

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

HEADWATER RESEARCH LLC,

Plaintiff,

v.

SAMSUNG ELECTRONICS CO., LTD. and
SAMSUNG ELECTRONICS AMERICA,
INC.,

Defendants.

Civil Action No. 2:23-cv-00627-JRG-RSP

JURY DEMANDED

**SAMSUNG ELECTRONICS CO., LTD. AND SAMSUNG
ELECTRONICS AMERICA, INC.’S P.R. 3-3 AND 3-4
INVALIDITY AND PATENT INELIGIBILITY CONTENTIONS**

Defendants Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, “Defendants” or “Samsung”) hereby provide the following Preliminary Invalidity Contentions (“Contentions”) to Plaintiff Headwater Research LLC (“Plaintiff” or “Headwater”) for U.S. Patent Nos. 10,028,144 (“the ’144 patent”) and 10,080,250 (“the ’250 patent”) (collectively, the “Asserted Patents”).

I. PRELIMINARY STATEMENT AND RESERVATION OF RIGHTS

In its Infringement Contentions dated November 7, 2024, Headwater asserted the following 20 claims (the “Asserted Claims”):

- Claims 1-18 of the ’144 patent; and
- Claims 1-2 of the ’250 patent.

Samsung notes this is all of the claims of each of the Asserted Patents; however, to the extent Headwater may be permitted to assert additional claims or arguments in the future, Samsung reserves all rights to disclose new or supplemental contentions regarding such claims and arguments.

Because the same claim scope must apply for both infringement and invalidity, these Contentions are based on Headwater's assertions in its Infringement Contentions. Samsung does not thereby implicitly or explicitly agree with Headwater's construction of the claims. Samsung reserves all rights to disclose new or supplemental invalidity contentions, including to address any construction of the claims rendered by the Court, changed theories of infringement, and any evidence obtained during the course of discovery.

Subject to the rights reserved in these Contentions, all Asserted Claims are invalid under at least one or more of 35 U.S.C. §§ 101, 102, 103, and/or 112. The Asserted Claims are invalid because they are anticipated and/or rendered obvious under 35 U.S.C. §§ 102 and 103. If Headwater contends or a fact-finder finds that one or more limitations of the Asserted Claims are not disclosed in the prior art identified as anticipatory, Samsung reserves the right to assert obviousness based on the identified references and/or to identify other references that would have rendered obvious the allegedly missing limitation. Furthermore, the obviousness combinations of references provided below and in the accompanying claim charts under 35 U.S.C. § 103 are exemplary only and are not intended to be exhaustive. If or when Headwater challenges the disclosure of any of these references with respect to particular limitations of the Asserted Claims, Samsung reserves the right to supplement these Contentions to assert additional or different bases for obviousness. Samsung reserves the right to use any combination of the references set forth in these Contentions to demonstrate the obviousness of the Asserted Claims. Additionally, certain claims of the Asserted Patents are invalid for failure to comply with the written description, enablement, and definiteness requirements of 35 U.S.C. § 112. The Asserted Claims are also invalid for lack of patentable subject matter under 35 U.S.C. § 101.

Samsung expressly reserves the right to amend, correct, and/or supplement these Contentions in accordance with the Procedural Schedule governing these cases.

* * *

These Contentions reflect Samsung's knowledge, investigation, and discovery as of the date of service. Samsung reserves the right to supplement these Contentions as appropriate and for any permissible reason. For example, pursuant to the Procedural Schedule, Samsung reserves the right to supplement these Contentions after subsequent case events, including any disclosure by Headwater of amended or supplemental infringement contentions, any ruling by the Court on claim construction, or in response to arguments made and positions taken by Headwater during fact and expert discovery. Samsung also reserves the right to supplement these Contentions if it becomes aware of additional prior art, becomes aware of additional features of the prior art references cited below, or becomes aware of any other relevant information through discovery, including non-party discovery, or otherwise. Samsung also reserves the right to modify or supplement its Contentions based on the Court's construction of the claims.

In addition to the charts attached hereto, Samsung expressly incorporates by reference, as if expressly set forth in these Contentions, all invalidity positions, prior art, and claim charts asserted against Headwater in any Headwater lawsuit or IPR proceeding by Samsung, prior defendants, petitioners, and potential or actual licensees to the Asserted Patents. Samsung also incorporates any future discovery responses and expert reports in such litigations or proceedings.

Samsung's citations to disclosures in any particular prior art reference are not (and are not intended to be) exhaustive but rather illustrative. Samsung reserves the right to rely on uncited portions of the prior art references and on other publications and expert testimony as aids in understanding and interpreting the cited portions, as providing context thereto, as additional

evidence that the prior art discloses a claim limitation or the alleged invention as a whole, as evidence of the state of the art at a particular time, as evidence of the obviousness factor of contemporaneous development by others, and as evidence of motivation to combine. Samsung also reserves the right to rely on uncited portions of the prior art references, other publications, and testimony, including expert testimony, to establish bases for combination of prior art references that render the charted claims obvious. Due to the related nature of the Asserted Patents, Samsung also reserves the right to rely on any cited portions of a prior art reference for one Asserted Patent against all Asserted Patents. Samsung also reserves the right to rely upon any documentary or testimonial evidence of the existence of any systems that embodied or practiced the disclosures found in the accompanying invalidity charts, for example as discussed in the prior art references cited herein, as such systems may qualify as prior art under 35 U.S.C. § 102(g).¹

Samsung intends to rely on admissions concerning the scope of the prior art relevant to the Asserted Patents found in, *inter alia*: the patent prosecution histories for the Asserted Patents and related patents and/or patent applications (including all prior art cited therein); any deposition testimony of the named inventors on the Asserted Patents and related patents and/or patent applications in this matter or any other matter; evidence and testimony relating to the level of skill in the art; and the papers filed and any evidence submitted by Headwater in connection with this matter.

Samsung reserves the right to assert that the Asserted Claims are invalid under 35 U.S.C. § 102(f) in the event Samsung obtains additional evidence that the inventors named in any of the Asserted Patents did not invent the subject matter claimed therein. Should Samsung obtain such

¹ Citations herein refer to the pre-AIA version of Title 35 of the U.S. Code.

evidence, it will provide the name of the person(s) from whom and the circumstances under which the alleged invention or any part of it was derived.

These Contentions are not intended to include or otherwise reflect Samsung's claim interpretations. Because the Court has not yet construed any of the claims in this litigation, Samsung bases these Contentions at least on its present understanding of Headwater's view and application of the claim scope, to the extent that view can be inferred from Headwater's actual and/or apparent application of those claims. But Samsung does not adopt any constructions or interpretations impliedly or expressly in these Contentions. Moreover, Samsung's Contentions may reflect alternative positions as to claim construction and scope.

For the purposes of these Contentions, Samsung has made assumptions regarding possible meanings of indefinite claim terms. By making these assumptions, Samsung does not admit that any claim language satisfies 35 U.S.C. § 112. Similarly, the use of asserted claim terms herein should not be understood to mean that such terms, as used in the Asserted Patents or claims thereof, are definite or otherwise comply with the conditions of patentability under 35 U.S.C. § 112. Likewise, the use of asserted claim terms herein should not be understood to suggest or imply a common, usual, ordinary, customary, plain, or accepted meaning in the art for any such terms.

By providing these Contentions, Samsung is not waiving nor limiting its rights to make arguments in the future about the proper scope of the claims or to advance alternative constructions to those Headwater advocates. Samsung expressly reserves the right to argue for such alternative claim constructions during this litigation and to supplement these Contentions after the Court has issued a claim construction ruling.

Samsung's factual investigations, including its investigation of prior art and grounds for invalidity, is ongoing. Further, Samsung's invalidity positions will be the subject of expert

testimony. Samsung reserves the right to supplement these Contentions, including, without limitation, adding additional prior art and grounds of invalidity in accordance with the Federal Rules of Civil Procedure and Procedural Schedule in these cases, or otherwise.

II. PERSON HAVING ORDINARY SKILL IN THE ART

A person of ordinary skill in the art (“POSITA” or “POSA”), as of the priority date of the asserted patents, would have had at least a Bachelor’s degree in Electrical Engineering, Computer Engineering, Computer Science, or equivalent, and at least 2-5 years of industry experience in networking security, mobile device communications security, and/or wireless digital communications systems security. Additional education might compensate for less experience, and vice versa.

III. IDENTIFICATION OF RELEVANT PRIOR ART

A. Priority Dates

Headwater’s Infringement Contentions appear to allege that the ’144 patent claims priority to Provisional Application No. 61/206,354 (the “’354 application”), filed on January 28, 2009, and that the ’250 patent claims priority to Application No. 13/248,028 (the “’028 application”), filed on September 28, 2011.² Headwater has not met its burden of establishing that the claims of the Asserted Patents are entitled to these priority dates. *See In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1376 (Fed. Cir. 2016) (A “patentee bears the burden of establishing that its claimed invention is entitled to an earlier priority date.”).

² While Headwater’s Infringement Contentions do not specifically identify the applications to which the Asserted Patents allegedly claim priority, Headwater’s Infringement Contentions assert that the Asserted Patents are entitled to priority dates coinciding with the above-listed applications cited on the face of the Asserted Patents. *See* Headwater’s P.R. 3-1(e) disclosures. To the extent that Headwater later asserts it is relying on a different application for priority, Samsung expressly reserves the right to modify these Contentions accordingly.

For a patent to claim priority back to the filing date of a particular patent application, all the limitations must appear in the specification of the application to which priority is claimed. However, as to the '144 patent, the '354 application's specification clearly fails to disclose at least the following asserted claim limitations, including but not limited to those limitations reciting "kernel execution partition," "application execution partition," "protected execution partition," "operating system packet network stack," "application identification agent," "particular individual flow," "service measurement agent," "classified individual flows," "application-specific traffic policy controls," "device agents with limited privileges," "privilege to configure the application-specific traffic policy controls of the policy control agent," "privilege to receive at least one of Internet data packet traffic passing between the operating system packet network stack and the WWAN modem," "device-assisted services partition," "device service state information," "a service control link configured to securely communicate with a network service controller," "service control link . . . further configured to receive at least one of the application-specific traffic policy controls from the network service controller," "service control link . . . further configured to transmit at least some of the device service state information to the network service controller," "secure virtual execution environment," "exclusive privilege," "modem control link," and "user-interface agent."

As to the '250 patent, the '028 application's specification clearly fails to disclose at least the following asserted claim limitations, including but not limited to those limitations reciting "secure policy information," "application-specific execution environment policy," "configurable communication security policy," "secure stored information," "first set of multiple device application instances," "first secure application environment," "second set of device application instances," "outside of the first secure application environment," "first secure tunnel," "network

tunnel endpoint,” “network data communications to and from device application instances,” “first configuration,” and “network path outside of the first secure tunnel.” Thus, each alleged priority application fails to disclose any claims depending therefrom:

1. '144 patent

- **Claims 1-18:** “kernel execution partition”
- **Claims 1-18:** “application execution partition”
- **Claims 1-18:** “protected execution partition”
- **Claims 1-18:** “an operating system packet network stack to pass Internet data packet traffic between the WWAN modem and one or more applications executing in the application execution partition”
- **Claims 1-18:** “an application identification agent to classify individual flows of the Internet data packet traffic passing through the stack according to which of the one or more applications is associated with a particular individual flow”
- **Claims 1-18:** “a service measurement agent to measure, for classified individual flows, an amount of the Internet data packet traffic associated with each of the one or more applications”
- **Claims 1-18:** “a policy control agent to apply application-specific traffic policy controls to classified individual flows”
- **Claims 1-18:** “device agents with limited privileges to access processes executing in the kernel execution partition”
- **Claims 1-18:** “privilege to configure application-specific traffic policy controls of the policy control agent”
- **Claims 1-18:** “privilege to receive at least one of internet data packet traffic passing between the operating system packet network stack and the WWAN modem”
- **Claims 1-18:** “traffic information including the measured amount of the Internet data packet traffic associated with each of the one or more applications.”
- **Claims 2, 18:** “device-assisted-services agent to communicate with at least one device agent executed in the protected execution partition”
- **Claims 3, 4, 6-10:** “one or more memory partitions to store program code for the respective processes of the operating system packet network stack, the application identification

agent, the service measurement agent, the policy control agent, and the one or more device agents”

- **Claims 3, 4, 6-10:** “one or more processors configured to retrieve the stored program code from the one or more memory partitions to execute the respective processes”
- **Claims 4-5:** “separately protected device-assisted services partition to store the program code for the one or more device agents”
- **Claims 4-5:** “access control integrity agent having exclusive permission to update program code stored in the separately protected device-assisted services partition”
- **Claim 5:** “access control integrity agent further configured to validate the program code for the one or more device agents”
- **Claims 6-10:** “a device-assisted services partition to store device service state information”
- **Claims 6-10:** “device service state information only modifiable by the one or more device agents”
- **Claims 7-10:** “one or more device agents further comprising a service control link configured to securely communicate with a network service controller”
- **Claims 8-10:** “service control link is further configured to receive at least one of the application-specific traffic policy controls from the network service controller”
- **Claims 9-10:** “the service control link is further configured to transmit at least some of the device service state information to the network service controller”
- **Claim 10:** “one or more device agents are further configured to retain the transmitted device service state information until after an instruction is received from the network service controller acknowledging that the device service state information can be deleted”
- **Claim 11:** “one or more device agents further configured to, based on the application-specific traffic policy controls, configure application settings for the one or more applications”
- **Claim 12:** “one or more device agents further configured to calculate, separate from the traffic information, a service usage measurement for the Internet data packet traffic passing between the operating system packet network stack and the WWAN modem”
- **Claim 13:** “one or more device agents further configured to encrypt Internet data packet traffic passing from the operating system packet network stack to the WWAN modem”
- **Claim 14:** “the protected execution partition comprises a secure virtual execution environment”

- **Claim 15:** “the privilege to configure the application-specific traffic policy controls of the policy control agent is an exclusive privilege for one or more of the device agents executed in the protected execution partition”
- **Claims 16-17:** “the WWAN modem comprising a modem execution partition configured to calculate, separate from the traffic information, a service usage measurement for the Internet data packet traffic passing between the operating system packet network stack and the WWAN modem”
- **Claim 17:** “the modem execution partition further comprising a modem control link to communicate the calculated service usage measure to at least one of a network service controller and at least one device agent executed in the protected execution partition”
- **Claim 18:** “a user interface”
- **Claim 18:** “at least one device-assisted-services agent comprising a user-interface agent to display to a user, and allow modification to, at least one policy setting affecting at least one of the application-specific policy controls”

2. '250 patent

- **Claim 1:** “secure policy information”
- **Claim 1:** “application-specific execution environment policy”
- **Claims 1-2:** “configurable communication security policy”
- **Claims 1-2:** “secure stored information”
- **Claim 1:** “first set of multiple device application instances”
- **Claims 1-2:** “first secure application environment”
- **Claims 1-2:** “second set of device application instances”
- **Claims 1-2:** “outside of the first secure application environment”
- **Claims 1-2:** “first secure tunnel”
- **Claim 1:** “network tunnel endpoint”
- **Claims 1-2:** “network data communications to and from device application instances”
- **Claim 2:** “first configuration, which indicates that application instances in the second set of device application instances are not allowed to use the first secure tunnel”

- **Claim 2:** “network path outside of the first secure tunnel”

Thus, the Asserted Claims cannot claim priority to January 28, 2009 and September 28, 2011, respectively. Nevertheless, even under Headwater’s incorrect priority dates, the Asserted Patents are invalid.

