008	Robinson et al.	N/A	N/A
2009/0261783	12/2008	Gonzales et al.	N/A	N/A
2009/0262715	12/2008	Juang	N/A	N/A
2009/0271514	12/2008	Thomas et al.	N/A	N/A
2009/0282127	12/2008	Leblanc et al.	N/A	N/A
2009/0286507	12/2008	O'Neil et al.	N/A	N/A
2009/0287921	12/2008	Zhu et al.	N/A	N/A
2009/0288140	12/2008	Huber et al.	N/A	N/A
2009/0291665	12/2008	Gaskarth et al.	N/A	N/A
2009/0292815	12/2008	Gao et al.	N/A	N/A
2009/0293378	12/2008	Benson	N/A	N/A
2009/0299857	12/2008	Brubaker	N/A	N/A
2009/0307696	12/2008	Vals et al.	N/A	N/A
2009/0307746	12/2008	Di et al.	N/A	N/A
2009/0315735	12/2008	Bhavani et al.	N/A	N/A
2009/0318124	12/2008	Haughn	N/A	N/A
2009/0320110	12/2008	Nicolson et al.	N/A	N/A
2010/0010873	12/2009	Moreau	N/A	N/A
2010/0017506	12/2009	Fadell	N/A	N/A
2010/0020822	12/2009	Zerillo et al.	N/A	N/A
2010/0027469	12/2009	Gurajala et al.	N/A	N/A
2010/0027525	12/2009	Zhu	N/A	N/A
2010/0027559	12/2009	Lin et al.	N/A	N/A
2010/0030890	12/2009	Dutta et al.	N/A	N/A
2010/0041364	12/2009	Lott et al.	N/A	N/A
2010/0041365	12/2009	Lott et al.	N/A	N/A
2010/0041391	12/2009	Spivey et al.	N/A	N/A
2010/0042675	12/2009	Fujii	N/A	N/A
2010/0043068	12/2009	Varadhan et al.	N/A	N/A
2010/0046373	12/2009	Smith et al.	N/A	N/A
2010/0069074	12/2009	Kodialam et al.	N/A	N/A
2010/0071053	12/2009	Ansari et al.	N/A	N/A
2010/0075666	12/2009	Garner	N/A	N/A
2010/0077035	12/2009	Li et al.	N/A	N/A
2010/0080202	12/2009	Hanson	N/A	N/A
2010/0082431	12/2009	Ramer et al.	N/A	N/A
2010/0088387	12/2009	Calamera	N/A	N/A

2010/0103820	12/2009	Fuller et al.	N/A	N/A
2010/0105378	12/2009	Shi et al.	N/A	N/A
2010/0113020	12/2009	Subramanian et al.	N/A	N/A
2010/0115048	12/2009	Scahill	N/A	N/A
2010/0121744	12/2009	Belz et al.	N/A	N/A
2010/0131584	12/2009	Johnson	N/A	N/A
2010/0142478	12/2009	Forssell et al.	N/A	N/A
2010/0144310	12/2009	Bedingfield	N/A	N/A
2010/0151866	12/2009	Karpov et al.	N/A	N/A
2010/0153781	12/2009	Hanna	N/A	N/A
2010/0167696	12/2009	Smith et al.	N/A	N/A
2010/0183132	12/2009	Satyavolu et al.	N/A	N/A
2010/0188975	12/2009	Raleigh	N/A	N/A
2010/0188990	12/2009	Raleigh	N/A	N/A
2010/0188992	12/2009	Raleigh	N/A	N/A
2010/0188994	12/2009	Raleigh	N/A	N/A
2010/0190469	12/2009	Vanderveen et al.	N/A	N/A
2010/0191576	12/2009	Raleigh	N/A	N/A
2010/0191612	12/2009	Raleigh	N/A	N/A
2010/0191846	12/2009	Raleigh	N/A	N/A
2010/0192170	12/2009	Raleigh	N/A	N/A
2010/0192212	12/2009	Raleigh	N/A	N/A
2010/0195503	12/2009	Raleigh	N/A	N/A
2010/0197268	12/2009	Raleigh	N/A	N/A
2010/0198698	12/2009	Raleigh et al.	N/A	N/A
2010/0198939	12/2009	Raleigh	N/A	N/A
2010/0199325	12/2009	Raleigh	N/A	N/A
2010/0227632	12/2009	Bell et al.	N/A	N/A
2010/0235329	12/2009	Koren et al.	N/A	N/A
2010/0241544	12/2009	Benson et al.	N/A	N/A
2010/0248719	12/2009	Scholaert	N/A	N/A
2010/0254387	12/2009	Trinh et al.	N/A	N/A
2010/0280878	12/2009	Wilson et al.	N/A	N/A
2010/0284327	12/2009	Miklos	N/A	N/A
2010/0284388	12/2009	Fantini et al.	N/A	N/A
2010/0287599	12/2009	He et al.	N/A	N/A
2010/0311402	12/2009	Srinivasan et al.	N/A	N/A
2010/0318652	12/2009	Samba	N/A	N/A
2010/0322071	12/2009	Avdanin et al.	N/A	N/A
2010/0325420	12/2009	Kanekar	N/A	N/A
2011/0004917	12/2010	Saisa et al.	N/A	N/A
2011/0013569	12/2010	Scherzer et al.	N/A	N/A
2011/0019574	12/2010	Malomsoky et al.	N/A	N/A
2011/0071854	12/2010	Medeiros et al.	N/A	N/A
2011/0081881	12/2010	Baker et al.	N/A	N/A
2011/0082790	12/2010	Baker et al.	N/A	N/A
2011/0110309	12/2010	Bennett	N/A	N/A
2011/0126141	12/2010	King et al.	N/A	N/A
2011/0145920	12/2010	Mahaffey et al.	N/A	N/A
2011/0159818	12/2010	Scherzer et al.	N/A	N/A

2011/0173678	12/2010	Kaippallimalil et al.	N/A	N/A
2011/0177811	12/2010	Heckman et al.	N/A	N/A
2011/0182220	12/2010	Black et al.	N/A	N/A
2011/0185202	12/2010	Black et al.	N/A	N/A
2011/0195700	12/2010	Kukuchka et al.	N/A	N/A
2011/0238545	12/2010	Fanaian et al.	N/A	N/A
2011/0241624	12/2010	Park et al.	N/A	N/A
2011/0244837	12/2010	Murata et al.	N/A	N/A
2011/0249668	12/2010	Milligan et al.	N/A	N/A
2011/0252430	12/2010	Chapman et al.	N/A	N/A
2011/0264923	12/2010	Kocher et al.	N/A	N/A
2011/0277019	12/2010	Pritchard, Jr.	N/A	N/A
2011/0294502	12/2010	Oerton	N/A	N/A
2012/0011017	12/2011	Wolcott et al.	N/A	N/A
2012/0020296	12/2011	Scherzer et al.	N/A	N/A
2012/0029718	12/2011	Davis	N/A	N/A
2012/0101952	12/2011	Raleigh et al.	N/A	N/A
2012/0108225	12/2011	Luna et al.	N/A	N/A
2012/0122514	12/2011	Cheng et al.	N/A	N/A
2012/0144025	12/2011	Melander et al.	N/A	N/A
2012/0155296	12/2011	Kashanian	N/A	N/A
2012/0166364	12/2011	Ahmad et al.	N/A	N/A
2012/0166604	12/2011	Fortier et al.	N/A	N/A
2012/0195200	12/2011	Regan	N/A	N/A
2012/0196644	12/2011	Scherzer et al.	N/A	N/A
2012/0215682	12/2011	Lent et al.	N/A	N/A
2012/0238287	12/2011	Scherzer	N/A	N/A
2012/0330792	12/2011	Kashanian	N/A	N/A
2013/0024914	12/2012	Ahmed et al.	N/A	N/A
2013/0029653	12/2012	Baker et al.	N/A	N/A
2013/0030960	12/2012	Kashanian	N/A	N/A
2013/0058274	12/2012	Scherzer et al.	N/A	N/A
2013/0065555	12/2012	Baker et al.	N/A	N/A
2013/0072177	12/2012	Ross et al.	N/A	N/A
2013/0084835	12/2012	Scherzer et al.	N/A	N/A
2013/0095787	12/2012	Kashanian	N/A	N/A
2013/0117140	12/2012	Kashanian	N/A	N/A
2013/0144789	12/2012	Aaltonen et al.	N/A	N/A
2013/0176908	12/2012	Baniel et al.	N/A	N/A
2013/0196685	12/2012	Griff et al.	N/A	N/A
2013/0225151	12/2012	King et al.	N/A	N/A
2013/0286942	12/2012	Bonar et al.	N/A	N/A
2013/0326356	12/2012	Zheng et al.	N/A	N/A
2014/0071895	12/2013	Bane et al.	N/A	N/A
2014/0073291	12/2013	Hildner et al.	N/A	N/A
2014/0074719	12/2013	Gressel et al.	N/A	N/A
2014/0080539	12/2013	Scherzer et al.	N/A	N/A
2014/0082142	12/2013	Geffin	N/A	N/A
2014/0198687	12/2013	Raleigh	N/A	N/A
2014/0226624	12/2013	Woo et al.	N/A	N/A

2014/0241342	12/2013	Constantinof	N/A	N/A
2015/0039763	12/2014	Chaudhary et al.	N/A	N/A
2015/0181628	12/2014	Haverinen et al.	N/A	N/A
2015/0341226	12/2014	Griff et al.	N/A	N/A
2016/0026964	12/2015	Rogers et al.	N/A	N/A
2016/0057011	12/2015	Drope	N/A	N/A
2016/0358204	12/2015	Cavanaugh et al.	N/A	N/A
2017/0063695	12/2016	Ferrell	N/A	N/A
2018/0262947	12/2017	Raleigh et al.	N/A	N/A
2020/0077892	12/2019	Tran	N/A	N/A
2020/0092707	12/2019	Raleigh	N/A	N/A
2022/0014512	12/2021	Raleigh et al.	N/A	N/A

FOREIGN PATENT DOCUMENTS

Patent No.	Application Date	Country	CPC
2688553	12/2007	CA	N/A
1310401	12/2000	CN	N/A
1345154	12/2001	CN	N/A
1508734	12/2003	CN	N/A
1538730	12/2003	CN	N/A
1567818	12/2004	CN	N/A
101035308	12/2005	CN	N/A
1801829	12/2005	CN	N/A
1802839	12/2005	CN	N/A
1889777	12/2005	CN	N/A
101155343	12/2005	CN	N/A
1867024	12/2005	CN	N/A
1878160	12/2005	CN	N/A
1937511	12/2006	CN	N/A
101123553	12/2006	CN	N/A
101080055	12/2006	CN	N/A
101114878	12/2007	CN	N/A
101115248	12/2007	CN	N/A
101127988	12/2007	CN	N/A
101183958	12/2007	CN	N/A
101335666	12/2007	CN	N/A
101341764	12/2008	CN	N/A
101437224	12/2008	CN	N/A
101815275	12/2009	CN	N/A
101911772	12/2009	CN	N/A
1855817	12/2011	CN	N/A
1098490	12/2000	EP	N/A
1247411	12/2001	EP	N/A
1289326	12/2002	EP	N/A
1484871	12/2003	EP	N/A
1463238	12/2003	EP	N/A
1484871	12/2003	EP	N/A
1503548	12/2004	EP	N/A
1545114	12/2004	EP	N/A

1739518	12/2006	EP	N/A
1772988	12/2006	EP	N/A
1850575	12/2006	EP	N/A
1887732	12/2007	EP	N/A
1942698	12/2007	EP	N/A
1978772	12/2007	EP	N/A
2007065	12/2007	EP	N/A
2026514	12/2008	EP	N/A
2381711	12/2010	EP	N/A
1247411	12/2010	EP	N/A
2466831	12/2011	EP	N/A
2154602	12/2016	EP	N/A
3148713	12/2000	JP	N/A
2005339247	12/2004	JP	N/A
2006041989	12/2005	JP	N/A
2006155263	12/2005	JP	N/A
2006197137	12/2005	JP	N/A
2006344007	12/2005	JP	N/A
2007318354	12/2006	JP	N/A
2008301121	12/2007	JP	N/A
2009111919	12/2008	JP	N/A
2009212707	12/2008	JP	N/A
2009218773	12/2008	JP	N/A
2009232107	12/2008	JP	N/A
20040053858	12/2003	KR	N/A
100658566	12/2005	KR	N/A
100958566	12/2009	KR	N/A
1998058505	12/1997	WO	N/A
1999027723	12/1998	WO	N/A
1999065185	12/2000	WO	N/A
0208863	12/2001	WO	N/A
2002045315	12/2001	WO	N/A
2002067616	12/2001	WO	N/A
2002093877	12/2001	WO	N/A
03017065	12/2002	WO	N/A
2003014891	12/2002	WO	N/A
2003017063	12/2002	WO	N/A
2003017065	12/2002	WO	N/A
2003058880	12/2002	WO	N/A
03/100581	12/2002	WO	N/A
03100581	12/2002	WO	N/A
2004028070	12/2003	WO	N/A
2004064306	12/2003	WO	N/A
2004095753	12/2004	WO	N/A
2005008995	12/2004	WO	N/A
2005053335	12/2004	WO	N/A
2005083934	12/2004	WO	N/A
2006004467	12/2005	WO	N/A
2006004784	12/2005	WO	N/A
2006012018	12/2005	WO	N/A

2006012610	12/2005	WO	N/A
2006050758	12/2005	WO	N/A
2006077481	12/2005	WO	N/A
2006093961	12/2005	WO	N/A
2006120558	12/2005	WO	N/A
2006130960	12/2005	WO	N/A
2007001833	12/2006	WO	N/A
2007014630	12/2006	WO	N/A
2007018363	12/2006	WO	N/A
2007053848	12/2006	WO	N/A
2007068288	12/2006	WO	N/A
2007097786	12/2006	WO	N/A
2007107701	12/2006	WO	N/A
2007120310	12/2006	WO	N/A
2007124279	12/2006	WO	N/A
2007126352	12/2006	WO	N/A
2007129180	12/2006	WO	N/A
2007133844	12/2006	WO	N/A
2004077797	12/2007	WO	N/A
2008017837	12/2007	WO	N/A
2008051379	12/2007	WO	N/A
2008066419	12/2007	WO	N/A
2008080139	12/2007	WO	N/A
2008080430	12/2007	WO	N/A
2008099802	12/2007	WO	N/A
2008/113986	12/2007	WO	N/A
2009002949	12/2007	WO	N/A
2009008817	12/2008	WO	N/A
2009002949	12/2008	WO	N/A
2006073837	12/2008	WO	N/A
2007069245	12/2008	WO	N/A
2009091295	12/2008	WO	N/A
2010088413	12/2009	WO	N/A
2010128391	12/2009	WO	N/A
2010128391	12/2010	WO	N/A
2011002450	12/2010	WO	N/A
2011149532	12/2010	WO	N/A
2012050937	12/2011	WO	N/A
2012050937	12/2011	WO	N/A

OTHER PUBLICATIONS

Mobile Network Evolution: GSM to UMTS, Conningtech (May 8, 2008, 12:26 pm), https://conningtech.wordpress.com/2008/05/08/mobile-network-evolution-gsm-to-umts/ (last visited May 23, 2024). cited by applicant

Patent Owner's Preliminary Response, *Samsung Electronics Co., Ltd*. v. *Headwater Research LLC*, No. IPR2023-01462, Paper 6 (PTAB Jan. 4, 2024). cited by applicant

File History of IPR2024-00945; filed on Jun. 7, 2024. cited by applicant

IPR2024-00945: Petition for Inter Partes Review of U.S. Pat. No. 9,215,613, filed on Jun. 7, 2024. cited by applicant

Defendants' Motion to Focus Patent Claims, *Headwater Research LLC* v. *AT&T Services, Inc*., No.

2:23-cv-00397, ECF No. 53 (E.D. Tex. Apr. 11, 2024). cited by applicant

Defendants' Motion for Entry of an Order Focusing Asserted Patent Claim and Prior Art, *Headwater Research LLC* v. *T-Mobile USA, Inc*., No. 2:23-cv-00379, ECF No. 58 (E.D. Tex. Apr. 30, 2024). cited by applicant

Defendants' Motion for Entry of an Order Focusing Asserted Patent Claim and Prior Art, *Headwater Research LLC* v. *Verizon Communications Inc*., No. 2:23-cv-00352, ECF No. 63 (E.D. Tex. May 1, 2024). cited by applicant

IPR2024-00942 Petition for Inter Partes Review of U.S. Pat. No. 8,589,541, dated Jun. 7, 2024. cited by applicant

IPR2024-00942 File History of Petition for Inter Partes Review of U.S. Pat. No. 8,589,541, dated Jun. 7, 2024. cited by applicant

IPR2024-00943 Petition for Inter Partes Review of U.S. Pat. No. 8,589,541, dated Jun. 7, 2024. cited by applicant

IPR2024-00943 File History of Petition for Inter Partes Review of U.S. Pat. No. 8,589,541, dated. cited by applicant

IPR2024-00944 Petition for Inter Partes Review of U.S. Pat. No. 8,589,541, dated Jun. 7, 2024. cited by applicant

IPR2024-00944 File History of Petition for Inter Partes Review of U.S. Pat. No. 8,589,541, dated. cited by applicant

Jon Inouye et al., “Dynamic Network Reconfiguration Support for Mobile Computers”, Proceedings of the 3rd annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '97), published Sep. 1997. cited by applicant

“Ads and movies on the run,” the Gold Coast Bulletin, Southport, Qld, Jan. 29, 2008. cited by applicant

“ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example,” Document ID 70917, Jan. 10, 2008. cited by applicant

“Communication Concepts for Mobile Agent Systems,” by Joachim Baumann et al.; Inst. Of Parallel and Distributed High-Performance Systems, Univ. of Stuttgart, Germany, pp. 123-135, 1997. cited by applicant

“End to End QoS Solution for Real-time Multimedia Application;” Computer Engineering and Applications, 2007, 43 (4): 155-159, by Tan Zu-guo, Wang Wen-juan; Information and Science School, Zhanjian Normal College, Zhan jiang, Guangdong 524048, China. cited by applicant

“Jentro Technologies launches Zenlet platform to accelerate location-based content delivery to mobile devices,” The Mobile Internet, Boston, MA, Feb. 2008. cited by applicant

“The Construction of Intelligent Residential District in Use of Cable Television Network,” Shandong Science, vol. 13, No. 2, Jun. 2000. cited by applicant

3rd Generation Partnership Project, “Technical Specification Group Core Network and Terminals; Access Network Discovery and Selection Function (ANDSF) Management Object (MO),” Release 9, Document No. 3GPP TS 24.312, V9.1.0, Mar. 2010. cited by applicant

3rd Generation Partnership Project, “Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access,” Release 8, Document No. 3GPP TS 23.401, V8.4.0, Dec. 2008. cited by applicant

3rd Generation Partnership Project, “Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture,” Release 8, Document No. 3GPP TS 23.203, V8.4.0, Dec. 2008. cited by applicant

3rd Generation Partnership Project; “Technical Specification Group Services and System Aspects; IP Flow Mobility and seamless WLAN offlload; Stage 2,” Release 10, Document No. 3GPP TS 23.261, V1.0.0, Mar. 2010. cited by applicant

Accuris Networks, “The Business Value of Mobile Data Offload—a White Paper”, 2010. cited by

applicant

Ahmed et al., “A Context-Aware Vertical Handover Decision Algorithm for Multimode Mobile Terminals and Its Performance,” BenQ Mobile, Munich Germany; University of Klagenfurt, Klagenfurt, Austria; 2006. cited by applicant

Ahmed et al., “Multi Access Data Network Connectivity and IP Flow Mobility in Evolved Packet System (EPS),” 2010 IEEE. cited by applicant

Alonistioti et al., “Intelligent Architectures Enabling Flexible Service Provision and Adaptability,” 2002. cited by applicant

Amazon Technologies, Inc., “Kindle™ User's Guide,” 3rd Edition, Copyright 2004-2009. cited by applicant

Android Cupcake excerpts, The Android Open Source Project, Feb. 10, 2009. cited by applicant

Anton, B. et al., “Best Current Practices for Wireless Internet Service Provider (WISP) Roaming”; Release Date Feb. 2003, Version 1.0; Wi-Fi Alliance—Wireless ISP Roaming (WISPr). cited by applicant

Blackberry Mobile Data System, version 4.1, Technical Overview, 2006. cited by applicant

Byrd, Open Secure Wireless, May 5, 2010. cited by applicant

Chandrasekhar et al., “Femtocell Networks: A Survey,” Jun. 28, 2008. cited by applicant

Chaouchi et al., “Policy Based Networking in the Integration Effort of 4G Networks and Services,” 2004 IEEE. cited by applicant

Cisco Systems, Inc., “Cisco Mobile Exchange (CMX) Solution Guide: Chapter 2—Overview of GSM, GPRS, and UMTS,” Nov. 4, 2008. cited by applicant

Client Guide for Symantec Endpoint Protection and Symantec Network Access Control, 2007. cited by applicant

Dikaiakos et al., “A Distributed Middleware Infrastructure for Personalized Services,” Nov. 24, 2003. cited by applicant

Dixon et al., Triple Play Digital Services: Comcast and Verizon (Digital Phone, Television, and Internet), Aug. 2007. cited by applicant

Droid Wall 1.3.7 description Apr. 28, 2010 obtained from https://www.freewarelovers.com/android/apps/droid-wall. cited by applicant

Ehnert, “Small application to monitor IP trafic on a Blackberry—1.01.03”, Mar. 27, 2008; http://www.ehnert.net/MiniMoni/. cited by applicant

European Commission, “Data Roaming Tariffs—Transparency Measures,” obtained from EUROPA—Europe's Information Society Thematic Portal website, Jun. 24, 2011: “http://ec.europa.eu/information_society/activities/roaming/data/measures/index_en.htm.”. cited by applicant

Farooq et al., “An IEEE 802.16 WiMax Module for the NS-3 Simulator,” Mar. 2-6, 2009. cited by applicant

Fujitsu, “Server Push Technology Survey and Bidirectional Communication in HTTP Browser,” Jan. 9, 2008 (JP). cited by applicant

Han et al., “Information Collection Services for Qos-Aware Mobile Applications,” 2005. cited by applicant

Hartmann et al., “Agent-Based Banking Transactions & Information Retrieval—What About Performance Issues?” 1999. cited by applicant

Hewlett-Packard Development Company, LP, “IP Multimedia Services Charging,” white paper, Jan. 2006. cited by applicant

Hossain et al., “Gain-Based Selection of Ambient Media Services in Pervasive Environments,” Mobile Networks and Applications. Oct. 3, 2008. cited by applicant

Jing et al., “Client-Server Computing in Mobile Environments,” GTE Labs. Inc., Purdue University, ACM Computing Surveys, vol. 31, No. 2, Jun. 1999. cited by applicant

Kasper et al., “Subscriber Authentication in mobile cellular Networks with virtual software SIM

Credentials using Trusted Computing," Fraunhofer-Institute for Secure Information Technology SIT, Darmstadt, Germany; ICACT 2008. cited by applicant

Kassar et al., "An overview of vertical handover decision strategies in heterogeneous wireless networks," ScienceDirect, University Pierre & Marie Curie, Paris, France, Jun. 5, 2007. cited by applicant

Kim, "Free wireless a high-wire act; MetroFi needs to draw enough ads to make service add profits," San Francisco Chronicle, Aug. 21, 2006. cited by applicant

Knight et al., "Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standarization Efforts," IEEE Communications Magazine, Jun. 2004. cited by applicant

Koutsopoulou et al., "Charging, Accounting and Billing Management Schemes In Mobile Telecommunication Networks and the Internet," IEEE Communications Surveys & Tutorials, First Quarter 2004, vol. 6, No. 1. cited by applicant

Koutsopoulou et al., "Middleware Platform for the Support of Charging Reconfiguration Actions," 2005. cited by applicant

Kuntze et al., "Trustworthy content push," Fraunhofer-Institute for Secure Information Technology SIT; Germany; WCNC 2007 proceedings, IEEE. cited by applicant

Kyriakakos et al., "Ubiquitous Service Provision in Next Generation Mobile Networks," Proceedings of the 13th IST Mobile and Wireless Communications Summit, Lyon, France, Jun. 2004. cited by applicant

Li, Yu, "Dedicated E-Reading Device: The State of the Art and The Challenges," Scroll, vol. 1, No. 1, 2008. cited by applicant

Loopt User Guide, metroPCS, Jul. 17, 2008. cited by applicant

Muntermann et al., "Potentiale und Sicherheitsanforderungen mobiler Finanzinformationsdienste und deren Systeminfrastrukturen," Chair of Mobile Commerce & Multilateral Security, Goethe Univ. Frankfurt, 2004. cited by applicant

NetLimiter Lite 4.0.19.0; http://www.heise.de/download/netlimiter-lite-3617703.html from vol. 14/2007. cited by applicant

Nilsson et al., "A Novel MAC Scheme for Solving the QoS Parameter Adjustment Problem in IEEE802.11e EDCA," Feb. 2006. cited by applicant

IPR2023-01157 Patent Owner's Preliminary Response, dated Oct. 24, 2023. cited by applicant

IPR2023-01157 Petitioner's Reply to Patent Owner's Preliminary Response, dated Dec. 6, 2023. cited by applicant

IPR2023-01157 Patent Owner's Preliminary Sur-Reply, dated Dec. 20, 2023. cited by applicant

IPR2023-01157 Decision Granting Institution of Inter Partes Review, dated Jan. 22, 2024. cited by applicant

IPR2023-01157 Patent Owner's Response to the Petition, dated May 8, 2024. cited by applicant

IPR2023-01226 Patent Owner's Preliminary Response, dated Nov. 15, 2023. cited by applicant

IPR2023-01226 Petitioner's Pre-Institution Reply, dated Dec. 14, 2023. cited by applicant

IPR2023-01226 Patent Owner's Preliminary Sur-Reply, dated Dec. 21, 2023. cited by applicant

IPR2023-01226 Decision Granting Institution of Inter Partes Review, dated Feb. 8, 2024. cited by applicant

IPR2023-01226 Patent Owner's Response to the Petition, dated May 16, 2024. cited by applicant

IPR2023-01250 Patent Owner's Preliminary Response, dated Dec. 22, 2023. cited by applicant

IPR2023-01250 Petitioner's Pre-Institution Reply, Jan. 22, 2024. cited by applicant

IPR2023-01250 Patent Owner's Preliminary Sur-Reply, Feb. 1, 2024. cited by applicant

IPR2023-01250 Decision Granting Institution of Inter PartesReview, dated Mar. 12, 2024. cited by applicant

IPR2023-01253 Patent Owner's Preliminary Response, dated Dec. 22, 2023. cited by applicant

IPR2023-01253 Petitioner's Pre-Institution Reply, dated Jan. 22, 2024. cited by applicant

IPR2023-01253 Patent Owner's Preliminary Sur-Reply, dated Feb. 1, 2024. cited by applicant

IPR2023-01253 Decision Denying Institution of Inter Partes Review, dated Mar. 21, 2024. cited by applicant
IPR2023-01336 Patent Owner's Preliminary Response, dated Dec. 29, 2023. cited by applicant
IPR2023-01336 Petitioner's Reply, dated Feb. 5, 2024. cited by applicant
IPR2023-01336 Patent Owner's Preliminary Sur-Reply, dated Feb. 20, 2024. cited by applicant
IPR2023-01336 Decision Granting Institution of Inter Partes Review, dated Mar. 25, 2024. cited by applicant
IPR2023-01337 Patent Owner's Preliminary Response, dated Dec. 29, 2023. cited by applicant
IPR2023-01337 Petitioner's Reply, dated Feb. 5, 2024. cited by applicant
IPR2023-01337 Patent Owner's Preliminary Sur-Reply, dated Feb. 20, 2024. cited by applicant
IPR2023-01337 Decision Granting Institution of Inter Partes Review, dated Mar. 12, 2024. cited by applicant
IPR2023-01360 Patent Owner's Preliminary Response, dated Jan. 4, 2024. cited by applicant
IPR2023-01360 Decision Granting Institution of Inter Partes Review, dated Apr. 1, 2024. cited by applicant
IPR2023-01361 Patent Owner's Preliminary Response, dated Jan. 4, 2024. cited by applicant
IPR2023-01361 Decision Denying Institution of Inter Partes Review, dated Mar. 29, 2024. cited by applicant
IPR2023-01361 Petitioner's Request for Rehearing, dated Apr. 26, 2024. cited by applicant
IPR2023-01362 Patent Owner's Preliminary Response, dated Jan. 4, 2024. cited by applicant
IPR2023-01362 Decision Denying Institution of Inter Partes Review, dated Mar. 29, 2024. cited by applicant
IPR2023-01362 Petitioner's Request for Rehearing, dated Apr. 26, 2024. cited by applicant
IPR2023-01462 Patent Owner's Preliminary Response, dated Jan. 4, 2024. cited by applicant
IPR2023-01462 Decision Denying Institution of Inter Partes Review, dated Mar. 29, 2024. cited by applicant
IPR2023-01462 Petitioner's Request for Rehearing, dated Apr. 26, 2024. cited by applicant
Arai, Masato, et al; “A Proposal for an Effective Information Flow Control Model for Sharing and Protecting Sensitive Information”, Proc. 7th Australasian Information Security Conference (AISC 2009), Wellington, New Zealand. cited by applicant
Banchs, et. al., Distributed weighted fair queuing in 802.11 wireless LAN, 2002 IEEE International Conference on Communications, Conference Proceedings. ICC 2002 pp. 3121-3127), 2002. cited by applicant
File History of U.S. Pat. No. 9,277,433 (Raleigh, et al.), issued Mar. 1, 2016. cited by applicant
Burt, “Competition in Mobile Chips to Grow in 2009: In-Stat,” eWEEK, Aug. 18, 2009, downloaded from the internet at https://www.eweek.com/pc-hardware/competition-inmobile-chips-to-grow-in-2009-in-stat/ on Jul. 29, 2023. cited by applicant
Enck, et al., Understanding Android Security, IEEE Security & Privacy Magazine, vol. 7, No. 1, 78 pages, Jan./Feb. 2009. cited by applicant
Excerpts, Rosen, et al. “UNIX: The Complete Reference”, Second Edition, McGraw-Hill 2007. cited by applicant
Bray, et. al., Extensible Markup Language (XML) 1.1 (Second Edition), W3C, 2006, Aug. 16, 2006, 41 pages, downloaded from the internet at https://www.w3.org/TR/2006/REC-xml11-20060816/ on Jul. 29, 2023. cited by applicant
File History of IPR2023-01250; filed on Aug. 14, 2023. cited by applicant
File History of IPR2023-01253, filed on Aug. 11, 2023. cited by applicant
File History of U.S. Pat. No. 9,143,976 (Raleigh, et al.), issued Sep. 22, 2015. cited by applicant
Nichols, et. al., IETF RFC 2474, “Definition of the Differentiated Services Field (DS Field) in the IPV4 and IPv6 Headers,” Dec. 1998, downloaded from the internet t https://datatracker.ietf.org/doc/html/rfc2474 on Jul. 29, 2023. cited by applicant

Blake, et al., IETF RFC 2475, “An Architecture for Differentiated Services,” Dec. 1998, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc2475 on Jul. 29, 2023. cited by applicant

Durham, et al., IETF RFC 2748, “The COPS (Common Open Policy Service) Protocol,” Jan. 2000, downloaded from the internet at https://www.rfc-editor.org/rfc/rfc2748.html on Aug. 1, 2023. cited by applicant

Westerinen, et al., IETF RFC 3198, Terminology for Policy-Based Management, Nov. 2001, available at https://www.ietf.org/rfc/rfc3198.txt. cited by applicant