To the extent it is later argued by Headwater, or otherwise determined that a different priority date applies, Samsung reserves the right to amend these Contentions accordingly.

B. Prior Art Patent Publications

Based on their investigation to date, Samsung has provided in the list below the prior art patent publications presently known to Samsung that it contends anticipate and/or render obvious the Asserted Claims. The prior art identified in these Contentions discloses (*i.e.*, anticipates and/or renders obvious) the elements of the Asserted Claims either explicitly or inherently. Similarly, the prior art patent publications listed on the face of the Asserted Patents discloses (*i.e.*, anticipates and/or renders obvious) the elements of the Asserted Claims either explicitly or inherently, and Samsung reserves the right to rely on any such reference.

Prior-art patents or publications included in these Contentions may be related (such as a divisional, continuation, continuation-in-part, parent, or child) to earlier or later-filed patents or publications, may have counterparts filed in other jurisdictions, or may incorporate (or be incorporated by) other patents or publications by reference. The listed patents or publications are intended to be representative of these other patents or publications to the extent they exist. Samsung accordingly reserves the right to modify, amend, or supplement these Contentions with these related patents or publications, as well as other prior art references, upon further investigation. Additionally, any reference in these Contentions, including the appendices and exhibits thereto, to a specific subsection or subsections of 35 U.S.C. § 102, is merely exemplary, and Samsung

expressly reserves the right to rely on additional or other sections of 35 U.S.C. § 102, as appropriate. If Headwater asserts that one or more of these references or systems fails to disclose one or more elements of a claim, Samsung reserves the right to also use those references to invalidate the claim under 35 U.S.C. § 103.

Discovery is ongoing, and Samsung's prior art investigation and third-party discovery is therefore not yet complete. Samsung reserves the right to present additional items of prior art under 35 U.S.C. §§ 102 and/or 103 that are located during the course of discovery or further investigation. For example, Samsung expects to receive documents from additional third parties either through informal requests or under subpoenas that are believed to have knowledge, documentation, and/or corroborating evidence concerning some of the prior art listed and discussed below. These third parties include without limitation the authors, inventors, or assignees of the references listed in these disclosures.

Patent Publication	Publication/Issue Date
U.S. Patent Application Pub. No. 2004/0267897 ("Hill")	December 30, 2004
U.S. Patent Application Pub. No. 2005/0273850 ("Freund")	December 8, 2005
U.S. Patent Application Pub. No. 2003/0204596 ("Yadav")	October 30, 2003
U.S. Patent No. 8,549,173 ("Wu")	October 1, 2013
U.S. Patent Application Pub. No. 2008/0183996 ("Field")	July 31, 2008
International Pub. No. WO 2009/112044 ("Malomsoky")	September 17, 2009
International Pub. No. WO 2007/023467 ("Tonsing '467")	March 1, 2007

International Pub. No. WO 2007/118638 (“Oester”)	October 25, 2007
U.S. Patent Application Pub. No. 2006/0136679 (“O’Connor”)	December 21, 2004
U.S. Patent Application Pub. No. 2009/0282474 (“Chen ’474”)	May 8, 2008
Japanese Patent Application Pub. No. JP 2007-081950 (“Tokitaka”)	March 29, 2007
U.S. Patent Application Pub. No. 2010/0146582 (“Jaber”)	June 10, 2010
U.S. Patent Application Pub. No. 2008/0155092 (“Kumar”)	June 26, 2008
U.S. Patent Application Pub. No. 2007/0006282 (“Durham”)	January 4, 2007
U.S. Patent Application Pub. No. 2005/0004879 (“Mathias”)	January 6, 2005
U.S. Patent Application Pub. No. 2007/0256127 (“Kraemer”)	November 1, 2007
U.S. Patent Application Pub. No. 2007/0195742 (“Erdman”)	August 23, 2007
U.S. Patent Application Pub. No. 2009/0249330 (“Abercrombie”)	October 1, 2009
U.S. Patent Application Pub. No. 2007/0190977 (“Fok”)	August 16, 2007
U.S. Patent Application Pub. No. 2009/0204723 (“Tonsing ’723”)	August 13, 2009
U.S. Patent Application Pub. No. 2005/0288056 (“Bajikar ’056”)	December 29, 2005
KR 10-0501210 (“Kim ’210”)	July 18, 2005
CN 1423460A (“He”)	June 11, 2003

U.S. Patent No. 7,240,240 ("Balakrishnan")	July 3, 2007
U.S. Patent No. 7,669,242 ("Sahita")	February 23, 2010
U.S. Patent Application Pub. No. 2008/0163370 ("Maynard")	July 3, 2008
U.S. Patent Application Pub. No. 2004/0255162 ("Kim '162")	December 16, 2004
U.S. Patent No. 8,261,320 ("Serenyi")	September 4, 2012
U.S. Patent No. 7,290,028 ("Brabson")	October 30, 2007
U.S. Patent No. 7,168,078 ("Bar")	January 23, 2007
U.S. Patent No. 6,185,568 ("Douceur '568")	February 6, 2001
U.S. Patent No. 6,041,053 ("Douceur '053")	March 21, 2000
U.S. Patent No. 6,463,470 ("Mohaban")	October 8, 2002
U.S. Patent Application Pub. No. 2009/0013407 ("Doctor")	January 8, 2009
U.S. Patent Application Pub. No. 2008/0244725 ("Dewan")	October 2, 2008
U.S. Patent Application Pub. No. 2002/0138643 ("Shin")	September 26, 2002
U.S. Patent Application Pub. No. 2009/0037594 ("Sever")	February 5, 2009
U.S. Patent Application Pub. No. 2008/0134330 ("Kapoor")	June 5, 2008
U.S. Patent Application Pub. No. 2008/0034418 ("Venkatraman")	February 7, 2008
U.S. Patent Application Pub. No. 2008/0225748 ("Khemani")	September 18, 2008

KR 10-0614775 (“Seo”)	August 22, 2006
U.S. Patent Application Pub. No. 2007/0041323 (“Kitahara”)	February 22, 2007
U.S. Patent Application Pub. No. 2005/0108534 (“Bajikar ’534”)	May 19, 2005
U.S. Patent Application Pub. No. 2008/0046965 (“Wright ’965”)	February 21, 2008
U.S. Patent No. 8,107,973 (“Sjothun”)	January 31, 2012
U.S. Patent No. 8,108,933 (“Mahaffey ’933”)	January 31, 2012
U.S. Patent No. 8,505,095 (“Mahaffey ’095”)	August 6, 2013
U.S. Patent No. 9,367,680 (“Mahaffey ’680”)	June 14, 2016
U.S. Patent Application Pub. No. 2007/0006294 (“Hunter”)	January 4, 2007
U.S. Patent No. 9,043,919 (“Wyatt”)	May 26, 2015
International Pub. No. WO 2007/112641 (“Zhang”)	October 11, 2007
Australian Patent Application No. 2008323922 (“Alperovitch”)	October 3, 2013
U.S. Patent Application Pub. No. 2006/0039354 (“Rao”)	February 23, 2006
U.S. Patent Application Pub. No. 2007/0006289 (“Limont”)	January 4, 2007
U.S. Patent Application Pub. No. 2004/0123153 (“Wright ’153”)	June 24, 2004
U.S. Patent Application Pub. No. 2006/0183461 (“Pearce”)	August 17, 2006

U.S. Patent Application Pub. No. 2007/0288989 (“Aarnos”)	December 13, 2007
U.S. Patent Application Pub. No. 2007/0104169 (“Polson”)	May 10, 2007
U.S. Patent Application Pub. No. 2012/0117478 (“Vadde”)	May 10, 2012
U.S. Patent No. 6,578,077 (“Rakoshitz”)	June 10, 2003
International Pub. No. WO 2004/107672 (“Kelz”)	December 9, 2004
U.S. Patent Application Pub. No. 2005/0213763 (“Owen”)	September 29, 2005
U.S. Patent Application Pub. No. 2009/0063869 (“Kohavi”)	January 17, 2007
U.S. Patent Application Pub. No. 2008/0235756 (“Cohen 756”)	June 28, 2007
U.S. Patent Application Pub. No. 2009/0204964 (“Foley 964”)	October 14, 2008
U.S. Patent No. 7,246,374 (“Simon”)	July 17, 2007
U.S. Patent Application Pub. No. 2008/0040470 (“Bogner”)	February 14, 2008
U.S. Patent Application Pub. No. 2007/0294690 (“Taillefer”)	December 20, 2007
U.S. Patent Application Pub. No. 2006/0143700 (“Herrmann”)	June 29, 2006
U.S. Patent Application Pub. No. 2007/0277240 (“Durfee”)	November 29, 2007
U.S. Patent Application Pub. No. 2003/0177389 (“Albert”)	September 18, 2003
U.S. Patent Application Pub. No. 2007/0204166 (“Tome”)	August 30, 2007

U.S. Patent No. 7,257,815 (“Gbadegesin”)	August 14, 2007
U.S. Patent No. 6,477,648 (“Schell”)	November 5, 2002
U.S. Patent Application Pub. No. 2007/0217409 (“Mann”)	September 20, 2007
U.S. Patent Application Pub. No. 2008/0194296 (“Roundtree”)	August 14, 2008
U.S. Patent Application Pub. No. 2008/0276299 (“Lee”)	November 6, 2008
U.S. Patent Application Pub. No. 2007/0234035 (“Hall”)	October 4, 2007
U.S. Patent Application Pub. No. 2008/0022094 (“Gupta”)	January 24, 2008
U.S. Patent Application Pub. No. 2004/0123153 (“Wright”)	June 24, 2004
U.S. Patent Application Pub. No. 2007/0005919 (“van Riel”)	January 4, 2007
U.S. Patent Application Pub. No. 2007/0157025 (“Sastry”)	July 5, 2007
U.S. Patent Application Pub. No. 2008/0127355 (“Lorch”)	May 29, 2008
EP 1812844A1 (“Edwards”)	August 1, 2007
U.S. Patent Application Pub. No. 2006/0041761 (“Neumann”)	February 23, 2006
U.S. Patent Application Pub. No. 2002/0194496 (“Griffin”)	December 19, 2002
U.S. Patent Application Pub. No. 2004/0230794 (“England”)	November 18, 2004
U.S. Patent Application Pub. No. 2004/0003262 (“England ‘262”)	January 1, 2004

U.S. Patent Application Pub. No. 2005/0114683 (“Jin”)	May 26, 2005
U.S. Patent Application Pub. No. 2005/0033980 (“Willman”)	February 10, 2005
U.S. Patent Application Pub. No. 2004/0025016 (“Focke”)	February 5, 2004
U.S. Patent No. 6,772,416 (“White”)	August 3, 2004
U.S. Patent Application Pub. No. 2006/0026677 (“Edery”)	February 2, 2006
U.S. Patent No. 5,398,196 (“Chambers”)	March 14, 1995
U.S. Patent Application Pub. No. 2004/0187023 (“Alagna”)	September 23, 2004
U.S. Patent Application Pub. No. 2002/0178375 (“Whittaker”)	November 28, 2002
U.S. Patent Application Pub. No. 2006/0053426 (“Dive-Reclus”)	March 9, 2006
U.S. Patent Application Pub. No. 2006/0149968 (“Edery ’968”)	July 6, 2006
U.S. Patent Application Pub. No. 2008/0235001 (“Cohen”)	September 25, 2008
U.S. Patent Application Pub. No. 2006/0095971 (“Costea”)	May 4, 2006
U.S. Patent Application Pub. No. 2006/0161982 (“Chari”)	July 20, 2006
U.S. Patent Application Pub. No. 2007/0101435 (“Konanka”)	May 3, 2007
U.S. Patent Application Pub. No. 2006/0230452 (“Field”)	October 12, 2006
International Pub. No. WO 2008/055156 (“Keromytis”)	May 8, 2008

International Pub. No. WO 2008/069945 (“Hubbard”)	June 12, 2008
U.S. Patent Application Pub. No. 2009/0222907 (“Guichard”)	September 3, 2009
U.S. Patent Application Pub. No. 2007/0094725 (“Borders”)	April 26, 2007
International Pub. No. WO 2007/050667 (“Stolfo”)	May 3, 2007
U.S. Patent No. 5,615,263 (“Takahashi”)	March 25, 1997
U.S. Patent Application Pub. No. 2010/0031325 (“Maigne”)	February 4, 2010
U.S. Patent Application Pub. No. 2011/0003580 (“Belrose”)	January 6, 2011
U.S. Patent Application Pub. No. 2009/0292893 (“Henry”)	November 26, 2009
U.S. Patent Application Pub. No. 2010/0195833 (“Priestly”)	August 5, 2010
U.S. Patent Application Pub. No. 2002/0099952 (“Lambert”)	July 25, 2002
U.S. Patent Application Pub. No. 2009/0282474 (“Chen”)	November 12, 2009
U.S. Patent Application Pub. No. 2005/0076209 (“Proudlar”)	April 7, 2005
U.S. Patent Application Pub. No. 2002/0180778 (“Proudlar ‘778”)	December 5, 2002
U.S. Patent Application Pub. No. 2009/0307781 (“Iga”)	December 10, 2009
U.S. Patent No. 8,095,786 (“Kshirsagar”)	January 10, 2012

C. **Prior Art Non-Patent Publications**^{3,4}

Non-Patent Publication	Publication Date
Tzu-Chi Huang, et al., <i>Dual-Mode Execution Environment for Active Network</i> , Journal of Systems Architecture (2009)	2009
Tarek S. Sobh, <i>AFKS: A Kernel-Mode Firewall System</i> , Fourth International Conference on Informatics and Systems (2006)	2006
D.R. Engler, et al., <i>Exokernel: An Operating System Architecture for Application-Level Resource Management</i> , ACM SIGOPS Operating Systems Review (1995)	1995
Stephen Chong, et al., <i>Secure Web Applications via Automatic Partitioning</i> , Proceedings of Twenty-First ACM SIGOPS Symposium on Operating Systems Principles (2007)	2007
Geon-Woo Kim & Wook-Jong Han, <i>Security Flow Control by Dynamic Stack Allocation</i> , 6th International Conference on Advanced Communication Technology (2004)	2004
Reiner Sailer, et al., <i>Attestation-Based Policy Enforcement for Remote Access</i> , Proceedings of the 11th ACM Conference on Computer and Communications Security (2004)	2004
M. Archer, et al., <i>Specification and Verification of Secure Concurrent and Distributed Software Systems</i> (1992)	1992
Chris Taylor, <i>Operating System Security: Microsoft Palladium</i> (2003)	2003
Yacine Gasmi, et al., <i>Flexible and Secure Enterprise Rights Management Based on Trusted Virtual Domains</i> , Proceedings of the 3rd ACM Workshop on Scalable Trusted Computing (2008)	2008

³ Any discussion of a non-patent publication in either Section III.C or in one of the claim charts included herewith that discloses a corresponding product or system shall also apply with equal force to the underlying product or system. In other words, both the non-patent publication and the underlying product or system themselves qualify as prior art in the context that they are used herein.

⁴ Discovery is currently ongoing, and Samsung will supplement these Contentions with respect to the public availability, as necessary, of any non-patent publication if and when more information becomes available. Indeed, Samsung expects to receive documents from third parties either through informal requests or under subpoenas that are believed to have knowledge, documentation, and/or corroborating evidence concerning the public availability of the identified non-patent publications.