Babiarz, et al., IETF RFC 4594, Configuration Guidelines for DiffServ Service Classes, Aug. 2006, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc4594 on Jul. 29, 2023. cited by applicant

Schulzrinne, et al., IETF RFC 4745, “Common Policy: A Document Format for Expressing Privacy Preferences,” Feb. 2007, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc4745 on Jul. 29, 2023. cited by applicant

IETF RFC 791, Internet Protocol, Sep. 1981, downloaded from the internet at https://www.ietf.org/rfc/rfc791.txt on Jul. 28, 2023. cited by applicant

IPR2023-01250: Petition for Inter Partes Review of U.S. Pat. No. 9,277,433, filed on Aug. 14, 2023. cited by applicant

IPR2023-01253; Petition for Inter Partes Review of U.S. Pat. No. 9,143,976, filed on Aug. 11, 2023. cited by applicant

Model-View-Controller, Microsoft Patterns & Practices, Mar. 17, 2014, 9 pages, downloaded from the internet at http://msdn2.microsoft.com/ en-us/library/ms978748.aspx on Jul. 29, 2023. cited by applicant

Overview of the IEEE 802.11 Standard, Dec. 6, 2001, downloaded from the internet at https://www.informit.com/articles/article.aspx?p=24411&seqNum=5 on Jul. 29, 2023. cited by applicant

Samsung Stipulation letter, dated Aug. 11, 2023 in *Headwater Research LLC* v. *Samsung Electronics Co., Ltd. et al.*, Case No. 2:22-cv-00422, E.D. Texas. cited by applicant

Samsung Stipulation letter, dated Aug. 14, 2023 in *Headwater Research LLC* v. *Samsung Electronics Co., Ltd., et al.*, Case No. 2:22-cv-00422, E.D. Texas. cited by applicant

Shuler, “How Does the Internet Work?”, downloaded from, the internet at https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper. htm on Jul. 29, 2023. cited by applicant

Excerpts, Computer Networks, Fourth Edition, by Andrew Tanenbaum, Prentice Hall, 2003. cited by applicant

Excerpts, Stevens “TCP/IP Illustrated”, vol. 1, Addison-Wesley Publishing Company, 1994. cited by applicant

USB720 Modem Hardware User Manual, 2006, downloaded from the internet at http://s7.vzw.com/is/content/Verizon-Wireless/Devices/Verizon/Userguides/vzw-usb720-modemum.pdf on Jul. 31, 2023. cited by applicant

Want, “When Cell Phones Become Computers”, IEEE Pervasive Computing, vol. 8, Apr.-Jun. 2009, pp. 2-5. cited by applicant

IPR2023-01157: Petition for Inter Partes Review of U.S. Pat. No. 11,405,224, filed Jul. 20, 2023. cited by applicant

IPR2023-01226: Petition for Inter Partes Review of U.S. Pat. No. 10,237,773, filed Jul. 21, 2023. cited by applicant

Complaint filed in *Headwater Research LLC* v. *Samsung Electronics Co., Ltd., Samsung Electronics America, Inc.*, dated Oct. 26, 2022, Case No. 2:22-cv-00422, E.D. Texas. cited by applicant

First Amended Complaint filed in *Headwater Research LLC* v. *Samsung Electronics Co., Ltd.*, *Samsung Electronics America, Inc*., dated Nov. 30, 2022, Case No. 2:22-cv-00422, E.D. Texas. cited by applicant

Complaint filed in *Headwater Research LLC* v. *Samsung Electronics Co., Ltd. et al*., dated Dec. 6, 2022, Case No. 2:22-cv-00467, E.D. Texas. cited by applicant

File History of U.S. Pat. No. 9,277,445 (Raleigh et al.), issued Mar. 1, 2016. cited by applicant

File History of IPR2023-01157, filed Jul. 20, 2023. cited by applicant

File History of IPR2023-01226, filed Jul. 21, 2023. cited by applicant

Samsung Stipulation letter, dated Jul. 21, 2023 in *Headwater Research LLC* v. *Samsung Electronics Co., Ltd., et al*. Case No. 2:22-cv-00467, E.D. Texas. cited by applicant

Samsung Stipulation letter, dated Jul. 20, 2023 in *Headwater Research LLC* v. *Samsung Electronics Co., Ltd., et al*. Case No. 2:22-cv-00422, E.D. Texas. cited by applicant

A. Freier, et al., The Secure Sockets Layer (SSL) Protocol Version 3.0, Internet Engineering Task Force (IETF), Request for Comments: 6101, ISSN: 2070-1721, Aug. 2011, available at https://datatracker.ietf.org/doc/html/rfc6101. cited by applicant

M. V. Pedersen, F. H. P. Fitzek, and T. Larsen, “Implementation and Performance Evaluation of Network Coding for Cooperative Mobile Devices,” ICC Workshops—2008 IEEE International Conference on Communications Workshops, Beijing, China: IEEE, May 2008, pp. 91-96. doi: 10.1109/ICCW.2008.22. cited by applicant

W. R. Stevens, “TCP/IP Illustrated, vol. 1,” 2003, ISBN: 0-13-141155-1 (“Stevens”). cited by applicant

Bajaj, et al., IETF RFC 3198, Web Services Policy 1.2—Framework (WS-Policy), Apr. 25, 2006, downloaded from the internet at https://www.w3.org/Submission/WS-Policy/ on Aug. 29, 2023. cited by applicant

Sloman, et al., “Security and management policy specification.” IEEE Network, Mar./Apr. 2002 pp. 10-19. cited by applicant

Lu, et al., “Comparing system level power management policies.” IEEE Design & Test of Computers, Mar./Apr. 2001 pp. 10-19. cited by applicant

Davie, et al., IETF RFC 3246, An Expedited Forwarding PHB (Per-Hop Behavior), Mar. 2002, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc3246 on Sep. 5, 2023. cited by applicant

Excerpts, The New Penguin Dictionary of Computing, by Dick Pountain, 2001. cited by applicant

Westerinen, et al., IETF RFC 3198, Terminology for Policy-Based Management, Nov. 2001, downloaded from the internet at https://www.ietf.org/rfc/rfc3198.txt on Aug. 15, 2023. cited by applicant

Yavatkar, IETF RFC 2753, A Framework for Policy-Based Admission Control, Jan. 2000, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc2753 on Sep. 5, 2023. cited by applicant

IPR2023-01360; Petition for Inter Partes Review of U.S. Pat. No. 9,609,544, filed on Sep. 11, 2023. cited by applicant

IPR2023-01361; Petition for Inter Partes Review of U.S. Pat. No. 9,271,184, filed on Sep. 8, 2023. cited by applicant

IPR2023-01362; Petition for Inter Partes Review of U.S. Pat. No. 9,271,184, filed on Sep. 8, 2023. cited by applicant

IPR2023-01336; Petition for Inter Partes Review of U.S. Pat. No. 9,137,701, filed on Aug. 25, 2023. cited by applicant

IPR2023-01337; Petition for Inter Partes Review of U.S. Pat. No. 9,521,578, filed on Aug. 25, 2023. cited by applicant

IPR2023-01462; Petition for Inter Partes Review of U.S. Pat. No. 9,277,445, filed on Sep. 28, 2023. cited by applicant

Nuzman et al., “A compund model for TCP connection arrivals for LAN and WAN applications,”

Oct. 22, 2002. cited by applicant
Open Mobile Alliance (OMA), Push Architecture, Candidate Version 2.2; Oct. 2, 2007; OMA-AD-Push-V2_2-20071002-C. cited by applicant
Oppliger, Rolf, “Internet Security: Firewalls and Bey,” Communications of the ACM, May 1997, vol. 40. No. 5. cited by applicant
Quintana, David, “Mobile Multitasking,” Apr. 14, 2010. cited by applicant
Rao et al., “Evolution of Mobile Location-Based Services,” Communication of the ACM, Dec. 2003. cited by applicant
Richtel, “Cellphone consumerism; If even a debit card is too slow, now you have a new way to act on impulse: [National Edition],” National Post, Canada, Oct. 2, 2007. cited by applicant
Rivadeneyra et al., “A communication architecture to access data services through GSM,” San Sebastian, Spain, 1998. cited by applicant
Roy et al., “Energy Management in Mobile Devices with the Cinder Operating System”, Stanford University, MIT CSAIL, Jun. 3, 2010. cited by applicant
Ruckus Wireless—White Paper; “Smarter Wi-Fi for Mobile Operator Infrastructures” 2010. cited by applicant
Sabat, “The evolving mobile wireless value chain and market structure,” Nov. 2002. cited by applicant
Sadeh et al., “Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application,” ISR School of Computer Science, Carnegie Mellon University, 2007. cited by applicant
Schiller et al., “Location-Based Services,” The Morgan Kaufmann Series in Data Management Systems, 2004. cited by applicant
Sharkey, “Coding for Life—Battery Life, That Is,” May 27, 2009. cited by applicant
Sharkey, Jeff, “Coding for Life—Battery Life, That Is,” May 27, 2009. cited by applicant
Steglich, Stephan, “I-Centric User Interaction,” Nov. 21, 2003. cited by applicant
Sun et al., “Towards Connectivity Management Adaptability: Context Awareness in Policy Representation and End-to-end Evaluation Algorithm,” Dept. of Electrical and Information Engineering, Univ. of Oulu, Finland, 2004. cited by applicant
Thurston, Richard, “WISPr 2.0 Boosts Roaming Between 3G and Wi-Fi”; Jun. 23, 2010; Web page from zdnet.com; Zdnet.com/wispr-2-0-boosts-roaming-between-3g-and-wi-fi-3040089325/. cited by applicant
Van Eijk, et al., “GigaMobile, Agent Technology for Designing Personalized Mobile Service Brokerage,” Jul. 1, 2002. cited by applicant
VerizonWireless.com news, “Verizon Wireless Adds to Portfolio of Cosumer-Friendly Tools With Introduction of Usage Controls, Usage Controls and Chaperone 2.0 Offer Parents Full Family Security Solution,” Aug. 18, 2008. cited by applicant
Windows7 Power Management, published Apr. 2009. cited by applicant
Wireless Broadband Alliance, “WISPr 2.0, Apr. 8, 2010”; Doc. Ref. No. WBA/RM/WISPr, Version 01.00. cited by applicant
Zhu et al., “A Survey of Quality of Service in IEEE 802.11 Networks,” IEEE Wireless Communications, Aug. 2004. cited by applicant
Complaint for Patent Infringement in *Headwater Research LLC* v. *Samsung Electronics Co., Ltd et al.*, 2-23-cv-00641 (EDTX), Dec. 29, 2023). cited by applicant
David Flanagan, O'Reilly & Associates, Inc., “Java in a Nutshell,” 1996, ISBN: 1-56592-183-6. cited by applicant
Korhonen, “Host Identity Protocol (HIP) Implementation in the Symbian Environment,” Master of Science Thesis, Tampere University of Technology (Dec. 10, 2007). cited by applicant
Welsh, “Incorporating Memory Management into User-Level Network Interfaces.” IEEE Micro, 18(2), 1998, 10 pages. cited by applicant

Carter, Casey et al., “Contact networking: a localized mobility system,” Proceedings of the 1st International Conference on Mobile systems, Applications and Services, 2003. cited by applicant

S. Lee & N. Golmie, “Power-Efficient Interface Selection Scheme using Paging of WWAN for WLAN in Heterogeneous Wireless Networks,” 2006 IEEE International Conference on Communications (Istanbul, 2006), 1742-1747. cited by applicant

M. Stemm et al., “A network measurement architecture for adaptive applications,” Proceedings of the 2000 IEEE Infocom Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No. 00CH37064), Tel Aviv, Israel, 2000, 285-294. cited by applicant

K. Ravindran & V. Bansal, “Delay compensation protocols for synchronization of multimedia data streams,” IEEE Transactions on Knowledge and Data Engineering, vol. 5, No. 4, 574-589, Aug. 1993. cited by applicant

D. C. Verma, “Simplifying network administration using policy-based management.” IEEE Network, vol. 16, No. 2, 20-26, Mar. 2002. cited by applicant

G. Nychis & D. R. Licata, “The impact of background network traffic on foreground network traffic.” Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM), 2001. cited by applicant

I. Pronchev. “Packet Capturing Using the Linux Netfilter Framework.” Technical Report, Technische Universität München, 1-31, Jul. 2006. cited by applicant

A.-J. Moerdijk and L. Klostermann, “Opening the networks with Parlay/OSA: standards and aspects behind the APIs.” IEEE Network, vol. 17, No. 3, pp. 58-64, May-Jun. 2003. cited by applicant

J. B. D. Joshi, E. Bertino, U. Latif and A. Ghafoor, “A generalized temporal role-based access control model.” IEEE Transactions on Knowledge and Data Engineering, vol. 17, No. 1, pp. 4-23, Jan. 2005. cited by applicant

Lymberopoulos et al., “An Adaptive Policy-Based Framework for Network Services Management,” Journal of Network and Systems Management, vol. 11, No. 3, Sep. 2003. cited by applicant

Richard Stevens et al., “UNIX Network Programming vol. 1, Third Edition: The Sockets Networking API,” 2004, ISBN: 0-13-141155-1. cited by applicant

IPR2024-01407 Petition for Inter Partes Review of U.S. Pat. No. 9,179,359. cited by applicant

Boutaba and Polyrakis, “Toward Extensible Policy Enforcement Points”, in M. Sloman, J. Lobo, and E. Lupu (Eds.): Policy 2001,LNCS 1995, pp. 247-261 (© Springer-Verlag Berlin Heidelbergm 2001). cited by applicant

Beigi et al., “Policy Transformation Techniques in Policy-based Systems Management”, Proceedings Fifth IEEE International Workshop on Policies for Distributed Systems and Networks (2004). cited by applicant

Chaouchi et al., “Policy Based Networking in Integration Effort of 4G Networks and Services”, 2004 IEEE 59th Vehicular Technology Conference, VTC 2004—Spring, pp. 2977-2981 vol. 5. cited by applicant

Verma et al., “Simplifying Network Administration Using Policy-Based Management”, IEEE Network, pp. 20-26 (Mar./Apr. 20). cited by applicant

3GPP TS 23.203 (v8.4.0 (Dec. 2008) (3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 8)). cited by applicant

Plaintiff Headwater Research LLC's Disclosure of Asserted Claims and Infringement Contentions, case No. 2:23-cv-00398, -397. cited by applicant

File History of IPR2024-01041, filed Jun. 20, 2024. cited by applicant

IPR2024-01041 Petition for Inter Partes Review of U.S. Pat. No. 8,924,543, filed Jun. 20, 2024. cited by applicant

File History of IPR2024-01042, filed Jun. 20, 2024. cited by applicant

IPR2024-01042 Petition for Inter Partes Review of U.S. Pat. No. 8,924,543, filed Jun. 20, 2024. cited by applicant
Reexamination Application Serial No. 90/119,610—Order Granting Request for Ex Parte Reexamination of U.S. Pat. No. 9,143,976, dated Oct. 23, 2024. cited by applicant
Reexamination Application Serial No. 90/019,644—Order Granting Request for Ex Parte Reexamination of U.S. Pat. No. 9,277,445, dated Nov. 8, 2024. cited by applicant
Reexamination Application Serial No. 90/019,643—Order Granting Request for Ex Parte Reexamination of U.S. Pat. No. 9,271,184, dated Nov. 8, 2024. cited by applicant
Flinn, Jason, et al. “The case for intentional networking,” Proceedings of the 10th Workshop on Mobile Computing Systems and Applications, 2009. cited by applicant
David Flanagan, O'Reilly & Associates, Inc., “Java in a Nutshell,” 1996, ISBN: I-56592-183-6. cited by applicant
Buxton, B., “Integrating the Periphery and Context: A New Model of Telematics,” in Proceedings of Graphics Interface '95, in GI'95. 1995. cited by applicant
Hinckley et al., “Foreground and background interaction with sensor-enhanced mobile devices,” ACM Trans. Comput. Hum. Interact., vol. 12, No. 1, pp. 31-52, Mar. 2005. cited by applicant
Petition for Inter Partes Review of U.S. Pat. No. 9,143,976 Pursuant To 35 U.S.C. §§ 311-319, 37 C.F.R. § 42 in *Samsung Electronics Co Ltd* v. *Headwater Research LLC*, IPR2023-01253, Paper 2 (PTAB Aug. 11, 2023). cited by applicant
Decision Denying Institution of Inter Partes Review in *Samsung Electronics Co Ltd* v. *Headwater Research LLC*, IPR2023-01253, Paper 9 (PTAB Mar. 21, 2024). cited by applicant
File History of U.S. Pat. No. 9,143,976. cited by applicant
Request for Ex Parte Reexamination of U.S. Pat. No. 9,143,976, filed Aug. 5, 2024. cited by applicant
Joint Claim Construction and Prehearing Statement, *Headwater Research LLC* v. *Motorola Mobility LLC, et al.*, No. 4:23-cv-04496-JST (N.D. Cal. Jun. 11, 2024) (ECF No. 64). cited by applicant
IPR2024-01180 Petition for Inter Partes Review, filed Aug. 12, 2024. cited by applicant
D. P. Bovet, “Understanding the Linux Kernel,” 2000, ISBN: 0-596-00002-2. cited by applicant
U.S. Appl. No. 61/082,160. cited by applicant
Petition for Inter Partes Review of U.S. Pat. No. 9,277,445 Pursuant To 35 U.S.C. §§ 311-319, 37 C.F.R. § 42 in *Samsung Electronics Co Ltd* v. *Headwater Research LLC*, IPR2023-01462, Paper 2 (PTAB Sep. 28, 2023). cited by applicant
Decision Denying Institution of Inter Partes Review in *Samsung Electronics Co Ltd* v. *Headwater Research LLC*, IPR2023-01462, Paper 9 (PTAB Mar. 29, 2024). cited by applicant
File History of U.S. Pat. No. 9,277,445. cited by applicant
Request for Ex Parte Reexamination of U.S. Pat. No. 9,277,445. cited by applicant
Feldmeier, C.C. “Multiplexing issues in communication system design.” In Proceedings of the ACM symposium on Communications architectures & protocols (SIGCOMM '90). Association for Computing Machinery, New York, NY, USA, 209-219, 1990. cited by applicant
Petition for Inter Partes Review of U.S. Pat. No. 9,271,184 Pursuant To 35 U.S.C. §§ 311-319, 37 C.F.R. § 42 in *Samsung Electronics Co Ltd* v. *Headwater Research LLC*, IPR2023-01361, Paper 3 (PTAB Sep. 8, 2023). cited by applicant
Decision Denying Institution of Inter Partes Review in *Samsung Electronics Co Ltd* v. *Headwater Research LLC*, IPR2023-01361, Paper 10 (PTAB Mar. 29, 2024). cited by applicant
Petition for Inter Partes Review of U.S. Pat. No. 9,271,184 Pursuant To 35 U.S.C. §§ 311-319, 37 C.F.R. § 42 in *Samsung Electronics Co Ltd* v. *Headwater Research LLC*, IPR2023-01362, Paper 3 (PTAB Sep. 8, 2023). cited by applicant
Decision Denying Institution of Inter Partes Review in *Samsung Electronics Co Ltd* v. *Headwater Research LLC*, IPR2023-01362, Paper 10 (PTAB Mar. 29, 2024). cited by applicant

File History of U.S. Pat. No. 9,271,184. cited by applicant
Request for Ex Parte Reexamination of U.S. Pat. No. 9,271,184. cited by applicant
IPR2024-01181 Petition for Inter Partes Review, filed Aug. 12, 2024. cited by applicant
Enable-ExchangeCertificate, Microsoft, https://learn.microsoft.com/en-us/powershell/module/exchange/enable-exchangecertificate?view =exchange-ps (last visited May 15, 2024). cited by applicant
Larry L. Peterson & Bruce S. Davie, Computer Networks: A Systems Approach (3d ed. 2003). cited by applicant
Elizabeth Woyke, World's Most Wired Airports, NBC News (Mar. 11, 2008, 10:02 AM), https://www.nbcnews.com/id/wbna23391922 (last visited May 15, 2024). cited by applicant
Madison Avenue Calling, Gainesville Sun (Jan. 19, 2007, 11:00 PM), https://www.gainesville.com/story/news/2007/01/20/madison-avenue-calling/31509806007/ (last visited May 15, 2024). cited by applicant
Spyros Sakellariadis, Using Exchange Server with SMTP and POP3, ITPro Today (May 31, 1998), https://www.itprotoday.com/email-and-calendaring/using-exchange-server-smtp-and-pop3#close-modal (last visited May 16, 2024). cited by applicant

---

Primary Examiner: Huq; Obaidul

Attorney, Agent or Firm: Farjami & Farjami LLP

Background/Summary

INCORPORATION BY REFERENCE (1) The following U.S. applications are hereby incorporated by reference for all purposes: application Ser. No. 13/239,321, filed Sep. 21, 2011, entitled SERVICE OFFER SET PUBLISHING TO DEVICE AGENT WITH ON-DEVICE SERVICE SELECTION; application Ser. No. 13/237,827, filed Sep. 20, 2011, entitled ADAPTING NETWORK POLICIES BASED ON DEVICE SERVICE PROCESSOR CONFIGURATION, now U.S. Pat. No. 8,832,777 (issued Sep. 9, 2014); application Ser. No. 12/695,019, filed Jan. 27, 2010, entitled DEVICE ASSISTED CDR CREATION, AGGREGATION, MEDIATION AND BILLING, now U.S. Pat. No. 8,275,830 (issued Sep. 25, 2012); application Ser. No. 12/380,780, entitled AUTOMATED DEVICE PROVISIONING AND ACTIVATION, filed Mar. 2, 2009, now U.S. Pat. No. 8,839,388 (issued Sep. 16, 2014); application Ser. No. 12/380,778, filed Mar. 2, 2009, entitled VERIFIABLE DEVICE ASSISTED SERVICE USAGE BILLMG WITH INTEGRATED ACCOUNTING, MEDIATION ACCOUNTING, AND MULTI-ACCOUNT, now U.S. Pat. No. 8,321,526 (issued Nov. 27, 2012); Provisional Application No. 61/206,354, entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD, filed Jan. 28, 2009; Provisional Application No. 61/206,944, entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD, filed Feb. 4, 2009; Provisional Application No. 61/207,393, entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed Feb. 10, 2009; Provisional Application No. 61/207,739, entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed Feb. 13, 2009; Provisional Application No. 61/270,353, filed on Jul. 6, 2009, entitled DEVICE ASSISTED CDR CREATION, AGGREGATION, MEDIATION AND BILLING; Provisional Application No. 61/264,126, filed Nov. 24, 2009, entitled DEVICE ASSISTED SERVICES ACTIVITY MAP; Provisional Application No. 61/384,456 entitled SECURING SERVICE PROCESSOR WITH SPONSORED SIMS, filed Sep. 20, 2010; and Provisional Application No. 61/385,020 entitled SERVICE USAGE RECONCILIATION SYSTEM OVERVIEW, filed Sep. 21, 2010.

BACKGROUND

(1) With the advent of mass market digital communications and content distribution, many access networks such as wireless networks, cable networks and DSL (Digital Subscriber Line) networks are pressed for user capacity, with, for example, EVDO (Evolution-Data Optimized), HSPA (High Speed Packet Access), LTE (Long Term Evolution), WiMax (Worldwide Interoperability for Microwave Access), and Wi-Fi (Wireless Fidelity) wireless networks increasingly becoming user capacity constrained. Although wireless network capacity will increase with new higher capacity wireless radio access technologies, such as MIMO (Multiple-Input Multiple-Output), and with more frequency spectrum being deployed in the future, these capacity gains are likely to be less than what is required to meet growing digital networking demand.

(2) Similarly, although wire line access networks, such as cable and DSL, can have higher average capacity per user, wire line user service consumption habits are trending toward very high bandwidth applications that can quickly consume the available capacity and degrade overall network service experience. Because some components of service provider costs go up with increasing bandwidth, this trend will also negatively impact service provider profits.

Description

BRIEF DESCRIPTION OF THE DRAWINGS

(1) Various embodiments are disclosed in the following detailed description and the accompanying drawings.

(2) FIG. **1** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments.

(3) FIG. **2** illustrates another wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments.

(4) FIG. **3** illustrates another wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments.

(5) FIG. **4** illustrates provisioning of a wireless network for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments.

(6) FIG. **5** illustrates a network architecture for providing device assisted CDRs in accordance with some embodiments.

(7) FIG. **6** illustrates another network architecture for providing device assisted CDRs in accordance with some embodiments.

(8) FIG. **7** illustrates another network architecture for providing device assisted CDRs in accordance with some embodiments.

(9) FIG. **8** illustrates another network architecture for providing device assisted CDRs in accordance with some embodiments.

(10) FIG. **9** is a functional diagram illustrating a device based service processor and a service controller in accordance with some embodiments.

(11) FIG. **10** provides a table summarizing various service processer functional elements in accordance with some embodiments.

(12) FIG. **11** provides a table summarizing various service controller functional elements in accordance with some embodiments.

(13) FIG. **12** illustrates a device stack providing various service usage measurement from various points in the networking stack for a service monitor agent, a billing agent, and an access control integrity agent to assist in verifying the service usage measures and billing reports in accordance with some embodiments.

(14) FIG. **13** illustrates an embodiment similar to FIG. **12** in which some of the service processor is implemented on the modem and some of the service processor is implemented on the device

application processor in accordance with some embodiments.

(15) FIGS. **14**A through **14**E illustrate various embodiments of intermediate networking devices that include a service processor for the purpose of verifiable service usage measurement, reporting, and billing reports in accordance with some embodiments.

(16) FIG. **15** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including a proxy server in accordance with some embodiments.

(17) FIG. **16** is a functional diagram illustrating the service control device link of the service processor and the service control service link of the service controller in accordance with some embodiments.

(18) FIG. **17** is a functional diagram illustrating framing structure of a service processor communication frame and a service controller communication frame in accordance with some embodiments.

(19) FIGS. **18**A through **18**J provide tables summarizing various service processor heartbeat functions and parameters in accordance with some embodiments.

(20) FIGS. **19**A through **19**S provide tables summarizing various device based service policy implementation verification techniques in accordance with some embodiments.

(21) FIGS. **20**A through **20**E provide tables summarizing various techniques for protecting the device based service policy from compromise in accordance with some embodiments.

(22) FIG. **21** illustrates an example embodiment of a process to start or stop a data session with SGSN notification.

(23) FIG. **22** illustrates an example embodiment of a process to start or stop a data session with GGSN notification.

(24) FIG. **23** illustrates an example embodiment with network system elements that can be included in a service controller system to facilitate a device-assisted services (DAS) implementation and the flow of information between those elements.

(25) FIG. **24** illustrates an example embodiment of a service controller reconciliation processing procedure that may be used to detect fraud using information from the end-user device and information from a second source.

(26) FIG. **25** illustrates an example embodiment can be advantageous in cases where it is desirable to identify service usage classifications in the network for the purpose of providing a device user or service sponsor with the opportunity to pay for access network service usage that is classified by application or website.

DETAILED DESCRIPTION

(27) The invention can be implemented in numerous ways, including as a process; an apparatus; a system; a composition of matter; a computer program product embodied on a computer readable storage medium; and/or a processor, such as a processor configured to execute instructions stored on and/or provided by a memory coupled to the processor. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. In general, the order of the steps of disclosed processes may be altered within the scope of the invention. Unless stated otherwise, a component such as a processor or a memory described as being configured to perform a task may be implemented as a general component that is temporarily configured to perform the task at a given time or a specific component that is manufactured to perform the task. As used herein, the term ‘processor’ refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.

(28) A detailed description of one or more embodiments of the invention is provided below along with accompanying figures that illustrate the principles of the invention. The invention is described in connection with such embodiments, but the invention is not limited to any embodiment. The scope of the invention is limited only by the claims and the invention encompasses numerous alternatives, modifications and equivalents. Numerous specific details are set forth in the following description in order to provide a thorough understanding of the invention. These details are

provided for the purpose of example and the invention may be practiced according to the claims without some or all of these specific details. For the purpose of clarity, technical material that is known in the technical fields related to the invention has not been described in detail so that the invention is not unnecessarily obscured.

(29) There are many new types of digital devices where it is becoming desirable, for example, to connect these devices to wireless networks including wireless wide area networks (WWAN, such as 3G and 4G) and/or wireless local area (WLAN) networks. These devices include, for example, consumer electronics devices, business user devices, and machine to machine devices that benefit from flexible wide area data connections and the Internet. Example devices include netbooks, notebooks, mobile Internet devices, personal navigation (e.g., GPS enabled) devices, music and multimedia players, eReaders, industrial telemetry, automotive emergency response and diagnostics, 2-way home and industrial power metering and control, vending machines, parking meters, and many other devices. For example, it is highly advantageous to offer service usage and service billing plans for such devices that are more optimal for each type of device and each type of desired user experience. To accomplish this, more sophisticated service usage measuring and service usage billing systems are needed as compared to the conventional network based techniques in existence today. By providing more flexibility in service measurement and billing, more advantageous and cost effective service plans can be created for, for example, the new WWAN connected devices cited above for all three markets (e.g., consumer, business and machine to machine) that still maintain the necessary profit. margins for the WWAN carriers to be successful with these various service businesses.

(30) Accordingly, various embodiments disclosed herein provide for a new and flexible augmentation or replacement for existing carrier network service usage measurement, service usage accounting, and service usage billing systems and techniques.

(31) A charging data record (CDR) is a term that as used herein defines a formatted measure of device service usage information, typically generated by one or more network functions that supervise, monitor, and/or control network access for the device. CDRs typically form the basis for recording device network service usage, and often form the basis for billing for such usage. Various embodiments are provided herein for device assisted CDR creation, mediation, and billing. There are many limitations to the capabilities of service usage recording, aggregation and/or billing when CDRs are generated exclusively by network based functions or equipment. Accordingly, by either augmenting network based service usage measures with device based service usage measures, or by replacing network based service usage measures with device based service usage measures, it is possible to create a CDR generation, aggregation, mediation and/or billing solution that has superior or more desirable capabilities/features. While in theory, many of the service usage measures that can be evaluated on a device can also be evaluated in the network data path using various network equipment technologies including but not limited to deep packet inspection (DPI), there are many examples where measuring service usage at the device is either more desirable or more practical, or in some cases it is the only way to obtain the desired measure. Such examples include but are not limited to the following: Application layer service usage measures (e.g., traffic usage categorized by application or by combinations of application, destination, and/or content type); Usage measures that do not involve user traffic but instead involve network overhead traffic (e.g., basic connection maintenance traffic, signaling traffic, network logon/AAA/authentication/monitoring traffic, service software update traffic); Usage that is associated with services that are charged to another entity other than the end user (e.g., basic network connection service offer traffic, traffic associated with providing network access to or downloading service marketing information, traffic associated with advertiser sponsored services, traffic associated with content provider sponsored services, 911 service traffic); Usage measures involving encrypted traffic (e.g., traffic that is run over encrypted networking protocols or between secure end points); Implementing service usage measure collection and/or service usage billing

across multiple networks that may have different and in some cases incompatible, inaccessible (to the CDR system of record) or incomplete service usage measurement capabilities; Service usage measurement and/or service usage billing capabilities that are not supported by the present network gateways, routers, MWC/HLRs, AAA, CDR aggregation, CDR mediation, billing and/or provisioning systems; New service usage measures and/or new service usage billing capabilities that are desirable to implement in a manner that does not require major changes or upgrades to the existing network gateways, routers, MWC/HLRs, AAA, CDR aggregation, CDR mediation, billing and/or provisioning systems; New service usage measures and/or new service usage billing capabilities that are desirable to implement in a manner that allows for rapid definition and implementation of new service measures and/or billing plans; New service usage measures and/or new service usage billing capabilities that are desirable to implement in a manner that may be implemented in a manner that enables multiple device group definitions in which each device group gets a customized programmable definition for service usage collection, accounting and/or billing; Multi device billing; Multi user billing; Intermediate device billing with single user and multi user with and without multi device; Content downloads from a specific source to a specific application with the content being of a specific type or even identified down to a particular content ID; and/or Various other single event transactions used for billing purposes.