D. Balfanz & Daniel R. Simon, <i>WindowBox: A Simple Security Model for the Connected Desktop</i> (2000)	2000
Tal Garfinkel, et al., <i>Terra: A Virtual Machine-Based Platform for Trusted Computing</i> , ACM SIGOPS Operating Systems Review (2003)	2003
Sectéra Edge™ Secure Mobile Environment Portable Electronic Device, General Dynamics (2007)	2007
Paul England & John Manferdelli, <i>Virtual Machines for Enterprise Desktop Security</i> , 11 Information Security Tech. Rpt. 193 (2006)	2006
Peter C. S. Kean & Glen Durfee, <i>Practical Uses of Virtual Machines for Protection of Sensitive User Data</i> , Proc. of the 3 rd Int'l Conference on Information Security Practice & Experience 145 (2007)	2007
Bruno Blanchard, et al., <i>Introduction to Workload Partition Management in IMB AIX Version 6.1</i> (2007)	2007
IATAC, <i>Generating Policies for Defense in Depth (DiD)</i> , Vol. 9 No. 3 IAnewsletter (2006)	2006
D. Kuhlmann, et al., <i>An Open Trusted Computing Architecture – Secure Virtual Machines Enabling User-Defined Policy Enforcement</i> (2006)	2006
Amy Carroll, et al., <i>Microsoft Palladium: A Business Overview</i> (2002)	2002
Glenn Durfee, et al., <i>Posture-Based Data Protection</i> (2006)	2006
Jerome Azema & Gilles Fayad, <i>M-Shield™ Mobile Security Technology: Making Wireless Secure</i> (2008)	2008

Global Platform, <i>Why the Mobile Industry is Evolving Toward Security</i> (2007)	2007
VMware White Paper, <i>Understanding Full Virtualization, Paravirtualization, and Hardware Assist</i> (2007)	2007
Rich Uhlig, et al., <i>Intel Virtualization Technology</i> (2005)	2005
R. J. Creasy, <i>The Origin of the VM/370 Time-Sharing System</i> (1981)	1981
Microsoft Software License Terms, <i>Windows Vista Home Basic, Windows Vista Home Premium, Windows Vista Ultimate</i> (2007)	2007
Android Developers, <i>Android 2.3 Platform Highlights</i> , 2010, downloaded from the internet at Android 2.3 Platform Highlights Android Developers (vanderbilt.edu) on July 17, 2024.	2010
Android Developers, <i>Android 2.3 Platform</i> , 2010, downloaded from the internet at Android 2.3 Platform Android Developers (vanderbilt.edu) on July 17, 2024.	2010
BlackBerry Pearl 9105 Smartphone – 5.0 User Guide	2010
BlackBerry Bold 9000 Smartphone – 4.6 User Guide	2008
BlackBerry Bold 9000 Smartphone – 5.0 User Guide	2009
BlackBerry Bold 9700 Smartphone – 5.0 User Guide	2009
BlackBerry Storm 2 9520/9550 Smartphones – 5.0 User Guide	2010
BlackBerry Curve 9330 Smartphone – 5.0 User Guide	2010
BlackBerry Torch 9800 Smartphone – 6.0 User Guide	2010
BlackBerry Bold 9000 Press Release, May 12, 2008, downloaded from the internet at https://web.archive.org/web/20080517012537/http://press.rim.com/release.jsp?id=1562 on July 16, 2024	2008

Blake, et al., <i>An Architecture for Differentiated Services</i> , IETF RFC 2475 (1998), downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc2475 on July 29, 2023	1998
Buiati, et al., <i>A Secure Autoconfiguration Protocol for MANET Nodes</i> , Int'l Conference on Ad-Hoc Networks & Wireless 108-121 (2004)	July 2004
Damianou, et al., <i>The Ponder Policy Specification Language</i> , Policies for Distributed Sys. and Networks: International Workshop 18-38 (2001)	2001
Steve Babin, <i>Developing Software for Symbian OS</i> (2006)	2006
Andrew Tanenbaum, <i>Computer Networks</i> (4th ed. 2003)	2003
Lev Grossman, <i>Invention of the year: The iPhone</i> , Time Magazine Online (Nov. 1, 2007), downloaded from the internet at https://content.time.com/time/specials/2007/article/0,28804,1677329_1678542_1677891,00.html on May 28, 2024.	2007
<i>Apple iPhone</i> , GSM Arena, downloaded from the internet at https://www.gsmarena.com/apple_iphone-1827.php on July 16, 2024.	2024
Apple iPhone 3G, GSM Arena, downloaded from the internet at https://www.gsmarena.com/apple_iphone_3g-2424.php on January 13, 2025.	2025
Apple iPhone 3GS, GSM Arena, downloaded from the internet at https://www.gsmarena.com/apple_iphone_3gs-2826.php on January 13, 2025.	2025
Apple iPhone 4, GSM Arena downloaded from the internet at https://www.gsmarena.com/apple_iphone_4-3275.php on January 13, 2025.	2025
BlackBerry Bold 9000, GSM Arena, downloaded from the internet at https://www.gsmarena.com/blackberry_bold_9000-2370.php on January 13, 2025.	2025
BlackBerry Bold 9700, GSM Arena, downloaded from the internet at https://www.gsmarena.com/blackberry_bold_9700-2963.php on January 13, 2025.	2025

BlackBerry Bold 9780, GSM Arena, downloaded from the internet at https://www.gsmarena.com/blackberry_bold_9780-3431.php on January 13, 2025.	2025
BlackBerry Storm2 9550, GSM Arena, downloaded from the internet at https://www.gsmarena.com/blackberry_storm2_9550-2970.php on January 13, 2025.	2025
BlackBerry Curve 3G 9330, GSM Arena, downloaded from the internet at https://www.gsmarena.com/blackberry_curve_3g_9330-3591.php on January 13, 2025.	2025
BlackBerry Torch 9800, GSM Arena, downloaded from the internet at https://www.gsmarena.com/blackberry_torch_9800-3203.php on January 13, 2025.	2025
Samsung Google Nexus S, GSM Arena, downloaded from the internet at https://www.gsmarena.com/samsung_google_nexus_s-3620.php on January 13, 2025.	2025
Google Android OS 2.3 Gingerbread User's Guide	2011
Hiertz, et. al., <i>The IEEE 802.11 Universe</i> , IEEE Communications Magazine 48(1), 62-70 (2010)	2010
IETF RFC 5246, The Transport Layer Security (TLS) Protocol, version 1.2, August 2008, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc5246 on May 9, 2024	2008
Internet Traffic Manager	Aug. 11, 2009
iPhone User Guide For iPhone OS 3.1 Software	2009
iPod Touch User Guide For iOS 4.1 Software	2011
iPhone User Guide For iOS 4.2 and 4.3 Software	2011
Liao, S.H., 2005. Expert system methodologies and applications—a decade review from 1995 to 2004. Expert systems with applications, 28(1), pp. 93-103 (“Liao”)	2005
Lobo, et. al., (1999). A policy description language. AAAI/IAAI, 1999, 291-298 (“Lobo”)	1999

Klug, Brian, Nexus S and Android 2.3 Review: Gingerbread for the Holidays, AnandTech, December 14, 2010, downloaded from the internet at https://www.anandtech.com/show/4059/nexus-s-and-android-23-review-gingerbread-for-the-holidays/3 on July 17, 2024.	2010
Mansour, et al., 2001. Jitter control in QoS networks. IEEE/ACM Transactions On Networking, 9(4), pp.492-502.	2001
Meier, Reto, (2009). Professional Android Application Development	2009
Nexus One User's Guide	Mar. 15, 2010
Nexus S User's Guide	2011
T-Mobile G1 User Guide	Sept. 8, 2008
Samsung Galaxy User Manual	July 2009
(SIM-SPL) Simplified Policy Language. Document Number DSP0231, version, 1 ("CIM-SPL")	2009
Stone, G.N., Lundy, B. and Xie, G.G., 2001. Network policy languages: a survey and a new approach, IEEE network, 15(1), pp.10-21 ("Stone")	2001
Ben Morris, <i>The Symbian OS Architecture Sourcebook: Design and Evolution of a Mobile Phone OS</i> (2007)	2007
Ross Anderson, <i>Security Engineering</i> (2d ed. 2008)	2008
IETF RFC 793, <i>Transmission Control Protocol</i> (1981), available at https://www.ietf.org/rfc/rfc793.txt	September 1981
<i>The TLS Protocol Version, v. 1.0</i> (1999), available at https://datatracker.ietf.org/doc/html/rfc2246	January 1999
<i>The Transport Layer Security ("TLS") Protocol, v. 1.1</i> (2006), available at https://www.ietf.org/rfc/rfc4346.txt	April 2006
Michael D. Schroeder et al., <i>A Hardware Architecture for Implementing Protection Rings</i> , 15 Ass'n of Comput. Mach. 157-70 (1972)	March 1972

Jerome H. Saltzer et al., <i>The Protection of Information in Computer Systems</i> (1975), available at https://www.cs.virginia.edu/~evans/cs551/saltzer/ (also published in IEEE Proceedings, Vol. 63, No. 9, Sept. 1975)	1975
Bo Li et al., <i>Symbian OS Platform Security Model</i> (2010), available at https://www.usenix.org/system/files/login/articles/73507-li.pdf	2010
<i>The SSL Protocol, v. 3.0, Internet Draft</i> (1996), available at https://web.archive.org/web/19970614041044/http://home.netscape.com/eng/ssl3/ssl-toc.html and https://web.archive.org/web/19970617034012/http://home.netscape.com/eng/ssl3/3-SPEC.HTM#1	March 1996
Peter James, <i>Secure Portable Execution Environments: A Review of Available Technologies</i> (2008)	January 2008
Malcom Taylor et. al., <i>Extended Abstract: A Hardware-Assisted Data Hiding Based Approach in Building High Performance Secure Execution Systems</i> , 2008 IEEE Int'l Workshop on Hardware-Oriented Security & Trust (HOST) 93-96 (2008)	2008
<i>Security and Permissions in Android</i> , Android (2007), archived at https://web.archive.org/web/20071130085113/http://code.google.com/android/devel/security.html#manifest	2007
<i>Android Building Blocks</i> , Android (2007), archived at https://web.archive.org/web/20071205131148/http://code.google.com/android/devel/building-blocks.html	2007
<i>Accessing Content Providers</i> , Android (2007), archived at https://web.archive.org/web/20071126171746/http://code.google.com/android/devel/data/contentproviders.html	2007
<i>android.app.NotificationManager</i> , Android (2007), archived at https://web.archive.org/web/20071215121116/http://code.google.com/android/reference/android/app/NotificationManager.html	2007
Nazmul Idris, <i>Android Activity and Sub-activity Tutorial</i> , Developer Life (July 15, 2008), https://developerlife.com/2008/07/15/android-app-lifecycleactivity-intent-and-service-draft/	July 2008

<i>T-Mobile Unveils the T-Mobile G1 — the First Phone Powered by Android</i> , T-Mobile (Sept. 22, 2008), https://www.tmobile.com/news/press/t-mobile-unveils-the-t-mobile-g1-the-first-phone-powered-by	September 2008
<i>T-Mobile G1 Unveiled</i> , CNET (Sept. 23, 2008), https://www.cnet.com/pictures/photos-t-mobile-g1-unveiled/	September 2008
Tom Spring, <i>In Pictures: 15 Killer Android Apps for the G1</i> , PCWorld (Oct. 17, 2008), https://www.pcworld.com/article/537123/android_apps-3.html , archived at https://web.archive.org/web/20081020041608/http://www.pcworld.com/article/152384-11/in_pictures_15_killer_android_apps_for_the_g1.html	October 2008
Marisa Taylor, <i>The Best Android Apps of 2009</i> , Wall Street Journal (Dec. 22, 2009), https://www.wsj.com/articles/BL-DGB-9571	December 2009
Rob Jackson, <i>Paid Android Apps Coming Early 2009</i> , Phandroid (Oct. 22, 2008), https://phandroid.com/2008/10/22/paidandroid-apps-coming-early-2009/	October 2008
Greg Kumparak, <i>iTunes Rewind Highlights The Best Apps Of 2009</i> , TechCrunch+ (Dec. 8, 2009), https://techcrunch.com/2009/12/08/itunes-rewind-highlights-the-best-apps-of-2009/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAABwpWGIQMLH9RH4dCLei90rUZtxchUu69NlOPHAlf1E37FwRi6Z2Z7VkFWpumOCGRD-kUeR6GisiHEuV6-t01t6uEvYkqyLd4uzUO1K-ZmrcvqRg5cVL3a5Ll8-wTJcGr2NVlIDrFmCtqFJbl0i5YewT03omj6v2Uf68Ov44	December 2009
<i>T-Mobile G1 with Google – Black</i> , T-Mobile (2008) (archived)	2008
<i>Everything You Love About the Web, Now on a Phone</i> , T-Mobile (2008) (archived)	2008
<i>T-Mobile G1 to Run on Qualcomm’s Advanced, Dual-Core Chipset</i> , Qualcomm (Sept. 22, 2008), https://www.qualcomm.com/news/releases/2008/09/t-mobile-g1-run-qualcomms-advanced-dual-core-chipset	September 2008
iPhone User Guide for iPhone and iPhone 3G	2008

<i>Apple iPhone – CPU, Device Specifications</i> , https://www.devicespecifications.com/en/model-cpu/48792734	
<i>AARM1176JZF-S Technical Reference Manual</i> , ARM Developer (Nov. 27, 2009), https://developer.arm.com/documentation/ddi0301/h/	November 2009
<i>Apple MacBook “Core 2 Duo” 2.4 13” (Unibody) Specs</i> , EveryMac.com, https://everymac.com/systems/apple/macbook/specs/macbook-core-2-duo-2.4-aluminum-13-late-2008-unibody-specs.html	
<i>Intel Core 2 Duo Processor P8600</i> , Intel, https://www.intel.com/content/www/us/en/products/sku/35568/intel-core2-duo-processor-p8600-3m-cache-2-40-ghz-1066-mhz-fsb/specifications.html	
<i>Apple Introduces the New iPhone 3G</i> , Apple (June 9, 2008), https://www.apple.com/newsroom/2008/06/09Apple-Introduces-the-New-iPhone-3G/	June 2008
<i>iPhone 3G – Technical Specifications</i> , Apple Support, https://support.apple.com/en-us/112496	
<i>RIM Introduces the BlackBerry Bold Smartphone</i> , RIM (May 12, 2008), archived at https://web.archive.org/web/20080517012537/http://press.rim.com:80/release.jsp?id=1562	May 2008
<i>VMware Products</i> , VMware, archived at https://web.archive.org/web/20080218232419/http://www.vmware.com/products/	
<i>VMware, Understanding Full Virtualization, Paravirtualization, and Hardware Assist</i> (2007)	September 11, 2007
ARM, <i>ARM Architecture Overview</i> (2009), available at https://web.eecs.umich.edu/~prabal/teaching/eecs373-f10/readings/ARM_Architecture_Overview.pdf	2009
ARM, <i>ARM Security Technology: Building a Secure System Using TrustZone Technology</i> (2009), available at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjI7_vlqfiKAxWmkokEHRXpAj8QFnoECA8QAQ&url=https%3A%2F%2Fdocumentation-service.arm.com%2Fstatic%2F5f212796500e883ab8e74531&usg=AOvVaw1Pe2c9ygxbbg8PjsGQV9XZ&opi=89978449	2009

Intel, <i>Intel Trusted Execution Technology Architectural Overview</i> (2003)	2003
Texas Instruments, <i>OMAP Platform Security Features</i> (2003)	2003
Texas Instruments, <i>OMAP 2 Architecture: OMAP2420 Processor</i> (2005)	2005
Texas Instruments, <i>OMAP 3 Family of Multimedia Applications Processors</i> (2007)	2007
OMTP, <i>Advanced Trusted Environment: OMTP TR1</i> (2009)	2009

Moreover, the prior art non-patent publications listed on the face of the Asserted Patents discloses (*i.e.*, anticipates and/or renders obvious) the elements of the Asserted Claims either explicitly or inherently, and Samsung reserves the right to rely on any such reference.

D. Prior Art Systems and/or Knowledge

The Asserted Claims are invalid under 35 U.S.C. §§ 102 and/or 103 based on prior art items offered for sale or publicly used or known or prior inventions, such as prior art products, including systems embodying any alleged inventions or structures described in, and/or any knowledge disclosed by or referred to in, any of the prior art patents or prior art publications identified above in Sections III.B and III.C. Because Samsung has not yet completed discovery in this case, Samsung reserves the right to supplement theses Contentions with facts, documents, or other information learned at a later point through third-party discovery or further investigation. For example, Samsung expects to receive documents from additional third parties either through informal requests or under subpoenas that are believed to have knowledge, documentation, and/or corroborating evidence concerning some of the prior art listed above and below and/or additional prior art. These third parties include without limitation the authors, inventors, or assignees of the references listed in these Contentions. In addition, Samsung reserves the right to assert invalidity

under other sections of 35 U.S.C. § 102 to the extent that discovery or further investigation yield information forming the basis for such invalidity.

Moreover, all of the systems and products listed below qualify as prior art to each of the Asserted Patents under at least pre-AIA 35 U.S.C. §§ 102(a)/(b). Such systems and products were known, used, offered for sale, and/or sold in the United States prior to the appropriate priority date corresponding to each of the Asserted Patents.

Devices
General Dynamics Sectéra Edge
Android Devices (including HTC Dream/T-Mobile G1, Samsung GT-I7500 Galaxy, Nexus One, Nexus S and emulators) ⁵
Apple Devices (including iPhone, iPhone 3G, iPhone 3GS, iPhone 4, and emulators)
Symbian Devices (including Nokia E90, N95, N97, E72, and emulators)
Windows Mobile Devices (including HTC Ozone, HTC Imagio XV6975, HTC Tilt 2, HTC Pure, Samsung C6620, Samsung Intrepid SPH-i350, and emulators)
BlackBerry Devices (including BlackBerry Curve 8330/8900, BlackBerry Bold 9000, BlackBerry Storm 9500/9530, BlackBerry Bold 9780, BlackBerry Bold 9700, BlackBerry Curve 3G 9330, BlackBerry Storm 2 9250/9550, BlackBerry Torch 9800, BlackBerry Pearl 9105, and emulators)
Windows XP Devices (including devices with Windows XP installed and emulators)
Motorola devices, including the Motorola E815
Mobile devices supporting Wireless Application Protocol (WAP)
Devices implementing ARM TrustZone
Devices implementing Intel Trusted Execution Technology (TXT), including Intel vPro processors
Texas Instruments Open Multimedia Applications Platform (OMAP)
Devices implementing Open Mobile Terminal Platform (OMTP) Advanced Trusted Environment: OMTP TR1 standard and related standards
Devices implementing VMware Inc.'s Virtualization Platform (including Full Virtualization, Paravirtualization, and Hardware Assist)

⁵ See, e.g., SAMSUNG_PRIORART5_0000676-1009; SAMSUNG_PRIORART5_0000086-88; SAMSUNG_PRIORART5_0000089-229; SAMSUNG_PRIORART5_0000463-466; SAMSUNG_PRIORART5_0000467-470; SAMSUNG_PRIORART5_0000471-475; SAMSUNG_PRIORART5_0000476-491; SAMSUNG_PRIORART5_0000492-495; SAMSUNG_PRIORART5_0000496-499; SAMSUNG_PRIORART5_0000500-504; SAMSUNG_PRIORART5_0000505-518; SAMSUNG_PRIORART5_0000519-524; SAMSUNG_PRIORART5_0000525-531; SAMSUNG_PRIORART5_0000443-444; SAMSUNG_PRIORART5_0000532-668; Section IV.B.2, *infra*.

Devices implementing Intel Virtualization Technology
Devices implementing the Virtual Machine Facility (VM/370)
Devices implementing Microsoft Windows (including Windows Vista Home Basic, Windows Vista Home Premium, and Windows Vista Ultimate)

Operating Systems
Android including Android Versions m3-rc20a (released November 12, 2007), m3-rc22a (released November 16, 2007), m3-rc37a (released December 14, 2007), m5-rc14 (released February 12, 2008), Android 1.0 (released September 2008), Android 1.1 (released February 2009), Android Cupcake (1.5) (released April 2009), Android Donut (1.6) (released September 2009), Android Eclair (2.0, 2.0.1, 2.1) (released October 2009 - January 2010), Android Froyo 2.2 (released May 2010), and Android Gingerbread 2.3 (released December 2010) ⁶
iPhone OS including iPhone OS 1.0 (released June 29, 2007), iPhone OS 2.0 (released July 11, 2008), iPhone OS 3.0 (released June 19, 2009), and iPhone OS 4.0 (released June 21, 2010)
Symbian OS including Symbian OS 9.1 (released 2005), Symbian OS 9.2, 9.3 (released 2006), Symbian OS 9.4 (released 2007), and associated platforms including S60 3rd Edition (released 2001/2002), S60 3rd Edition, Feature Pack 1 and Feature Pack 2, and S60 5th Edition (released October 2008)
BlackBerry OS including BlackBerry OS 1, BlackBerry OS 2, BlackBerry OS 3 (released March 2002), BlackBerry OS 4.0 (released June 2003), BlackBerry OS 4.1 (released January 2006), BlackBerry OS 4.2 (released June 2007), BlackBerry OS 4.3 (released October 2007), BlackBerry OS 4.5/4.6 (released June 2008), BlackBerry OS 4.7 (released November 2008), BlackBerry OS 5.0 (released August 2009), and BlackBerry OS 6.0 (released July 2010)
Windows Mobile including Windows Mobile 5.0 (released May 9, 2005), Windows Mobile 6.0 (released February 12, 2007), Windows Mobile 6.1 (released April 1, 2008), Windows Mobile 6.5 (released May 11, 2009), and Windows Mobile 7 (released October 21, 2010)
Windows XP including its various editions such as Home Edition and Tablet PC Edition (Windows XP was initially released October 2001)

⁶ See, e.g., SAMSUNG_PRIORART5_0000230-445; SAMSUNG_PRIORART5_0000001; SAMSUNG_PRIORART5_0000084; SAMSUNG_PRIORART5_0000085; SAMSUNG_PRIORART5_0000669; SAMSUNG_PRIORART5_0000670; SAMSUNG_PRIORART5_0000672; SAMSUNG_PRIORART5_0000674; SAMSUNG_PRIORART5_0001010; SAMSUNG_PRIORART5_0001093; SAMSUNG_PRIORART5_0001106; SAMSUNG_PRIORART5_0001112; SAMSUNG_PRIORART5_0001122; SAMSUNG_PRIORART5_0001123; SAMSUNG_PRIORART5_0001124; SAMSUNG_PRIORART5_0001125; SAMSUNG_PRIORART5_0001126; SAMSUNG_PRIORART5_0001128; SAMSUNG_PRIORART5_0001130; Section IV.B.2, *infra*. For Android versions 1.0-2.3, code from earlier versions carried over into later versions. Thus, any code cited from an earlier version of Android also exists in the later version.

Windows NT including its various editions and later versions of Windows based on Windows NT, such as Windows Server 2008 R2 (released October 2009)
Linux operating systems, including its various editions, such as Ubuntu 10.04 (released April 2010), 10.10 (released October 2010)

Applications/Services/APIs
Microsoft Applications/Services/APIs (including Microsoft Connection Manager, Windows Media Player Mobile, Windows Live, MyPhone, Direct Push, Messaging API (MAPI), Outlook Object Model (POOM) API, Wireless Application Protocol (WAP) API, HTTPS/SSL related APIs, CryptoAPI, Security Support Provider Interface (SSPI), Message Queuing (MSMQ) API, and Open Mobile Alliance (OMA) device management for over-the-air (OTA) provisioning)
Apple Applications/Services (including Mail, Calendar, MobileMe, Messages, Voicemail, and VPN)
Citrix Applications (including XenApp, XenDesktop, NetScaler, Citrix Receiver, and Citrix Cloud Bridge)
BlackBerry Applications/Services (including Mobile Data Service (MDS), Roxio Media Manager, Email, Preferred Wireless Network List, and applications interacting with BlackBerry Enterprise Server (“BES”) including BES for Microsoft Exchange and BES for MDS)
Wireless Application Protocol (WAP)
Gemalto Applications/Services/APIs (including those associated with LinqUs Device Manager, LinqUs OTA Manager, LinqUs Service Manager, LinqUs Roaming Services, Smart Card Web Server Technology, and/or MultimediaReady SIM card)
Telespree Applications/Services/APIs (including those associated with Telespree’s Self-service Automated Activation & Service Enrollment, Self-Service Account Maintenance (Self-Care), Self-Service Special Data Services, and/or Enterprise services)
Good Mobility Suite Applications/Services/APIs (including those associated with Good Mobile Messaging, Good Mobile Connection, Good Mobile Intranet, Good Mobile Messaging S/MIME, and/or Good Mobile Messaging Hosted Edition)

To the extent that Headwater later contends that the ItsOn Solution practiced the asserted claims of the ’144 patent (which issued on July 17, 2018 from an application filed on November 20, 2015) and the asserted claims of the ’250 patent (which issued on September 18, 2018 from an application filed on October 6, 2016), the ItsOn Solution could serve as prior art to, and thus invalidate, such claims—at least under Headwater’s apparent claim interpretation.

The Federal Circuit has held that “[t]he proper test for the public use prong of the [pre-AIA] § 102(b) statutory bar is whether the purported use: (1) was accessible to the public; or (2)

was commercially exploited.” See *Invitrogen Corp. v. Biocrest Mfg. L.P.*, 424 F.3d 1374, 1380 (Fed. Cir. 2005). Additionally, the on-sale bar of § 102(b) is triggered when the invention is both (1) the subject of a commercial offer for sale not primarily for experimental purposes and (2) ready for patenting. *Pfaff v. Wells Elecs., Inc.*, 525 U.S. 55, 67 (1998). Each of the systems and products listed above meets these criteria.

The above discussion is not exclusive. Samsung reserves the right to rely on both the listed products as well as other products that may become known and/or relevant during the course of this matter. Samsung also reserves the right to rely on forthcoming testimony and/or declarations from third-party witnesses, including but not limited to witnesses from Google, Apple, Microsoft, and RIM/BlackBerry relating to the above products, applications, and operating systems.

Any citation to one or more of these prior art references, or other prior art references regarding any method or system, should be construed to constitute not only a citation to the prior art reference itself but also a reference to the system itself. Discovery is ongoing in this case, and Samsung will supplement these Contentions if and when more information becomes available. For example, Defendants are already in the process of taking discovery from non-parties including Google, Apple, Microsoft, and RIM/BlackBerry in related matters, namely *Headwater Research LLC v. Samsung Electronics Co., Ltd., et al.*, No. 2:22-cv-00422 (E.D. Tex.) (“the -422 matter”); *Headwater Research LLC v. Samsung Electronics Co., Ltd., et al.*, No. 2:23-cv-00103 (E.D. Tex.) (“the -103 matter”) *Headwater Research LLC v. Samsung Electronics Co., Ltd., et al.*, No. 2:23-cv-00641 (E.D. Tex.) (“the -641 matter”); and *Headwater Research LLC v. Samsung Electronics Co., Ltd., et al.*, No. 2:24-cv-00228 (“the -228 matter”). Accordingly, Defendants reserve the right to modify, amend, and/or supplement these contentions as additional information becomes available from non-parties.

E. Prior Art Under 35 U.S.C. §§ 102(f) and 102(g)

Each prior art patent, publication, or product identified above was either effectively filed or issued (for patents), published (for publications) or known, used, offered for sale or sold (for products) before either the earliest claimed priority date of the Asserted Patents to which it is applied for invalidity, and none appears to have been abandoned, suppressed, or concealed, so each such reference also constitutes evidence of prior invention pursuant to 35 U.S.C. § 102(g), if it is in the U.S. The persons or entities involved with each such invention include the named inventors on the above-identified patents, the authors listed on the above-identified publications, and the entities and individuals identified in connection with the above-identified products.

Because Samsung has not yet completed discovery in this case, including taking depositions of the named inventors of the Asserted Patents, reviewing Headwater's productions, and seeking discovery of prior inventions by third parties, Samsung reserves the right to supplement these Contentions with facts, documents, or other information learned at a later point through discovery or further investigation.

IV. ANTICIPATION AND OBVIOUSNESS (35 U.S.C. §§ 102 AND 103)

The Asserted Claims are anticipated by and/or rendered obvious in view of one or more items of prior art identified in these Contentions, alone and/or in combination. Based on its investigation to date, Samsung has provided in the lists above the prior art presently known to Samsung that anticipates and/or renders obvious the Asserted Claims under at least Headwater's actual and/or apparent application of those claims. The prior art identified in these Contentions discloses (*i.e.*, anticipates and/or renders obvious) the elements of the Asserted Claims either explicitly or inherently.

Prior art patents or publications included in these Contentions may be related (such as a divisional, continuation, continuation-in-part, parent, or child) to earlier or later-filed patents or

publications, may have counterparts filed in other jurisdictions, or may incorporate (or be incorporated by) other patents or publications by reference. The listed patents or publications are intended to be representative of these other patents or publications to the extent they exist. Samsung accordingly reserves the right to modify, amend, or supplement these Contentions with these related patents or publications, as well as other prior art references, upon further investigation. Additionally, any reference in these Contentions, including the appendices and/or exhibits thereto, to a specific subsection or subsections of 35 U.S.C. § 102, is merely exemplary, and Samsung expressly reserves the right to rely on additional or other sections of 35 U.S.C. § 102, as appropriate.

Although Samsung's investigation is ongoing, information available to date indicates that each prior art system disclosed above was at least (1) known or used in this country before the alleged invention of the claimed subject matter of the Asserted Patents; (2) in public use, on sale, or offered for sale in this country more than one year before the effective filing date for the Asserted Patents; or (3) invented and not abandoned, suppressed, or concealed prior to the alleged invention of the Asserted Patents.

Much of the art identified in these Contentions reflects common knowledge and the state of the art prior to the filing or asserted priority dates of the Asserted Patents. As such, the obviousness combinations in these Contentions are intended to be exemplary. There are many possible combinations of the disclosed prior art, and the inclusion of certain exemplary combinations does not exclude other combinations. For example, where a particular contention calls for combining references, any of a number of references can be combined.

Depending on the construction of the claims of the Asserted Patents, and/or positions that Headwater or its expert witnesses may take concerning claim interpretation, infringement, and/or

invalidity issues, certain prior art references may be of greater or lesser relevance, and different combinations of these references may be implicated. Given this uncertainty, the charts may reflect alternative applications of the prior art against the Asserted Claims.