For these and other reasons, it is desirable to provide a system/process that utilizes device assisted service usage measures that provides either an enhancement of existing network based service usage CDR system capabilities and techniques and/or a replacement for network based CDR system capabilities and techniques.

(32) In some embodiments, techniques, such as a system and/or process, that utilize device assisted service usage measures include one or more of the following: (1) receiving a service usage measure from a device in communication with a wireless network, (2) verifying or protecting the validity of the service usage measure, (3) generating a CDR based on the service usage measure (e.g., device assisted CDR), (4) aggregating CDRs, and (5) mediating the CDR with network CDRs. In some embodiments, the techniques also include providing a design and provisioning of devices/network equipment to recognize the CDRs. In some embodiments, the techniques also include provisioning to recognize that the device belongs to a Device Assisted Services (DAS) device group and that corresponding CDRs should be accepted and mediated. In some embodiments, the device assisted CDRs are also generated using formats, network communications protocols, network device authentication and/or provisioning to allow device assisted CDRs into the network CDR system, encryption, and/or signatures as required by the network (e.g., to comply with network generated CDR requirements or based on any other network and/or service provider requirements and/or standards).

(33) In some embodiments, mediation rules include multi device, multi user, single user devices, and/or intermediate networking devices that can be single user or multi user, as described herein.

(34) In some embodiments, a device assisted CDR generator collects device based service usage measures that are used as the basis for, or as an enhancement (e.g., as a supplement or in addition) to, one or more (e.g., network generated) CDRs that provide one or more networking functions with properly formatted service usage reports that the network function(s) accepts as being transmitted from an authorized source, read, and utilized for helping to determine the service usage of a device or group of devices. In some embodiments, the network functions that the device assisted CDR generator shares CDRs with typically include one or more of the following: service usage/CDR aggregation and/or mediation servers, gateways, routers, communication nodes, Mobile Wireless Centers (MWCs, including HLRs), databases, AAA systems, billing interfaces, and billing systems. For example, the process of CDR creation in the CDR generator typically includes either using one or more device based measures of service usage, or one or more device based measures of service usage in combination with one or more network based measures of service usage, possibly processing one or more of such service usage measures according to a set of CDR

creation, CDR aggregation, and/or CDR mediation rules to arrive at a final device usage measure that is, for example, then formatted with the proper syntax, framed, possibly encrypted and/or signed, and encapsulated in a communication protocol or packet suitable for sharing with network functions. In some embodiments, the CDR generator resides in the device. In some embodiments, the CDR generator resides in a network server function that receives the device assisted service usage measures, along with possibly network based usage measures, and then creates a CDR (e.g., in the service controller **122**).

(35) In some embodiments, the device assisted CDR generator can reside in the service processor (e.g., service processor **115**), for example, in the service usage history or billing server functions. In some embodiments, the device assisted CDR generator resides in the device itself, for example, within the service processor functions, such as the billing agent or the service monitor agent.

(36) There are several factors that are considered in the various embodiments in order to create a useful, reliable, and secure device assisted CDR system, including, for example, but not limited to: Identification of each device based service usage measure with one or more usage transaction codes; Verification of the device based usage measure(s); Secure communication of the device based usage measures to the network; Efficient (e.g., low bandwidth) communication of the device based service usage measure; Coordination/comparison/aggregation of the device based service usage measure with network based service usage measure(s); Formatting the device based service usage measure into a CDR that can be properly communicated to the network functions and/or equipment that process service usage information; Causing the network based functions and/or equipment used for CDR collection, aggregation, mediation and/or billing to recognize, authorize, and accept communications and CDRs from the device assisted CDR generator, reading and properly implementing the correct network session context for the CDR so that the CDR is properly associated with the correct device/user/session; Implementing the CDR aggregation rules that determine how to collect and aggregate the device assisted CDRs as they are reported through the network CDR system hierarchy; Implementing the mediation rules that determine how the various device based service usage transaction code measures are combined and mediated with the other device based service usage transaction code measures to result in consistent service usage information for each of the transaction code categories maintained in the network; Implementing the mediation rules that determine how the device assisted CDRs are combined and mediated with network based CDRs to result in consistent service usage information for each of the transaction code categories maintained in the network; Implementing mediation rules to reconcile the variances between network based CDR usage measures and device assisted CDR usage measures; Classification of one or more device groups, with each group having the capability to uniquely define the service usage collection, accounting, and/or billing rules; Collecting CDRs generated on networks other than the home network so that service usage may be measured, accounted for, and/or billed for across multiple networks; Multi device billing; Multi user billing; and/or Intermediate device billing with single user and multi user with and without multi device.

(37) In some embodiments, verification of the relative accuracy of the device assisted service usage measure is provided. Given that, for example, the service usage measure is often being generated on an end user device or a device that is readily physically accessed by the general public or other non-secure personnel from a network management viewpoint, in some embodiments, the device agents used in one or more of the service processor **115** agents are protected from hacking, spoofing, and/or other misuse. Various techniques are provided herein for protecting the integrity of the agents used for generating the device assisted service usage measures.

(38) In some embodiments, the service usage measures are verified by network based cross checks using various techniques. For example, network based cross checks can provide valuable verification techniques, because, for example, it is generally not possible or at least very difficult to defeat well designed network based cross checks using various techniques, such as those described herein, even if, for example, the measures used to protect the device agents are defeated or if no

device protection measures are employed. In some embodiments, network based cross checks used to verify the device assisted service usage measures include comparing network based service usage measures (e.g. CDRs generated by service usage measurement apparatus in the network equipment, such as the BTS/BSCs **125**, RAN Gateways **410**, Transport Gateways **420**, Mobile Wireless Center/HLRs **132**, AAA **121**, Service Usage History/CDR Aggregation, Mediation, Feed **118**, or other network equipment), sending secure query/response command sequences to the service processor **115** agent(s) involved in device assisted CDR service usage measurement or CDR creation, sending test service usage event sequences to the device and verifying that the device properly reported the service usage, and using various other techniques, such as those described herein with respect to various embodiments.

(39) In some embodiments, one or more of the following actions are taken if the device based service usage measure is found to be in error or inaccurate: bill the user for usage overage or an out of policy device, suspend the device, quarantine the device, SPAN the device, and/or report the device to a network administration function or person.

(40) In some embodiments, the CDR syntax used to format the device assisted service usage information into a CDR and/or network communication protocols for transmitting CDRs are determined by industry standards (e.g., various versions of 3GPP TS 32.215 format and 3GPP2 TSG-X X.S0011 or TIA-835 format). In some embodiments, for a given network implementation the network designers will specify modifications of the standard syntax, formats and/or network communication/transmission protocols. In some embodiments, for a given network implementation the network designers will specify syntax, formats, and/or network communication/transmission protocols that are entirely different than the standards.

(41) In some embodiments, within the syntax and formatting for the CDR the device assisted service usage is typically categorized by a transaction code. For example, the transaction code can be similar or identical to the codes in use by network equipment used to generate CDRs, or given that the device is capable of generating a much richer set of service usage measures, the transaction codes can be a superset of the codes used by network equipment used to generate CDRs (e.g., examples of the usage activities that can be labeled. as transaction codes that are more readily supported by device assisted CDR systems as compared to purely network based CDR systems are provided herein).

(42) In some embodiments, the device sends an identifier for a usage activity tag, an intermediate server determines how to aggregate into CDR transaction codes and which CDR transaction code to use.

(43) In some embodiments, the device service processor **115** compartmentalizes usage by pre-assigned device activity transaction codes (e.g., these can be sub-transactions within the main account, transactions within a given bill-by-account transaction or sub-transactions within a bill-by-account transaction). The device implements bill-by-account rules to send different usage reports for each bill-by-account function. In some embodiments, the service controller **122** programs the device to instruct it on how to compartmentalize these bill-by-account service usage activities so that they can be mapped to a transaction code.

(44) In some embodiments, the device reports less compartmentalized service usage information and the service controller **122** does the mapping of service usage activities to CDR transaction codes, including in some cases bill-by-account codes.

(45) In some embodiments, the CDR sent to **118** or other network equipment, for example, can include various types of transaction codes including but not limited to a raw device usage CDR, a bill-by-account (e.g., a sub-activity transaction code) CDR, a billing offset CDR, and/or a billing credit CDR. For example, the decision logic (also referred to as business rules or CDR aggregation and mediation rules) that determines how these various types of CDR transaction codes are to be aggregated and mediated by the core network and the billing system can be located in the network equipment (e.g., a network element, such as service usage **118**), in the service controller **122**,

and/or in the billing system **123**.

(46) In some embodiments, the device assisted CDR generator uses the device assisted service usage measures to generate a CDR that includes service usage information, service usage transaction code(s), and, in some embodiments, network information context. In some embodiments, the service usage information, transaction code, and/or network information context is formatted into communication framing, syntax, encryption/signature, security and/or networking protocols that are compatible with the formatting used by conventional networking equipment to generate CDRs. For example, this allows networking equipment used for CDR collection, recording, aggregation, mediation, and/or conversion to billing records to properly accept, read, and interpret the CDRs that are generated with the assistance of device based service usage measurement. In some embodiments, the device assisted service measures are provided to an intermediate network server referred to as a service controller (e.g., service controller **122**). In some embodiments, the service controller uses a CDR feed aggregator for a wireless network to collect device generated usage information for one or more devices on the wireless network; and provides the device generated usage information in a syntax (e.g., charging data record (CDR)), and a communication protocol (e.g., 3GPP or 3GPP2, or other communication protocol(s)) that can be used by the wireless network to augment or replace network generated usage information for the one or more devices on the wireless network.

(47) In some embodiments, mediation rules include multi device, multi user, single user devices, intermediate networking devices that can be single user or multi user. For example, the device assisted CDRs can be formatted by the device assisted CDR generator to include a transaction code for one user account, even though the CDRs originate from multiple devices that all belong to the same user. This is an example for a multi-user device assisted CDR billing solution. In another example for a multi-user device assisted CDR billing solution, device assisted CDRs from multiple devices and multiple users can all be billed to the same account (e.g., a family plan or a corporate account), but the bill-by-account CDR transaction records can be maintained through the billing system so that sub-account visibility is provided so that the person or entity responsible for the main account can obtain visibility about which users and/or devices are creating most of the service usage billing. For example, this type of multi-user, multi-device device assisted CDR billing solution can also be used to track types of service usage and/or bill for types of service usage that are either impossible or at least very difficult to account and/or bill for with purely network based CDR systems. In some embodiments, bill-by-account CDR transaction records can be used to provide sponsored transaction services, account for network chatter, provide service selection interfaces, and other services for multi-user or multi-device service plans.

(48) In addition to conventional single user devices (e.g., cell phones, smart phones, netbooks/notebooks, mobile internet devices, personal navigation devices, music players, electronic eReaders, and other single user devices) device assisted service usage measurement and CDRs are also useful for other types of network capable devices and/or networking devices, such as intermediate networking devices (e.g., 3G/4G WWAN to WLAN bridges/routers/gateways, femto cells, DOCSIS modems, DSL modems, remote access/backup routers, and other intermediate network devices). For example, in such devices, particularly with a secure manner to verify that the device assisted service usage measures are relatively accurate and/or the device service processor **115** software is not compromised or hacked, many new service provider service delivery and billing models can be supported and implemented using the techniques described herein. For example, in a WiFi to WWAN bridge or router device multiple user devices can be supported with the same intermediate networking device in a manner that is consistent and compatible with the central provider's CDR aggregation and/or billing system by sending device assisted CDRs as described herein that have a service usage and/or billing code referenced to the end user and/or the particular intermediate device.

(49) In some embodiments, the device assisted CDRs generated for the intermediate networking

device are associated with a particular end user in which there can be several or many end users using the intermediate networking device for networking access, and in some embodiments, with each end user being required to enter a unique log-in to the intermediate networking device. For example, in this way, all devices that connect using WiFi to the intermediate networking device to get WWAN access generate CDRs can either get billed to a particular end user who is responsible for the master account for that device, or the CDRs can get billed in a secure manner, with verified relative usage measurement accuracy to multiple end users from the same intermediate networking device. In another example, an end user can have one account that allows access to a number of intermediate networking devices, and each intermediate networking device can generate consistent device assisted CDRs with transaction codes for that end user regardless of which intermediate networking device the end user logs in on.

(50) In some embodiments, some of the services provided by the intermediate networking device are billed to a specific end user device assisted CDR transaction code, while other bill-by-account services are billed to other transaction code accounts, such as sponsored partner transaction service accounts, network chatter accounts, sponsored advertiser accounts, and/or service sign up accounts. For example, in this manner, various embodiments are provided in which intermediate networking devices (e.g., a WWAN to WiFi router/bridge) can sold to one user but can service and be used to bill other users (e.g., and this can be covered in the first purchasing user's service terms perhaps in exchange for a discount), or such intermediate networking devices can be located wherever access is desired without concern that the device will be hacked into so that services can be acquired without charge.

(51) In some embodiments, various types of service usage transactions are billed for on the intermediate networking device, to any of one or more users, in which the information required to bill for such services is not available to the central provider or MVNO network equipment, just as is the case with, for example, conventional single user devices. In view of the various embodiments and techniques described herein, those skilled in the art will appreciate that similar service models are equally applicable not just to WWAN to WiFi intermediate networking devices, but also to the Femto Cell, remote access router, DOCSIS, DSL and other intermediate WWAN to WiFi networking devices.

(52) FIG. **1** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments. As shown, FIG. **1** includes a 4G/3G/2G wireless network operated by, for example, a central provider. As shown, various wireless devices **100** are in communication with base stations **125** for wireless network communication with the wireless network, and other devices **100** are in communication with Wi-Fi Access Points (APs) or Mesh 702 for wireless communication to Wi-Fi Access CPE 704 in communication with central provider access network **109**. In some embodiments, each of the wireless devices **100** includes a service processor **115** (as shown), and each service processor connects through a secure control plane link to a service controller **122**. In some embodiments, the network based service usage information (e.g., CDRs) is obtained from one or more network elements. As shown, an MVNO core network **210** also includes a CDR storage, aggregation, mediation, feed **118**, a MVNO billing interface **122**, and a MVNO billing system **123** (and other network elements as shown in FIG. **1**).

(53) As shown in FIG. **1**, a CDR storage, aggregation, mediation, feed **118** (e.g., service usage **118**, including a billing aggregation data store and rules engine) is a functional descriptor for, in some embodiments, a device/network level service usage information collection, aggregation, mediation, and reporting function located in one or more of the networking equipment components attached to one or more of the sub-networks shown in FIG. **1** (e.g., central provider access network **109** and/or central provider core network **110**), which is in communication with the service controller **122**, and a central billing interface **127**. As shown in FIG. **1**, service usage **118** is shown as a function in communication with the central provider core network **110**. In some embodiments, the CDR

storage, aggregation, mediation, feed **118** function is located elsewhere in the network or partially located in elsewhere or integrated with as part of other network elements. In some embodiments, CDR storage, aggregation, mediation, feed **118** functionality is located or partially located in the AAA server **121** and/or the mobile wireless center/Home Location Register (HLR) **132** (as shown, in communication with a DNS/DHCP server **126**). In some embodiments, service usage **118** functionality is located or partially located in the base station, base station controller and/or base station aggregator, collectively referred to as base station **125** in FIG. **1**. In some embodiments, CDR storage, aggregation, mediation, feed **118** functionality is located or partially located in a networking component in the central provider access network **109**, a networking component in the core network **110**, the central billing system **123**, the central billing interface **127**, and/or in another network component or function. This discussion on the possible locations for the network based and device based service usage information collection, aggregation, mediation, and reporting function (e.g., CDR storage, aggregation, mediation, feed **118**) can be easily generalized as described herein and as shown in the other figures described herein by one of ordinary skill in the art. Also as shown in FIG. **1**, the service controller **122** is in communication with the central billing interface **123** (also sometimes referred to as the external billing management interface or billing communication interface) **127**, which is in communication with the central billing system **123**. As shown, an order management **180** and subscriber management **182** are also in communication with the central provider core network **110** for facilitating order and subscriber management of services for the devices **100** in accordance with some embodiments.

(54) In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) provides a device/network level service usage information collection, aggregation, mediation, and reporting function. In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) collects device generated usage information for one or more devices on the wireless network (e.g., devices **100**); and provides the device generated usage information in a syntax and a communication protocol that can be used by the wireless network to augment or replace network generated usage information for the one or more devices on the wireless network. In some embodiments, the syntax is a charging data record (CDR), and the communication protocol is selected from one or more of the following: 3GPP, 3GPP2, or other communication protocols. In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) includes a service usage data store (e.g., a billing aggregator) and a rules engine for aggregating the collected device generated usage information. In some embodiments, the syntax is a charging data record (CDR), and the network device is a CDR feed aggregator, and the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) also aggregates CDRs for the one or more devices on the wireless network; applies a set of rules to the aggregated CDRs using a rules engine (e.g., bill by account, transactional billing, and/or any other billing or other rules for service usage information collection, aggregation, mediation, and reporting), and communicates a new set of CDRs for the one or more devices on the wireless network to a billing interface or a billing system (e.g., providing a CDR with a billing offset by account/service). In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) communicates a new set of CDRs for the one or more devices on the wireless network to a billing interface or a billing system. In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) communicates with a service controller to collect the device generated usage information for the one or more devices on the wireless network. In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) communicates with a service controller, in which the service controller is in communication with a interface or a billing system. In some embodiments, the CDR

storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) communicates the device generated usage information to a billing interface or a billing system. In some embodiments, the CDR storage, aggregation, mediation, feed (and/or other network elements or combinations of network elements) communicates with a transport gateway and/or a Radio Access Network (RAN) gateway to collect the network generated usage information for the one or more devices on the wireless network. In some embodiments, the service controller **122** communicates the device generated service usage information to the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements).

(55) In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) performs rules for performing a bill by account aggregation and mediation function. In some embodiments, the service controller **122** in communication with the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) performs a rules engine for aggregating and mediating the device generated usage information. In some embodiments, a rules engine device in communication with the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) performs a rules engine for aggregating and mediating the device generated usage information.

(56) In some embodiments, the rules engine is included in (e.g., integrated with/part of) the CDR storage, aggregation, mediation, feed **118**. In some embodiments, the rules engine and associated functions, as described herein, is a separate function/device. In some embodiments, the service controller **122** performs some or all of these rules engine based functions, as described herein, and communicates with the central billing interface **127**. In some embodiments, the service controller **122** performs some or all of these rules engine based functions, as described herein, and communicates with the central billing system **123**.

(57) In some embodiments, duplicate CDRs are sent from the network equipment to the billing system **123** that is used for generating service billing. In some embodiments, duplicate CDRs are filtered to send only those CDRs/records for devices controlled by the service controller and/or service processor (e.g., the managed devices). For example, this approach can provide for the same level of reporting, lower level of reporting, and/or higher level of reporting as compared to the reporting required by the central billing system **123**.

(58) In some embodiments, a bill-by-account billing offset is provided. For example, bill-by-account billing offset information can be informed to the central billing system **123** by providing a CDR aggregator feed that aggregates the device based service usage data feed to provide a new set of CDRs for the managed devices to the central billing interface **127** and/or the central billing system **123**. In some embodiments, transaction billing is provided using similar techniques. For example, transaction billing log information can be provided to the central billing interface **127** and/or the central billing system **123**.

(59) In some embodiments, the rules engine (e.g., performed by the service usage **118** or another network element, as described herein) provides a bill-by-account billing offset. For example, device generated usage information (e.g., charging data records (CDRs)) includes a transaction type field (e.g., indicating a type of service for the associated service usage information). The rules engine can apply a rule or a set of rules based on the identified service associated with the device generated usage information to determine a bill-by-account billing offset (e.g., a new CDR can be generated to provide the determined bill-by-account billing offset). In some examples, the determined bill-by-account billing offset can be provided as a credit to the user's service usage account (e.g., a new CDR can be generated with a negative offset for the user's service usage account, such as for network chatter service usage, or transactional service usage, or for any other purposes based on one or more rules performed by the rules engine).

(60) As another example, for a transactional service, a first new CDR can be generated with a

negative offset for the user's service usage account for that transactional service related usage, and a second new CDR can be generated with a positive service usage value to charge that same service usage to the transactional service provider (e.g., Amazon, eBay, or another transactional service provider). In some embodiments, the service controller **122** generates these two new CDRs, and the service usage **118** stores, aggregates, and communicates these two new CDRs to the central billing interface **127**. In some embodiments, the service controller **122** generates these two new CDRs, and the service usage **118** stores, aggregates, and communicates these two new CDRs to the central billing interface **127**, in which the central billing interface **127** applies rules (e.g., performs the rules engine for determining the hill-by-account billing offset).

(61) In some embodiments, the service controller **122** sends the device generated CDRs to the rules engine (e.g., service usage **118**), and the rules engine applies one or more rules, such as those described herein and/or any other billing/service usage related rules as would be apparent to one of ordinary skill in the art. In some embodiments, the service controller **122** generates CDRs similar to other network elements, and the rules (e.g., bill-by-account) are performed in the central billing interface **127**. For example, for the service controller **122** to generate CDRs similar to other network elements, in some embodiments, the service controller **122** is provisioned on the wireless network and behaves substantially similar to other CDR generators on the network) as would be apparent to one of ordinary skill in the art.

(62) In some embodiments, the service controller **122** is provisioned as a new type of networking function that is recognized as a valid and secure source for CDRs by the other necessary elements in the network (e.g., the Service Usage History/CDR Aggregation and Mediation Server **118**). In some embodiments, in which the network apparatus typically only recognize CDRs from certain types of networking equipment (e.g., RAN Gateway **410** or Transport Gateway **420** (as shown in FIG. **3**)), then the Service Controller **122** can provide authentication credentials to the other networking equipment that indicate it is one of the approved types of equipment (e.g., for purposes of generating/providing CDRs). In some embodiments, the link between the Service Controller **122** and the necessary CDR aggregation and mediation equipment is secured, authenticated, encrypted and/or signed.

(63) In some embodiments, the CDR storage, aggregation, mediation, feed **118** discards the network based service usage information (e.g., network based CDRs) received from one or more network elements. In these embodiments, the service controller **122** can provide the device based service usage information (e.g., device based CDRs) to the CDR storage, aggregation, mediation, feed **118** (e.g., the CDR storage, aggregation, mediation, feed **118** can just provide a store, aggregate, and communication function(s)), and the device based service usage information is provided to the central billing interface **127** or the central billing system **123**.

(64) In some embodiments, the device based CDRs and/or new CDRs generated based on execution of a rules engine as described herein is provided only for devices that are managed and/or based on device group, service plan, or any other criteria, categorization, and/or grouping.

(65) FIG. **2** illustrates another wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments. As shown in FIG. **2**, some devices **100** are in communication with DOCSIS Head End **125** and some devices **100** are in communication with DSLAM **125**, which are in communication with the central provider access network **109**.

(66) FIG. **3** illustrates another wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments. Referring now to the 4G/3G/2G access network as shown in FIG. **3**, the 4G/3G and 3G/2G base stations/nodes **125** are in communication with a 4G/3G/2G Radio Access Network (RAN) gateway **410** via a radio access network **405**, which are in communication with a 4G/3G/2G transport gateway **420** via an access transport network **415**. The central provider core network **110** is in network communication with the access transport network **415** (e.g., via a dedicated/leased line, and as shown, via a firewall

124). The Internet **120** is available via a firewall **124** and the transport gateway(s) **420**, as shown. Also, as shown, a network apparatus provisioning system **160**, order management **180**, and subscriber management **182** are in communication with the central provider core network **110**. As shown, a AAA server **121**, a mobile wireless center/Home Location Register (HLR) **132**, a DNS/DHCP **126**, and CDR storage, aggregation, mediation, feed **118** are also in communication with the access transport network **415**. The central billing system **123** and the central billing interface **127** are shown in communication with the central provider core network **110**.

(67) As shown, FIG. **3** includes a 4G/3G/2G wireless network operated by, for example, a central provider. In some embodiments, each of the wireless devices **100** includes a service processor **115** (as shown), and each service processor connects through a secure control plane link to a service controller **122**. In some embodiments, the network based service usage information (e.g., network generated CDRs) is obtained from Radio Access Network (RAN) gateway(s) **410** and/or transport gateway(s) **420**. In some embodiments, device based service usage information (e.g., device assisted CDRs) are generated by the service processor **115** and/or service controller **122** for some or all of the wireless devices **100** using similar techniques as described herein, and in some embodiments, such device based service usage information (e.g., device assisted CDRs) is sent to the CDR storage, aggregation, mediation, feed **118** (e.g., the CDR storage, aggregation, mediation, feed **118** can just provide a store, aggregate, and communication function(s)), and/or to the central billing interface **127** or the central billing system **123**, as similarly described herein with respect to various embodiments.

(68) FIG. **4** illustrates provisioning of a wireless network for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments. As shown in FIG. **4**, the provisioning of various network equipment is provided as shown to recognize each other as an authorized source of CDRs (e.g., this can be done manually or in an automated manner). For example, order management **180**, subscriber management, billing interface **127**, billing system **123**, network provisioning system **160**, service controller **122**, access network AAA server **121**, mobile wireless center **132**, and CDR storage, aggregation, mediation feed **118** communicate with each other for such provisioning, which can be implemented using various techniques. In some embodiments, the various network elements are provisioned to recognize device assisted CDRs being generated by the service controller **122**, which, for example, can be provided to the billing interface **127** and/or the billing system **123**. In some embodiments, network generated CDRs are provided by RAN/Access gateway **410**, aggregation/transport gateway **425**, and/or base station controller **125**. In some embodiments, other network elements generate/receive/store device assisted CDRs.

(69) In some embodiments, provisioning of various network equipment is provided to recognize a given device as belonging to a device group that supports a service usage and/or billing plan that relies upon and/or utilizes device assisted CDRs.

(70) In some embodiments, the CDR formats, transaction codes, and CDR transmission destinations are programmed for each device that generates CDRs, including the service controller **122** (e.g., in some embodiments, the service controller **122** is the intermediary for CDRs) and/or service processor **115** (e.g., in some embodiments, the device sends CDRs to network CDR aggregation or billing interface **127**/billing system **123** with no intermediate server function).

(71) FIG. **5** illustrates a network architecture for providing device assisted CDRs in accordance with some embodiments. As shown, network generated CDRs are sent from various network elements to the CDR storage, aggregation, mediation, feed **118** and the service controller **122**, as shown in dashed lines with arrows in FIG. **5**. In some embodiments, the network generated CDRs are used for verification of device assisted service (DAS) usage and/or billing information. In some embodiments, the network generated CDRs are provided to the service controller **122**, and the service controller **122** implements aggregation and/or mediation rules to examine and, in some cases, aggregate and/or mediate network generated/based CDRs with device assisted/based CDRs.

(72) In some embodiments, device assisted CDRs are sent from the service controller **122** to CDR storage, aggregation, mediation, feed **118** and communicated to the billing system **123**, as shown in solid lines with arrows in FIG. **5**. In some embodiments, CDR storage, aggregation, mediation, feed **118** uses DAS service usage CDRs to augment network generated/based CDRs with bill-by-account transaction codes (e.g., as similarly described herein). In some embodiments, CDR storage, aggregation, mediation, feed **118** implements aggregation and/or mediation rules to account for DAS CDR usage amount in a new bill-by-account transaction code and removes the same service usage amount from the bulk device account transaction code. In some embodiments, a first DAS CDR is sent for the new bill by account transaction code, and a second DAS CDR is sent to be used as a correction (credit) to the main device usage account transaction code, and CDR storage, aggregation, mediation, feed **118** implements the rules to perform this mediation. In some embodiments, a first DAS CDR is used for a given bill-by-account transaction code, and a second DAS CDR is used as the main device account transaction code, in which the service controller **122** (or device) has already implemented the mediation rules so that CDR storage, aggregation, mediation, feed **118** simply passes such DAS CDRs to billing after aggregating them.

(73) FIG. **6** illustrates another network architecture for providing device assisted CDRs in accordance with some embodiments. FIG. **6** also shows the communication of device assisted CDRs and network generated CDRs using solid and dashed lines with arrows, respectively. As shown, in some embodiments, CDR storage, aggregation, mediation, feed **118** sends network based CDRs to service controller **122** for various purposes, such as those previously described herein.

(74) In some embodiments, service controller **122** sends DAS CDRs to billing for various uses by the billing system **123**. In some embodiments, the billing system **123** uses DAS service usage CDRs to augment network based CDRs with bill-by-account transaction codes. In some embodiments, the billing system **123** implements aggregation and/or mediation rules to account for DAS CDR usage amount in a new bill-by-account transaction code and removes the same service usage amount from the bulk device account transaction code. In some embodiments, a first DAS CDR is sent for the new bill by account transaction code, and a second DAS CDR is sent to be used as a correction (credit) to the main device usage account transaction code, and the billing system **123** implements the rules to perform this mediation. In some embodiments, a first DAS CDR is used for a given bill-by-account transaction code, and a second is used as the main device account transaction code, in which the service controller **122** (or device) has already implemented the mediation rules so that the billing system **123** simply passes such DAS CDRs after aggregating them.

(75) FIG. **7** illustrates another network architecture for providing device assisted CDRs in accordance with some embodiments. FIG. **7** also shows the communication of device assisted CDRs and network generated CDRs using solid and dashed lines with arrows, respectively. FIG. **7** is similar to FIG. **6**, except as shown in FIG. **7**, service usage information is passed through the billing interface **127** instead of the billing CDR aggregation interface. For example, the service usage detailed bill-by-account information and offset (credit) information can be formatted as a CDR or can be formatted in a higher level syntax as required by the billing interface **127**.

(76) FIG. **8** illustrates another network architecture for providing device assisted CDRs in accordance with some embodiments. FIG. **8** also shows the communication of device assisted CDRs and network generated CDRs using solid and dashed lines with arrows, respectively. In some embodiments, as shown in FIG. **8**, the central provider need not modify the existing CDR storage, aggregation, mediation, feed **118**, so the additional aggregation and mediation rules discussed above with respect to FIG. **5** are implemented as a new layer of rules in a new network function, shown as secondary DAS CDR aggregation mediation **118**A, that is located between the billing system and the CDR storage, aggregation, mediation, feed **118**. For example, this new network function (e.g., secondary DAS CDR aggregation mediation **118**A) can reside in the network (as shown) or in the service processor **115**, in the service controller **122**, or elsewhere in the network or

on the device.

(77) FIG. **9** is a functional diagram illustrating a device based service processor **115** and a service controller **122** in accordance with some embodiments. For example, this provides relatively full featured device based service processor implementation and service controller implementation. As shown, this corresponds to a networking configuration in which the service controller **122** is connected to the Internet **120** and not directly to the access network **1610**. As shown, a data plane (e.g., service traffic plane) communication path is shown in solid line connections and control plane (e.g., service control plane) communication path is shown in dashed line connections. As will be apparent, the division in functionality between one device agent and another is based on, for example, design choices, networking environments, devices and/or services/applications, and various different combinations can be used in various different implementations. For example, the functional lines can be re-drawn in any way that the product designers see fit. As shown, this includes certain divisions and functional breakouts for device agents as an illustrative implementation, although other, potentially more complex, embodiments can include different divisions and functional breakouts for device agent functionality specifications, for example, in order to manage development specification and testing complexity and workflow. In addition, the placement of the agents that operate, interact with or monitor the data path can be moved or re-ordered in various embodiments. For example, the functional elements shown in FIG. **9** are described below with respect to FIGS. **10** and **11**.