Citations to particular excerpts from the prior art are likewise exemplary and not exhaustive of the evidentiary support for the invalidity of the Asserted Patents contained in and/or concerning a particular piece of prior art. Samsung may rely on uncited portions of the prior art references, other documents or operational systems, the “Background of the Invention” and other relevant portions of the Asserted Patents, the prosecution histories of the Asserted Patents (including all cited references) and their related patents and applications, and forthcoming fact and expert testimony to provide context to aid in understanding the prior art reference and/or the cited portions of the references. Where Samsung cites to a particular figure in a reference, the citation encompasses the caption and description of the figure and any text relating to or discussing the figure. Likewise, where Samsung cites text referring to a figure, the citation includes the figure as well (and vice versa).

A. Prior Art Under 35 U.S.C. § 102

Samsung contends that at least the primary prior art references (Exs. A-01 through A-26 and B-01 through B-21) identified below, by themselves, anticipate the Asserted Claims:

Exhibits	Primary References and/or Systems
A-01	Hill
A-02	Freund
A-03	Yadav
A-04	Wu
A-05	Field

Exhibits	Primary References and/or Systems
A-06	Malomsoky
A-07	Tonsing '467
A-08	Oester
A-09	Tokitaka
A-10	Sever
A-11	Kapoor
A-12	Venkatraman
A-13	Khemani
A-14	Seo
A-15	Kitahara
A-16	Bajikar '534
A-17	Wright '965
A-18	Durham
A-19	Android
A-20	Apple
A-21	BlackBerry
A-22	VMware
A-23	ARM TrustZone
A-24	Intel Trusted Execution Technology ("TXT")
A-25	Texas Instruments Open Multimedia Applications Platform ("OMAP")
A-26	Open Mobile Terminal Platform ("OMTP") Advanced Trusted Environment
B-01	Owen
B-02	Henry

Exhibits	Primary References and/or Systems
B-03	Lambert
B-04	Bogner
B-05	Chen
B-06	Tome
B-07	Edery
B-08	Chari
B-09	Field
B-10	Iga
B-11	Kshirsagar
B-12	Andriod
B-13	Apple
B-14	BlackBerry
B-15	VMware Virtualization
B-16	Sectéra Edge
B-17	Intel Virtualization
B-18	IBM VM 370
B-19	Microsoft Windows
B-20	Kohavi
B-21	Linux Operating Systems

Specifically, Samsung contends that at least the references and/or systems in the table above independently anticipate the Asserted Claims under 35 U.S.C. §§ 102(a), (b), (e), (f) and/or (g), as set forth in the charts attached as:

- Exhibits A-01 through Exhibits A-26 for the asserted claims of the '144 patent; and

- Exhibits B-01 through Exhibits B-21 for the asserted claims of the '250 patent.

Where an asserted prior art reference in any attached claim charts relies on a claim of priority to assert a critical reference date under pre-AIA 35 U.S.C. § 102 *et seq.* (including pre-AIA § 102(e)), compliance with pre-AIA 35 U.S.C. § 112, first paragraph, or 35 U.S.C. § 112(a), is shown in an appendix to a given claim.

These charts, however, are exemplary. The claimed features are similarly described and suggested in other places (including in all of the documents cited during prosecution of each piece of prior art), and also were present when prior-art systems practicing the described prior art were used before the application that ultimately led to the Asserted Patents. Thus, where patents or other printed materials are disclosed, Samsung reserves the right to also rely on those materials as descriptions of systems, devices, or methods referenced therein, publicly used, and/or on sale or known in the United States. Further, Samsung reserves the right to rely on other evidence of the prior art beyond merely the exemplary references cited in the charts attached as Exhibits.

Where patents or other printed materials are disclosed, Samsung reserves the right to also rely on those materials as descriptions of systems, devices, or methods referenced therein, publicly used, and/or on sale or known in the United States. Samsung reserves the right to also use those references to invalidate the claim under 35 U.S.C. § 103.

B. Prior Art Under 35 U.S.C. § 103

To the extent that a primary reference is deemed, by itself, not to anticipate or render obvious a claim for failing to teach one or more limitations, the claim would nonetheless have been obvious to a POSITA at the time of the invention by the combination of the primary reference with one or more other primary references and/or the knowledge of someone skilled in the art.

Moreover, Exhibits A-A and B-B list secondary prior art references and identify, on limitation-by-limitation bases, exemplary disclosures where each secondary reference teaches the

limitations of the asserted claims. To the extent that a primary reference is deemed, by itself, not to anticipate or render obvious a claim for failing to teach one or more limitations, the claim would nonetheless have also been obvious to a POSITA at the time of the invention by the additional combination of the primary reference with one or more of the references listed as disclosing those alleged missing limitations in Exhibits A-A and B-B.

As such, a POSITA would have been motivated to combine any reference set forth in at least the following charts:

- Exhibit A-01 through Exhibit A-26 and Exhibit A-A for the asserted claims of the '144 patent; and
- Exhibit B-01 through Exhibit B-21 and Exhibit B-B for the asserted claims of the '250 patent.

Such combinations would be achieved, for example, by merely combining the disclosures described in the respective claim charts for each reference. These charts, however, are exemplary. The claimed features are similarly described and suggested in other places (including in all of the documents cited during prosecution of each piece of prior art), and also were present when prior-art systems practicing the described prior art were used before the application that ultimately led to the Asserted Patents.

Samsung's assertion that the combinations above render the asserted claims obvious under 35 U.S.C. § 103 is not, and is not intended to be, an admission or suggestion that each reference does not independently anticipate the Asserted Claims under 35 U.S.C. § 102. *See Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548 (Fed. Cir. 1983) (“[A]nticipation is the epitome of obviousness.” (quoting *In re Fracalossi*, 681 F.2d 792, 794 (CCPA 1982))). Further, the fact that certain secondary references are listed solely in Exhibits A-A and B-B is not intended to be an admission or suggestion that each individual reference cited therein does not also independently anticipate and/or render obvious the Asserted Claims under 35 U.S.C. §§ 102 and 103. Samsung

expressly reserves the right to rely on any secondary reference cited in Exhibits A-A and B-B as if it were set forth as a primary reference in Section IV.A, *supra*. Finally, the inclusion of the exemplary combinations in the attached Exhibits and Appendices does not exclude other combinations of prior art disclosed in this or previous sections.

1. Exemplary Combinations

Exemplary combinations of prior art references that render the Asserted Claims invalid as obvious under 35 U.S.C. § 103 are described in:

- Exhibit A-01 through Exhibit A-26 and Exhibit A-A for the asserted claims of the '144 patent; and
- Exhibit B-01 through Exhibit B-21 and Exhibit B-B for the asserted claims of the '250 patent.

Moreover, each prior art reference or system may be combined with (1) information known to persons skilled in the art at the time of the alleged invention; (2) any other anticipatory prior art references or systems; and (3) any of the additional prior art identified above or in the prosecution of the Asserted Patents and related applications.

Below are examples of prior art references and/or systems that would have been combined by one of ordinary skill in the art at the time of the alleged invention. These combinations are merely examples. The Asserted Claims are rendered obvious by:

- '144 patent:
 - Hill alone or in combination with one or more of Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
 - Freund alone or in combination with one or more of Hill, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone

Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.

- Yadav alone or in combination with one or more of Hill, Freund, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
- Wu alone or in combination with one or more of Hill, Freund, Yadav, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
- Field alone or in combination with one or more of Hill, Freund, Yadav, Wu, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
- Malomsoky alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, and Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
- Tonsing '467 alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
- Oester alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
- Tokitaka alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Sever, Kapoor, Venkatraman,

Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.

- Sever alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
- Kapoor alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
- Venkatraman alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
- Khemani alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
- Seo alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
- Kitahara alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.

- Bajikar '534 alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
- Wright '965 alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
- Durham alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
- Android Devices alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
- Apple Devices alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
- BlackBerry Devices alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
- VMware Devices alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, ARM TrustZone

Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.

- ARM TrustZone Devices alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, Intel TXT Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
 - Intel TXT Devices alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Texas Instruments OMAP Devices, and OMTP Advanced Trusted Environment Devices.
 - Texas Instruments OMAP Devices alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, and OMTP Advanced Trusted Environment Devices.
 - OMTP Advanced Trusted Environment Devices alone or in combination with one or more of Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, Durham, Android Devices, Apple Devices, BlackBerry Devices, VMWare Devices, ARM TrustZone Devices, Intel TXT Devices, and Texas Instruments OMAP Devices.
- '250 patent:
 - Owen alone or in combination with one or more of Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Andriod Devices, Apple Devices, BlackBerry Devices, VMware Virtualization Devices, Sectéra Edge Devices, Intel Virtualization Devices, Linux Operating Systems, IBM VM/370 Devices and Microsoft Windows Devices.
 - Henry alone or in combination with one or more of Owen, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Andriod Devices, Apple Devices, BlackBerry Devices, VMware Virtualization Devices, Sectéra Edge Devices, Intel Virtualization Devices, Linux Operating Systems, IBM VM/370 Devices and Microsoft Windows Devices.
 - Lambert alone or in combination with one or more of Owen, Henry, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Andriod Devices,

Apple Devices, BlackBerry Devices, VMware Virtualization Devices, Sectéra Edge Devices, Intel Virtualization Devices, Linux Operating Systems, IBM VM/370 Devices and Microsoft Windows Devices.

- Bogner alone or in combination with one or more of Owen, Henry, Lambert, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Andriod Devices, Apple Devices, BlackBerry Devices, VMware Virtualization Devices, Sectéra Edge Devices, Intel Virtualization Devices, Linux Operating Systems, IBM VM/370 Devices and Microsoft Windows Devices.
- Chen alone or in combination with one or more of Owen, Henry, Lambert, Bogner, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Andriod Devices, Apple Devices, BlackBerry Devices, VMware Virtualization Devices, Sectéra Edge Devices, Intel Virtualization Devices, Linux Operating Systems, IBM VM/370 Devices and Microsoft Windows Devices.
- Tome alone or in combination with one or more of Owen, Henry, Lambert, Bogner, Chen, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Andriod Devices, Apple Devices, BlackBerry Devices, VMware Virtualization Devices, Sectéra Edge Devices, Intel Virtualization Devices, Linux Operating Systems, IBM VM/370 Devices and Microsoft Windows Devices.
- Edery alone or in combination with one or more of Owen, Henry, Lambert, Bogner, Chen, Tome, Chari, Field, Iga, Kohavi, Kshirsagar, Andriod Devices, Apple Devices, BlackBerry Devices, VMware Virtualization Devices, Sectéra Edge Devices, Intel Virtualization Devices, Linux Operating Systems, IBM VM/370 Devices and Microsoft Windows Devices.
- Chari alone or in combination with one or more of Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Field, Iga, Kohavi, Kshirsagar, Andriod Devices, Apple Devices, BlackBerry Devices, VMware Virtualization Devices, Sectéra Edge Devices, Intel Virtualization Devices, Linux Operating Systems, IBM VM/370 Devices and Microsoft Windows Devices.
- Field alone or in combination with one or more of Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Iga, Kohavi, Kshirsagar, Andriod Devices, Apple Devices, BlackBerry Devices, VMware Virtualization Devices, Sectéra Edge Devices, Intel Virtualization Devices, Linux Operating Systems, IBM VM/370 Devices and Microsoft Windows Devices.
- Iga alone or in combination with one or more of Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Kohavi, Kshirsagar, Andriod Devices, Apple Devices, BlackBerry Devices, VMware Virtualization Devices, Sectéra Edge Devices, Intel Virtualization Devices, Linux Operating Systems, IBM VM/370 Devices and Microsoft Windows Devices.
- Kohavi alone or in combination with one or more of Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kshirsagar, Andriod Devices,

Apple Devices, BlackBerry Devices, VMware Virtualization Devices, Sectéra Edge Devices, Intel Virtualization Devices, Linux Operating Systems, IBM VM/370 Devices and Microsoft Windows Devices.

- Kshirsagar alone or in combination with one or more of Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Andriod Devices, Apple Devices, BlackBerry Devices, VMware Virtualization Devices, Sectéra Edge Devices, Intel Virtualization Devices, Linux Operating Systems, IBM VM/370 Devices and Microsoft Windows Devices.
- Android Devices alone or in combination with one or more of Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Apple Devices, BlackBerry Devices, VMware Virtualization Devices, Sectéra Edge Devices, Linux Operating Systems, Intel Virtualization Devices, IBM VM/370 Devices, and Microsoft Windows Devices.
- Apple Devices alone or in combination with one or more of Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Andriod Devices, BlackBerry Devices, VMware Virtualization Devices, Sectéra Edge Devices, Linux Operating Systems, Intel Virtualization Devices, IBM VM/370 Devices, and Microsoft Windows Devices.
- BlackBerry Devices alone or in combination with one or more of Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Andriod Devices, Apple Devices, VMware Virtualization Devices, Sectéra Edge Devices, Intel Virtualization Devices, Linux Operating Systems, IBM VM/370 Devices, and Microsoft Windows Devices.
- VMware Virtualization Devices alone or in combination with one or more of Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Andriod Devices, Apple Devices, BlackBerry Devices, Sectéra Edge Devices, Intel Virtualization Devices, Linux Operating Systems, IBM VM/370 Devices, and Microsoft Windows Devices.
- Sectéra Edge Devices alone or in combination with one or more of Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Andriod Devices, Apple Devices, BlackBerry Devices, VMware Virtualization Devices, Intel Virtualization Devices, Linux Operating Systems, IBM VM/370 Devices, and Microsoft Windows Devices.
- Intel Virtualization alone or in combination with one or more of Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Andriod Devices, Apple Devices, BlackBerry Devices, VMware Virtualization Devices, Sectéra Edge Devices, Linux Operating Systems, IBM VM/370 Devices, and Microsoft Windows Devices.
- IBM VM/370 Devices alone or in combination with one or more of Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi,

SAMSUNG'S INVALIDITY AND PATENT INELIGIBILITY CONTENTIONS

Kshirsagar, Andriod Devices, Apple Devices, BlackBerry Devices, VMware Virtualization Devices, Sectéra Edge Devices, Linux Operating Systems, Intel Virtualization Devices, and Microsoft Windows Devices.

- Microsoft Windows Devices alone or in combination with one or more of Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Andriod Devices, Apple Devices, BlackBerry Devices, VMware Virtualization Devices, Sectéra Edge Devices, Linux Operating Systems, Intel Virtualization Devices, and IBM VM/370 Devices.
- Linux Operating Systems alone or in combination with one or more of Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Andriod Devices, Apple Devices, BlackBerry Devices, VMware Virtualization Devices, Sectéra Edge Devices, Microsoft Windows Devices, Intel Virtualization Devices, and IBM VM/370 Devices.

2. Exemplary Motivations to Combine

To the extent a finder of fact finds that any primary prior art reference does not disclose one or more limitations of an asserted claim, the asserted claim is nevertheless obvious because the allegedly missing limitations contain nothing beyond ordinary improvements. In other words, the asserted claim combines known elements to achieve predictable results or chooses between clear alternatives known to those of skill in the art, particularly in view of the state of the art as reflected in the relevant prior art.