(78) As shown in FIG. **9**, service processor **115** includes a service control device link **1691**. For example, as device based service control techniques involving supervision across a network become more sophisticated, it becomes increasingly important to have an efficient and flexible control plane communication link between the device agents and the network elements communicating with, controlling, monitoring, or verifying service policy. In some embodiments, the service control device link **1691** provides the device side of a system for transmission and reception of service agent to/from network element functions. In some embodiments, the traffic efficiency of this link is enhanced by buffering and framing multiple agent messages in the transmissions. In some embodiments, the traffic efficiency is further improved by controlling the transmission frequency or linking the transmission frequency to the rate of service usage or traffic usage. In some embodiments, one or more levels of security or encryption are used to make the link robust to discovery, eavesdropping or compromise. In some embodiments, the service control device link **1691** also provides the communications link and heartbeat timing for the agent heartbeat function. As discussed below, various embodiments disclosed herein for the service control device link **1691** provide an efficient and secure solution for transmitting and receiving service policy implementation, control, monitoring and verification information with other network elements.

(79) As shown in FIG. **9**, the service controller **122** includes a service control server link **1638**. In some embodiments, device based service control techniques involving supervision across a network (e.g., on the control plane) are more sophisticated, and for such it is increasingly important to have an efficient and flexible control plane communication link between the device agents (e.g., of the service processor **115**) and the network elements (e.g., of the service controller **122**) communicating with, controlling, monitoring, or verifying service policy. For example, the communication link between the service control server link **1638** of service controller **122** and the service control device link **1691** of the service processor **115** can provide an efficient and flexible control plane communication link, a service control link **1653** as shown in FIG. **9**, and, in some embodiments, this control plane communication link provides for a secure (e.g., encrypted) communications link for providing secure, bidirectional communications between the service processor **115** and the service controller **122**. In some embodiments, the service control server link **1638** provides the network side of a system for transmission and reception of service agent to/from network element functions. In some embodiments, the traffic efficiency of this link is enhanced by

buffering and framing multiple agent messages in the transmissions (e.g., thereby reducing network chatter). In some embodiments, the traffic efficiency is further improved by controlling the transmission frequency and/or linking the transmission frequency to the rate of service usage or traffic usage. In some embodiments, one or more levels of security and/or encryption are used to secure the link against potential discovery, eavesdropping or compromise of communications on the link. In some embodiments, the service control server link **1638** also provides the communications link and heartbeat timing for the agent heartbeat function.

(80) In some embodiments, the service control server link **1638** provides for securing, signing, encrypting and/or otherwise protecting the communications before sending such communications over the service control link **1653**. For example, the service control server link **1638** can send to the transport layer or directly to the link layer for transmission. In another example, the service control server link **1638** further secures the communications with transport layer encryption, such as TCP TLS SSH version 1 or 2 or another secure transport layer protocol. As another example, the service control server link **1638** can encrypt at the link layer, such as using IPSEC, various possible VPN services, other forms of IP layer encryption and/or another link layer encryption technique.

(81) As shown in FIG. **9**, the service controller **122** includes an access control integrity server **1654**. In some embodiments, the access control integrity server **1654** collects device information on service policy, service usage, agent configuration and/or agent behavior. For example, the access control integrity server **1654** can cross check this information to identify integrity breaches in the service policy implementation and control system. In another example, the access control integrity server **1654** can initiate action when a service policy violation or a system integrity breach is suspected.

(82) In some embodiments, the access control integrity server **1654** (and/or some other agent of service controller **122**) acts on access control integrity agent **1694** reports and error conditions. Many of the access control integrity agent **1654** checks can be accomplished by the server. For example, the access control integrity agent **1654** checks include one or more of the following: service usage measure against usage range consistent with policies (e.g., usage measure from the network and/or from the device); configuration of agents; operation of the agents; and/or dynamic agent download.

(83) In some embodiments, the access control integrity server **1654** (and/or some other agent of service controller **122**) verifies device service policy implementations by comparing various service usage measures (e.g., based on network monitored information, such as by using IPDRs or CDRs, and/or local service usage monitoring information) against expected service usage behavior given the policies that are intended to be in place. For example, device service policy implementations can include measuring total data passed, data passed in a period of time, IP addresses, data per IP address, and/or other measures such as location, downloads, email accessed, URLs, and comparing such measures expected service usage behavior given the policies that are intended to be in place.

(84) In some embodiments, the access control integrity server **1654** (and/or some other agent of service controller **122**) verifies device service policy, and the verification error conditions that can indicate a mismatch in service measure and service policy include one or more of the following: unauthorized network access (e.g., access beyond ambient service policy limits); unauthorized network speed (e.g., average speed beyond service policy limit); network data amount does not match policy limit (e.g., device not stop at limit without re-up/revising service policy); unauthorized network address; unauthorized service usage (e.g., VOIP, email, and/or web browsing); unauthorized application usage (e.g., email, VOIP, email, and/or web); service usage rate too high for plan, and policy controller not controlling/throttling it down; and/or any other mismatch in service measure and service policy. Accordingly, in some embodiments, the access control integrity server **1654** (and/or some other agent of service controller **122**) provides a policy/service control integrity service to continually (e.g., periodically and/or based on trigger

events) verify that the service control of the device has not been compromised and/or is not behaving out of policy.

(85) As shown in FIG. **9**, service controller **122** includes a service history server **1650**. In some embodiments, the service history server **1650** collects and records service usage or service activity reports from the Access Network AAA Server **1621** and the Service Monitor Agent **1696**. For example, although service usage history from the network elements can in certain embodiments be less detailed than service history from the device, the service history from the network can provide a valuable source for verification of device service policy implementation, because, for example, it is extremely difficult for a device error or compromise event on the device to compromise the network based equipment and software. For example, service history reports from the device can include various service tracking information, as similarly described above. In some embodiments, the service history server **1650** provides the service history on request to other servers and/or one or more agents. In some embodiments, the service history server **1650** provides the service usage history to the device service history **1618**. In some embodiments, for purposes of facilitating the activation tracking service functions (described below), the service history server **1650** maintains a history of which networks the device has connected to. For example, this network activity summary can include a summary of the networks accessed, activity versus time per connection, and/or traffic versus time per connection. As another example, this activity summary can further be analyzed or reported to estimate the type of service plan associated with the traffic activity for the purpose of bill sharing reconciliation.

(86) As shown in FIG. **9**, service controller **122** includes a policy management server **1652**. In some embodiments, the policy management server **1652** transmits policies to the service processor **115** via the service control link **1653**. In some embodiments, the policy management server **1652** manages policy settings on the device (e.g., various policy settings as described herein with respect to various embodiments) in accordance with a device service profile. In some embodiments, the policy management server **1652** sets instantaneous policies on policy implementation agents (e.g., policy implementation agent **1690**). For example, the policy management server **1652** can issue policy settings, monitor service usage and, if necessary, modify policy settings. For example, in the case of a user who prefers for the network to manage their service usage costs, or in the case of any adaptive policy management needs, the policy management server **1652** can maintain a relatively high frequency of communication with the device to collect traffic and/or service measures and issue new policy settings. In this example, device monitored service measures and any user service policy preference changes are reported, periodically and/or based on various triggers/events/requests, to the policy management server **1652**. In this example, user privacy settings generally require secure communication with the network (e.g., a secure service control link **1653**), such as with the policy management server **1652**, to ensure that various aspects of user privacy are properly maintained during such configuration requests/policy settings transmitted over the network. For example, information can be compartmentalized to service policy management and not communicated to other databases used for CRM for maintaining user privacy.

(87) In some embodiments, the policy management server **1652** provides adaptive policy management on the device. For example, the policy management server **1652** can issue policy settings and objectives and rely on the device based policy management (e.g., service processor **115**) for some or all of the policy adaptation. This approach can require less interaction with the device thereby reducing network chatter on service control link **1653** for purposes of device policy management (e.g., network chatter is reduced relative to various server/network based policy management approaches described above). This approach can also provide robust user privacy embodiments by allowing the user to configure the device policy for user privacy preferences/settings so that, for example, sensitive information (e.g., geo-location data, website history) is not communicated to the network without the user's approval. In some embodiments, the policy management server **1652** adjusts service policy based on time of day. In some embodiments,

the policy management server **1652** receives, requests or otherwise obtains a measure of network availability and adjusts traffic shaping policy and/or other policy settings based on available network capacity.

(88) As shown in FIG. **9**, service controller **122** includes a network traffic analysis server **1656**. In some embodiments, the network traffic analysis server **1656** collects/receives service usage history for devices and/or groups of devices and analyzes the service usage. In some embodiments, the network traffic analysis server **1656** presents service usage statistics in various formats to identify improvements in network service quality and/or service profitability. In other embodiments, the network traffic analysis server **1656** estimates the service quality and/or service usage for the network under variable settings on potential service policy. In other embodiments, the network traffic analysis server **1656** identifies actual or potential service behaviors by one or more devices that are causing problems for overall network service quality or service cost.

(89) As shown in FIG. **9**, service controller **122** includes a beta test server **1658**. In some embodiments, the beta test server **1658** publishes candidate service plan policy settings to one or more devices. In some embodiments, the beta test server **1658** provides summary reports of network service usage or user feedback information for one or more candidate service plan policy settings. In some embodiments, the beta test server **1658** provides a mechanism to compare the beta test results for different candidate service plan policy settings or select the optimum candidates for further policy settings optimization.

(90) As shown in FIG. **9**, service controller **122** includes a service download control server **1660**. In some embodiments, the service download control server **1660** provides a download function to install and/or update service software elements (e.g., the service processor **115** and/or agents/components of the service processor **115**) on the device, as described herein.

(91) As shown in FIG. **9** service controller **122** includes a billing event server **1662**. In some embodiments, the billing event server **1662** collects billing events, provides service plan information to the service processor **115**, provides service usage updates to the service processor **115**, serves as interface between device and central billing server **1619**, and/or provides trusted third party function for certain ecommerce billing transactions.

(92) As shown in FIG. **9**, the Access Network AAA server **1621** is in network communication with the access network **1610**. In some embodiments, the Access Network AAA server **1621** provides the necessary access network AAA services (e.g., access control and authorization functions for the device access layer) to allow the devices onto the central provider access network and the service provider network. In some embodiments, another layer of access control is required for the device to gain access to other networks, such as the Internet, a corporate network and/or a machine to machine network. This additional layer of access control can be implemented, for example, by the service processor **115** on the device. In some embodiments, the Access Network AAA server **1621** also provides the ability to suspend service for a device and resume service for a device based on communications received from the service controller **122**. In some embodiments, the Access Network AAA server **1621** also provides the ability to direct routing for device traffic to a quarantine network or to restrict or limit network access when a device quarantine condition is invoked. In some embodiments, the Access Network AAA server **1621** also records and reports device network service usage (e.g., device network service usage can be reported to device service history **1618**).

(93) As shown in FIG. **9**, the device service history **1618** is in network communication with the access network **1610**. In some embodiments, the device service history **1618** provides service usage data records used for various purposes in various embodiments. In some embodiments, the device service history **1618** is used to assist in verifying service policy implementation. In some embodiments, the device service history **1618** is used to verify service monitoring. In some embodiments, the device service history **1618** is used to verify billing records and/or billing policy implementation. In some embodiments, the device service history **1618** is used to synchronize

and/or verify the local service usage counter.

(94) As shown in FIG. **9**, the central provider billing server **1619** is in network communication with the access network **1610**. In some embodiments, the central provider billing server **1619** provides a mediation function for central provider billing events. For example, the central provider billing server **1619** can accept service plan changes. In some embodiments, the central provider billing server **1619** provides updates on device service usage, service plan limits and/or service policies. In some embodiments, the central provider billing server **1619** collects billing events, formulates bills, bills service users, provides certain billing event data and service plan information to the service controller **122** and/or device **100**.

(95) As shown in FIG. **9**, in some embodiments, modem selection and control **1811** selects the access network connection and is in communication with the modem firewall **1655**, and modem drivers **1831**, **1815**, **1814**, **1813**, **1812** convert data traffic into modem bus traffic for one or more modems and are in communication with the modem selection and control **1811**. In some embodiments, different profiles are selected based on the selected network connection (e.g., different service profiles/policies for WWAN, WLAN, WPAN, Ethernet and/or DSL network connections), which is also referred to herein as multimode profile setting. For example, service profile settings can be based on the actual access network (e.g., home DSL/cable or work network) behind the Wi-Fi not the fact that it is Wi-Fi (or any other network, such as DSL/cable, satellite, or T-1), which is viewed as different than accessing a Wi-Fi network at the coffee shop. For example, in a Wi-Fi hotspot situation in which there are a significant, number of users on a DSL or T-1 backhaul, the service controller can sit in a service provider cloud or an MVNO cloud, the service controls can be provided by a VSP capability offered by the service provider or the service controller can be owned by the hotspot service provider that uses the service controller on their own without any association with an access network service provider. For example, the service processors can be controlled by the service controller to divide up the available bandwidth at the hotspot according to QoS or user sharing rules (e.g., with some users having higher differentiated priority (potentially for higher service payments) than other users). As another example, ambient services (as similarly described herein) can be provided for the hotspot for verified service processors.

(96) In some embodiments, the service processor **115** and service controller **122** are capable of assigning multiple service profiles associated with multiple service plans that the user chooses individually or in combination as a package. For example, a device **100** starts with ambient services that include free transaction services wherein the user pays for transactions or events rather than the basic service (e.g., a news service, eReader, PND service, pay as you go session Internet) in which each service is supported with a bill by account capability to correctly account for any subsidized partner billing to provide the transaction services (e.g., Barnes and Noble may pay for the eReader service and offer a revenue share to the service provider for any book or magazine transactions purchased from the device **100**). In some embodiments, the bill by account service can also track the transactions and, in some embodiments, advertisements for the purpose of revenue sharing, all using the service monitoring capabilities disclosed herein. After initiating services with the free ambient service discussed above, the user may later choose a post-pay monthly Internet, email and SMS service. in this case, the service controller **122** would obtain from the billing system **123** in the case of network based billing (or in some embodiments the service controller **122** billing event server **1622** in the case of device based billing) the billing plan code for the new Internet, email and SMS service. In some embodiments, this code is cross referenced in a database (e.g., the policy management server **1652**) to find the appropriate service profile for the new service in combination with the initial ambient service. The new superset service profile is then applied so that the user maintains free access to the ambient services, and the billing partners continue to subsidize those services, the user also gets access to Internet services and may choose the service control profile (e.g., from one of the embodiments disclosed herein). The superset profile is the profile that

provides the combined capabilities of two or more service profiles when the profiles are applied to the same device **100** service processor. In some embodiments, the device **100** (service processor **115**) can determine the superset profile rather than the service controller **122** when more than one "stackable" service is selected by the user or otherwise applied to the device. The flexibility of the service processor **115** and service controller **122** embodiments described herein allow for a large variety of service profiles to be defined and applied individually or as a superset to achieve the desired device **100** service features.

(97) As shown in FIG. **9**, an agent communication bus **1630** represents a functional description for providing communication for the various service processor **115** agents and functions. In some embodiments, as represented in the functional diagram illustrated in FIG. **9**, the architecture of the bus is generally multipoint to multipoint so that any agent can communicate with any other agent, the service controller or in some cases other components of the device, such user interface **1697** and/or modem components. As described below, the architecture can also be point to point for certain agents or communication transactions, or point to multipoint within the agent framework so that all agent communication can be concentrated, or secured, or controlled, or restricted, or logged or reported. In some embodiments, the agent communication bus is secured, signed, encrypted, hidden, partitioned and/or otherwise protected from unauthorized monitoring or usage. In some embodiments, an application interface agent (not shown) is used to literally tag or virtually tag application layer traffic so that the policy implementation agent(s) **1690** has the necessary information to implement selected traffic shaping solutions. In some embodiments, an application interface agent (not shown) is in communication with various applications, including a TCP application **1604**, an IP application **1605**, and a voice application **1602**.

(98) In some embodiments, device assisted services (DAS) techniques for providing an activity map for classifying or categorizing service usage activities to associate various monitored activities (e.g., by URL, by network domain, by website, by network traffic type, by application or application type, and/or any other service usage activity categorization/classification) with associated IP addresses are provided. In some embodiments, a policy control agent (not shown), service monitor agent **1696**, or another agent or function (or combinations thereof) of the service processor **115** provides a DAS activity map. In some embodiments, a policy control agent, service monitor agent, or another agent or function (or combinations thereof) of the service processor provides an activity map for classifying or categorizing service usage activities to associate various monitored activities (e.g., by Uniform Resource Locator (URL), by network domain, by website, by network traffic type, by application or application type, and/or any other service usage activity classification/categorization) with associated IP addresses. In some embodiments, a policy control agent, service monitor agent, or another agent or function (or combinations thereof) of the service processor determines the associated IP addresses for monitored service usage activities using various techniques to snoop the DNS request(s) (e.g., by performing such snooping techniques on the device **100** the associated IP addresses can be determined without the need for a network request for a reverse DNS lookup). In some embodiments, a policy control agent, service monitor agent, or another agent or function (or combinations thereof) of the service processor records and reports IP addresses or includes a DNS lookup function to report IP addresses or IP addresses and associated URLs for monitored service usage activities. For example, a policy control agent, service monitor agent, or another agent or function (or combinations thereof) of the service processor can determine the associated IP addresses for monitored service usage activities using various techniques to perform a DNS lookup function (e.g., using a local DNS cache on the monitored device **100**). In some embodiments, one or more of these techniques are used to dynamically build and maintain a DAS activity map that maps, for example, URLs to IP addresses, applications to IP addresses, content types to IP addresses, and/or any other categorization/classification to IP addresses as applicable. In some embodiments, the DAS activity map is used for various DAS traffic control and/or throttling techniques as described herein with

respect to various embodiments. In some embodiments, the DAS activity map is used to provide the user various UI related information and notification techniques related to service usage as described herein with respect to various embodiments. In some embodiments, the DAS activity map is used to provide service usage monitoring, prediction/estimation of future service usage, service usage billing (e.g., bill by account and/or any other service usage/billing categorization techniques), DAS techniques for ambient services usage monitoring, DAS techniques for generating micro-CDRs (e.g., also referred to as service usage partition, service usage recording partition, service charging bucket, device generated CDRs, such as in the case where the device and not a network component are generating the usage records, ambient usage records, specialized service usage records, or other terms to indicate a service usage data record generated to provide a more refined or detailed breakdown of service usage for the device), and/or any of the various other DAS related techniques as described herein with respect to various embodiments.

(99) In some embodiments, all or a portion of the service processor **115** functions disclosed herein are implemented in software. In some embodiments, all or a portion of the service processor **115** functions are implemented in hardware. In some embodiments, all or substantially all of the service processor **115** functionality (as discussed herein) is implemented and stored in software that can be performed on (e.g., executed by) various components in device **100**. In some embodiments, it is advantageous to store or implement certain portions or all of service processor **115** in protected or secure memory so that other undesired programs (and/or unauthorized users) have difficulty accessing the functions or software in service processor **115**. In some embodiments, service processor **115**, at least in part, is implemented in and/or stored on secure non-volatile memory (e.g., non volatile memory can be secure non-volatile memory) that is not accessible without pass keys and/or other security mechanisms. In some embodiments, the ability to load at least a portion of service processor **115** software into protected non-volatile memory also requires a secure key and/or signature and/or requires that the service processor **115** software components being loaded into non-volatile memory are also securely encrypted and appropriately signed by an authority that is trusted by a secure software downloader function, such as service downloader **1663** as shown in FIG. **16**. In some embodiments, a secure software download embodiment also uses a secure non-volatile memory. Those of ordinary skill in the art will also appreciate that all memory can be on-chip, off-chip, on-board and/or off-board.

(100) FIG. **10** provides a table summarizing various service processer **115** functional elements in accordance with some embodiments. Many of these agents are similarly described above, and the table shown in FIG. **10** is not intended to be an exhaustive summary of these agents, nor an exhaustive description of all functions that the agents perform or are described herein, but rather FIG. **10** is provided as a summary aid in understanding the basic functions of each agent in accordance with some embodiments and how the agents interact with one another, with the service controller server elements, and/or with other network functions in certain embodiments to form a reliable device based service delivery solution and/or platform.

(101) FIG. **11** provides a table summarizing various service controller **122** functional elements in accordance with some embodiments. Many of these agents/elements are similarly described above, and the table shown in FIG. **11** is not intended to be an exhaustive summary of these server elements, nor an exhaustive description of all functions that the elements perform or are described herein, but rather FIG. **11** is provided as a summary aid in understanding the basic functions of each element in accordance with some embodiments and how the elements interact with one another, certain network elements, and/or the service processor agents in certain embodiments to form a reliable device based service delivery solution and/or platform.

(102) FIG. **12** illustrates a device stack providing various service usage measurement from various points in the networking stack for a service monitor agent, a billing agent, and an access control integrity agent to assist in verifying the service usage measures and billing reports in accordance with some embodiments. As shown in FIG. **12**, several service agents take part in data path

operations to achieve various data path improvements, and, for example, several other service agents can manage the policy settings for the data path service, implement billing for the data path service, manage one or more modem selection and settings for access network connection, interface with the user and/or provide service policy implementation verification. Additionally, in some embodiments, several agents perform functions to assist in verifying that the service control or monitoring policies intended to be in place are properly implemented, the service control or monitoring policies are being properly adhered to, that the service processor or one or more service agents are operating properly, to prevent unintended errors in policy implementation or control, and/or to prevent tampering with the service policies or control. As shown, the service Measurement points labeled I through VI represent various service measurement points for service monitor agent **1696** and/or other agents to perform various service monitoring activities. Each of these measurement points can have a useful purpose in various embodiments described herein. For example, each of the traffic measurement points that is employed in a given design can be used by a monitoring agent to track application layer traffic through the communication stack to assist policy implementation functions, such as the policy implementation agent **1690**, or in some embodiments the modem firewall agent **1655** or the application interface agent, in making a determination regarding the traffic parameters or type once the traffic is farther down in the communication stack where it is sometimes difficult or impossible to make a complete determination of traffic parameters. The particular locations for the measurement points provided in these figures are intended as instructional examples, and other measurement points can be used for different embodiments, as will be apparent to one of ordinary skill in the art in view of the embodiments described herein. Generally, in some embodiments, one or more measurement points within the device can be used to assist in service control verification and/or device or service troubleshooting.

(103) In some embodiments, the service monitor agent and/or other agents implement virtual traffic tagging by tracking or tracing packet flows through the various communication stack formatting, processing and encryption steps, and providing the virtual tag information to the various agents that monitor, control, shape, throttle or otherwise observe, manipulate or modify the traffic. This tagging approach is referred to herein as virtual tagging, because there is not a literal data flow, traffic flow or packet tag that is attached to flows or packets, and the book-keeping to tag the packet is done through tracking or tracing the flow or packet through the stack instead. In some embodiments, the application interface and/or other agents identify a traffic flow, associate it with a service usage activity and cause a literal tag to be attached to the traffic or packets associated with the activity. This tagging approach is referred to herein as literal tagging. There are various advantages with both the virtual tagging and the literal tagging approaches. For example, it can be preferable in some embodiments to reduce the inter-agent communication required to track or trace a packet through the stack processing by assigning a literal tag so that each flow or packet has its own activity association embedded in the data. As another example, it can be preferable in some embodiments to re-use portions of standard communication stack software or components, enhancing the verifiable traffic control or service control capabilities of the standard stack by inserting additional processing steps associated with the various service agents and monitoring points rather than re-writing the entire stack to correctly process literal tagging information, and in such cases, a virtual tagging scheme may be desired. As yet another example, some standard communication stacks provide for unused, unspecified or otherwise available bit fields in a packet frame or flow, and these unused, unspecified or otherwise available bit fields can be used to literally tag traffic without the need to re-write all of the standard communication stack software, with only the portions of the stack that are added to enhance the verifiable traffic control or service control capabilities of the standard stack needing to decode and use the literal tagging information encapsulated in the available bit fields. In the case of literal tagging, in some embodiments, the tags are removed prior to passing the packets or flows to the network or to the applications utilizing the

stack. In some embodiments, the manner in which the virtual or literal tagging is implemented can be developed into a communication standard specification so that various device or service product developers can independently develop the communication stack and/or service processor hardware and/or software in a manner that is compatible with the service controller specifications and the products of other device or service product developers.

(104) It will be appreciated that although the implementation/use of any or all of the measurement points illustrated in FIG. **12** is not required to have an effective implementation, such as was similarly shown with respect to various embodiments described herein, various embodiments can benefit from these and/or similar measurement points. It will also be appreciated that the exact measurement points can be moved to different locations in the traffic processing stack, just as the various embodiments described herein can have the agents affecting policy implementation moved to different points in the traffic processing stack while still maintaining effective operation. In some embodiments, one or more measurement points are provided deeper in the modem stack where, for example, it is more difficult to circumvent and can be more difficult to access for tampering purposes if the modem is designed with the proper software and/or hardware security to protect the integrity of the modem stack and measurement point(s).

(105) Referring to FIG. **12**, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. Example measurement point VI resides within or just above the modem driver layer. For example, the modem driver performs modem bus communications, data protocol translations, modem control and configuration to interface the networking stack traffic to the modem. As shown, measurement point VI is common to all modem drivers and modems, and it is advantageous for certain embodiments to differentiate the traffic or service activity taking place through one modem from that of one or more of the other modems. In some embodiments, measurement point VI, or another measurement point, is located over, within or below one or more of the individual modem drivers. The respective modem buses for each modem reside between example measurement points V and VI. In the next higher layer, a modem selection & control layer for multimode device based communication is provided. In some embodiments, this layer is controlled by a network decision policy that selects the most desirable network modem for some or all of the data traffic, and when the most desirable network is not available the policy reverts to the next most desirable network until a connection is established provided that one of the networks is available. In some embodiments, certain network traffic, such as verification, control, redundant or secure traffic, is routed to one of the networks even when some or all of the data traffic is routed to another network. This dual routing capability provides for a variety of enhanced security, enhanced reliability or enhanced manageability devices, services or applications. In the next higher layer, a modem firewall is provided. For example, the modem firewall provides for traditional firewall functions, but unlike traditional firewalls, in order to rely on the firewall for verifiable service usage control, such as access control and security protection from unwanted networking traffic or applications, the various service verification techniques and agents described herein are added to the firewall function to verify compliance with service policy and prevent tampering of the service controls. In some embodiments, the modem firewall is implemented farther up the stack, possibly in combination with other layers as indicated in other Figures. In some embodiments, a dedicated firewall function or layer is provided that is independent of the other processing layers, such as the policy implementation layer, the packet forwarding layer and/or the application layer. In some embodiments, the modem firewall is implemented farther down the stack, such as within the modem drivers, below the modem drivers, or in the modem itself. Example measurement point IV resides between the modem firewall layer and an IP queuing and routing layer. As shown, an IP queuing and routing layer is separate from the policy implementation layer where the policy implementation agent implements a portion of the traffic control and/or service usage control

policies. As described herein, in some embodiments, these functions are separated so that a standard network stack function can be used for IP queuing and routing, and the modifications necessary to implement the policy implementation agent functions can be provided in a new layer inserted into the standard stack. In some embodiments, the IP queuing and routing layer is combined with the traffic or service usage control layer. For example, a combined routing and policy implementation layer embodiment can also be used with the other embodiments, such as shown in FIG. **12**. Measurement point III resides between the IP queuing and routing layer and a policy implementation agent layer. Measurement point II resides between the policy implementation agent layer and the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Measurement point I resides between the network services API layer and an application layer, shown as application service interface agent in the device communications stack of FIG. **12**.

(106) As shown in FIG. **12**, the application service interface layer is above the standard networking stack API and, in some embodiments, its function is to monitor and in some cases intercept and process the traffic between the applications and the standard networking stack API. In some embodiments, the application service interface layer identifies application traffic flows before the application traffic flows are more difficult or practically impossible to identify farther down in the stack. In some embodiments, the application service interface layer in this way assists application layer tagging in both the virtual and literal tagging cases. In the case of upstream traffic, the application layer tagging is straight forward, because the traffic originates at the application layer. In some downstream embodiments, where the traffic or service activity classification relies on traffic attributes that are readily obtainable, such as source address or URL, application socket address, IP destination address, time of day or any other readily obtained parameter, the traffic type can be identified and tagged for processing by the firewall agent or another agent as it initially arrives. In other embodiments, as described herein, in the downstream case, the solution is generally more sophisticated when a traffic parameter that is needed to classify the manner in which the traffic flow is to be controlled or throttled is not readily available at the lower levels of the stack, such as association with an aspect of an application, type of content, something contained within TLS, IPSEC or other secure format, or other information associated with the traffic. Accordingly, in some embodiments the networking stack identifies the traffic flow before it is fully characterized, categorized or associated with a service activity, and then passes the traffic through to the application interface layer where the final classification is completed. In such embodiments, the application interface layer then communicates the traffic flow ID with the proper classification so that after an initial short traffic burst or time period the policy implementation agents can properly control the traffic. In some embodiments, there is also a policy for tagging and setting service control policies for traffic that cannot be fully identified with all sources of tagging including application layer tagging.

(107) As shown in FIG. **12**, a service monitor agent, which is also in communication with the agent communication bus **1630**, communicates with various layers of the device communications stack. For example, the service monitor agent, performs monitoring at each of measurement points I through VI, receiving information including application information, service usage and other service related information, and assignment information. An access control integrity agent is in communication with the service monitor agent via the agent communications bus **1630**, as also shown.

(108) FIG. **13** illustrates an embodiment similar to FIG. **12** in which some of the service processor is implemented on the modem and some of the service processor is implemented on the device application processor in accordance with some embodiments. In some embodiments, a portion of

the service processor is implemented on the modem (e.g., on modem module hardware or modem chipset) and a portion of the service processor is implemented on the device application processor subsystem. It will be apparent to one of ordinary skill in the art that variations of the embodiment depicted in FIG. **13** are possible where more or less of the service processor functionality is moved onto the modem subsystem or onto the device application processor subsystem. For example, such embodiments similar to that depicted in FIG. **13** can be motivated by the advantages of including some or all of the service processor network communication stack processing and/or some or all of the other service agent functions on the modem subsystem (e.g., and such an approach can be applied to one or more modems). For example, the service processor can be distributed as a standard feature set contained in a modem chipset hardware of software package or modem module hardware or software package, and such a configuration can provide for easier adoption or development by device OEMs, a higher level of differentiation for the chipset or modem module manufacturer, higher levels of performance or service usage control implementation integrity or security, specification or interoperability standardization, and/or other benefits.

(109) Referring to FIG. **13**, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for modem MAC/PHY layer at the bottom of the device communications stack. Measurement point IV resides above the modem MAC/PHY layer. The modem firewall layer resides between measurement points IV and III. In the next higher layer, the policy implementation agent is provided, in which the policy implementation agent is implemented on the modem (e.g., on modem hardware). Measurement point II resides between the policy implementation agent and the modem driver layer, which is then shown below a modem bus layer. The next higher layer is shown as the IP queuing and routing layer, followed by the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Measurement point I resides between the network services API layer and an application layer, shown as application service interface agent in the device communications stack of FIG. **13**.

(110) FIGS. **14**A though **14**E illustrate various embodiments of intermediate networking devices that include a service processor for the purpose of verifiable service usage measurement, reporting, and billing reports in accordance with some embodiments. For example, FIGS. **14**A through **14**E illustrate various extended modem alternatives for access network connection through an intermediate modem or networking device combination that has a connection (e.g., LAN connection) to one or more devices **100**.