Moreover, as explained above, it would have been obvious to a person of skill in the art at the time of the alleged invention of the asserted claims to combine any primary reference with any combination of other primary references or secondary references so as to practice the asserted claims. To the extent that Headwater argues that any concept claimed in the asserted claims is not disclosed in a primary reference, it would, at a minimum, have been obvious to adapt the primary reference to include the concept or combine it with other primary references or secondary references that disclose the concept. Each concept described and claimed in the Asserted Patents

was known to those of skill in the art as available design choices for various security features, partitioning features, and networking features.

The Supreme Court has held that “[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). “When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one.” *Id.* at 417. As the Supreme Court made clear, “[f]or the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.” *Id.*

To determine whether there is an apparent reason to combine the known elements in the fashion claimed by the patent at issue, a court can “look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art.” *Id.* at 418. For example, obviousness can be demonstrated by showing “there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent’s claims.” *Id.* at 420. “[A]ny need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.” *Id.* Common sense also teaches that “familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle.” *Id.*

However, the Supreme Court in *KSR* held that a claimed invention can be obvious even if there is no explicit teaching, suggestion, or motivation for combining the prior art to produce that

invention. In summary, *KSR* holds that patents that are based on new combinations of elements or components already known in a technical field may be found to be obvious. *See generally KSR*, 127 S.Ct. 1727. Specifically, the Court in *KSR* rejected a rigid application of the “teaching, suggestion, or motivation [to combine]” test. *Id.* at 1741. “In determining whether the subject matter of a patent claim is obvious, neither the particular motivation nor the avowed purpose of the patentee controls. What matters is the objective reach of the claim.” *Id.* at 1741-42. “Under the correct analysis, any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.” *Id.* at 1742. A key inquiry is whether the “improvement is more than the predictable use of prior art elements according to their established functions.” *Id.* at 1740.

The rationale to combine or modify prior art references is significantly stronger when, as here, the references seek to solve the same problem, come from the same field, and correspond well to each other. *In re Inland Steel Co.*, 265 F.3d 1354, 1362 (Fed. Cir. 2001). The Federal Circuit has held that two references may be combined as invalidating art under similar circumstances, namely “[the prior art] focus[es] on the same problem that the . . . patent addresses: enhancing the magnetic properties of . . . steel. Moreover, both [prior art references] come from the same field Finally, the solutions to the identified problems found in the two references correspond well.” *Id.* at 1364 (concerning patents and prior art relating to improving the magnetic and electrical properties of steel).

In view of the Supreme Court’s *KSR* decision, the PTO issued a set of Examination Guidelines. Examination Guidelines for Determining Obviousness Under 35 U.S.C. §103 in view of the Supreme Court Decision in *KSR Int’l Co. v. Teleflex, Inc.*, 72 Fed. Reg. 57526 (Oct. 10,

2007). Those Guidelines summarized the *KSR* decision and identified various rationales for finding a claim obvious, including those based on other precedents. Those rationales include:

(A) Combining prior art elements according to known methods to yield predictable results;

(B) Simple substitution of one known element for another to obtain predictable results;

(C) Use of known technique to improve similar devices (methods, or products) in the same way;

(D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;

(E) “Obvious to try” – choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;

(F) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art;

(G) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

Id. at 57529. The above rationales likewise apply in rendering obvious the asserted claims of the Asserted Patents.

The references disclosed herein, alone or in combination, contain an explicit and/or implicit teaching or motivation to combine them due to the following: (1) the knowledge generally available to a POSITA; (2) the prior art references as understood by a POSITA; (3) the nature of the problem to be solved; (4) the fact that each prior art reference addresses similar problems; and (5) the knowledge of a POSITA that the disclosed elements had been or could be used together.

As an example of those reasons and motivations to combine, the various prior art publications and systems relied upon herein all generally relate to or include data classification and/or policy enforcement. *See* Exs. A-01 through B-21; Exs. A-A through B-B. The prior art depicts, discloses, and discusses similar components and techniques for partitioning computer

resources, measuring network traffic, managing access to resources or data, monitoring and cataloguing resource utilization, and improving device/network security and performance, among other things. *Id.* Thus, a person of ordinary skill in the art would understand the teachings of the references and systems to be applicable to one another. A POSITA would have also found it obvious to implement (*i.e.*, obvious to try) such combinations in order to utilize these well-known networking, security, data classification, and resource monitoring techniques in a wireless end-user device. *Id.*

For example, a POSITA would look to the primary and secondary references and systems discussed above to improve device/network security and enable or enhance a device's data classification and policy enforcement functionality. A POSITA would have understood and been aware of motivations to enhance device/network security. A POSITA would also have appreciated that this goal could be achieved by improving a device's data classification, resource monitoring, and policy enforcement capabilities.

Accordingly, a POSITA would find these goals and methods for achieving them obvious, would further seek to combine or modify the disclosure of any given primary and secondary references and/or systems to achieve those goals, and would have readily understood that doing so could increase device/network performance, improve user interactions and/or satisfaction, improve device/network security, and enhance policy enforcement capability. *See, e.g.*, Hill at [0011] ("A significant increase in the degree of responsiveness that server pools and data centers can provide is required to address these changes in the speed of business."), [0019] ("Another problem in current data center environments is that monitoring historical use of the resources consumed by applications (*e.g.*, to provide capacity planning data or for billing and charge-back reporting) is difficult since there is no centralized monitoring of the data center resources."), [0065]

(“The present invention provides a mechanism which enables these goals to be simultaneously achieved through a new data center technology that provides almost instantaneous global awareness across the data center as well as nearly instantaneous agility to react to changes.”); Freund at [0010] (“As more and more computers are now connected to the Internet, either directly (*e.g.*, over a dial-up or broadband connection with an Internet Service Provider or ‘ISP’) or through a gateway between a LAN and the Internet, a whole new set of challenges face LAN administrators and individual users alike: these previously closed computing environments are now open to a worldwide network of computer systems. A particular set of challenges involves attacks by perpetrators (hackers) capable of damaging the local computer systems, misusing those systems, and/or stealing proprietary data and programs.”), [0013] (“One particular problem that remains is how to secure individual end points—that is, the individual computers and devices that access a firm’s data (*e.g.*, data stored on corporate servers).”), [0013] (“[W]ith the ever-increasing availability of wireless network access points, the assumption that there is some sort of a protected or trusted environment within one’s enterprise becomes an increasingly more problematic assumption to make.”), [0018] (“What is needed is a system providing methodology for ensuring that the individual end points themselves are secure.”), [0069] (“In particular, any given server/access end point pair assumes that anything (*i.e.*, network segment) in between the two is suspect (*i.e.*, insecure). With this approach, any communication between an end point and a server is protected in a manner to provide ad hoc trusted communication between the two.”); Yadav at [0006] (“Providing QoS in a connectionless packet-switched network, such as an IP network, can be difficult due to the unpredictable nature of packet delivery caused by the best-efforts network environment.”), [0015] (“The network QoS systems and techniques described here accurately identify and take into consideration the applications currently running on a computing

system/machine in a networked environment . . . When applications invoked on a networked machine are accurately identified on the networked machine, network communications for invoked applications may be managed from within the network stack on the machine to implement QoS on a connectionless packet-switched network, such as an IP network.”); Wu at 1:54-61 (“Particular embodiments of the subject matter described in this specification can be implemented to realize one or more of the following advantages. The techniques described in this specification make it possible to change kernel behavior (*e.g.*, resource management rules or network routing rules) outside the kernel space. Resource management policies (including security policies) of an operating system can be implemented in user space.”), 3:11-17 (“In general, networked devices (*e.g.*, computer servers, mobile phones, hand-held electronic devices, networking switches, or routers) can be susceptible to Denial of Service (DoS) attacks. The DoS attacks can force the devices to waste precious system resources (*e.g.*, kernel memory 132) on fictitious information or requests, freezing up the resources and render the attacked the devices non-functional.”), 3:18-20 (“The user space resource management techniques described in this specification allow the developer to create customized rules for managing resources without modifying the kernel.”); Field at [0006] (“While these protection systems can be effective, they can also suffer from a few weaknesses. First, these systems often rely on obscurity and are thus vulnerable to exploitation if identified by the malware . . . Furthermore and related to the first, these protection systems generally operate in a same protection domain as that of the operating system (*e.g.*, within the privileged mode itself) . . . Finally, these protection systems initialize at the same time as the operating system or privileged mode.”), [0007] (“This document describes tools capable of enabling a protection agent to determine, from memory inaccessible from an operating-system privilege mode, whether one or more resources of an operating system have been modified.”),

[0021] (“The following document describes tools capable of operating a protection agent in a manner that makes the protection agent unalterable or inaccessible from an operating-system privilege mode. These tools thus enable protection of the protection agent itself, thereby ensuring the protection agent's ability to detect alterations to important operating-system resources.”); Malomsoky at 1 (“[P]assive methods for classifying network traffic have the disadvantage that the classification accuracy varies, for example, depending on the kind of application that has generated the network traffic, so that the overall classification accuracy is often not satisfying.”), 1-2 (“[K]nown active methods for classifying network traffic have the disadvantage that they do not capture all relevant network traffic and therefore do not provide accurate network traffic classification results.”), 2 (“A further disadvantage of known methods for classifying network traffic is the fact that there is no reliable technique for validating such methods available.”), 2 (“This need is satisfied according to a first aspect by a method for classifying network traffic in the form of data packets generated by multiple applications installed on a device. The method as performed by the device comprises the steps of receiving data packets belonging to one or more data flows, each data flow including the data packets generated by a specific one of the multiple applications, analyzing the received data packets to identify the application associated with each analyzed data packet, and classifying at least one data flow by including an application identifier in at least one of the data packets of this data flow.”); Tonsing at 27 (“It is contemplated that the invention could be used in the following list of illustrative examples of potential applications. This list is not intended to be exhaustive . . . Consolidation of application software which was running on multiple real machines (computers) into a single virtual machine . . . Consolidation of appliances to enable multiple appliances to be replaced with a smaller number of devices equipped with virtualisation technology . . . Enabling existing virtual machine systems to process and direct

(i.e. control the processing/forwarding of) network traffic . . . Hosting a new class of network infrastructure applications which combine traditional server like processing with traffic and flow directing/manipulating etc.”); Oester at 1-2 (“Due to this technological diversification and (still) missing standards, the problem arises for the user of such portable data carriers that for almost every service a special data carrier is involved.” (Google Patents translation)), 3 (“It is therefore the object of the present invention to provide a flexible and reliable detection of a claim of services of any third party by means of a security module.” (Google Patents translation)); Tokitaka (“PROBLEM TO BE SOLVED: To provide a mobile terminal that enables a user of the mobile terminal to reasonably and effectively avoid a high packet communication charge that the user does not desire although the user enjoys games, mail, etc.” (Google Patents translation)), (“SOLUTION: A packet quantity measurement node 116 and a packet quantity totaling part 131 are provided in the mobile terminal. The packet quantity measurement node 116 measures the number of packets sent through a communication path and the packet quantity totaling part 131 totals the amounts of packets accumulated by applications, so that the cumulative amounts of packets or packet charges corresponding to the cumulative amounts of packets are displayed at a display unit 162. Not only the cumulative amounts of packets by the applications, but also the cumulative amounts of packets and charges by specified items relating to one application, can be displayed.” (Google Patents translation)), (“As explained earlier, it is not impossible to check the cumulative amount of packets up to the previous day by accessing a predetermined website on the communication network. It can be cumbersome and some users of mobile terminals may continue to be defenseless without checking such accumulated packet volume, resulting in very high packet charges.” (Google Patents translation)); Sever at [0009] (“[T]here is a need in the art for new method that may offer a wider variety of options for controlling the transfer of information and the

access to external devices. A technique for addressing this need in the art would preferably (a) permit a user to transfer certain files but prevent files containing more sensitive or valuable information from being transferred or (b) may allow access to some of the functions of an external device while preventing access to other features.”), [0010] (“Furthermore, there is a need in the art for a method that may verify the environment to which a portable device is connected and restrict information access or information transfer capabilities based on the environment.”), [0011] (“In general, exemplary embodiments of the present invention can operate to analyze the data transportation to or from a physical communication port according to the relevant layers that are used in the communication protocol. Based on the employed security policy and the type of the communication that has been analyzed, a decision is made as to whether to allow the transportation of the data, block the transportation, modify the transportation, inform the user and/or the administrator about the transportation attempt, etc.”); Kapoor at [0009] (“Therefore, needs exist for improved ways of providing switching and security services for networked environments.”), [0010] (“Another need is for better intrusion detection and prevention.”), [0011] (“Systems that provide only intrusion detection may have substantial drawbacks in this environment including false alarms, low manageability, high maintenance, and no prevention of attacks.”); Venkatraman at [0003] (“Because all traffic corresponding to an address range is sent to the virtual private network, whether appropriately sent to the network or not, robust authorization policies must be created to filter appropriate virtual private network traffic from traffic that should not be sent on the virtual private network. Such policies are difficult to create and difficult to maintain. Also, blanket routing of all data communication to a virtual private network, whether appropriate or not, can increase security risks”), [0004] (“It would, therefore, be desirable to provide systems and methods to route data in a virtual private network environment on a more granular basis than

subnet identification.”); Khemani at [0004] (“With an increase in the number of policies, there also exists a need for specifying and implementing processing orders among policies and groups of policies”), [0005] (“Thus, there exists a need for configuration systems which allow a user to specify one or more actions for the case in which a policy is undefined”); Kitahara at [0006] (“Since it is difficult to predict an amount of traffic processed in a communication network, proper facilities and design of communication networks is difficult.”), [0006] (“Moreover, when a plurality of users shares one communication circuit, occupation of the circuit by a specific application of a specific user cannot be prevented”), [0007] (“[I]t is desirable to control the traffic generated by the specific application of the specific user, on the side of the communication network.”), [0008] (“[W]hen the traffic at a communication terminal is equally limited, QoS (Quality of Service) guarantee demanded by each application cannot be controlled, and sufficient quality of communication service cannot be maintained.”); Seo (“However, as hacking techniques are sophisticated and virus spreads can occur at nodes in the internal network, it is not easy for network administrators to understand why, when, where, and why such a network is paralyzed”) (“Moreover, as the generation of harmful traffic becomes more intelligent, even if a firewall is installed, the harmful traffic using the ports allowed by the firewall is increasing significantly, and more seriously, harmful traffic is generated from internal nodes as well as from outside.”) (“In order to solve the problem, a technique for filtering a packet using an intrusion detection system (IDS) or a virus firewall is used, but since the firewall system is a means installed on a boundary line, pattern matching of a data area of a packet is performed.”); Bajikar ’534 at [0006] (“[T]he following capabilities may be provided in a trusted environment external to the discrete SIM hardware device: 1) protected provisioning for a subscriber identification key Ki, 2) protected provisioning for the A5 algorithm (a cipher algorithm) in the Mobile Equipment (ME) and 3)