(111) In some embodiments, device **100** includes a 3G and/or 4G network access connection in combination with the WiFi LAN connection to the device **100**. For example, the intermediate device or networking device combination can be a device that simply translates the Wi-Fi data to the WWAN access network without implementing any portion of the service processor **115** as shown in FIG. **14**A. In some embodiments, an intermediate device or networking device combination includes a more sophisticated implementation including a networking stack and some embodiments a processor, as is the case for example if the intermediate networking device or networking device combination includes a router function, in which case the service processor **115** can be implemented in part or entirely on the intermediate modem or networking device combination. The intermediate modem or networking device combination can also be a multi-user device in which more than one user is gaining access to the 3G or 4G access network via the Wi-Fi LAN connection. In the case of such a multi-user network, the access network connection can include several managed service links using multiple instantiations of service processor **115**, each instantiation, for example, being implemented in whole or in part on device **100** with the intermediate modem or networking device combination only providing the translation services

from the Wi-Fi LAN to the WWAN access network.

(112) Referring now to FIGS. **14**B through **14**D, in some embodiments, the service processors **115** are implemented in part or in whole on the intermediate modem or networking device combination. In the case where the service processor **115** is implemented in part or in whole on the intermediate modem or networking device combination, the service processor **115** can be implemented for each device or each user in the network so that there are multiple managed service provider accounts all gaining access through the same intermediate modem or networking device combination. In some embodiments, the functions of service processor **115** are implemented on an aggregate account that includes the WWAN access network traffic for all of the users or devices connected to the Wi-Fi LAN serviced by the intermediate modem or networking device combination. In some embodiments, the central provider can also provide an aggregated account service plan, such as a family plan, a corporate user group plan and/or an instant hotspot plan. In the case where there is one account for the intermediate modem or networking device combination, the intermediate modem or networking device combination can implement a local division of services to one or more devices **100** or users in which the services are controlled or managed by the intermediate modem or networking device combination or the device **100**, but the management is not subject to service provider control and is auxiliary to the service management or service policy implementation performed by service processors **115**. In some embodiments, another service model can also be supported in which there is an aggregate service provider plan associated with one intermediate modem or networking device combination, or a group of intermediate modems or networking device combinations but where each user or device still has its own service plan that is a sub-plan under the aggregate plan so that each user or device has independent service policy implementation with a unique instantiation of service processor **115** rather than aggregate service policy implementation across multiple users in the group with a single instantiation of service processor **115**.

(113) As shown in FIG. **14**B, in some embodiments, device **100** includes a Wi-Fi modem, a Wi-Fi modem combined with a 3G and/or 4G WWAN modem on intermediate modem or networking device combination **1510**, and the intermediate modem or networking device combination forwards WWAN access network traffic to and from device **100** via the Wi-Fi link. For example, the service processor **115** can be implemented in its entirety on device **100** and the service provider account can be associated exclusively with one device. Similarly, as shown in FIG. **14**C, such an implementation can be provided using a different access modem and access network, such as a 2G and/or 3G WWAN, DSL wire line, cable DOCSIS wire line or fiber wire line configuration in place of the 3G and/or 4G access network connection to the intermediate modem or networking device combination **1510**. In addition, various other embodiments similarly use DSL as shown in FIG. **14**D, USB, Ethernet, Bluetooth, or another LAN or point to point connection from device **100** to the intermediate modem or networking device combination **1510**, or a femto cell modem and DSL/cable/T1/other combination as shown in FIG. **14**E.

(114) FIG. **15** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including a proxy server(s) **270** in accordance with some embodiments. As shown, FIG. **2** includes a proxy server(s) **270** in communication with a 4G/3G/2G wireless network operated by, for example, a central provider. For example, the proxy server(s) **270** can be used to implement and/or assist in providing various techniques described herein, such as service usage measurement and/or other techniques as described herein.

(115) In some embodiments, it may not be possible to accurately identify every network service access attempt or service usage (e.g., or traffic access) as belonging to a given service usage partition (e.g., a given ambient service usage, background network chatter usage, user service plan usage, emergency service usage, and/or other type of service usage). As used herein, the terms service usage partition, service usage recording partition, service charging bucket, and micro-CDRs are used interchangeably. Accordingly, it is desirable to provide a service charging bucket for traffic

that is allowed and not definitively identified as belonging to a known service charging bucket. This allows for techniques to employ an “allow but verify” approach to traffic that is likely to be legitimately associated with an ambient service or a user service or a network service that is intended to be allowed, but is not definitively identified as being associated with an allowed service.

(116) As an example, there may be a web site access associated with an ambient service that does not have a reference identifier or other traffic parameter that allows the service processor to associate it with the correct ambient service. In this case, a set of rules can be applied to determine if it is likely that the web site access is a legitimate access given the access control policies that are in place, and if it is the access can be allowed and the traffic usage either recorded in the ambient service charging bucket that it is suspected to be associated with, or the traffic usage can be charged to a network chatter service usage bucket, or the traffic usage can be charged to the user service usage bucket, or the traffic usage may be recorded in a “not classified but allowed” service charging bucket. In some embodiments, in which such traffic is charged to the “not classified but allowed” service usage charging bucket, additional verification measures are employed to ensure that the amount of traffic that is not classified but allowed does not grow too large or become a back-door for service usage errors. For example, the access control policy rules for allowing unclassified traffic can be relatively loose as long as the amount of service usage charges accumulating in the not classified charging bucket remains within certain bounds, and/or the rate of service usage charged to the not classified bucket remains within certain bounds, but if the not classified traffic becomes large or the rate of not classified traffic growth becomes large then the rules governing when to allow not classified traffic can be tightened.

(117) As another example, a browser application can access a web site that is known to be an ambient service website, and that web site might serve back a series of traffic flows, some of which are associated with the ambient service website through URL identifiers that are known to be part of the website, and other traffic can be associated with the ambient service website by virtue of a referring website tag or header, and some traffic can be returned to the same application with a relatively close time proximity to the other traffic as being identified as ambient traffic. In this example, as long as the not classified traffic service charging bucket does not exceed a given pre-set policy limit on its size, and/or does not grow faster than a given pre-set policy rate, and/or is received within a certain pre-set policy period of time difference from the time that other ambient service charging bucket traffic is received, then the not classified traffic is continued to be allowed. However, if the not classified traffic amount or rate of growth exceeds the pre-set policy limits, or if the period of time between when verified ambient service traffic is received and the not, classified traffic is received exceeds policy limits, then the not classified traffic can be blocked or other action can be taken to further analyze the not classified traffic.

(118) In some embodiments, it is important to provide a hierarchy of service usage charging rules for the various service usage partitions on a device. As an example, for a given service plan there can be two ambient service charging buckets, a network chatter (e.g., or network overhead) service charging bucket, and a user service plan service charging bucket and it is desirable to make sure that no ambient services or network overhead service or unclassified service is charged to the user service plan, and it is also desirable to ensure that all known ambient service traffic is charged to the appropriate ambient service partner, and it is desirable to ensure that no network overhead service or unclassified service is charged to ambient service partners. In such situations, a service charging bucket hierarchy can be provided as follows: determine if a traffic flow (e.g., or socket) is associated with network overhead, and if so allow it and charge that service bucket, then determine if a traffic flow (or socket) is associated with ambient service #1, and if so allow it and charge that service bucket, then determine if a traffic flow (or socket) is associated with ambient service #2, and if so allow it and charge that service bucket, then determine if a traffic flow (or socket) is associated with not classified traffic, and if so allow it and charge that service bucket, then if the

traffic is not associated with any of the above service charging buckets allow it and charge it to the user service plan charging bucket. In another example, if the user has not yet chosen to pay for a user service plan, then the same hierarchical access control and service charging policy can be used except the final step would be: then if the traffic is not associated with any of the above service charging buckets block the traffic. Hierarchical service charging bucket identification such as depicted in these examples can be a crucial aspect of a robust access control policy and/or service charging policy system. Many other access control policy hierarchies and service charging bucket policy hierarchies will now be apparent to one of ordinary skill in the art.

(119) In some embodiments, the not classified traffic is charged according to service charging rules that rely on the most likely candidate service charging bucket for the traffic. As another example, if the not classified traffic is being delivered to the same application as other known ambient service traffic and the time difference between delivery of the known ambient service traffic and the not classified traffic is small, then the not classified traffic can be charged to the ambient service in accordance with a pre-set charging policy rule specifying these conditions. Other embodiments that will now be apparent to one of ordinary skill in the art. For example, another charging rule for not classified traffic could be to perform a pro-rata allocation of the not classified traffic to all of the other service charging buckets with the pro-rata allocation being based on the percentage of the total traffic used by the device for each service charging bucket. As another example, the not classified traffic can be charged to a subset of the service charging buckets for the device (e.g., all ambient services plus the network overhead service) in accordance with the pro-rata share for each service included in the pro-rata split.

(120) In some embodiments, the user service plan agreement is structured so that the user acknowledges that ambient services in which the access connection to the service is sponsored, paid for, and/or partially subsidized by an entity other than the user are a benefit to the user, and/or the user acknowledges that there is no inherent right to free ambient services, and that the service usage accounting system may not always properly characterize usage for a sponsored or subsidized ambient service (e.g., or some other specialized service) in the correct accounting service charging bucket, and, thus, the user service plan account can be charged and/or billed with some of this traffic. By having the user acknowledge a service use agreement of this form then some ambient traffic can be charged to the user service plan account, including, for example, allowed but not classified traffic, excess ambient service usage beyond pre-set policy limits, ambient service usage during busy network periods or on congested network resources, and/or other criteria/measures. In some embodiments, the user might be notified that they are being charged for service activities that are sometimes subsidized or free to the user. As discussed above, it is important to ensure that a not classified service charging bucket does not become a back door for service charging errors or hacking. It will now be apparent to one of ordinary skill in the art that the not classified service usage charges can be verified in a variety of manners, including, for example, observing the size of the not classified service charging bucket as compared to other service usage charges on the device (e.g., total device service usage, ambient service usage, user bucket service usage, and/or other criteria/measures), capping the not classified bucket, and/or capping the rate of growth of the not classified bucket.

(121) In some embodiments, it is important to verify not only that the total device service usage amount is correct, but that the service usage is being reported in the proper service charging buckets. For example, if the service processor software can be hacked so that it correctly reports the total service usage, but reports user service plan traffic under one or more ambient service buckets, then simply verifying that the total amount of service usage is correct will not be sufficient to prevent the device from obtaining free user service that can be charged to ambient service partners. There are a variety of direct and indirect embodiments to accomplish this verification of service charging bucket divisions. For example, in direct verification embodiments, one or more alternative measures of service usage are employed to cross-check the accuracy of the service charging bucket

divisions. In indirect embodiments one of two classes of verification are employed: the size and rate of growth for service charging buckets is analyzed and compared to a pre-set group of policies to detect and/or modify service charging bucket growth that is out of policy and/or the proper operation of the service processor elements involved in service charging bucket partitioning is verified.

(122) Various embodiments involving direct verification of service charging bucket usage and/or accounting include the use of network based service usage measures such as CDRs, IPDRs, flow data records (e.g., FDRs—detailed reports of service usage for each service flow, such as network socket connection, opened and used to transmit data to or from the device), accounting records, interim accounting records or other similar usage records to verify that the device is within service policy and/or the device based service usage reports are accurate. Use of such network generated service usage records to directly verify service charging and/or proper service usage policy adherence are described herein. When network address destination and/or source information is available in these records, as described herein, this can be used in some embodiments to verify the service charging bucket accounting provided by the device service processor. In some embodiments, some types of service usage records include real-time data but not necessarily all of the useful information needed to help verify service charging bucket accounting, while other types of service usage records provide more detail (e.g., IP address for destination and source) but do not always arrive in real-time. For example, in some embodiments, FDRs are created each time a new service flow (e.g., network socket connection) is opened and then closed. At the time the service flow is closed, a (e.g., possibly time stamped) data usage record indicating source address, destination address and amount of data transmitted is created and sent to a charging aggregation function in the network. The charging aggregation function can then forward the FDRs to the service controller for verification or direct accounting of service charging bucket accounting. By comparing the FDR addresses with known ambient service traffic address associations, the partitioning of service charging buckets between one or more ambient services and other services such as a user service plan service charging bucket may be verified. However, in some cases it can be a long period of time for an FDR to be generated when a device service flow (e.g., socket) remains open for a long period of time, as in the case for example with a long file download, a peer to peer connection with a socket keep alive, or a proxy server service with a socket keep alive. In such cases, it can be disadvantageous to have large amounts of data to be transferred without an FDR to confirm device service processor based reports, and in some cases this can provide an opportunity for service processor service reporting hacks. This can be remedied in a variety of ways by using other network reported service usage information to augment the FDR information. For example, start and stop accounting records can sometimes be obtained in some embodiments from a network element such as a service gateway or the AAA servers (e.g., or other network equipment elements depending on the network architecture). Although start and stop records do not possess the detail of service usage information that FDRs, CDRs, IPDRs, interim accounting records or other service usage records posses, they do inform the service controller that a device is either connected to the network or has stopped connecting. If a device is connected to the network and is not transmitting device usage reports or heartbeats, then the service controller is alerted that an error or hacking condition is likely. As another example of how two or more types of network reported service usage information may be used to create a better real time or near real-time check on device service usage, if both FDRs and start/stop accounting records are available, the service controller can send a stop-then-resume service command to the device (e.g., or alternatively send a stop then resume service command to a network equipment element), which will cause the device to terminate all open service flows before re-initiating them, and once the service flows are stopped then the FDR flow records will be completed and transmitted for any service flows that were in process but unreported when the stop service command was issued. This will cause any long term open socket file transfers to be reported in the FDR flow records thus plugging the potential back

door hole in the FDR service usage accounting verification method.

(123) As another example showing how multiple types of network generated service usage accounting records may be used to complement each other and strengthen the verification of service charging bucket accounting partitions, interim data records can be used with FDRs. Interim data records are available in accordance with some embodiments, n which the interim data records are generated on a regularly scheduled basis by a network element (e.g., gateway, base station, HLR, AAA, and/or other network element/function). Interim data records are typically near real time records that report the aggregate traffic usage for the device as of a point in time, but often do not include traffic address information or other traffic details. In embodiments in which both interim accounting records and FDRs are available, when the interim accounting records are indicating service usage that is not being reported in the FDR stream this is evidence that a device has one or more long term socket connections that are open and are not terminating. In this case, the service controller can verify that the device based usage reports are properly accounting for the total amount of service usage reported by the interim accounting records, and/or the service controller can force an FDR report for the open sockets by issuing a stop-resume service command as similarly discussed above.

(124) As described herein, other embodiments involving direct verification of service charging bucket accounting can be provided. One example is to route ambient service traffic to a proxy server or router programmed to support only the network access allowed for the ambient service and to account for the ambient service usage. Additional proxy servers or routers can be similarly programmed for each ambient service that is part of the device service plan, and in some embodiments, another proxy server or router is programmed to support traffic control and account for the user service plan service access. By comparing the service usage accounting for each of these proxy servers or routers, the device generated service charging bucket accounting can be directly verified. In some embodiments, the usage accounting provided by the proxy servers or routers is used directly for service usage accounting.

(125) In some embodiments, ambient service partner feedback is used to verify service charging bucket accounting. For example, web servers used by ambient service partners to provide ambient services can identify a user device based on header information embedded in the HTML traffic, and then account for either the service used by the device during the ambient service sessions or account for the number of transactions the user completes. If service usage is recorded, then it can be reported to the service controller and be used directly to verify ambient service charging bucket accounting. If transactions are all that are recorded, then this can be reported to the service controller and the amount of ambient service used by the device can be compared with the number of transactions completed to determine if the ambient service usage is reasonable or should be throttled or blocked. It will now be apparent to one of ordinary skill in the art that other embodiments can be provided that employ more than one type of network generated service usage records to verify service usage accounting and/or verify service charging bucket accounting.

(126) Other embodiments involving indirect methods for verifying or controlling service charging bucket accounting include monitoring the size and/or growth rate of ambient service usage. In some embodiments, the access control policy rules call for restricting a given ambient service access when the amount of service usage charges accumulating in the ambient service charging bucket exceed a pre-set policy limit, and/or when the rate of service usage for the ambient service exceeds a pre-set policy limit. For example, once these limits are reached, the ambient service can be throttled back for a period of time, blocked for a period of time, or charged to the user service plan charging bucket. In some embodiments, before these actions are taken the user UI can be used to notify the user of the service policy enforcement action. In some embodiments, indirect verification of service charging bucket accounting includes the various techniques described herein for verifying proper operation of the service processor agent software and/or protecting the service processor agent software from errors, manipulation, or hacking.

(127) In some embodiments, the device service processor directs traffic destined for a given ambient service to a proxy server or router programmed to support that ambient service, and any traffic control policies and/or access control policies for the ambient service are implemented in the proxy server or router. For example, in such embodiments the proxy server or router can be programmed to only allow access to one or more ambient services that are authorized by the device service plan, with the proxy server or router controlling device access so that other network destinations cannot be reached. Continuing this example embodiment, the proxy server or router can account for the ambient service usage in an ambient service charging bucket as discussed elsewhere. In such proxy server or router ambient service control embodiments, the same traffic association techniques described elsewhere that allow incoming traffic associated with an ambient service website or other service to be identified, allowed or blocked, potentially throttled, and accounted for in a service charging bucket can be implemented in the proxy server or router programming. Such proxy server or router embodiments can also implement user service plan service charging buckets, user service plan traffic controls, and user service plan access control as discussed herein. In some embodiments, the proxy server or router analyzes the HTML traffic content of the traffic flows as described herein to perform such associations, traffic control and/or service usage accounting. Similarly, in some embodiments, a proxy server or router can provide the "surf-out" capabilities described herein by performing the same surf-out traffic associations (e.g., HTML branch reference associations and/or other branch associations) described herein. It will now be apparent to one of ordinary skill in the art that many of the adaptive ambient service control and service usage charging functions described herein for a service processor can be readily implemented with a proxy server or router that is appropriately programmed.

(128) In some embodiments, routing of device traffic for one or more ambient services and/or user service plan services to a proxy server or muter is accomplished by the device service processor using the device service processor traffic control embodiments described herein. In some embodiments, routing of device traffic for one or more ambient services and/or user service plan services to a proxy server or muter is accomplished by dedicated network equipment such as the gateways (e.g. SGSN, GGSN, PDSN, or PDN), home agents, HLRs or base stations, with the network equipment being provisioned by a service controller (e.g., or other interchangeable network element with similar functions for this purpose) to direct the device traffic to the proxy server or router. In some embodiments, the ambient service traffic or the user service plan traffic is controlled by the proxy server according to a service plan policy set supplied by the service controller (e.g., or equivalent network function for this purpose). The traffic control service policy thus implemented by the proxy server can control traffic based on one or more of the following: period of time, network address, service type, content type, application type, QoS class, time of day, network busy state, bandwidth, and data usage.

(129) In some embodiments, a proxy server or router is used to verify accounting for a given service, for example, an ambient service. In some embodiments, this is accomplished by the device service processor directing the desired service flows to a proxy server or router programmed to handle the desired service flows, with the proxy server or router being programmed to only allow access to valid network destinations allowed by the access control policies for the desired service, and the proxy server or router also being programmed to account for the traffic usage for the desired services. In some embodiments, the proxy service usage accounting may then be used to verify device based service usage accounting reported by the service processor. In some embodiments, the accounting thus reported by the proxy server or router can be used directly to account for service usage, such as ambient service usage or user service plan service usage.

(130) In some embodiments, in which a proxy server is used for device service usage accounting, the proxy server maintains a link to the device service notification UI via a secure communication link, such as the heartbeat device link described herein. For example, the proxy server or router can keep track of device service usage versus service plan usage caps/limits and notify the user device

UI through the device communication link (e.g., heartbeat link) between the service controller and the device. In some embodiments, the proxy server/router communicates with a device UI in a variety of ways, such as follows: UI connection through a device link (e.g., heartbeat link), through a device link connected to a service controller (e.g., or other network element with similar function for this purpose), presenting a proxy web page to the device, providing a pop-up page to the device, and/or installing a special portal mini-browser on the device that communicates with the proxy server/router. In some embodiments, the UI connection to the proxy server/router is used as a user notification channel to communicate usage notification information, service plan choices, or any of the multiple services UI embodiments described herein.

(131) In some embodiments for the proxy server/router techniques for implementing service traffic/access controls and/or service charting bucket accounting, it is desirable to have the same information that is available to the service processor on the device, including, for example, application associated with the traffic, network busy state, QoS level, or other information about the service activity that is available at the device. For example, such information can be used to help determine traffic control rules and/or special services credit is due (e.g., ambient services credit). In some embodiments, information available on the device can be communicated to the proxy server/router and associated with traffic flows or service usage activities in a variety of ways. For example, side information can be transmitted to the proxy server/router that associates a traffic flow or service activity flow with information available on the device but not readily available in the traffic flow or service activity flow itself. In some embodiments, such side information may be communicated over a dedicated control channel (e.g., the device control link or heartbeat link), or in a standard network connection that in some embodiments can be secure (e.g., TLS/SSL, or a secure tunnel). In some embodiments, the side information available on the device can be communicated to the proxy server/router via embedded information in data (e.g., header and/or stuffing special fields in the communications packets). In some embodiments, the side information available on the device can be communicated to the proxy server/router by associating a given secure link or tunnel with the side information. In some embodiments, the side information is collected in a device agent or device API agent that monitors traffic flows, collects the side information for those traffic flows, and transmits the information associated with a given flow to a proxy server/router. It will now be apparent to one of ordinary skill in the art that other techniques can be used to communicate side information available on the device to a proxy server/router.

(132) For example, just as the hierarchy of charging rules can be important for implementations in which the service processor is creating the service charging bucket accounting, it can also important in implementations that use a proxy server or router for service charging bucket accounting. Accordingly, various embodiments described herein for creating a hierarchy of service usage charging rules can be applied to proxy server or proxy router embodiments. It will be apparent to one of ordinary skill in the art that the service charging bucket embodiments and traffic control and access control embodiments described herein for allowed but not classified buckets apply equally to the proxy server/router embodiments. For example, pre-defined service policy rules can be programmed into the proxy server/router to control the traffic flows and/or place usage limits or access limits on an ambient service, or a user service plan service. It will also now be apparent to one of ordinary skill in the art that the embodiments described herein disclosing an initial allowed service access list, temporarily allowing additional service activities until they are determined to be allowed or not allowed, expanding the allowed service activity list, maintaining a not allowed service activity list and expanding the not allowed service activity list also apply equally to proxy server/router embodiments. Similarly, it will now be apparent to one of ordinary skill in the art that the proxy/server router embodiments can be employed to directly generate the service charging bucket (or micro-CDR) usage reports used to provide further detail and/or billing capabilities for service usage. In some embodiments, in which the device service processor directs traffic to a proxy server/router, there are advantageous design feature embodiments available that

can reduce the need to provision network to detect and force specialized device service traffic to the appropriate proxy server/router. For example, this can be done by creating a "usage credit" system for the services supported by the proxy server/outer. Total service usage is counted on the one hand by the device service processor, or by other network equipment, or by both. Credit on the other hand for ambient service or other specialized access service usage that is not charged to the user is then provided for services that the device directs through the proxy server/router destination (e.g., URL or route hop) supporting the particular ambient service or other specialized access service. If the device correctly directs traffic to the proxy server/router, then the counting and/or access rules are correctly implemented by the proxy server/router. The service can be thus controlled and/or accounted for. When the service is accounted for, the proxy server/router reports the service charging bucket accounting back to the service controller (e.g., or other network equipment responsible for service charging bucket/micro CDR mediation) and the user service plan service charging bucket account can be credited for the services. Traffic that reaches the proxy server/router is controlled by the access rules and/or traffic control rules and/or QoS control rules of the proxy server/router programming, so there is no question regarding the type of service that is supported with the service charging buckets that are reported to mediation functions (e.g., mediation functions can be performed by one or more of service controller, usage mediation, billing, AAA, and/or HLR/home agent). As the proxy server/router is in the network and can be physically secured and protected from hacking, there is high confidence that the service control and/or charging rules intended for ambient services or some other specialized service are properly implemented and that the proxy server/router connection is being used for the intended service and not some other unintended hacked service. If the device is somehow hacked or otherwise in error so that the traffic is not directed through the appropriate proxy server/router, then the proxy server/router does not log the traffic in micro CDRs/buckets and no specialized service usage credit is sent to the mediation functions, so there is no usage credit deducted from the device user service plan service usage totals. Thus, the user pays for the services when the device is hacked to avoid the proxy server/router. The user account service agreement can specify that if the user tampers with software and traffic is not routed to servers then credit will not be provided and user plan will be charged.

(133) In some proxy server/router embodiments, the usage credit is sometimes recorded by the proxy server/router detecting which device is performing the access. Device identification can be accomplished in a variety of ways including a header/tag inserted into the traffic by the device, a route in the network specified for that device, a secure link (e.g., TLS/SSL, IP Sec, or other secure tunnel), a unique device IP address or other credential (e.g., where proxy server/router has access to an active IP address look up function), a unique proxy server/router address and/or socket for the device.

(134) In some embodiments, the coordination of the device service controller traffic control elements with a proxy server/outer can make it simpler to locate, install, provision and operate the proxy servers. The proxy server/routers do not need to be located "in line" with the access network because it is the device's responsibility to make sure the traffic is routed to the servers/routers or else there is not credit and the user account is charged. In some embodiments, this makes it unnecessary or reduces the need to force device traffic routes in carrier network. In some embodiments, the proxy server/routers can be located in carrier network or on the Internet. If the proxy server/routers are on Internet, then traffic can be authenticated in a firewall before being passed to server/routers to enhance security to attack.

(135) In some embodiments, the service charging bucket recording software in the proxy server/router can be programmed into an ambient service partners network equipment directly thus eliminating the need for special apparatus. The ambient service partner's equipment (e.g., a web server, load balancer or router) can recognize the device using one of the techniques described above, aggregate the device service charging bucket accounting, and periodically send the usage

accounting to the service controller or other network service usage mediation function.

(136) Programming and/or provisioning the types of ambient services, user service plan services and/or specialized services disclosed in various embodiments described herein can be a complex process. In some embodiments, a simplified user programming interface, also referred to herein as a service design interface, is used to program the necessary policy settings for such services is desirable. For example, a service design interface is provided that organizes and/or categorizes the various policy settings that, are required to set up an ambient service (e.g., or other service) including one or more of the following: a policy list of service activities that are allowed under the ambient service (e.g., or other service), access control policies, rules for implementing and/or adapting an allowed list of network destinations, rules for implementing and/or adapting a blocked list of network destinations, service charging bucket policies, user notification policies, service control, and/or service charging bucket verification policies, actions to be taken upon verification errors. In some embodiments, the required information for one or more of these policy sets is formatted into a UI that organizes and simplifies the programming of the policies. In some embodiments, the UI is partly graphical to help the user understand the information and what settings need to be defined in order to define the service. In some embodiments, the UI is created with an XML interface. In some embodiments, the UI is offered via a secure web connection. In some embodiments, a basic service policy for an ambient service (e.g., or another service) is created that includes one or more of the above service policy settings, and then this service policy set becomes a list or an object that can be replicated and used in multiple service plan policy set definitions (e.g., “dragged and dropped” in a graphical UI). In some embodiments, the resulting set of policies created in this service design interface are then distributed to the necessary policy control elements in the network and/or on the device that act in coordination to implement the service policy set for a given device group. For example, if a service processor is used in conjunction with a service controller, then the service design interface can load the service policy settings subsets that need to be programmed on the service controller and the device service processor into the service controller, and the service controller loads the service controller policy settings subset into the service controller components that control the policies and loads the device policy settings subset to the devices that belong to that device group. In embodiments in which a proxy server/router is used to help control and account for services, in some embodiments, the service design interface loads the service policy settings subsets that need to be programmed on the proxy server/router into the proxy server/router. In embodiments where other network equipment (e.g., gateways, base stations, service usage recording/aggregation/feed equipment, AAA, home agent/HLR, mediation system, and/or billing system) need to be provisioned or programmed, in some embodiments, the service design interface also loads the appropriate device group policy subsets to each of the equipment elements. Accordingly, various techniques can be used as described herein to greatly simplify the complex task of translating a service policy set or service plan into all the myriad equipment and/or device settings, programming, and/or provisioning commands required to correctly implement the service. It will now be apparent to one of ordinary skill in the art that several of these techniques can similarly be used for the VSP service design interface.

(137) Those of ordinary skill in the art will appreciate that various other rules can be provided for the rules engine as described herein. Those of ordinary skill in the art will also appreciate that the functions described herein can be implemented using various other network architectures and network implementations (e.g., using various other networking protocols and corresponding network equipment and techniques).

(138) In device-assisted service (DAS) systems, end-user device agents can assist the network in policy implementation or enforcement. For example, device agents can assist the network in recordkeeping to allocate costs when end-user devices access data services over an access network, enforcing access control or service limit policies for the device, enforcing usage limits, or assisting

in notification policies for information regarding network access services that are in communication with the device end user. If a device is configured with a device agent configured to assist the network in policy implementation or enforcement, there may be a device portion of a network policy that is enforced on the device and a network portion of an access network service policy that is enforced by network elements in the network. In some access networks, network-based systems are employed to implement the network portion of the access network service policy, such as, for example, to manage the authentication process of allowing a device onto a network or to determine one or more network policies that should be enforced by the network elements such as access control policy, service usage limits, service usage accounting or billing policy, or service usage notification policy.

(139) To achieve an overall network service policy, the network portion of the access network service policy may be configured to work in conjunction with the device-based portion of the access network service policy to achieve an overall combined network service policy. If the device agents required to implement the device portion of the access network service policy are not present on the device or are not properly configured, then the overall combined network service policy can be in error or may not be possible to achieve, potentially resulting in an undesired network service policy implementation. In such cases, it is desirable for a network system to be employed to detect this condition and modify the network portion of an access network service policy enforced by the network-based elements so that a desired network service policy enforcement may be achieved.

(140) In some embodiments, a device agent that can assist the network in policy implementation or enforcement may be termed a “device policy implementation agent,” which in some embodiments may be part of the service processor.

(141) Examples of when it may be advantageous to adapt the network portion of an access network service policy in order to account for a missing or improperly configured service processor include but are not limited to: (i) a device credential has been moved to a device that does not have a service processor, (ii) a device credential has been moved to a device with a service processor with a different configuration than the service processor originally associated with the device credential, (iii) a device service processor has been tampered with or has an improper configuration.

(142) In some embodiments, the service processor is used to assist in classifying service usage into sub-categories for the purpose of usage accounting policy enforcement, access control policy enforcement, service usage limits, or notification policy enforcement that differs according to the category. In some embodiments, the classification can be for one or more device applications. In some embodiments the classification can be for one or more network destinations. In some embodiments the classification can be for one or more network types. In some embodiments a classification of service usage (herein referred to as a sponsored service or an ambient service) can be performed to facilitate allocating access network costs, in whole or in part, associated with the sponsored or ambient service to a service sponsor, the service sponsor being an entity other than the device user.

(143) What is needed is a network system that detects the presence and proper configuration of a service processor, or lack thereof, in the end-user device, wherein the service processor, if present, enforces a device portion of an access network service policy on a device configured with a device credential, and, if the service processor is present and properly configured, that causes a first network portion of an access network service policy to be enforced in the network, the first network portion of an access network service policy being configured to provide counterpart policy enforcement to a device portion of an access network service policy to achieve a first desired overall access network service policy; and if the service processor is not present and properly configured, that causes a second network portion of an access network service policy to be enforced in the network that is configured to operate without a device counterpart policy to achieve a second desired overall access network service policy.

(144) In some embodiments, a network system is used to detect when unscrupulous users attempt to acquire free data services by tampering with a service processor in order to use one service and have the service usage accounting allocated to a second service that is sponsored. For example, if a device sends reports of its data usage to the network, a user might attempt to hack the device so that its reports contain information that is more favorable to the user than it should be, e.g., by reporting less data usage than the device actually used. As another example, a device may contain a “sponsored SIM” card or another credential that allows the device to use a fixed amount of data, possibly associated with a particular service, at a reduced charge or at no charge to the user. Unscrupulous users may attempt to find ways to increase their quantity of free or subsidized data usage with sponsored SIM cards.

(145) Bandwidth limitations in the wireless access network are making unlimited data plans less attractive to service providers. At the same time, users of end-user devices want to have more control over their devices' data usage to control costs. The ability to track a device's data usage with high accuracy, on a more granular level than simply by measuring aggregate data usage, is an important enabler new service offerings that meet both of these needs. For example, accurate tracking of a device's data usage on a service-by-service or application-by-application basis, or on even finer levels, will allow service providers to offer a la carte service plans that allow users to choose customized application- or service-specific data plans.

(146) Therefore, there is a need for security measures to prevent policy errors caused by changing device credentials, improper configuration of a service processor, or fraud in DAS systems. In particular, there is a need for tools that allow the network to detect fraudulent end-user device activity.

(147) Disclosed herein are various embodiments to prevent, detect, or take action in response to moving a device credential from one device to another, improper configuration of a service processor, a missing service processor, or tampering with a service processor in device-assisted services (DAS) systems.

(148) In some embodiments, the service controller in the network authenticates the service processor and checks that it is reporting the end-user device's usage in the expected manner, e.g., at expected times, including expected information, with expected indicia of authenticity, etc.

(149) In some embodiments, when the end-user device reports usage, the service controller checks whether the reports sent by the service processor are consistent with reports from a trusted source, such as a network element.

(150) In some embodiments, when the service controller detects fraudulent or potentially fraudulent activities, the service controller notifies a network administrator or network resource, which can then further evaluate the situation and decide how to respond. In some embodiments, the subscriber's billing rate is increased.

(151) In some embodiments, a device client configured to implement a device portion of a network access service policy (e.g., an access control policy or traffic control policy, a device software or operating environment security policy, a service usage limit, a service accounting or charging policy, a service notification policy, or another policy) may be termed a “device policy implementation client,” which in some embodiments may be part of the service processor. Also without loss of generality, the term “service controller” may be used to refer to a service processor authentication and management system. Both the service processor and service controller may have functions in addition to those described herein.

(152) In some embodiments, a device is configured with a properly configured service processor responsible for implementing or enforcing a device portion of a first access network service policy. In some embodiments, the device is configured without a properly configured service processor. In some embodiments, a service controller can be configured to determine whether the service processor is present on the device and, if so, whether it is properly configured.

(153) In some embodiments, if the service controller determines that the device is configured with

a properly configured service processor, the service controller causes a network based access network service policy enforcement system to implement or enforce a first network-based portion of the first access network service policy. In this case, because the service controller has verified that a properly configured service processor is present on the device, the service controller system operates under the premise that the device is properly implementing or enforcing the device portion of the first access network service policy. If, however, the service controller determines that a properly configured device service processor is not present on the device, the service controller causes a network-based access network service policy enforcement system to implement or enforce a second network based portion of the first access network service policy. In this case, the service controller system operates under the premise that the device is not properly implementing or enforcing a device portion of an access network service policy.

(154) In some embodiments, an end-user device is configured with: (1) a wireless modem to connect to a wireless access network (or another network access modem to connect to another type of access network); (2) one or more device credential sources (e.g., a SIM card, a soft-SIM, a universal SIM, an IMSI source, a wireless modem, a phone number source, an IMEI source, an MEID source, a user password or PIN, a MAC address source, an IP address source, a secure device identifier source, a device secure communication encryption key source, etc.) that store a device credential and provide the device credential to one or more network service policy enforcement elements (e.g., AAA, HLR, PCRF, access network authentication system, admission system or log-in system) for the purpose of seeking or gaining admission to the wireless access network (or other access network); and (3) a service processor (e.g., a device client) configured to implement or enforce a device-based portion of a wireless access network service policy and communicate with a network-based service controller in order to provide service processor authentication information configured to allow verification that the service processor is present and properly configured on the device.

(155) In some embodiments, a network-based system is configured with: (1) one or more network-based device authentication or admission elements (e.g., AAA, HLR, PCRF, access network authentication system, admission system, log-in system, etc.) configured to receive a device credential from an end-user device that is attempting to receive or is receiving access network services; (2) one or more service policy enforcement elements (e.g., a network gateway, router, GGSN, SGSN, proxy, charging element, notification trigger element, etc.) configured to implement an access network service policy that is associated with the device credential; (3) a service processor authentication and management system (e.g., a service controller) configured to receive service processor authentication information and use the information to verify that the service processor is present and properly configured on the device. In some embodiments, the service processor authentication and management system is further configured to: (a) in the event that the service processor is present and properly configured on the device, cause the access network service policy that is associated with the device credential to be executed as a first network portion of an access network service; or (b) in the event that the service processor is not present on the device and properly configured, cause the access network service policy that is associated with the device credential to be executed as a second network portion of an access network service.

(156) Without loss of generality, in the following related embodiments the terms, “SIM card” and “SIM” are used to represent a device credential source. As would be appreciated by one of ordinary skill in the art, other device credential sources (e.g., a soft-SIM, a universal SIM, an IMSI source, a wireless modem, a phone number source, an IMEI source, an MEID source, a MAC address source, an IP address source, a secure device identifier source, a device secure communication encryption key source, etc.) can be interchanged with SIM card in many of the embodiments. For example, in embodiments in which a SIM card is moved from one device to another, another type of device credential could be moved instead (e.g., soft SIM, universal SIM, an IMSI source, a wireless modem, a phone number source, an IMEI source, an MEID source, a MAC address

source, an IP address source, a secure device identifier source, a device secure communication encryption key source, etc.). As another example, when a user tampers with a service processor associated with a SIM, the user could be tampering with a service processor associated with another type of device credential (e.g., soft SIM, universal SIM, an IMSI source, a wireless modem, a phone number source, an IMEI source, an MEID source, a MAC address source, an IP address source, a secure device identifier source, a device secure communication encryption key source, etc.). There are many other example embodiments where the term "SIM" can be exchanged for another source of device credentials, with the embodiments being too numerous to list and yet evident to one of ordinary skill in the art in the context of the teachings herein.

(157) In some embodiments, the one or more device credential sources include a SIM card. In some embodiments, the service controller can be configured to recognize which device or service processor the SIM is associated with, use the SIM and device association to look up a desired device portion of a wireless access network service policy, and communicate the policy to the appropriate device service processor. In some embodiments, the two different device portions of a wireless access network policy are determined according to a device group or user group service policy definition that includes one or more SIM credentials and/or one or more service processor credentials, and these policy definitions are entered in a virtual service provider work station that manages the service controller and/or device service processor policies.

(158) In some embodiments, the service controller is configured to recognize when the SIM card from a first device with a first service processor has been moved to a second device with a second service processor. In some such embodiments, the service controller can be configured to recognize which device or service processor the SIM is associated with, use the SIM and device association to look up a desired network portion of a wireless access network service policy, and cause the network portion of a wireless access network service policy to be implemented or enforced in one or more network service policy enforcement elements. In some embodiments, the two different network portions of a wireless access network policy are determined according to a device group or user group service policy definition that includes one or more SIM credentials and/or one or more service processor credentials, and these policy definitions are entered in a virtual service provider work station that manages the service controller and/or network service policy enforcement element policies.

(159) In some embodiments, the one or more device credential sources include a SIM card. In some embodiments, the service controller is configured to detect when a device user has moved the SIM card from a first device configured with a properly configured service processor to a second device that is not configured with a properly configured service processor. In some embodiments, the service controller can be configured to determine that the first device is configured with a properly configured service processor and communicate a device portion of a wireless access network service policy to the appropriate device service processor. In some embodiments, the device portion of a wireless access network policy is determined according to a device group or user group service policy definition that includes a SIM credential and/or a service processor credential, and these policy definitions are entered in a virtual service provider work station that manages the service controller and/or device service processor policies. In some embodiments, the service controller is configured to determine that the first device is configured with a properly configured service processor and cause a first network portion of a wireless access network service policy to be implemented or enforced in one or more network service policy enforcement elements. In some embodiments the service controller is configured to determine that the second device is not configured with a properly configured service processor and cause a second network portion of a wireless access network service policy to be implemented or enforced in one or more network service policy enforcement elements. In some embodiments, the device portion of a wireless access network policy is determined according to a device group or user group service policy definition that includes a SIM credential, and these policy definitions are entered in a virtual service provider

work station that manages the service controller and/or network service policy enforcement element policies.

(160) In some of these embodiments, the differences between the first network portion of a wireless access network service policy and the second network portion of a wireless access network service policy can include a difference in network access privileges, a difference in allowable network destinations, a difference in service usage accounting or billing for “bulk” access, a difference in service usage accounting or billing for a classification of access, a difference in service usage accounting rates or billing rates for “bulk” access, a difference in service usage accounting rates or billing rates for a classification of access, a difference in sponsored (ambient) service accounting or billing, a difference in service speed or quality, a difference in which networks the device or user has access to, a difference in the service usage notification that is provided to the end user, a difference in roaming service policies or permissions or accounting/billing rates, a quarantining of the device or user access capabilities, differences between (e.g., disabling or otherwise modifying) one or more features of device operation, or suspending the device from access to the network.

(161) In some embodiments, a SIM and a service processor are associated with a classification of service usage and a corresponding device portion of access network service policy enforcement. The service controller is then responsible for properly authenticating the proper configuration of the service processor in association with the SIM in order to determine the appropriate network portion of network access service policy that should be enforced.

(162) In some embodiments, a SIM and a service processor are associated with one or more application-specific services wherein the device network access service has policy elements that are specific to a device software or firmware application. A software or firmware application-specific service can include but is not limited to a service with specific policy elements associated with a user application program; an operating system program, library or function; a background application service such as an application update, content caching, software update or other background application service.

(163) In some embodiments, a SIM and a service processor are associated with one or more network-destination-specific services wherein the device network access service has policy elements that are specific to a network destination or resource. A network destination or resource can include but is not limited to a server, gateway, destination address, domain, website or URL.

(164) In some embodiments, a SIM and a service processor are associated with any combination of a device application, network destination or resource; a type of network; a roaming condition (e.g., a home or roaming network); a time period; a level of network congestion; a level of network quality-of-service (QoS); and a background or foreground communication.

(165) In some embodiments, a SIM and a service processor are associated with one or more sponsored services (also referred to herein as ambient services), wherein a portion or all of the service usage accounting for one or more classifications of service usage are accounted to, charged to, or billed to a service sponsor rather than the device user or party who pays for the user service plan. The portion of service that is sponsored can be, all of the device access or a portion or classification of the device access. In some embodiments, the classification of the sponsored portion of service (e.g., the identification of the portion of the device's use of the access network that should be allocated to the service sponsor) is accomplished on the device with a service processor. In some embodiments, the classification of the sponsored portion of service is accomplished in the network using DPI elements, gateway elements, server elements, proxy elements, website elements or web service elements. In some embodiments, the classification of the sponsored portion of service is accomplished with a classification policy implemented by a combination of a service processor on the device (e.g., steering a classification of service to a given network element via a re-direction, re-route, or tunnel [e.g. secure SSL, VPN, APN or other tunnel protocol]) and one or more network elements (e.g., DPI elements, gateway elements, server elements, proxy elements, website elements or web service elements). In some embodiments, the

portion of service that is sponsored includes service for one device application or a group of device applications. In some embodiments, the portion of service that is sponsored includes service for a network destination or resource, a server or website, or a group of network destinations, servers or websites. In some embodiments, the portion of service that is sponsored includes service on a specific type of network. In some embodiments, the portion of service that is sponsored includes service on a home network or a roaming network. In some embodiments, the portion of service that is sponsored includes service during a time period. In some embodiments, the portion of service that is sponsored includes service for a certain range of network congestion. In some embodiments, the portion of service that is sponsored can include service for a certain range of network QoS. In some embodiments, the portion of service that is sponsored includes service for a network background or foreground data communication. In some embodiments, the portion of service that is sponsored includes any combination of device application, network destination or resource, a type of network, a roaming condition (e.g., home or roaming network), a time period, a level of network congestion, a level of network QoS, and a background or foreground communication.

(166) In some embodiments, a SIM (or other source of user credential or device credential, as explained previously) is installed in or present in association with a device configured with a device service processor configuration that provides access network policy enforcement. In such embodiments, one or more network elements can implement or enforce a network-based portion of access network policy enforcement, and the device service processor can be configured to implement or enforce a device-based portion of access network policy enforcement. In some embodiments, one or more SIM credentials can be used at least in part to identify the network-based portion of access network policy. In some embodiments, one or more SIM credentials can be used at least in part to identify the device-based portion of access network policy.

(167) In some embodiments that include a SIM module policy association, the policy enforcement includes one or more of access control policy enforcement, service usage limit, access accounting policy enforcement, and access service user notification policy enforcement. In some embodiments, the access control policy enforcement includes one or more of allowing, limiting, blocking, deferring, delaying or traffic shaping device network access for “bulk” access (e.g., “not classified” access), or one or more specific classifications of access network service activities. In some embodiments, the access accounting policy enforcement includes one or more of counting an amount of “bulk” (e.g., “unclassified”) access network service usage, or counting an amount of access network service usage for one or more specific classifications of access network service activities. In some embodiments, the access service notification policy enforcement includes one or more of notifying an end user when a pre-defined service usage condition occurs for “bulk” (e.g. “unclassified”) access network service usage or notifying an end user when a pre-defined service usage condition occurs for one or more specific classifications of access network service activities. Examples of specific classifications of access network service activities include access by an application or OS function, access to one or more network destinations or network resources (such as a web site, domain, IP address or other address identifier, URL, socket tuple, network server, network route or APN, network gateway or proxy, network content source or sub-network). Additional examples of specific classifications of access network service activities include device access to network services with different QoS service levels. In some embodiments, a portion of the policies associated with specific classifications of access network service are implemented or enforced with a device-based service processor, and other portions of access network service policy are enforced in one or more network-based elements.

(168) In some embodiments in which one or more network elements implement or enforce a network-based portion of access network policy enforcement and a device service processor is configured to implement or enforce a device-based portion of access network policy enforcement, one or more device SIM credentials are identified and used at least in part to determine the policies enforced by the network. In such embodiments, the device service processor can be relied upon to

implement or enforce certain aspects of access network service policy that are not implemented or enforced in the network.

(169) In some embodiments, a first portion of access network service policy is determined at least in part by one or more SIM credentials and is implemented by one or more network elements, and a second portion of access network service policy is intended to be implemented by a device-based service processor, but the SIM is installed in a device that is not configured with a service processor capable of implementing the second portion of access network service policy. In some such embodiments, a network element identifies whether the SIM is installed in a device that is configured with a service processor capable of implementing the second portion of access network service policy intended to be implemented on the device. In some embodiments, the identification is accomplished by a network system that implements one or more of the following device configuration detection and network policy selection functions: (1) Identify when a SIM whose credentials are used at least in part to identify a network-based portion of access network policy is installed in a device configured to include a service processor capable of implementing or enforcing a device-based portion of access network service policy, and provision a first network-based service policy in one or more network-based policy enforcement elements that implement or enforce access network service policy; (2) Identify when a SIM whose credentials are used at least in part to identify the network-based portion of access network policy is installed in a device that is not configured to include a service processor capable of implementing or enforcing a device-based portion of access network service policy and implement a second network-based service policy in one or more network-based policy enforcement elements that implement or enforce access network service policy.

(170) In some embodiments, when it is determined that a SIM whose credentials are used at least in part to identify the network-based portion of access network policy is installed in a device configured to include a service processor capable of implementing or enforcing a device-based portion of access network service policy, a network-based service policy provisioning system provisions a first network-based service policy into one or more network elements (e.g., programs or sends the policy to one or more network elements) and also provisions a device-based service policy into a device service processor. In some embodiments, when it is determined that a SIM whose credentials are used at least in part to identify the network-based portion of access network policy is installed in a device that is not configured to include a service processor capable of implementing or enforcing a device-based portion of access network service policy, a network-based service policy provisioning system provisions a second network-based service policy into one or more network elements, and there is no policy provisioning for a device-based service processor.

(171) Such embodiments are advantageous, for example, when a device-based service processor is capable of implementing or enforcing a network access service policy that has fine grain classification aspects that are not otherwise implemented or enforced in the network. For example, in some embodiments a SIM is installed in a first device configuration that includes a device-based service processor capable of classifying access network service usage associated with one or more device software applications and enforce a policy for access control, service limit, access accounting or access service notification for that classification. In this case a first set of network-based access network service policies may be provisioned into the network elements that implement or enforce access network service policy. If the same SIM is installed in a second device configuration that does not include the described service processor capability, a second set of network-based access network service policies may be provisioned into the network elements that implement or enforce access network service policy. In such embodiments, the first device configuration can include a trusted access control or service limit policies in the service processor that determine the network access allowances for one or more applications, and the first network service policies are configured to facilitate this device-based application access control or service

limitation. In contrast, the second device configuration, having no service processor, has no trusted access control or service limitation policies, and therefore the second network service policies may be configured in a manner that allows access only if the service plan or service account associated with the SIM (or second device or SIM user) includes permissions for “bulk” access, “unclassified” access, or access that is classified by the network and not by the device.

(172) In some embodiments, the second network service policies are configured to modify the classification of network access services in accordance with capabilities that exist only in the network without the assistance of a device-assisted classification component.

(173) In some embodiments, the second network service policies include a second access service accounting or charging rate that is different than the access service accounting or charging rate of the first network service policies. For example, the method of service accounting or service charging to the end user in the case where the SIM is installed in a device configuration that includes a service processor capability (e.g., the device is capable of performing service classification, accounting, control or notification functions) can be different than the method of service accounting or service charging to the end user in the case where the SIM is installed in a device configuration that does not include the service processor capability. For example, if the SIM is installed in a device configuration that includes a service processor capability, a given application (e.g., social networking application, email application, search application, voice application, news application, etc.) might have a first service accounting or charging policy defining a first charging measure (e.g., time-based usage for an application, website, content type, service type QoS class; or e.g., megabyte-based usage for an application, website, content type, service type QoS class, etc.) and/or first charging rate (e.g., $X per minute; or e.g., $Y per megabyte, etc.) when the device configuration includes a service processor capability, whereas when the SIM is not installed in a device configuration that includes a service processor capability, all traffic may be rated in the same manner (e.g., time-based or megabyte-based), potentially with a higher price. In some embodiments, when the SIM is not installed in a device configuration that includes a service processor capability, the device network access permissions are altered, or the device's communications may be quarantined or blocked.

(174) In some embodiments, when a SIM is installed in a device with a first device configuration, the service processor is configured to differentially treat one or more classifications of access network service activities based on network congestion level, time of day, QoS level or background/foreground access (e.g., background content caching or background upload of device/user analytics, background software or OS updates, background application/server communications, etc.), but the same SIM can alternatively be installed in a device without such service processor capabilities (e.g., a device with a second device configuration). In such an embodiment, one or more of the network-based portions of access control or service limitation policy, network-based portion of accounting or charging policy, or network-based portion of user notification policy can be varied depending on whether the SIM is installed in a device with the first device configuration or the second device configuration. For example, if the SIM is recognized by the network in association with the first device configuration, a lower accounting rating or service usage price can be applied to traffic that is (i) allocated to background status, (ii) is controlled based on network congestion level, (iii) is controlled based on time of day, (iv) is controlled based on a lower QoS classification allowance, etc., whereas if the SIM is recognized by the network in association with the second device configuration, a single, potentially higher accounting rating or service usage price can be applied. In some embodiments, if the SIM is recognized by the network in association with the second device configuration the device network access permissions can be altered, or the device's communications can be quarantined or blocked.

(175) In some embodiments, when a SIM is determined by a network element to be installed in a device configuration that includes a service processor service usage charging capability, one or more network elements are configured to zero-rate the device access (i.e., the one or more network

elements will not apply the service usage accounting recorded by one or more network elements to the user's bill), and user service accounting or charging is turned over to a service controller that receives service usage accounting or charging information from the service processor.

(176) In some embodiments, when a SIM is determined by a network element to be installed in a device configuration that includes a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications to one or more proxy gateway/servers, one or more network elements are configured to zero-rate the device access (i.e., the one or more network elements will not apply the service usage accounting recorded by one or more network elements to the user's bill), and user service accounting or charging is turned over to one or more proxy gateway/servers configured to account or charge for device service usage.

(177) In some embodiments, when a SIM is determined by a network element to be installed in a device configuration that includes a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications to one or more proxy gateway/servers, the one or more proxy gateway/servers perform additional traffic access control or service limitation policy implementation or enforcement for the one or more classifications of service usage.

(178) In some embodiments, when a SIM is determined by a network element to be installed in a device configuration that includes a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications to one or more proxy gateway/servers, the one or more proxy gateway/servers perform additional service usage classification for the purpose of service usage accounting, access control, service limiting or user notification.

(179) In some embodiments, when a SIM is determined by a network element to be installed in a device configuration that does not include a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications to one or more proxy gateway/servers, network elements other than the proxy gateway/servers account for service usage, potentially at a different rate than when a SIM is determined by a network element to be installed in a device configuration that includes a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications.

(180) In some embodiments in which the device configuration includes a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications to one or more proxy gateway/servers, the device routing, re-directing, or steering is accomplished by routing, re-directing, or steering the device traffic for one or more service usage classifications to a specific network destination or resource associated with the proxy gateway/server. In some embodiments, the routing, re-directing, or steering is accomplished using a secure tunnel through the network. In some embodiments the routing, re-directing, or steering is accomplished with a VPN or APN tunnel.

(181) In some embodiments, a network-based service charging policy system is used in conjunction with a user service agreement confirmation system, wherein the user agreement confirmation system provides confirmation that the user has agreed to access service usage terms that stipulate a first rate of access service usage accounting or charging when a SIM is detected in association with a device configuration that includes a service processor capability, and a second rate of access service usage accounting or charging when a SIM is detected in association with a device configuration that does not include a service processor capability. In some embodiments, if a user removes or tampers with a device configuration that includes a service processor capability, or if a user installs a SIM in a device that is not configured with a service processor capability, the user service usage billing conditions are changed. In some embodiments, depending on the device configuration (e.g., with or without a service processor capability), the user is billed at a different rate for “bulk” service usage, or is billed at a different rate for one or more classifications of service usage.

(182) In some embodiments, a network-based service charging policy system is used in conjunction

with a user service agreement confirmation system, wherein the user agreement confirmation system provides confirmation that the user has agreed to access service usage terms that stipulate a first set of access service privileges when a SIM is detected in association with a device configuration that includes a service processor capability, and a second set of access service privileges when a SIM is detected in association with a device configuration that does not include a service processor capability. In some embodiments, if a user removes or tampers with a device configuration that includes a service processor capability, or if a user installs a SIM in a device that is not configured with a service processor capability, the user service usage permissions are modified. In some embodiments, this modification can include altering the allowed network destinations, altering the allowed network services, altering the allowed network resources, quarantining access or blocking access.

(183) In some embodiments the presence of a device service processor in combination with a SIM results in the service controller providing advantageous network access services to the user. Examples include but are not limited to the sponsored services discussed herein, user-paid application-based services (e.g., user-paid services where access for one or more device applications is included in a service allowance with potentially lower cost than overall internet access), user-paid destination services (e.g., user-paid services where access for one or more network destinations or resources is included in a service allowance with potentially lower cost than overall internet access), roaming services (e.g., services that aid the user when the device is connected to a roaming network, such as by informing the user that she is roaming and asking if she wishes to continue or block roaming service usage, up to date roaming service usage indication or cost indication, roaming service rate indications, allowing a user to decide which device service usage classifications he wishes to allow while roaming, etc.), or service usage notification services (e.g., providing the user with an update of how much service usage or cost has been incurred, informing the user of what service plans are available, informing the user when a service plan sign up may be advantageous to the user based on an activity or group of activities the user is attempting, or providing the user with a set of service plan sign up choices that can be selected and purchased in a device user interface (UI), etc.). In some embodiments, these user services are made possible by the capabilities of the service processor on the device in conjunction with a specific configuration of a service controller or other network elements on an access service provider network.

(184) In some embodiments, if the SIM for a first network service provider is removed from the device and another SIM for a second network or service provider is installed, the user may not have access to the same services. In some embodiments, the service processor on the device detects that the SIM has been changed and informs the user through a device user interface (UI) notification that if the user changes SIMS or service provider networks, the user will lose certain services. In some embodiments, the services that will be lost are listed in a UI notification. In some embodiments the UI notification states that if the user wishes to regain access to certain services, the user can re-install the original SIM.

(185) In some embodiments, one or more network elements determine whether an end-user device has an active service processor. In some embodiments, a service controller in the network authenticates the service processor.

(186) In some embodiments, the service controller performs authentication of the service processor to ensure that it is present and properly configured to implement a device portion of an access network service policy. FIGS. **16** and **17** show a system diagram for a device service processor to service controller communication link that can aid in secure communication and service processor authentication and verification functions.

(187) FIG. **16** is a functional diagram illustrating service control device link **1691** of service processor **115** and the service control service link **1638** of service controller **122** in accordance with some embodiments. In particular, service control device link **1691** of service processor **115** and

service control service link **1638** of service controller **122** as shown in FIG. **16** provide for secure control plane communication over service control link **1653** between service processor **115** and service controller **122** in accordance with some embodiments. Various embodiments include two or three layers of encryption in the service control link, with one embodiment or layer being implemented in the encrypt functions (**2408**, **2428**) and decode functions (**2412**, **2422**), and another embodiment or layer implemented in the transport services stack (**2410**, **2420**). An optional third embodiment or layer of encryption is implemented below the transport services stack, for example, with IPSEC or another IP layer encryption, VPN or tunneling scheme. For example, various known security encryption techniques can be implemented in the encrypt functions (**2408**, **2428**), with public/private or completely private keys and/or signatures so that very strong levels of security for service processor control plane traffic can be achieved even through the basic transport services (**2410**, **2420**) implemented with standard secure or open Internet networking protocols, such as TLS or TCP. For example, the service processor agent communications local to the device can be conducted to and from the service controller elements via service control device link **1691** connection to agent communication bus **1630**. The combination of service control device link **1691** and agent communication bus **1630**, which in some embodiments is also securely encrypted or signed, provides a seamless, highly secure, asynchronous control plane connection between the service processor and service controller server elements and the service controller and service controller agents that works over a wide range of access networks, such as any access network that has the capability to connect IP or TCP traffic to another TCP or IP endpoint on the access network, another private network or over the Internet. As described herein, in some embodiments, agent communication bus **1630** also provides a fourth level of encrypted or signed communication to form a secure closed system on the device for agent to agent communication, fur example, making it very difficult or practically impossible for software or applications to gain access to one or more of the a service processor agents on the device in any way other than service control device link **1691**. In this way, in some embodiments, agent communication bus **1630** and the service processor agents can only be accessed by one another as necessary or permitted by agent communication policies, or by the service controller or other authorized network function with proper security credentials communicating over service control device link **1691**. Additionally, in some embodiments, communications between a subset of two or more agents, or between one or more agents and one or more service controller server elements are encrypted with unique keys or signatures in such a way that a fourth level of security providing private point to point, point to multipoint, or multipoint to multipoint secure communication lines is provided.

(188) In some embodiments, all of service control device link **1691** communications are transformed into a continuous control plane connection, with a frequency based on the rate of service usage, a minimum set period between connections, and/or other methods for establishing communication frequency. In some embodiments, this heartbeat function provides a continuous verification link by which the service controller verifies that the service processor and/or device are operating properly with the correct service policies being implemented. In view of the following heartbeat function embodiments described herein, it will be apparent to one of ordinary skill in the art that different approaches for implementing the various heartbeat embodiments are possible, and it will be clear that there are many ways to achieve the essential features enabling a reliable, sometimes continuous control link and verification function for the purpose of assisting control of service usage in a verifiable manner. As shown, inside service processor **115**, service control device link **1691** includes heartbeat send counter **2402** in communication with agent communication bus **1630**. For example, heartbeat send counter **2402** can provide a count for triggering when a service processor **115** communication (e.g., periodic communication based on a heartbeat mechanism) should be sent to service controller **122**, and heartbeat buffer **2404**, also in communication with agent communication bus **1630**, buffers any such information for the next service processor **115** communication, in accordance with various heartbeat based embodiments, as similarly described

herein. Heartbeat buffer **2404** is in communication with framing element **2406** and encrypt element **2408** for framing and encrypting any service processor **115** communications transmitted to service controller **122** by transport services stack **2410** over service control link **1653**. Similarly, as shown inside service controller **122**, service control server link **1638** includes heartbeat send counter **2434** in communication with service controller network **2440**, and heartbeat buffer **2432**, also in communication with service controller network **2440**, which buffers any such information for the next service controller **122** communication, in accordance with various heartbeat based embodiments, as similarly described herein. Heartbeat buffer **2432** is in communication with framing element **2430** and encrypt element **2428** for framing and encrypting any such service controller **122** communications transmitted to service processor **115** by transport services stack **2420** over service control link **1653**.

(189) As also shown inside service processor **115** of FIG. **16**, service control device link **1691** includes decode element **2412** for decoding any received service controller **122** communications (e.g., decrypting encrypted communications), unpack element **2414** for unpacking the received service controller **122** communications (e.g., assembling packetized communications), and agent route **2416** for routing the received service controller **122** communications (e.g., commands, instructions, heartbeat related information or status reports, policy related information or configuration settings and/or updates, challenge/response queries, agent refreshes and/or new software for installation) to the appropriate agent of service processor **115**. Similarly, as shown inside service controller **122**, service control server link **1638** also includes decode element **2422** for decoding any received service processor **115** communications (e.g., decrypting encrypted communications), unpack element **2424** for unpacking the received service processor **115** communications (e.g., assembling packetized communications), and agent route **2426** for routing the received service processor **115** communications (e.g., responses to instructions and/or commands, heartbeat related information or status reports, policy related information or configuration settings and/or updates, challenge/response queries, agent status information, network service/cost usage and/or any other reporting related information) to the appropriate agent of service controller **122**. Accordingly, as described herein with respect to various embodiments, the various secure communications between service controller **122** and service processor **115** can be performed using the embodiment as shown in FIG. **16**, and those of ordinary skill in the art will also appreciate that a variety of other embodiments can be used to similarly provide the various secure communications between service controller **122** and service processor **115** (e.g., using different software and/or hardware architectures to provide secure communications, such as using additional and/or fewer elements/functions or other design choices for providing such secure communications).

(190) In some embodiments, an efficient and effective communication framing structure between the service processor and service controller is provided, and the following embodiments (e.g., as shown and described with respect to FIG. **17**) teach such a structure that packs the various service processor agent control plane communications and the various service controller element control plane connections into a format that does not consume excessive bandwidth to enable a continuous control plane connection between the device and service controller. In some embodiments, an efficient and effective communication framing structure between the service processor and service controller is provided to buffer such communication messages for some period of time before framing and transmitting, such as in a heartbeat frequency that is based on rate of service usage. In some embodiments, an efficient and effective communication framing structure between the service processor and service controller is provided to allow for the frame to be easily packed, encrypted, decoded, unpacked and the messages distributed. In view of the various embodiments described herein, it will be apparent to one of ordinary skill in the art that many framing structures will work for the intended purpose of organizing or framing agent communications and the uniqueness and importance of combining such a system element with the device service controller

functions, the service processor functions, the service control verification functions and/or the other purposes.