protected provisioning for security policies.”); Wright ’965 at [0009] (“But mobile users can pick up valuable corporate information, such as that stored on their laptops, and walk away from the corporate network, and connect to other networks with different security policies.”), [0009] (“Each environment presents different challenges to protect the information on the mobile device while allowing access to e-mail, the Internet, and company Virtual Private Networks (VPNs).”), [0010] (“Unfortunately, security settings for one situation can compromise data security in another”), [0012] (“Simple to use, mobile-aware security tools providing different levels of security protection for different locations and/or security features are highly desirable.”); Durham at [0002] (“That is, when new malware is discovered, identifying characteristics are used to identify future instances of the malware. Applying this detection technique to a network may allow spread of malware under some conditions.”), [0003] (“Current network access control architectures are typically limited to static role designations that usually correspond to a particular class of device (e.g. access requester, Policy Enforcement Point, access server, Policy Decision Point). Furthermore, the definition of the network boundary is implicitly defined by the topology of devices acting as Policy Enforcement Points.”); Owen at [0002] (“As the PC began to displace the corporate mainframe computer, however, issues of control began to re-emerge. Corporate Information Technology (IT) departments, increasingly saw the desktop PC as part of the corporate infrastructure. This caused tension between an original goal of the PC revolution, that the user controls their own computer, and the new role they played in the corporation. This conflict continues today and is played out on a regular basis in companies around the world.”), [0003] (“A similar tension exists with handheld and other portable computers. Such as wireless mobile communication devices. However, the situation with handheld computers is more complex for several reasons. Since handheld computers are becoming relatively inexpensive, many users

purchase such devices for personal use. Such user-purchased devices cannot be said to be owned by a corporation of which the user is an employee, but they often come to contain corporate data such as contacts, calendar entries and email. Even when a handheld computer is purchased by a corporate employer and provided to an employee, the handheld computer is likely to be used outside the corporate premises. This may require external access to the corporate infrastructure. Allowing an unsecured device to access the corporate network offers potential for security breaches. Furthermore, when a handheld computer is enabled for wireless communications, a carrier becomes another interested party with respect to the handheld computer. The carrier owns and operates a wireless communication network in which the handheld computer is configured to operate, and therefore may want to exercise control over the traffic on that network. As well, the carrier may wish to add to their revenue by offering additional services to handheld computers. A carrier may thus be at odds with a corporate IT department in regard to handheld computer control, particularly where IT department controls may potentially increase network traffic or affect the carrier's ability to offer these services and thus reduce their revenue.”), [0004] (“Therefore, there remains a need for a system and method for secure control of a wireless communication device, which allows each individual stakeholders, including the user, corporate owner or corporate system operator, carrier, and possibly other stakeholders, to control their device assets without affecting the other stakeholders.”), [0005] (“According to an aspect of the invention, a system for secure control of a wireless mobile communication device comprises at least one domain, each domain including an asset of the wireless mobile communication device, and a domain controller configured to receive a request to perform-an operation affecting at least one of the assets, to determine whether the request originated with an entity that has a trust relationship with the domain that includes the at least one affected asset, and to permit completion of the operation where the

request originated with an entity that has a trust relationship with the domain that includes the at least one affected asset.”), [0006] (“In accordance with another aspect of the invention, a method for secure control of a wireless mobile communication device, comprises segregating assets of the wireless mobile communication device into a plurality of domains, each domain including at least one asset of the wireless mobile communication device, receiving a request to perform an operation affecting at least one of the assets, determining whether the operation is permitted by the domain that includes the affected asset, and allowing the operation to be completed where the operation is permitted by the domain that includes the affected asset.”); Henry at [0006] (“The use of desktop, laptop, and handheld computing and communication devices as platforms for digital communication of sensitive or proprietary data and digital rights controlled content continues to drive security innovations in the computing industry”), [0007] (“In addition to the protection of digital content rights, another factor which continues to drive improvements in computer system security is use restrictions which may be applied to the host platforms themselves.”), [0010] (“Consider the two primary security features provided for by the well-known x86 architecture: paged virtual memory and privileged execution. Under paged virtual memory, the underlying operating system defines a separate virtual address space along with access rights (e.g., execute only, read only) for each application that is being executed, thus precluding another surreptitious application from executing within the defined space or modifying its data. But the data associated with virtual address translation (i.e., page tables) can be easily snooped and changed since the data is resident in system memory and is presented external to the host microprocessor on its system bus.”), [0012] (“With privileged execution, the architecture provides several levels of execution privileges, CPL0 through CPL3. Accordingly, certain system resources and instructions may only be accessed by applications which are executing at higher privilege levels.”), [0013] (“As a result,

various methods and apparatus have been developed which are more closely concentrated toward the prevention of intentional intrusion or takeover of a platform.), [0019] (“Accordingly, the present inventors have noted that it is clearly desirable to provide a microprocessor which is capable of executing an application or application thread comprising general purpose instructions (i.e., any of the instructions in the microprocessor's instruction set) within a secure execution environment.”), [0020] (“It is additionally desirable that the secure execution environment be isolated from any of the known methods of snooping and tampering.”), [0022] (“The present invention provides a superior technique over that which has heretofore been provided that enables the execution of secure application programs in a general purpose microprocessor platform.”); Lambert at [0003] (“However, in most enterprise environments, particularly in larger environments in which some flexibility is important with respect to what various employees need to do with computers to perform their jobs, users are able to run unknown and/or untrusted code, that is, programs outside of the supported set. As a result, administrators begin to lose control over what software code the enterprise's machines are executing.”), [0004] (“To prevent this, virus protection software is provided. Contemporary virus protection software typically comprises virus scanning engines that operate based on signature-based pattern matching, in which files are scanned for known viruses and design pattern matching strings to characteristically identify instances of that identical virus. One problem with this approach is that it is reactive rather than proactive . . .”), [0007] (“In sum, in contemporary computer systems, running unknown code cannot be prevented, and indeed is necessary to an extent in many enterprises, yet doing so leads to increased support costs in system maintenance and helpdesk time, and decreased user productivity.”), [0008] (“Briefly, the present invention provides an improved computer security system and method wherein software that possibly includes executable code is identified and

classified, and then a rule corresponding to the classification (or if none correspond, a default rule) automatically and transparently determines the software's ability to execute. A set of rules for a machine or user may be maintained in a restriction policy, e.g., in a group policy object distributable over a network, and a restriction policy can be applied per machine and/or per user of a machine. Depending on what the rule specifies for the classification that is determined for any given software module (e.g., software file), the software may execute in a normal (unrestricted) execution environment (context), in a restricted execution environment, or the software may be prevented from running at all.”), [0009] (“The present invention provides various ways to identify/classify software, along with a highly flexible policy-based infrastructure to enforce decisions about whether software can run, and if so, how much the software will be restricted when it runs.”); Bogner at [0004] (“Communication security is often a prime consideration in the design and deployment of extranet applications, especially since extranet communication traffic traverses a public network and since user computers are often not under the control of the organization. Several methods and systems for increasing the security of extranet communication are known in the art.”), [0009] (“Embodiments of the present invention provide a system for communication with a server, the system including:”), [0010] (“a user computer, which is configured to run a first operating environment for performing general-purpose operations, and a second operating environment, which is configured expressly for interacting with the server in a communication session and is isolated from the first operating environment such that the general-purpose operations performed in the first operating environment do not affect operation of the second operating environment; and”), [0011] (“a central management subsystem, which is external to the server and to the user computer and is coupled to monitor the operation of the second operating environment running on the user computer and to control the communication session based on the

monitored operation.”), [0056] (“One of the prime challenges faced by extranet applications is to secure the operating environment of the user computer, i.e., the computer operating system and the different applications and processes it runs.”) [0058] (“In view of the difficulties described above, embodiments of the present invention provide improved methods and systems for establishing and conducting secure communication sessions between user computers and data centers or other servers. In the embodiments that are described hereinbelow, each user computer runs two operating environments that are decoupled, or isolated, from one another. One operating environment, referred to as a Trusted Operating Environment (TOE), is configured expressly for interacting with the data center using the extranet application. The other operating environment, referred to as a General-Purpose Operating Environment (GPOE), runs applications and processes other than the extranet application in question.”); Chen at [0006] (“Some techniques have been developed to mitigate the negative impacts of viruses . . . However, code written for such approaches typically has a performance disadvantage in comparison to executing native code.”), [0040] (“Hence, what is needed is a third level of security 104 that supports the execution of, but also limits the effects of, untrusted programs.”), [0045] (“In summary, existing techniques for executing untrusted program code typically sacrifice some aspects of programmability, safety, operating system portability, and/or performance. One embodiment of the present invention facilitates executing an untrusted native code module safely and securely on a substantially similar set of hardware. This embodiment protects the host process and the rest of the host device from malicious behavior by the untrusted module while providing performance which is substantially similar to native code performance.”); Tome at [0002] (“This invention relates to a trusted host platform that permits a single trusted host platform to simultaneously interface with several disparate security domains, each of which is managed disparately, and which do not share a

common or federated trust model.”), [0003] (“Conventional “trusted networks” include various networks of differing security classifications that meet at a desktop using a single multi-homed compartmented workstation, several workstations, or a thin client computer . . . What is needed is an improved a trusted host platform.”), [0004] (“According to various embodiments of the invention, a trusted host platform operates in an independent network to simultaneously securely connect to and operate on multiple other independent networks (security domains) without exposing the various security domains to each other, while protecting and maintaining separation of data within each security domain. The trusted host platform includes numerous improvements and refinements over extant systems that permit this functionality to be provided less expensively and with higher reliability and levels of assurance.”); Edery at [0005] (“Unfortunately, particularly the Internet and other public networks have also become a major source of potentially system-fatal or otherwise damaging computer code commonly referred to as “viruses.””), [0006] (“Efforts to forestall viruses from attacking networked computers have thus far met with only limited success at best. Typically, a virus protection program designed to identify and remove or protect against the initiating of known viruses is installed on a network firewall or individually networked computer. The program is then inevitably surmounted by some new virus that often causes damage to one or more computers.”), [0007] (“To make matters worse, certain classes of viruses are not well recognized or understood, let alone protected against.”), [0008] (“Accordingly, there remains a need for efficient, accurate and flexible protection of computers and other network connectable devices from malicious Downloadables.”), [0009] (The present invention provides protection systems and methods capable of protecting a personal computer (“PC”) or other persistently or even intermittently network accessible devices or processes from harmful, undesirable, suspicious or other “malicious” operations that might otherwise be effectuated by remotely operable code.

While enabling the capabilities of prior systems, the present invention is not nearly so limited, resource intensive or inflexible, and yet enables more reliable protection.”), [0018] (“Embodiments also provide for determining protection policies that can be downloaded and/or ascertained from other security information (e.g. browser settings, administrative policies, user input, uploaded information, etc.). Different actions in response to different Downloadable operations, clients, users and/or other criteria are also enabled, and embodiments provide for implementing other security measures, such as verifying a downloadable source, certification, authentication, etc. Appropriate action can also be accomplished automatically (e.g. programmatically) and/or in conjunction with alerting one or more users/administrators, utilizing user input, etc.”); Chari at [0002] (“Computer security has become a major concern.”), [0006] (“Thus, there is a need for tight computer security that adequately filters attempts to introduce malicious code, stops unauthorized activity before damage occurs and collects data for analyzing attacks.”), [0007] (“It is a purpose of the invention to protect computer resources from attacks;”), [0010] (“The present invention relates to an intrusion detection system (IDS), method of protecting computers against intrusions and program product therefor. The IDS determines which applications are to run in native environment (NE) and places the remaining applications in a sandbox.”); Field at [0002] (“An unfortunate reality of operating a computer, especially one connected to a network, is that the computer is constantly under attack . . . For purposes of the present invention, these attacks will be generally referred to hereafter as malware.”), [0003] (“As malware is a reality for computers generally, and for network computers in particular, various tools have been devised and deployed to prevent malware from performing its malicious intent on a computer . . . However, the most commonly used tool in protecting a computer against malware is antivirus software.”), [0012] (“Accordingly, as files and/or content are obtained, they could be

tagged with origin information. Still further, it would be beneficial if a computer system could identify the location from which a file or content has been obtained and act upon it according to its trustworthiness as identified in a set of predetermined rules, a white-list of trusted sites, and/or a black-list of untrustworthy sites.”), [0013] (“A computer system for providing enhanced security with regard to obtained files, the computer system is presented. The computer system includes a processor and a memory. Moreover, the computer system further includes a file system. Upon obtaining a file from an external location, the computer system is configured to tag the obtained file with tagging information regarding the origin of the obtained file.”); Iga at [0004] (“According to the conventional technology disclosed in the Patent Reference 1, the application introduced or obtained from the outside is loaded in a memory where access to the outside of the memory is limited or the API call in the application is converted by the conversion code module and, when the call is made, whether or not the application can be executed is checked. That is, the application is executed in the isolated execution environment. By configuring as above, while system resources such as user data, a library, or device driver existing outside of the execution environment are protected, an untrusted application can be executed with safety.”), [0005] (“However, in the above technology disclosed in the patent application, the application introduced or obtained from the outside is allowed to use a library, device driver, or a like only via the API. Every time the API call is made, whether or not the application can be executed is judged by the conversion code module and, therefore, due to overhead incurring at this time of point, execution speed of the application decreases.”), [0006] (“Thus, according to the present invention, it is made possible to provide a program execution control method, program execution control device, and program execution control program which are capable of resolving the conventional technological problems to execute a program containing an untrusted code and to reduce the overhead.”), [0007]

(“The first program execution control method of the present invention is a method of controlling execution of a program on a computer including a step of arranging at least part of each of a device driver, library, and user data provided in the computer in such a way that the part can be referred to from a program running in an execution environment in which access to the outside of the execution environment is limited and of executing the program in the execution environment.”); Kohavi at [0004] (“Threats to the security of an IT infrastructure can be roughly divided into two groups: Intrusions to organizational IT infrastructures, and Information Leakage.”), [0014] (“Existing solutions usually require classification of organizational data and restricting the operations of users when processing confidential data or accessing sensitive sources. However, existing solutions create tradeoffs between protection and usability.”), [0039] (“Furthermore, the methods described hereinabove require a separate set of systems and platforms or well defined regions dedicated for confidential data. The regions have to be well separated and protected from the rest of the network. The regions are limited with respect to using the network's infrastructure and systems.”), [0041] (“According to one aspect of the present invention there is provided an apparatus for securing data, the apparatus comprising: a secure environment definer configured to define a secure environment within an existing user environment, the definer configured to define a boundary about the environment across which data cannot pass and a channel out of the secure environment, the secure environment definer further being configured to define a filter associated with the channel out of the secure environment, the filter being definable to control passage of data out of the secure environment.”); Kshirsagar at 1:12-25 (“Enterprises may use virtual private networks (VPN) to allow employees to securely communicate with servers at an enterprise location. For example, an enterprise may provide a VPN gateway that is coupled to a protected network. An employee using a client device at a remote location may establish a VPN connection to the VPN

gateway through the Internet. Subsequently, the VPN gateway forwards network traffic flowing through the VPN connection to servers on the protected network. In this way, the employee may communicate with servers on the protected network. In some circumstances, it may be advantageous for only certain applications to communicate through the VPN tunnel. For instance, limiting use of the VPN tunnel to certain applications may reduce the processing burden on a VPN gateway.”), 2:12-34 (“In general, the invention is directed to the secure communication of network traffic from specific applications operating on a client device to a server device using a network-layer virtual private network (i.e., a Layer 3 VPN). A module on a client device intercepts application-level network traffic from applications executing on the client device as the network traffic is delivered to the operating system. Based on the application that originated the traffic, the module determines whether to send the network traffic through a network-layer VPN tunnel from the client device to a gateway device or to output the traffic as clear text, i.e., unsecured. Thus, the module makes this determination on an application-by-application basis. In a network-layer VPN tunnel, network-layer packets are encapsulated within packets conforming to a network-layer tunneling protocol. This network-layer VPN tunnel may be defined by a network address of a physical adapter of the client device and a network address of the VPN gateway. The client device forwards the network traffic through the VPN tunnel based on the determination. As a Layer 3 VPN, the techniques provide application-specific security while potentially avoiding the need for the interposition of a VPN proxy on the client device, as is often required by higher-level VPNs.”).