(191) FIG. **17** is a functional diagram illustrating a framing structure of service processor communication frame **2502** and service controller communication frame **2522** in accordance with some embodiments. In particular, service control device link **1691** of service processor **115** and service control service link **1638** of service controller **122** (e.g., as shown in FIG. **16**) provide for secure control plane communication over service control link **1653** between service processor **115** and service controller **122** using communication frames in the format of service processor communication frame **2502** and service controller communication frame **2522** as shown in FIG. **17** in accordance with some embodiments. As shown, service processor communication frame **2502** includes service processor framing sequence number **2504**, time stamp **2506**, agent first function ID **2508**, agent first function message length **2510**, agent first function message **2512**, and, assuming more than one message is being transmitted in this frame, agent Nth function ID **2514**, agent Nth function message length **2516**, and agent Nth function message **2518**. Accordingly, service processor communication frame **2502** can include one or more messages as shown in FIG. **17**, which can depend on networking frame length requirements and/or other design choices. Similarly, as shown, service controller communication frame **2522** includes service controller framing sequence number **2524**, time stamp **2526**, agent first function ID **2528**, agent first function message length **2530**, agent first function message **2532**, and, assuming more than one message is being transmitted in this frame, agent Nth function ID **2534**, agent Nth function message length **2536**, and agent Nth function message **2538**. Accordingly, service controller communication frame **2522** can include one or more messages as shown in FIG. **17**, which can depend on networking frame length requirements and/or other design choices.

(192) FIGS. **18**A through **18**J, **19**A through **19**S, and **20**A through **20**E present numerous embodiments that can be used in isolation or in combination by a service controller in authenticating the service processor to ensure that it is present and properly configured to implement a device portion of an access network service policy. FIGS. **18**A through **18**J provide tables summarizing various service processor heartbeat functions and parameters (e.g., implemented by various agents, components, and/or functions implemented in software and/or hardware) in accordance with some embodiments. Many of these heartbeat functions and parameters are similarly described above, and the tables shown in FIGS. **18**A through **18**J are not intended to be an exhaustive summary of these heartbeat functions and parameters, but rather are provided as an aid in understanding these functions and parameters in accordance with some heartbeat based embodiments described herein.

(193) FIGS. **19**A through **19**S provide tables summarizing various device based service policy implementation verification techniques in accordance with some embodiments. Many of these device based service policy implementation verification techniques are similarly described above, and the tables shown in FIGS. **19**A through **19**S are not intended to be an exhaustive summary of these device based service policy implementation verification techniques, but rather are provided as an aid in understanding these techniques in accordance with some device based service policy embodiments described herein.

(194) FIGS. **20**A through **20**E provide tables summarizing various techniques for protecting the device based service policy from compromise in accordance with some embodiments. Many of these techniques for protecting the device based service policy from compromise are similarly described above, and the tables shown in FIGS. **20**A through **20**E are not intended to be an exhaustive summary of these techniques for protecting the device based service policy from compromise, but rather are provided as an aid in understanding these techniques in accordance with some device based service policy embodiments described herein.

(195) FIG. **21** illustrates an example embodiment of a process to start or stop a data session with SGSN notification. End-user device **100** attempts to start a data session by sending a GPRS Attach

message to SGSN **2230**. SGSN **2230** notifies service controller **122** that end-user device **100** has started a data session. Service controller **122** waits for a pre-determined time, for example, one minute, to receive a login or authentication request from service processor **115**. In some embodiments, service controller **122** sets a login timer. If service controller **122** receives the login or authentication request before the timer expires, it attempts to authenticate service processor **115**.

(196) One or more authentication errors may occur when service controller **122** attempts to authenticate service processor **115**. For example, service processor **115** may have invalid credentials. As another example, service processor **115** may send invalid application or kernel signatures. As another example, service processor **115** may report end-user device "root" detection errors. As another example, service processor **115** may contact service controller **122** using an identifier that is already in use by a different end-user device.

(197) If service controller **122** does not receive the request from service processor **115** within the pre-determined time, or if service controller **122** is unable to authenticate service processor **115** for some reason, service controller **122** assumes that either (1) end-user device **100** does not contain a service processor, and is therefore unable to participate in device-assisted services, or (2) although end-user device **100** has a service processor, service processor **115** has been disabled. Service controller **122** sends a notification ("No active SP" message) to data rating element **2220** to indicate that end-user device **100** does not have the ability to provide the information necessary for data mediation element **2210** to generate detailed data usage reports, e.g., "micro-CDRs." In some embodiments, service controller **122** sends a trigger to the network to indicate that end-user device **100** should be charged for usage at "standard" bulk rates. In some embodiments, service controller **122** specifies a "standard" bulk rate charging code in the CDRs it sends to data mediation element **2210**. In some embodiments, data rating element **2220** determines data usage by end-user device **100** based on carrier-based records.

(198) If service controller **122** receives the login or authentication request from service processor **115** within the pre-determined time and successfully authenticates service processor **115**, service controller **122** sends a notification ("Device OK" message) to data rating element **2220** to indicate that end-user device **100** has a service processor and is capable of supporting device-assisted services. In some embodiments, data rating element **2220** expects to receive "micro-CDR" reports from data mediation element **2210** when service controller **122** has determined that end-user device **100** has an active service processor. In some embodiments, data rating element **2220** determines usage based on the micro-CDRs, which contain more granular information than ordinary CDRs. For example, whereas an ordinary CDR might simply report that an end-user device used 100 Megabytes (MB) of data, a set of micro-CDRs might report that the end-user device used 15 MB of e-mail, 35 MB of social networking, and 50 MB of streaming video.

(199) In some embodiments, data mediation element **2210** sends carrier-based usage reports (e.g., CDRs) to service controller **122**. Service controller **122** queries usage database **2200** for device-based usage reports (e.g., micro-CDRs) for end-user device **100**. Service controller **122** determines the data usage of end-user device **100** from. the carrier-based usage reports. Service controller **122** determines the data usage of end-user device **100** from the device-based usage reports. Service controller **122** compares the usage determined from the carrier-based usage reports to the usage determined from the device-based usage reports. If service controller **122** determines that the two usage measures do not match (e.g., are not identical or are not within a threshold of each other), service controller **122** sends a notification (e.g., a fraud alert) to data rating element **2220** to indicate that the end-user device is in a fraud state, and data rating element **2220** should bill usage for end-user device **100** based on carrier-based usage reports. Service controller **122** sends the carrier-based usage reports and device-based usage reports to data mediation element **2210**.

(200) When the "CPRS detach" message is received by SGSN **2230**, SGSN **2230** sends a notification to service controller **122** that the data session for end-user device **100** is closed.

(201) FIG. **22** illustrates an example embodiment of a process to start or stop a data session with

GGSN notification. The process is similar to that described with reference to FIG. **21**, except in how the data session starts and ends. End-user device **100** starts a data session by sending data traffic to GGSN **2240**. GGSN **2240** recognizes the start of a new data session and notifies service controller **122** that end-user device **100** has started a data session. When GGSN **2240** determines that the data session has closed, it sends a notification to service controller **122** that the data session for end-user device **100** is closed.

(202) As discussed above, in some embodiments a device service processor can provide information to assist in classification of service usage for any combination of device application, network destination or resource, a type of network, roaming condition (e.g., home or roaming network), a time period, a level of network congestion, a level of network QoS, and a background or foreground communication. In some embodiments, when a service processor provides service usage for a classification of service usage involving one or more of device application, network destination or resource, a type of network, roaming condition (e.g., home or roaming network), a time period, a level of network congestion, a level of network QoS, and a background or foreground communication, service processor **115** generates a service usage report, called a “micro-CDR,” that is then communicated to a network element (e.g., a service controller). The micro-CDR provides a service usage accounting breakdown in finer detail (e.g., including information about a device application, network destination or resource, a type of network, roaming condition (e.g., home or roaming network), a time period, a level of network congestion, a level of network QoS, and a background or foreground communication) than a “bulk” CDR that does not provide such a usage accounting breakdown.

(203) In some embodiments, a device is configured to receive access network services and is further configured to include a service processor capability to account for one or more service activity classifications and send the accounting to a service controller. In some embodiments the service controller is configured to communicate at least a portion of the service processor service accounting as a service usage credit to a service usage reconciliation system. Note that a service usage reconciliation system is also referred to herein in various embodiments as a service usage mediation system or similar term involving mediation. In some embodiments, the service usage reconciliation system is configured to remove a credit from a user service accounting or usage bill. In some embodiments, the service usage credit that is removed from a user service accounting or usage bill is allocated to sponsor service accounting or bill.

(204) In some embodiments it is advantageous to reconcile the micro-CDR service usage accounting reports received from a service processor against a trusted source. In some embodiments, this is accomplished through a system that provides usage credit for one or more micro-CDR usage reports that are reconciled with or validated by a trusted source. In some embodiments, if such credit is provided, the corresponding usage is removed from the user “bulk” usage and re-assigned to the user according to service usage accounting rules associated with the micro-CDR classification. In some embodiments the micro-CDR accounting rules can be designed to account micro-CDR service usage report accounting to a paid user service classification (e.g., a device application based service accounting, a network destination or resource based service accounting, a roaming service usage accounting, etc.). In some embodiments, the micro-CDR accounting rules can be designed to account micro-CDR service usage report accounting to a sponsored service classification (e.g., a sponsored device application based service accounting, a sponsored network destination or resource-based service accounting, a sponsored background classification of service usage, a sponsored content source classification of service usage, a sponsored shopping service, etc.).

(205) In some embodiments the trusted source used to validate micro-CDR service usage classification reports is an FDR (flow data record) source that reports a detailed level of classification that indicates network source or destination (e.g., domain, URL, IP address, etc.) and possibly one or more ports and protocols. In some embodiments, the source of the FDR is a

network element. In some embodiments the source of the FDR is a device agent. In some embodiments, the agent that generates the FDR report is located in a secure execution environment on the device. In some embodiments, the agent that generates the FDR report is located in a secure hardware environment on the device. In some embodiments, the agent that generates the FDR report uses a secure transmission protocol with the service controller that is sequenced and signed and/or encrypted in a manner wherein if the sequence of FDR reports or the content of FDR reports is tampered with, then an FDR integrity violation may be detected by the service controller. In some embodiments, a communication from the service controller to the agent generating the FDR reports is sequenced and signed and/or encrypted in a manner wherein if the sequence of FDR reports or the content of FDR reports is tampered with, then an FDR integrity violation may be detected by the agent generating the FDR reports. In some embodiments, when the agent generating the FDR reports detects an FDR integrity violation, the agent generating the FDR reports causes device access to be quarantined or blocked for one or more access networks. In some embodiments, other device communication links than access network links can also be quarantined or blocked, including one or more of wired device access ports (e.g., Ethernet, USB, firewire, etc.), Bluetooth, WiFi, and near field communications.

(206) In some embodiments, the trusted source used to validate micro-CDR service usage classification reports is a network-based element such as a server, gateway, proxy or router that processes the classification of service associated with the micro-CDR. In some embodiments, the network-based element classifies service usage associated with the micro-CDR, measures the service usage, and provides a service usage classification report back to a service controller so that it can be reconciled against the micro-CDR reports.

(207) In some embodiments, a device is configured to receive access network services and is further configured to include a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications to one or more proxy gateway/servers. In some such embodiments, a service usage reconciliation system is configured to receive device service usage information (e.g., a credit amount) from the one or more proxy gateway/servers, and the service usage information is used in removing an amount (e.g., a credit amount) from service usage allocated to or charged to a user bill by the service usage reconciliation system. In some embodiments, the device routing is accomplished by routing, re-directing, or steering device traffic for one or more service usage classifications to a specific network destination or resource associated with the proxy gateway/server. In some embodiments, the routing, re-directing, or steering is accomplished using a secure tunnel through the network. In some embodiments the routing, re-directing, or steering is accomplished using an SSL, VPN or APN tunnel.

(208) In some embodiments, a device service processor classifies service usage according to a service classification policy and routes, re-directs, or steers the traffic associated with the classification policy to a network element (e.g., a server, gateway, proxy or router that processes the classification of service associated with the micro-CDR) that generates the micro-CDR for that service usage accounting. In this manner, the device can associate service usage for device applications or OS functions with a specific network destination that in turn further processes the traffic and generates the appropriate micro-CDRs that are sent to the service controller for reconciliation (e.g., mediation) as described above. The service processor can steer the traffic classified according to the classification policy by re-directing the traffic to the network destination associated with the appropriate network element, routing the traffic to the network destination associated with the appropriate network element, or tunneling or securely tunneling (e.g. SSL, VPN, APN) the traffic to the network destination associated with the appropriate network element.

(209) In some embodiments, the trusted source used to validate micro-CDR service usage classification reports is a server or website that provides the service, and the validation is provided in the form of good customer feedback associated with a user credential, a service processor credential or a device credential that can be used to determine which device or user to provide the

credit to. For example, if a website is associated with the service usage classification defined for a micro-CDR, and the website is visited by a device with a given device credential or user credential, and the website servers track the number of visits, number of transactions, amount of business generated, amount of data communicated or another measure of device interaction with the website, then a summary of this device interaction with the website can be communicated to the service controller and the service controller can provide credit for the micro-CDR.

(210) In some embodiments, another means of limiting the possibility of improper service usage accounting due to improper configuration of a service processor or tampering with a service processor can be accomplished by capping the amount of service over a given period of time that is allowed for a given micro-CDR service usage classification category (e.g., by limiting the amount of service usage in a given period of time for one or more service usage classifications including a device application, network destination or resource, a type of network, a roaming condition (e.g., home or roaming network), a time period, a level of network congestion, a level of network QoS, or a background or foreground communication). In some embodiments, capping the amount of service over a given period of time that is allowed for a given micro-CDR service usage classification category is advantageous as a way of limiting service usage costs for a user-paid service that is based on a specific classification of service usage. In some embodiments, capping the amount of service over a given period of time that is allowed for a given micro-CDR service usage classification category is advantageous as a way of limiting service usage costs for a sponsored service that is based on a specific classification of service usage. In some embodiments, the possibility of service usage report tampering for one or more micro-CDR service usage classification categories is limited by combining reconciliation of service usage using one or more of start/stop accounting, CDR feedback, FDR feedback, etc., and setting a limit on the usage that is allowed for one or more of the micro-CDR service usage classification categories.

(211) In some embodiments, the possibility of service usage report tampering for one or more micro-CDR service usage classification categories is limited by comparing the total service usage for all combined micro-CDR service usage classifications against the total amount of service used in bulk CDR reports received from a trusted source.

(212) In some embodiments using associative classification (also referred to as adaptive ambient service usage classification), some service usage that can not be directly identified as belonging to a give micro-CDR service usage classification is assigned to the micro-CDR service usage classification based on one or more of: (i) time proximity with one or more known service usage flows identified as belonging to the micro-CDR classification, (ii) a maximum amount of service usage (e.g., byte count) that has occurred since one or more known service usage flows that belong the micro-CDR classification were identified, or (iii) the fact that the unidentified service usage is associated with the same application as one or more known service usage flows that belong to the micro-CDR classification.

(213) In some such associative classification (adaptive ambient service classification) embodiments, service usage fraud exposure can be limited by setting a limit on the amount of service usage that can be “unaccounted for” so that if the majority of usage can be classified as belonging to a micro-CDR service usage classification category, the unaccounted-for service usage is allowed to be accounted for in the same micro-CDR accounting. In this manner, if fraudulent service usage activity results in a large percentage of service usage that is not known to be classified as belonging to the micro-CDR usage classification category, a micro-CDR accounting integrity violation can be declared. Service usage above the limits that cannot be reconciled (accounted for) can alternatively be accounted for (e.g., charged to the user) at an agreed-upon contract rate. In some embodiments, the agreed-upon rate is as high or higher than the rate for user paid bulk services (e.g., higher than the rate at which sponsored and specialized application or website based services are billed). In some embodiments, the user is sent a notification by the service controller that the user is being billed at the higher rate. In some embodiments, the user

signs up to a service agreement wherein the user agrees to be billed at the higher rate in the event that the service processor is compromised or the micro-CDR accounting is compromised.

(214) In some embodiments, the micro-CDR reports include the amount of service usage that was identified by the service processor as known to belong to the micro-CDR service usage category. In some embodiments, a flow identifier (e.g., domain, URL, IP address, port, or device application associated with [originating or terminating] the flow) can be provided in the micro-CDR reports for service usage known to belong to the micro-CDR classification. In some embodiments, the service controller samples or scans these “known good” micro-CDR flow identifiers to ensure that the flows do in fact belong to the micro-CDR service usage classification, and if they do not a micro-CDR accounting integrity violation can be declared. In some embodiments a flow identifier (e.g., domain, URL, IP address, port, or device application associated with [originating or terminating] the flow) can be provided in the micro-CDR reports for service usage that cannot be classified as belonging to the micro-CDR classification. In some embodiments, the service controller samples or scans these “unknown” micro-CDR flow identifiers to determine if the service destination patterns indicate fraudulent service usage that is inconsistent with micro-CDR classification policies, and if so a micro-CDR accounting integrity violation can be declared.

(215) In some embodiments, a SIM that is expected to be installed in a device configured with a properly configured service processor is allocated a relatively small service usage cap in a network portion of an access network service usage policy so that the device can connect to the network and allow the service processor to authenticate with the service controller. By limiting the initial amount of service usage allowed prior to the service processor authentication with the service controller, it is not possible to get a large amount of service prior to ensuring that a properly configured service processor is present on the device. In some embodiments, once the device service processor is authenticated, an increment can be added to the usage limit in the network portion of the access network service policy. In some embodiments, additional usage limit increments can be added to the network portion of the access network service policy as device service processor generated CDRs, FDRs or micro-CDRs are received by the service controller. In some embodiments, if at any time the flow of CDRs, FDRs or micro-CDRs from the device is tampered with or stopped, the service controller stops incrementing the usage limit in the network portion of access network service policy, and the device access is denied. Alternatively, in some embodiments, rather than stopping service when a service processor is removed or tampered with, the network portion of the access network service policy calls for the application of a higher rate of billing as compared to one or more micro-CDR billing rates for micro-CDR credits provided by the service controller (e.g., user paid application based services, user paid website based services, user paid content services, sponsored application based services, sponsored website based services or sponsored content based services). In some embodiments, if the service processor ceases to send micro-CDRs to the service controller, the user ceases to be credited for the micro-CDR service usage and all usage is billed at a bulk rate that may be higher than the micro-CDR service rates.

(216) In some embodiments, a SIM is provided or sold to a user wherein the SIM is associated with sponsored services that are based on network access service policies configured in the network policy enforcement elements and a service controller. In such embodiments, the problem arises that the SIM may be installed in a device that does not have a properly configured service processor, giving rise to the possibility that a user could receive unintended free services with the sponsored SIM. Embodiments described above can be used to limit the amount of access the SIM is allowed to receive prior to service processor authentication with the service controller by limiting the initial service usage amount allowed in the initial network portion of access network service policy. However, if a number of sponsored SIMs are readily available and inexpensive or free, a user could potentially swap several SIMs into the device and remove each SIM when the service controller fails to authenticate the service processor. In some embodiments, the service controller recognizes the SIM and a second device credential (e.g., an IMEI, a modem credential or a device credential)

the first, time the sponsored SIM acquires service usage and fails to authenticate the service processor for that device. Once the service processor fails to authenticate with the service controller, the service controller re-sets the network portion of the access network service policy to deny service the next time a SIM attempts to authenticate with the device credential associated with the original SIM.

(217) In some embodiments, good customer feedback may be used as a micro-CDR credit source directly without a service processor on the device. For example, in some embodiments, a website is associated with the service usage classification defined for a micro-CDR, and the website or server that is visited by a device with a given device credential or user credential tracks one or more of the number of visits, number of transactions, amount of business generated, amount of data communicated or another measure of device interaction with the website or server, creates a summary report of this device interaction with the website or server, and then communicates the summary report to a service controller. The service controller can then reconcile the good customer feedback summary report of the device interaction with the website or server by applying a user service usage credit rating rule to deduct a bulk portion of service usage from the user account and add a classification of service usage to the user account that is rated for billing purposes by a rating rule for the given micro-CDR classification. Alternatively, the service controller can deduct a portion of the good customer micro-CDR service usage accounting or billing from the user account and add it to a sponsor entity account, such as the entity that provides the website or server service. In this way, a micro-CDR service usage charging system can be implemented in a network for classification service usage with specialized service usage classification rating, for both user paid classification and sponsored classifications, without the need for a service processor on the device.

(218) FIG. **23** illustrates an exemplary embodiment with network system elements that can be included in a service controller system to facilitate a device-assisted services (DAS) implementation and the flow of information between those elements. FIG. **23** shows the flow of information to facilitate reconciliation of device-generated data usage records with network-generated (e.g., wireless network carrier-generated) data usage records associated with an end-user device. In addition, FIG. **23** shows the flow of information from a carrier to an end-user device for the purpose of publishing an offer set. A user of the end-user device may then select or act on the offer set.

(219) Carrier-generated charging data records (CDRs) or real-time reporting records (RTRs) (or other real-time or near-real-time usage record formats such as, e.g., FDRs, batch processed usage records, continuous usage record event feeds or SMS formatted usage record messages) flow from carrier **2650** (which can be, e.g., a real time reporting system, a network gateway, a network usage charging system element, a AAA, an HLR, a billing element, etc.) to load balancer **2652** to RTR filtering element **2654**.

(220) In some embodiments, load balancer **2652** selects one of many CDR/RTR processing threads that are available in the service controller information processing system. In some embodiments, the processing thread is an asynchronous software or firmware program running on a gateway or server CPU. In some embodiments, the processing thread is a virtual machine processing thread that exists in a resource pool of gateway or server CPUs or virtual machines, which may include geographically separated or redundant resource pools. As illustrated in FIG. **23**, each processing thread includes the functional steps of CDR/RTR filtering **2654**, JMS queue **2656**, CDR/RTR processor **2658** and the interface to CDR/RTR database **2660**. In some embodiments, processing threads are asynchronous in that they are initiated when load balancer **2652** directs one or more CDR/RTR data transfers to the thread and terminated when the processed CDR/RTR information has been processed and deposited into CDR/RTR database **2660**. Note that FIG. **23** shows only one of potentially many available CDR/RTR processing threads.

(221) CDR/RTR filtering element **2654** selects the records that are associated with devices that include a device client that communicates with the service controller (e.g., the device client can be

a service processor configured to provide service usage notification updates, on-device service plan purchase or activation with UI options display and user selection actions, device-assisted access control policy enforcement, device-assisted service usage charging policy enforcement, device-assisted service notification messages, etc.). In some embodiments, devices supporting DAS are identified by device credentials or user credentials that are communicated to the service controller as described herein, where the device credential or user credential are members of a device group or user group that is managed by the service controller.

(222) In some embodiments, CDR/RTR filtering element **2654** may be used advantageously to quickly receive and acknowledge a CDR/RTR record to provide asynchronous functionality because of real-time processing requirements, server processing thread scalability and maintainability requirements, or server processing thread geographic redundancy requirements. In some embodiments, filtering eliminates unnecessary load on JMS queue **2656** and/or CDR/RTR database **2660**. CDR/RTR filtering element **2654** places the records from end-user devices known to be configured with a device client (e.g., a service processor configured to provide service usage notification updates, on-device service plan purchase or activation with UI options display and user selection actions, device-assisted access control policy enforcement, device-assisted service usage charging policy enforcement, device-assisted service notification messages) that communicates with the service controller through Java messaging service (JMS) queue **2656**. In some embodiments, CDR/RTR filtering element **2654** filters out device records for devices that may have a form of service processor, but the service processor has not properly authenticated with the service controller. In some embodiments, the device clients that are known to be configured with a device client that communicates with the service controller are determined by looking up a device credential or user credential associated with CDRs or RTRs in a device group or user group management database (e.g., in SDC database **2692** or subscriber management system **182** (shown, e.g., in FIGS. **1-3**)).

(223) JMS queue **2656** buffers the CDR/RTR information remaining after CDR/RTR filtering **2654** and allocates one or more CDRs/RTRs to a service usage processing thread in CDR/RTR processor **2658**. In some embodiments, JMS queue **2656** is a persistent queue. In some embodiments, JMS queue **2656** is a primary messaging system between applications.

(224) CDR/RTR processor **2658** retrieves the records from JMS queue **2656**, transforms the records, and stores them in CDR/RTR database **2660**. In some embodiments, CDR/RTR processor **2658** is an application or a process thread. In some embodiments, CDR/RTR processor **2658** pulls a CDR/RTR record from JMS queue **2656**, transforms the record, and stores the transformed record in CDR/RTR database **2660** in one transaction in order to provide fault tolerance in the case of system failure. In some embodiments, CDR/RTR processor **2658** formats the CDR/RTR information to provide a common service usage information format to facilitate one or more of service usage processing, reporting, analysis, comparison, mediation and reconciliation operations performed within the service controller system. In some embodiments, CDR/RTR processor **2658** observes CDR/RTR time stamps and time synchronizes, time aligns, or time aggregates multiple CDR/RTR reports so that a more consistent measure of usage with a common time reference can be achieved within the service controller system for one or more of service usage processing, reporting, analysis, comparison, mediation and reconciliation purposes.

(225) In some embodiments, end-user devices capable of DAS reporting (e.g., devices configured with a device client that communicates with the service controller, such as a service processor described herein) connect periodically or on occasion to usage reporting gateway **2672** to report their data usages. In some embodiments, DAS reporting information includes but is not limited to one or more of user service plan purchase or activation selection choices, device user service policy configuration preference selections (e.g., user-generated service policy assignments for applications, websites, network types, or home/roaming policies), DAS service usage reports, DAS device policy state reports, DAS software environment integrity reports, and other reports listed in

the tables in FIGS. **18** through **20**.

(226) In some embodiments, DAS device usage reports and analytics flow from carrier device network **2668** (e.g., devices configured with service processors that are in communication with the service controller) to load balancer **2670** to usage reporting gateway **2672**. In some embodiments, load balancer **2670** selects one of many usage reporting processing threads that are available in the service controller information processing system. In some embodiments, the usage reporting processing thread is an asynchronous software or firmware program running on a gateway or server CPU. In some embodiments, the usage reporting processing thread is a virtual machine processing thread that exists in a resource pool of gateway or server CPUs or virtual machines, which may include geographically separated or redundant resource pools. As illustrated in FIG. **23**, each usage reporting processing thread consists of the functional steps of usage reporting gateway **2672**, JMS queue **2674**, report processor **2676**, and the interface to usage report database **2678**. In some embodiments, usage reporting processing threads are asynchronous in that they are initiated when load balancer **2670** directs one or more usage reporting data transfers to a thread and terminated when the processed usage reporting information has been processed and deposited into usage report database **2678**. Note that FIG. **23** shows only one of potentially many available usage reporting processing threads.

(227) Usage reporting gateway **2672** accepts reports from devices configured with a device client (e.g., a service processor configured to provide service usage notification updates, on-device service plan purchase or activation with UI options display and user selection actions, device assisted access control policy enforcement, device assisted service usage charging policy enforcement, device assisted service notification messages) that communicates with the service controller and places the reports on JMS queue **2674**. In some embodiments, usage reporting gateway **2672** only accepts device reports from device service processors that have authenticated with the service controller system. In some embodiments, usage reporting gateway **2672** only accepts device reports from device service processors configured with device credentials or user credentials that are members of a device group or user group that is managed by the service controller. In some embodiments, usage reporting gateway **2672** rejects reports from end-user devices without authenticated service processors. In some embodiments, usage reporting gateway **2672** is an application or a process thread. In some embodiments, usage reporting gateway **2672** quickly receives and acknowledges end-user device reports. In some embodiments, usage reporting gateway **2672** provides asynchronous functionality that is advantageous to support real-time processing requirements.

(228) In some embodiments, the end-user device is authenticated before reports are put onto JMS queue **2674**. In some embodiments, JMS queue **2674** is a persistent queue. In some embodiments, JMS queue **2674** is a primary messaging system between applications.

(229) Report processor **2676** retrieves reports from JMS queue **2674**, transforms the reports, and stores the transformed reports in usage report database **2678**. In some embodiments, report processor **2676** is an EAI. In some embodiments, report processor **2676** retrieves reports from JMS queue **2674**, transforms the reports, and stores the transformed reports in usage report database **2678** in a single transaction in order to provide fault tolerance in case of system failure. In some embodiments, report processor **2676** formats the device usage report information to provide a common service usage information format to facilitate one or more of service usage processing, reporting, analysis, comparison mediation and reconciliation purposes internal processing and comparison within the service controller system. In some embodiments, report processor **2676** observes device usage report time stamps and time synchronizes, time aligns or time aggregates multiple device usage reports so that a more consistent measure of usage with a common time reference can be achieved within the service controller system for one or more of service usage processing, reporting, analysis, comparison mediation and reconciliation purposes.

(230) In some embodiments, CDR/RTR filtering **2654**, CDR/RTR processor **2658**, report processor

2676, and usage reporting gateway **2672** share a host.

(231) In some embodiments, micro-CDR generator **2680** retrieves records from CDR/RTR database **2660** and retrieves reports from usage report database **2678**. In some embodiments, micro-CDR generator **2680** determines a service usage amount for a micro-CDR service usage classification, assigns a usage accounting identifier to the micro-CDR report that identifies the usage as being accounted to a device user for the device associated with a device credential or user credential, and reports this amount of service usage to the carrier network **2666** (in the exemplary embodiment of FIG. **23**, through JMS queue **2662** and FTP or publisher **2664**). In some embodiments, micro-CDR generator **2680** determines a service usage amount for a micro-CDR service usage classification, assigns a usage accounting identifier to the micro-CDR report that identifies the usage as being accounted to a service sponsor, and reports this amount of service usage to carrier network **2666**. In some embodiments the micro-CDR for the sponsored service usage report also includes an identifier for a device credential or user credential. In some embodiments, the amount of service usage accounted for in the micro-CDR is mediated or reconciled off of a device or user bulk service usage accounting. In some embodiments, micro-CDR generator **2680** sends micro-CDRs to JMS queue **2662**. In some embodiments, FTP or publisher **2664** retrieves micro-CDRs from JMS queue **2662** and pushes the micro-CDRs to carrier **2666**.

(232) In some embodiments, fraud analyzer **2682** retrieves records from CDR/RTR database **2660**. In some embodiments, fraud analyzer **2682** retrieves reports form usage report database **2678**. In some embodiments, fraud analyzer **2682** retrieves micro-CDRs from micro-CDR generator **2680**. In some embodiments, fraud analyzer **2682** performs a fraud analysis using one or more of the record and report information sources consisting of CDR/RTR database **2660**, usage report database **2678**, and micro-CDR generator **2680**. In some embodiments, fraud analyzer **2682** compares usage records associated with a specific device or user credential from one or more of CDR/RTR database **2660**, usage report database **2678**, and micro-CDR generator **2680** to determine if service usage is outside of pre-defined service usage policy behavior limits. In some embodiments, fraud analyzer **2682** compares service usage information associated with a specific device or user credential from one or more of CDR/RTR database **2660**, usage report database **2678**, and micro-CDR generator **2680** to determine if a pre-defined service usage limit has been reached or exceeded. In some embodiments, fraud analyzer **2682** compares service usage information associated with a specific device or user credential from one or more of CDR/RTR database **2660**, usage report database **2678** and micro-CDR generator **2680** to determine if the specific device or user is exhibiting a service usage behavior that is outside of pre-defined statistical limits as compared to the service usage behavior of a device or user population. In some embodiments, fraud analyzer **2682** stores the results of its fraud analysis in data warehouse **2694**. In some embodiments, fraud analyzer **2682** sends fraud alerts to carrier network **2666**.

(233) In some embodiments, a service design center is used to create service offers (e.g., service plan offers to purchase or activate a bulk service plan, an application specific service plan, an application group-specific service plan, a website service plan, a website-group service plan, etc.). In some embodiments, the service offers are published to DAS-enabled devices. To publish an offer to one or more devices in carrier device network **2668**, carrier **2696** enters information in service design center **2690**. Service design center (SDC) **2690** stores the offer set in SDC database **2692**. The offer set then flows to device message queue **2688**. In some embodiments, device message queue **2688** is a database-backed persistent queue. In some embodiments, when an end-user device with an authenticated service processor connects to offer set gateway **2686**, offer set gateway **2686** pushes the offer set, to the end-user device. In some embodiments, offer set gateway pushes the offer set to the end-user device at the next usage report. In some embodiments the new offer is an offer to purchase or activate a service plan, and the offer notification is configured with offer acceptance features that allow the device user to select an option to purchase or activate the service

offer in the device UI.

(234) In some embodiments, a list of service offers that are available to a device group or user group, wherein the list of service offers is created in a service design center user interface, is stored in SDC database **2692** and published to the devices that belong to the device group or user group.

(235) In some embodiments, an offer set is defined in service design center (SDC) **2690**. In some embodiments, this offer set includes multiple service plans that can be communicated to the device service processor for display to the device end user for service plan selection, purchase or activation through the device UI. In some embodiments, the offer set UI display is configured to allow the user to purchase or activate a service plan within the offer set in real-time or near-real-time. In some embodiments, the offer set information is received from the service controller and the offer set information is processed for UI display by a device service processor. In some embodiments, service processor offer set information processing and UI display is configured to allow the user to purchase or activate a service plan within the offer set in real-time or near-real-time. In some embodiments, the user's selection of a service plan for purchase or activation is communicated to the user via an offer set UI display that is configured by a service processor, and the service processor communicates with a service controller via a communication interface to the notification and offer set gateway **2686** to purchase or activate the service plan in real-time or near real-time. In some embodiments the notification and offer set gateway **2686** communicates the user selection of service plan to the offer user selection receiver **2710**, which then causes the service plan policy enforcement settings corresponding to the user's service plan selection to be implemented by communicating the user's service plan selection to network provisioning system **160** (or subscriber management **182**, order management **180**, mobile wireless center **132**, billing **123**, etc.), which in turn communicates with carrier network **2712** to cause the proper service plan policy enforcement settings to he programmed in the various network elements responsible for service plan policy enforcement. In this manner, in some embodiments the network service policy enforcement required to implement the new service plan for the device can be provisioned in the various network elements responsible for network-based policy enforcement (e.g., aggregation/transport gateways **420** [e.g., PDN or GGSN], mobile wireless center **132** [e.g., HLR], AAA server **121**, RAN/access gateway **410** [e.g., SGSN, PDSN], BSC **125**). In some embodiments, the network service policy enforcement that implement the new service plan for the device can be provisioned in the various service processor device agents responsible for network based policy enforcement. In some embodiments, when the service plan policy provisioning is complete, the service controller communicates with the device service processor that the new service plan has been purchased or activated. In some embodiments, the service processor communicates a message from the service controller to the device UI that the new service plan has been purchased or activated.

(236) In some embodiments, the service processor offer set information processing and UI display is configured to allow the user to purchase or activate a service plan within the offer set in real-time or near-real-time. In some embodiments, the user's selection of a service plan for purchase or activation is accepted by an offer set UI display that is configured by a service processor, and the service processor communicates with a service controller to allow the user to purchase or activate the service plan in real-time or near real-time, and the service plan policy settings are communicated by the service controller to the service processor so that the service processor policy enforcement agents that implement the new service plan for the device can be provisioned.

(237) In some embodiments, the provisioning of the various network elements responsible for network-based policy enforcement (so that the device can receive the proper service plan allowances and policies) can take a considerable amount of time, for example minutes or even longer, and this can create a poor user experience that is not real-time or near-real-time. In such cases, the service controller can create a temporary service lease by provisioning a subset of the various network elements responsible for network based policy enforcement to allow for a

temporary service plan that is put in place before all of the required network elements responsible for network-based policy enforcement and possibly service usage accounting or billing can be provisioned. For example, the temporary lease can provision some or all of the required traffic path or data path processing elements to allow the device service usage classifications that correspond to the allowable service usage classifications in the service plan that the user has selected, but do not account the usage to the correct service usage accounting or billing system configuration until the provisioning of the accounting or billing elements is complete. As another example, during the temporary service lease period before the provisioning of the accounting or billing elements is complete, the service controller can track service usage that is incurred during the temporary service lease period and, after the provisioning of the accounting or billing elements is complete, transfer the service usage that is incurred during the temporary service lease period to the appropriate service usage record database so that the usage incurred during the temporarily service lease period is properly accounted for or billed. In another example embodiment, during the temporary service lease the service controller causes a temporary service provisioning to take effect in the various network elements responsible for network access control, wherein the temporary service provisioning provides for all or a subset of the necessary data path provisioning required to allow the service plan allowances that correspond to the access control policies for the service plan the user has selected, and the service usage incurred during the temporary service lease period is accounted to a temporary accounting other than the final accounting that will be in effect once the provisioning of the new user-selected service plan is in full effect. In some embodiments, the temporary accounting is a catch bucket account that is configured to track device usage during the temporary lease period. In some embodiments, the temporary accounting has a service usage rating other than the service usage rating that will be in effect after the new user-selected service plan is fully provisioned (e.g., a zero-rated accounting). In some embodiments, the service usage during the temporary lease period is tracked and then transferred to the appropriate service accounting after the new user selected service plan is fully provisioned.

(238) In some embodiments, some of the delay in activating a new service plan directly on a device UI can be related to performing a credit check or user service standing check for the user's credit credentials or service account credentials. In such cases, embodiments similar to those disclosed above can be used to provide a temporary service lease, possibly with temporary service accounting that is eventually transferred to the final usage accounting. If during the temporary service lease period an indication is returned to the service controller that the user's credit or user service standing is insufficient to provide the service plan the user has selected, then the user can be notified of this issue, possibly with instructions on how to resolve the issue, and the temporary service lease can be revoked, thus disabling the network access permissions that would have been provided to the device if the credit check had been approved and the final service plan provisioning had taken place. In such embodiments, the usage can be tracked during the temporary lease period prior to revoking the temporary lease, and this service usage can be accounted to an account used for the purpose of tracking usage lost due to failed credit checks or failed user service standing checks. In some embodiments, the usage incurred during a temporary lease that is eventually revoked due to a failed credit check or failed user service standing check can be accounted back to another user accounting or billing, and in some embodiments this is in accordance with a user service agreement.

(239) As one of ordinary skill in the art will now recognize, prior to the time that the network can fully provision a new service plan selected by a device user on a device UI, there are many additional related embodiments too numerous to list here to facilitate rapidly enabling device network access permissions that are identical to or similar to the network access permissions the device would eventually be allowed after the new user selected service plan is fully provisioned so that the device user can enjoy a relatively short time delay from the time the user selects a service plan for purchase or activation on a device and the time the network is fully provisioned to

implement the new service plan.

(240) In some embodiments, the service processor is configured to display one or more service plan offers to the device end user, and the time at which this display takes place is determined by what the user is doing with the device or where the device is located (e.g., the end-user device attempts to access the network, an application on the device attempts to access the network, a given application or set of applications are used or attempted to be used, the device enters a roaming state, etc.). In some embodiments, the service processor determines the time at which the one or more service offers are to be displayed to the device user by detecting what the user is doing with the device or a condition of the device caused by the user (e.g., that the device is roaming, etc.).

(241) In some embodiments, a service design center is used to create device user notification messages (e.g., a service offer message, a service usage notification message, a message indicating an amount of bulk service used, a notification indicating an amount of a micro-CDR service classification used, a notification indicating that a bulk usage limit has been reached, a notification indicating that a micro-CDR usage classification usage limit has been reached, etc.). In some embodiments, the notification messages are published to a device service processor (or a group of device service processors that belong to a device group or a user group), and the service processor determines when a trigger condition exists for displaying a specific notification message. In some embodiments, a service usage notification trigger condition (e.g., a state of device usage such as a state of bulk service usage or attempted usage, application usage or attempted usage, website usage or attempted usage, home/roaming usage or attempted usage, cellular/WiFi usage or attempted usage, etc.) is associated with each message. In some embodiments, the service processor on a device determines when the trigger condition has been met and displays a pre-stored notification message associated with the trigger condition. In some embodiments, a network element determines when the trigger condition has been met and uses the notification and offer set gateway **2686** via device message queue **2688** to transmit the notification message to the device for display by the device service processor. In some embodiments, a device service notification message includes a service usage update from CDR/RTR database **2660**, which is sent through notification and offer set gateway **2686** via device message queue **2688**. In some embodiments, a device service notification message includes a service usage update from micro-CDR generator **2680**, which is sent through notification and offer set gateway **2686** via device message queue **2688**. In some embodiments, service usage updates from one or more of CDR/RTR database **2660** or micro-CDR generator **2680** are sent through the notification and offer set gateway **2686** via device message queue **2688** on a recurring basis. In some embodiments, the recurring basis is based on a pre-determined amount of usage being reached (e.g., a pre-determined byte count, pre-determined time count or pre-determined percentage of a pre-determined limit, etc.). In some embodiments the recurring basis is based on a usage notification update frequency or time interval.

(242) FIG. **24** illustrates an example embodiment of a service controller reconciliation processing procedure that may be used to detect fraud using information from the end-user device and information from a second source (explained below). Service processor **115** (not shown) or an application on end-user device **100** (not shown) generates usage measures **2300**. Based on usage measures **2300**, end-user device **100** sends first usage records to service controller **122**, or service controller **122** requests first usage records from end-user device **100**. Service controller **122** processes the first usage records in device usage record pre-processing **2310**. In some embodiments, device usage record pre-processing **2310** modifies the format of the first usage records to facilitate one or more of service usage processing, reporting, analysis, comparison, mediation and reconciliation operations performed within the service controller system. In some embodiments, device usage record pre-processing **2310** observes the first usage records and time stamps and time synchronizes, time aligns or time aggregates multiple first usage records so that a more consistent measure of usage with a common time reference can be achieved within the service controller system for one or more of service usage processing, reporting, analysis,

comparison, mediation and reconciliation purposes. Service controller **122** stores the first usage records in device usage records **2320**.

(243) A second source (not shown) generates or provides second service usage measures **2370**. In some embodiments, the second source is a network element, such as a mediation element, a gateway, a real-time reporting element, a charging element, a billing element, or the like. In some embodiments, the second source is a database. In some embodiments, the second source is a roaming partner network element. In some embodiments, the second source is an element on end-user device **100** that generates secure device data records. In some embodiments, the second source is a partner network destination that provides information about customer usage of or transactions with that destination. In some embodiments, the second source is an application on end-user device **100**.

(244) Based on the second service usage measures, the second source sends second usage records (described below) to service controller **122**, or service controller **122** obtains the second usage records from the second source. Service controller **122** processes the second usage records in record normalization, time reconciliation and pre-preprocessing **2360**. In some embodiments, record normalization, time reconciliation and pre-preprocessing **2360** modifies the format of the second usage records to facilitate one or more of service usage processing, reporting, analysis, comparison, mediation and reconciliation operations performed within the service controller system. In some embodiments, record normalization, time reconciliation and pre-preprocessing **2360** observes the second usage records and time stamps and time synchronizes, time aligns or time aggregates multiple second usage records so that a more consistent measure of usage with a common time reference can be achieved within the service controller system for one or more of service usage processing, reporting, analysis, comparison, mediation and reconciliation purposes. Service controller **122** stores the second usage records in second source usage records **2350**.

(245) Service controller **122** applies reconciliation and verification processing algorithms **2340** to reconcile records in device usage records **2320** with records in second source usage records **2350** and to validate records in device usage records **2320**. Service controller **122** stores information based on the results of reconciliation and verification processing algorithms **2340** in data warehouse **2330**.

(246) In some embodiments, reconciliation and verification processing algorithms **2340** reconcile detailed classifications of service usage (e.g., micro-CDRs) off of a bulk service usage accounting and onto a micro-CDR classification of service usage accounting. In some embodiments, reconciliation and verification processing algorithms **2340** accomplish charging for a detailed classifications of service usage by providing a detailed micro-CDR charging code identifier in the micro-CDR usage record communicated to the carrier network mediation or billing system. In some embodiments, reconciliation and verification processing algorithms **2340** accomplish charging for a detailed classification of service usage by mediating out (or subtracting) the amount of service usage reported in the micro-CDR from the amount of service usage accounted to bulk service usage. In some embodiments, reconciliation and verification processing algorithms **2340** sends charging data records (e.g., CDRs, micro-CDRs, etc.) to operator data mediation **2380**.

(247) In some embodiments, reconciliation and verification processing algorithms **2340** perform a fraud analysis using information from one or both of second source usage records **2350** and device usage records **2320**. In some embodiments, reconciliation and verification processing algorithms **2340** compares usage records associated with a specific device or user credential from one or both of second source usage records **2350** and device usage records **2320** to determine if service usage is outside of pre-defined service usage policy behavior limits. In some embodiments, reconciliation and verification processing algorithms **2340** compares service usage information associated with a specific device or user credential from one or both of second source usage records **2350** and device usage records **2320** to determine if a pre-defined service usage limit has been reached or exceeded. In some embodiments, reconciliation and verification processing algorithms **2340** compares service

usage information associated with a specific device or user credential from one or both of second usage records **2350** and device usage records **2320** to determine if the specific device or user is exhibiting a service usage behavior that is outside of pre-defined statistical limits as compared to the service usage behavior of a device or user population. In some embodiments, reconciliation and verification processing algorithms **2340** stores the results of its fraud analysis in data warehouse **2330**. In some embodiments, reconciliation and verification processing algorithms **2340** sends fraud alerts to operator CRM system **2390** (e.g., a carrier fraud processing system, carrier personnel, a device user, a system administrator, etc.).

(248) In some embodiments, the second usage records comprise information from multiple other measures or reports. In some embodiments, the second usage records are based on information, measures, or reports from end-user device **100**. In some embodiments, the second usage records are based on information, measures, or reports from other end-user devices. In some embodiments, the second usage records are determined based on information, measures, or reports from one or more network elements (e.g., a base station, the RAN, the core, or using device-assisted means, etc.).

(249) In some embodiments, the second usage records comprise a measure of bulk (e.g., aggregate or unclassified) data usage by end-user device **100**. For example, in some embodiments, the second usage records comprise a bulk usage report, specific to end-user device **100**, generated by the network, by an application service provider, or by a server. In some embodiments, the second usage records are based on information in one or more previous reports sent by end-user device **100**.

(250) In some embodiments, the second usage records comprise information associated with the access network state. In some embodiments, the second usage records are determined from network state tagged information. In some embodiments, the second usage records comprise information from a device data record (DDR), which may indicate the network busy state and the network type. In some embodiments, the second usage records are determined from DDR network state tagged information.

(251) In some embodiments, the second usage records comprise information from flow data record. In some embodiments, the flow data record (FDR) reports a detailed level of service usage classification that indicates service usage broken down by network source or destination (e.g. domain, URL, IP address, etc.) and possibly one or more ports and protocols. In some embodiments, the FDR reports a detailed level of service usage classification that indicates usage broken down by device user application or OS application. In some embodiments, the FDR reports a detailed level of service usage classification that indicates service usage broken down by time of day, network congestion state or service QoS level. In some embodiments, the FDR reports a detailed level of service usage broken down by network type (e.g. 2G, 3G, 4G, WiFi, etc.). In some embodiments, the FDR reports a detailed level of service usage broken down by home or roaming network.

(252) In some embodiments, the FDRs are sourced from a network element capable of classifying traffic (e.g., a deep packet inspection [DPI] gateway, a proxy server, a gateway or server dedicated to a given service classification, a good customer feedback source described elsewhere herein, etc.). In some embodiments, the second usage records are derived from a device service monitor. In some embodiments, the second usage records are derived from a trusted device service monitor. In some embodiments, the trusted device service monitor is located in a secure execution environment on the device that cannot be accessed by a user or user installed application software.

(253) In some embodiments, the second usage records allow service controller **122** to determine whether the access behavior of end-user device **100**, given the network state, indicates that end-user device **100** is implementing the correct policy controls. In some embodiments, service controller **122** confirms that service processor **115** is reporting the correct network state in its data usage reports. In some embodiments, a network element determines the correct network state based on a group of devices. The information is reported to service controller **122** or another suitable network function. Service controller **122** (or other suitable network function) characterizes portions of the

sub-network (e.g., base stations, base station sectors, geographic areas, radio access network (RAN), etc.) based on the population of end-user devices connected to that sub-network portion. The network element can also gather network busy-state measures from network equipment, such as from base stations or by sampling the RAN, to determine the second measure.

(254) In some embodiments, the second usage records provide information about a cap on the aggregate amount of data usage by end-user device **100**. Service controller **122** verifies that the total data usage by end-user device **100**, as reported in the first usage records, does not exceed the cap. If the first usage records provide data usage amounts for individual services used by end-user device **100**, service controller **122** verifies that the sum of the usage amounts for the individual services does not exceed the cap.

(255) In some embodiments, the network classifies FDRs to known service components, determines credits of classified usage for each service component, ensures that the service component usage does not exceed specified limits (or matches end-user device reports for the component), and checks whether the sum of the components matches the bulk measure.

(256) There are several potentially fraudulent circumstances that may be detected by service controller **122** using one or more of the embodiments disclosed herein, such as the example embodiment illustrated in FIG. **24**. In some embodiments, service controller **122** generates a fraud alert if it receives carrier-based usage reports from a network element and UDRs from service processor **115**, but the usage counts contained in the reports are not in agreement within a specified tolerance. In order to generate a fraud alert under these circumstances, in some embodiments service controller **122** accounts for unsent usage reports that may still be on end-user device **100**.

(257) FIG. **25** illustrates an example embodiment that can be advantageous in cases where it is desirable to identify service usage classifications in the network for the purpose of providing a device user or service sponsor with the opportunity to pay for access network service usage that is classified by application or website. FIG. **25** also illustrates exemplary elements that, in some embodiments, provide for generation of micro-CDRs based on a network classification of micro-CDR service usage category. FIG. **25** also illustrates an exemplary means of transmitting the network generated micro-CDRs to carrier network **2666** for billing purposes. In some embodiments, the micro-CDRs generated in the network are used to implement user paid application plans, website plans or content type plans. In some embodiments, the micro-CDRs generated in the network are used to implement sponsored application plans, website plans or content type plans.

(258) The exemplary system illustrated in FIG. **25** operates on the same principles as the exemplary system illustrated in FIG. **23**. Detailed usage reporting for micro-CDR generation is obtained from an FDR source in carrier network **2698** (e.g., the source may be a DPI gateway, proxy server, dedicated service server, good customer feedback, etc.). The FDRs from the FDR source are passed by load balancer **2700** to detailed usage reporting gateway **2702**. In some embodiments, detailed usage reporting gateway **2702** observes FDR time stamps, and time synchronizes, time aligns or time aggregates multiple FDR reports so that a more consistent measure of usage with a common time reference can be achieved within the service controller system for one or more of service usage processing, reporting, analysis, comparison, mediation and reconciliation purposes. The processed FDRs are passed by detailed usage reporting gateway **2702** to JMS queue **2704**, which in turn passes them to detailed report processor **2706**. The other functions in FIG. **25** are similar to those described in the context of FIG. **23**. As would be appreciated by one of ordinary skill in the art, the exemplary embodiment of FIG. **25** provides the advantages of micro-CDR service usage accounting for user-paid application and website services or sponsored application or website services.

(259) In some embodiments, the FDR (flow data record) reports a detailed level of service usage classification that indicates service usage broken down by network source or destination (e.g. domain, URL, IP address, etc.) and possibly one or more ports and protocols. In some

embodiments, the FDR reports a detailed level of service usage classification that indicates usage broken down by device user application or OS application. In some embodiments, the FDR reports a detailed level of service usage classification that indicates service usage broken down by time of day, network congestion state or service QoS level. In some embodiments, the FDR reports a detailed level of service usage broken down by network type (e.g. 2G, 3G, 4G, WiFi, etc.). In some embodiments, the FDR reports a detailed level of service usage broken down by home or roaming network.

(260) In some embodiments, the FDRs are sourced from a network element capable of classifying traffic (e.g., the source is a deep packet inspection [DPI] gateway, a proxy server, a gateway or server dedicated to a given service classification, etc.). In some embodiments, the FDRs are derived from a device service monitor. In some embodiments, the FDRs are derived from a trusted device service monitor. In some embodiments, the trusted device service monitor is located in a secure execution environment on the device that can not be accessed by a user or user installed application software.

(261) In some embodiments, the FDRs not only report service usage that is attempted and allowed by a device, but also service usage that is attempted and not allowed by a device. In some embodiments, an FDR that reports service usage that is attempted but not allowed can include the various classification capabilities described herein. In this manner, an FDR can not only detect bulk service usage or classified service usage for an application, website, network type, etc., but can also detect when a user is attempting to gain access services for bulk services or classified services for an application, website, network type, etc.

(262) In some embodiments, the micro-CDR usage accounting derived from network usage monitoring sources is fed back to a user service usage notification function in a device service processor in order to provide a service usage classification breakdown for user-paid application and website services or sponsored application or website services. This path is indicated in FIG. **25** by the dashed line connection from micro-CDR generator **2680** to device message queue **2688** and the subsequent processing and transmission of a micro-CDR service usage classification update to the device service processor vial notification and offer set gateway **2686**.

(263) In some embodiments, the service processor is configured to display one or more service plan offers to the device end user, and the time at which this display takes place is determined by what the user is doing with the device (e.g., the user attempts to access the network, an application on the device attempts to access the network, a given application or set of applications are used or attempted to be used, the device enters a roaming state, etc.). In some embodiments, the service controller determines the time at which the one or more service offers are to be displayed to the device user by detecting what the user is doing with the device. In some embodiments the service controller detects what the user is doing with the device by observing the access patterns or attempted access patterns in the FDRs or micro-CDRs. In some embodiments, the service controller observes FDRs that report an access service attempt from the device that was denied, and this triggers the service processor to initiate a device notification message that provides a service offer, and the service offer notification is transmitted via the notification and offer set gateway **2686**. In some embodiments, the service controller observes FDRs that report an access service attempt from the device for a classification of service usage such as an application or website that was denied, and this triggers the service processor to initiate a device notification message that provides a service offer for an application service or a website service, and the service offer notification is transmitted via the notification and offer set gateway **2686**.

(264) In some embodiments, the interface protocols for notification and offer set gateway **2686** can be exposed to device OEMs or application developers in the form of an API. In some embodiments, the API for notification and offer set gateway **2686** provides for a uniform means for device application software or OS software developers to write various application software that can utilize a uniform interface for requesting from a service controller a listing of service offers that

are available to a device and displaying the listing to the device user interface. In some embodiments, a list of service offers that are to be made available to a device group or user group is created using a service design center user interface, stored in an SDC database, and published to the API for notification and offer set gateway **2686**. In some embodiments, the service plan enforcement policies for one or more of network access permissions or traffic control, service usage limitations, service usage charging or accounting, or service usage notification can also be configured in service design center **2690**. In some embodiments, the API for notification and offer set gateway **2686** provides for a uniform means for device application software or OS software developers to write various application software that can utilize a uniform interface for providing user service plan choices for service purchase or activation in a device UI, collect the user choice and transmit the user choice to a service controller that then activates the new service for the device. In some embodiments, the available service plan listing or service plan purchase or activation user selection components of the API for notification and offer set gateway **2686** is created with an XML interface. In some embodiments, the available service plan listing or service plan purchase or activation user selection components of the API for notification and offer set gateway **2686** is offered via a secure web connection.

(265) In some embodiments, the interface protocols for notification and offer set gateway **2686** can be exposed to sponsored device providers or sponsored application providers in the form of an API. In some embodiments, the API for notification and offer set gateway **2686** provides for a uniform means for sponsored service providers to develop device application software or OS software that can utilize a uniform interface for requesting from a service controller activation of a sponsored service plan for the device from a service controller. In some embodiments, the sponsored service plan offered and activated through the API is for sponsoring all device access. In some embodiments, the sponsored service plan offered and activated through the API is for sponsoring an application or group of applications. In some embodiments, the sponsored service plan offered and activated through the API is for sponsoring a website or group of websites. In some embodiments, the API for notification and offer set gateway **2686** provides for a uniform means for sponsored device application software or OS software developers to write various application software that can utilize a uniform interface for activating a sponsored service plan for the device, an application or a website.

(266) In some embodiments the interface protocols for notification and offer set gateway **2686** can be exposed to device OEMs or application developers in the form of an API that provides a uniform interface for device application software or OS software to request service usage information updates from a service controller. In some embodiments, the service usage information updates are provided by the service controller in the form of bulk service usage. In some embodiments, the service usage information updates are provided by the service controller in the form of service usage classification or micro-CDR service usage updates. In some embodiments, a device user software application or OS function is configured to utilize a uniform interface for obtaining service usage updates from a service controller, and displaying the service usage updates to a device user interface. In some embodiments the service usage update displayed to the device UI is in the form of a gauge, meter, bar, amount used, amount remaining, percent used or percent remaining. In some embodiments, a device user software application or OS function is configured to utilize a uniform interface for obtaining service usage updates for a classification of service usage (e.g., an application classification or website classification, or another classification) from a service controller, and displaying the service usage updates to a device user interface. In some embodiments, a group of one or more service usage notifications that are to be provided by the API for notification and offer set gateway **2686** to devices that belong to a device group or user group are created using a service design center user interface, stored in SDC database **2692** and published to the API for notification and offer set gateway **2686**. In some embodiments, the service plan notification policies (e.g., the conditions that trigger a given service usage notification and the

information content of the notification) can also be configured in service design center **2692**. In some embodiments, the service usage notification interface component of the API for notification and offer set gateway **2686** is created with an XML interface. In some embodiments, the service usage notification interface component of the API for notification and offer set gateway **2686** is offered via a secure web connection.

(267) In some embodiments, the API for notification and offer set gateway **2686** comprises a secure interface that can only be accessed by providing a device credential corresponding to a known device or user account on the network (e.g. a SIM card credential, an IMSI, a phone number, an MDID, a signed API communication, an encrypted API communication or another form of secure device agent communication with the API). In some embodiments, the API for notification and offer set gateway **2686** comprises a secure interface that can only be accessed by providing a user credential corresponding to a known device or user account on the network (e.g. a user PIN, password, secure question answer, biometric credential or other secure user credential available in general only to a device user or an entity trusted by the device user). In some embodiments, the API for notification and offer set gateway **2686** comprises a secure interface that can only be accessed by providing an application credential (e.g. application certificate, signature, hash information, signed communication, encrypted communication, encrypted message or other application credential that securely identifies an application or OS function) corresponding to a known application that is allowed to access the API for notification and offer set gateway **2686**. In some embodiments, a device software application or OS function must provide a secure device credential, secure application credential or secure user credential in accordance with a proper pre-defined API format to obtain service usage notification information from the API for notification and offer set gateway **2686**. In some embodiments, a device software application or OS function must provide a secure device credential, secure application credential or secure user credential in accordance with a proper pre-defined API format to obtain service offer set information from the API for notification and offer set gateway **2686**. In some embodiments, a device software application or OS function must provide a secure device credential, secure application credential or secure user credential in accordance with a proper pre-defined API format to communicate user service plan selection information to the API for notification and offer set gateway **2686**. In some embodiments, a device software application or OS function must provide a secure device credential, secure application credential or secure user credential to the API for notification and offer set gateway **2686** in order to receive a sponsored service. In some embodiments, the API for notification and offer set gateway **2686** comprises a secured XML interface. In some embodiments, the API for notification and offer set gateway **2686** comprises a secure web connection.

(268) Although the foregoing embodiments have been described in some detail for purposes of clarity of understanding, the invention is not limited to the details provided. There are many alternative ways of implementing the invention. The disclosed embodiments are illustrative and not restrictive.

Claims

1. A wireless network for communication with an end-user wireless device, the wireless network comprising: a memory storing a service offer set including a first service plan and a second service plan, the first service plan providing a first function for the end-user wireless device to communicate using the wireless network and the second service plan providing a second function for the end-user wireless device to communicate using the wireless network, the first function enabling at least one of a first network traffic type or a first application type and a second network traffic type enabling at least one of a second network traffic type or a second application type, the first function being different than the second function; and one or more network elements configured to: obtain the service offer set including the first service plan and the second service

plan from the memory of the wireless network; send, to the end-user wireless device, information associated with the service offer set including the first service plan and the second service plan, the information enabling the end-user wireless device to present, through a user interface of the end-user wireless device, the first service plan and the second service plan; receive an offer set user selection from the end-user wireless device, the offer set user selection indicating a user selection of one of the first service plan or the second service plan; and in response to the offer set user selection, provision the first function enabling the at least one of the first network traffic type or the first application type when the user selection indicates the first service plan, or provision the second function enabling the at least one of the second network traffic type or the second application type when the user selection indicates the second service plan.

2. The wireless network of claim 1, wherein the end-user wireless device is provided with a temporary service lease to allow the end-user wireless device communicate over the wireless network.

3. The wireless network of claim 2, wherein the temporary service lease is revoked after a period of time.

4. The wireless network of claim 3, wherein the one or more network elements are further configured to: provide a notification that the temporary service lease has been revoked.

5. The wireless network of claim 1, wherein the one or more network elements are further configured to: authenticate a secure credential from the end-user wireless device in a verification process verifying a configuration of the end-user wireless device.

6. The wireless network of claim 1, wherein the wireless network is one of a 2G wireless network, a 3G wireless network, a 4G wireless network or a Wi-Fi wireless network.

7. The wireless network of claim 1, wherein the first function is associated with a first service policy and the second function is associated with a second service policy.

8. The wireless network of claim 7, wherein the one or more network elements are further configured to enforce the first service policy when the user selection indicates the first service plan, or enforce the second service policy when the user selection indicates the second service plan.

9. A method for use by a wireless network for communication with an end-user wireless device, the wireless network including a memory storing a service offer set including a first service plan and a second service plan, the first service plan providing a first function for the end-user wireless device to communicate using the wireless network and the second service plan providing a second function for the end-user wireless device to communicate using the wireless network, the first function enabling at least one of a first network traffic type or a first application type and a second network traffic type enabling at least one of a second network traffic type or a second application type, the first function being different than the second function, the method comprising: obtaining the service offer set including the first service plan and the second service plan from the memory of the wireless network; sending, to the end-user wireless device, information associated with the service offer set including the first service plan and the second service plan, the information enabling the end-user wireless device to present, through a user interface of the end-user wireless device, the first service plan and the second service plan; receiving an offer set user selection from the end-user wireless device, the offer set user selection indicating a user selection of one of the first service plan or the second service plan; and in response to the offer set user selection, provisioning the first function enabling the at least one of the first network traffic type or the first application type when the user selection indicates the first service plan, or provisioning the second function enabling the at least one of the second network traffic type or the second application type when the user selection indicates the second service plan.

10. The method of claim 9, wherein the end-user wireless device is provided with a temporary service lease to allow the end-user wireless device communicate over the wireless network.

11. The method of claim 10, wherein the temporary service lease is revoked after a period of time.

12. The method of claim 11, further comprising: providing a notification that the temporary service

lease has been revoked.

13. The method of claim 9, further comprising: authenticating a secure credential from the end-user wireless device in a verification process verifying a configuration of the end-user wireless device.

14. The method of claim 9, wherein the wireless network is one of a 2G wireless network, a 3G wireless network, a 4G wireless network or a Wi-Fi wireless network.

15. The method of claim 9, wherein the first function is associated with a first service policy and the second function is associated with a second service policy.

16. The method of claim 15, further comprising: enforcing the first service policy when the user selection indicates the first service plan, or enforcing the second service policy when the user selection indicates the second service plan.