One of skill in the art would also have been motivated to combine the different publications and patents that were authored by employees of a given company or assigned to the same assignee and/or related to the same subject matter. Additionally, one of skill in the art would have been motivated to combine different references that were authored, developed, or invented by the same

individual(s) related to the same subject matter. The common inventor/author/architect of the references demonstrate that they relate to continued work in a common field of effort and continued related developments in that field. One of skill in the art would, therefore, combine the references related to each individual. Additionally, based on the teachings of the references and/or the knowledge of one of ordinary skill, one of skill in the art would have been motivated to combine different references from the same company. For example, a POSITA would have been motivated to combine prior art systems or products (*e.g.*, BlackBerry Devices) with any related or applicable patent or non-patent documentation or literature relating to that system or owned by the same entity, including for the reason that these materials are related. Similarly, one of skill in the art would have been motivated to combine prior art systems or products (*e.g.*, Windows Mobile Devices) with any related or applicable patent or non-patent documentation or literature relating to that system or owned by the same entity, including for the reason that these materials are related.

Further, below are additional motivations to combine prior art for particular claim limitations. The following discussions of specific claim limitations are merely examples and are not limiting. For example, where a POSITA would have been motivated to combine references which together render obvious limitations from the independent claims, a POSITA would have also been motivated to combine said references in such a way as to render obvious various asserted dependent claims. The motivations identified with respect to any one Asserted Patent apply with equal force to any of the other Asserted Patents by virtue of their relationship and similarities.

a. '144 patent

To the extent that any primary reference is deemed not to anticipate a claim for failing to teach a wireless wide area network (“WWAN”) modem, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses a WWAN modem. For example, several prior art references and systems, including at least Hill,

Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, and Durham, as well as the charted systems, disclose WWAN modems. *See* Exs. A-01–A-26; *see also* A-A. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing a security and/or network policy on a device. In addition, wireless wide area networks were well-known as of the critical date, and WWAN modems were commonly used to enable devices to access wireless wide area networks. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include a WWAN modem. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a kernel execution partition, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses a kernel execution partition. For example, several prior art references and systems, including at least Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, and Durham, as well as the charted systems, disclose a kernel execution partition. *See* Exs. A-01–A-26; *see also* A-A. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing a security and/or network policy on a device. In addition,

operating system kernels were well-known as of the critical date, and partitioning was a common technique for increasing security and efficiency of computer systems. Further, it was well-known that a partition could be dedicated to operating system kernel functionalities. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include a kernel execution partition. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a protected execution partition, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses a protected execution partition. For example, several prior art references and systems, including at least Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, and Durham, as well as the charted systems, disclose a protected execution partition. *See* Exs. A-01–A-26; *see also* A-A. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing a security and/or network policy on a device. In addition, as of the critical date, partitioning was a well-known technique for increasing security and efficiency of computer systems. Further, the concept of a “protected” or “trusted” partition—for example, a partition with added security measures—was well-known. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include a

protected execution partition. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach an operating system packet network stack, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses an operating system packet network stack. For example, several prior art references and systems, including at least Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, and Durham, as well as the charted systems, disclose an operating system packet network stack. *See* Exs. A-01–A-26; *see also* A-A. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing a security and/or network policy on a device. In addition, network stacks were well-known and well-understood as of the critical date. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include an operating system packet network stack. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach an application identification agent, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses an application identification agent. For example, several prior art references and systems, including at least Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, and Durham, as well as the charted systems, disclose an application identification agent. *See* Exs. A-01–A-26; *see also* A-A. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing a security and/or network policy on a device. In addition, as of the critical date, it was well-known that security and/or network policy enforcement may include controlling the flow of data to and from applications running on a device. Further, the concept of classifying data traffic based on the applications the data is associated with was well-known as of the critical date. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include an application identification agent. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a service measurement agent, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses an service measurement agent. For example, several prior art references and systems, including

at least Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, and Durham, as well as the charted systems, disclose a service measurement agent. *See* Exs. A-01–A-26; *see also* A-A. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing a security and/or network policy on a device. In addition, as of the critical date, it was well-known that security and/or network policy enforcement may include measuring the amount of data flowing to and from applications running on a device. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include a service measurement agent. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a policy control agent, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses a policy control agent. For example, several prior art references and systems, including at least Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, and Durham, as well as the charted systems, disclose a policy control agent. *See* Exs. A-01–A-26; *see also* A-A. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally

relate to enforcing a security and/or network policy on a device. In addition, the concept of a dedicated application or agent tasked with applying an application-specific network and/or security policy was well-known as of the critical date. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include a policy control agent. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a device agent with a privilege to configure application-specific traffic policy controls, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses a device agent with a privilege to configure application-specific traffic policy controls. For example, several prior art references and systems, including at least Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, and Durham, as well as the charted systems, disclose a device agent with a privilege to configure application-specific traffic policy controls. *See* Exs. A-01–A-26; *see also* A-A. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing a security and/or network policy on a device. In addition, applications and/or agents with privileges to configure traffic policy controls were well-known as of the critical date. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include a device agent with a privilege to configure application-specific traffic policy controls.

A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a device agent with a privilege to receive internet data packet traffic passing between the operating system packet network stack and the WWAN modem, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses such a device agent. For example, several prior art references and systems, including at least Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, and Durham, as well as the charted systems, disclose a device agent with a privilege to receive internet data packet traffic passing between the operating system packet network stack and the WWAN modem. *See* Exs. A-01–A-26; *see also* A-A. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing a security policy and/or network admin policy on a device. In addition, a POSITA would have understood that important data (for instance, data critical to policy enforcement) may be intercepted between a device's WWAN modem and network stack. Further, applications and/or agents with privileges to receive such data passing between a device's WWAN modem and network stack were well-known as of the critical date. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include a device agent with a privilege to receive internet data packet traffic passing between the operating system packet network stack and the WWAN

modem. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach one or more memory partitions, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses one or more memory partitions. For example, several prior art references and systems, including at least Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, and Durham, as well as the charted systems, disclose one or more memory partitions. *See* Exs. A-01–A-26; *see also* A-A. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing a security and/or network policy on a device. In addition, partitioning device memory was a well-known technique as of the critical date. Further, a POSITA would have understood the benefits (*e.g.*, security benefits) associated with partitioning memory and storing program code for different applications in different partitions. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include one or more memory partitions to store program code for the respective processes and agents required by the claims. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a separately-protected device-assisted services partition, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses a separately-protected device-assisted services partition. For example, several prior art references and systems, including at least Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, and Durham, as well as the charted systems, disclose a separately-protected device-assisted services partition. *See* Exs. A-01–A-26; *see also* A-A. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing a security and/or network policy on a device. In addition, as discussed, partitioning device memory was a well-known technique as of the critical date. Further, a POSITA would have understood the benefits (*e.g.*, security benefits) associated with partitioning memory, separately protecting the different partitions, and storing program code for different applications in different partitions. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include a separately-protected device-assisted services partition. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach an access control integrity agent, it would have been obvious to a POSITA

at the time of the invention to combine the primary reference with any of the prior art that discloses an access control integrity agent. For example, several prior art references and systems, including at least Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, and Durham, as well as the charted systems, disclose an access control integrity agent. *See* Exs. A-01–A-26; *see also* A-A. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing a security and/or network policy on a device. In addition, the concept of providing an application or agent with exclusive permission to update program code for the applications and/or agents stored on the device was well-known as of the critical date. Further, a POSITA would have understood the benefits (*e.g.*, security benefits) associated providing such an agent with exclusive permission to update program code and the ability to validate program code. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include an access control integrity agent. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a device-assisted services partition to store device service state information, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses a device-assisted services partition to store device service state information. For example, several prior art references and systems,

including at least Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, and Durham, as well as the charted systems, disclose a device-assisted services partition to store device service state information. *See* Exs. A-01–A-26; *see also* A-A. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing a security and/or network policy on a device. In addition, monitoring and storing device state information was well-known as of the critical date. Further, a POSITA would have understood that monitoring and storing device state information can aid in enforcing a security and/or network policy on a device. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include a device-assisted services partition to store device service state information. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a service control link, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses a service control link. For example, several prior art references and systems, including at least Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, and Durham, as well as the charted systems, disclose a service control link. *See* Exs. A-01–A-26; *see also* A-A. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or

features. For example, a POSITA would understand that each of these references generally relate to enforcing a security and/or network policy on a device. In addition, service control links were well-known and well-understood as of the critical date. Further, a POSITA would have understood that a service control link can be an integral component in a security and/or network policy enforcement system (*e.g.*, a distributed system including both a wireless device and a network service controller). Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include a service control link. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a network service controller, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses a network service controller. For example, several prior art references and systems, including at least Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, and Durham, as well as the charted systems, disclose a network service controller. *See* Exs. A-01–A-26; *see also* A-A. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing a security and/or network policy on a device. In addition, network service controllers were well-known and well-understood as of the critical date. Further, a POSITA would have understood that a network service controller can be an integral component

in a security and/or network policy enforcement system (*e.g.*, enabling management of a security/network policy in a distributed network). Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include a network service controller. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a user-interface agent, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses a user-interface agent. For example, several prior art references and systems, including at least Hill, Freund, Yadav, Wu, Field, Malomsoky, Tonsing '467, Oester, Tokitaka, Sever, Kapoor, Venkatraman, Khemani, Seo, Kitahara, Bajikar '534, Wright '965, and Durham, as well as the charted systems, disclose a user-interface agent. *See* Exs. A-01–A-26; *see also* A-A. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing a security and/or network policy on a device. In addition, user interfaces were well-known and well-understood as of the critical date. Further, a POSITA would have found it beneficial to display security/network policy related information to a user and to allow the user, via the user interface, to modify policy settings. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include a user interface. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the

POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

b. '250 patent

To the extent that any primary reference is deemed not to anticipate a claim for failing to teach storing secure policy information, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses storing secure policy information. For example, several prior art references and systems, including at least Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, as well as the charted systems disclose storing secure policy information. *See* Exs. B-01–B-21; *see also* B-B. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing/implementing a security policy on a device. In addition, secure policy information was well known as of the critical date and commonly used to maintain security and manage service usage while operating a device. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include storing secure policy information. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach an application-specific execution environment policy, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses an application-specific execution environment policy. For example, several prior art references and systems, including at least Owen, Henry, Lambert, Bogner, Chen,

Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Linux Operating Systems, as well as the charted systems disclose an application-specific execution environment policy. *See* Exs. B-01–B-21; *see also* B-B. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing/implementing a security policy on a device. In addition, policies were well known as of the critical date and commonly used to establish security rules. Further, the concept of an “application-specific” policy—for example, a policy for a particular application—was well-known. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include an application-specific execution environment policy. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA’s knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a configurable communication security policy, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses a configurable communication security policy. For example, several prior art references and systems, including at least Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Linux Operating Systems, as well as the charted systems disclose a configurable communication security policy. *See* Exs. B-01–B-21; *see also* B-B. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these

references generally relate to enforcing/implementing a security policy on a device. In addition, communication security policies were well known as of the critical date and were commonly used to establish security rules to secure data communications over a network. Furthermore, the concept of an “configurable” communication security policy—for example, a communication security policy that can be altered—was well-known. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include a configurable communication security policy. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA’s knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach secure stored information, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses secure stored information. For example, several prior art references and systems, including at least Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Linux Operating Systems, as well as the charted systems, disclose secure stored information. *See* Exs. B-01–B-21; *see also* B-B. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing/implementing a security policy on a device. In addition, secure stored information was well known as of the critical date and commonly related to security policies and used to maintain security while operating a device. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include

secure stored information. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a set of multiple device application instances, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses a set of multiple device application instances. For example, several prior art references and systems, including at least Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, as well as the charted systems disclose a set of multiple device application instances. *See* Exs. B-01–B-21; *see also* B-B. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing/implementing a security policy on a device. In addition, device application instances were well known as of the critical date and commonly ran on devices. Further, the concept of “a [] set of multiple device application instances”—for example, a classified group and/or list of multiple device application instances, was well-known. Further, a POSITA would have understood a set of multiple device application instances can be classified such that they will be run in a secure manner. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include a set of multiple device application instances. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the

POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a secure application environment, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses a secure application environment. For example, several prior art references and systems, including at least Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, as well as the charted systems disclose a secure application environment. *See* Exs. B-01–B-21; *see also* B-B. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing/implementing a security policy on a device. In addition, a secure application environment was well known as of the critical date and commonly used to run certain applications in a protected environment. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include a set of multiple device application instances. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a secure tunnel, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses a secure tunnel. For example, several prior art references and systems, including at least Owen, Henry,

Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, as well as the charted systems disclose a secure tunnel. *See* Exs. B-01–B-21; *see also* B-B. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing/implementing a security policy on a device. In addition, a secure tunnel was well known as of the critical date and commonly used to protect data communications over a network. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include a set of multiple device application instances. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA’s knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a network tunnel endpoint, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses a network tunnel endpoint. For example, several prior art references and systems, including at least Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Linux Operating Systems as well as the charted systems disclose a network tunnel endpoint. *See* Exs. B-01–B-21; *see also* B-B. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing/implementing a security policy on a device. In addition, a network tunnel endpoint was well known as of the critical date and commonly used to begin/end the transmission of packets. Further, a POSITA would have

understood that a network tunnel endpoint can be an integral component in a security policy enforcement/implementation system to secure data communications over a network. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include a set of multiple device application instances. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a network path, it would have been obvious to a POSITA at the time of the invention to combine the primary reference with any of the prior art that discloses a network path. For example, several prior art references and systems, including at least Owen, Henry, Lambert, Bogner, Chen, Tome, Edery, Chari, Field, Iga, Kohavi, Kshirsagar, Linux Operating Systems, as well as the charted systems disclose a network path. *See* Exs. B-01–B-21; *see also* B-B. It would have been obvious to a person skilled in the art to incorporate such functionality, components, and/or features. For example, a POSITA would understand that each of these references generally relate to enforcing/implementing a security policy on a device. In addition, a network path was well known as of the critical date and commonly used to route network traffic, including through a secure route or outside a secure route. Thus, design and market forces would have motivated a POSITA to modify any of the primary references to include a set of multiple device application instances. A POSITA would also have had a reasonable expectation of success in making such modifications to any primary reference. A POSITA would have understood that these references, as well as the POSITA's knowledge, disclose interrelated teachings based on

routine technologies and would have been amenable to various well-understood and predictable combinations.

3. Lack of Secondary Indicia of Nonobviousness

Samsung is not aware of any evidence that would tend to establish any secondary considerations of non-obviousness. This lack of evidence further renders the Asserted Claims obvious. Proving any such secondary considerations is Headwater's burden. *See, e.g., ZUP, LLC v. Nash Mfg., Inc.*, 896 F.3d 1365, 1373 (Fed. Cir. 2018) (“[A] patentee bears the burden of production with respect to evidence of secondary considerations of nonobviousness.”). Accordingly, Samsung reserves all rights regarding its full contention in this respect until after Headwater completes its final and binding disclosure of any such evidence and contentions. In the meantime, Samsung notes the complete lack of any such evidence in the record.

Headwater has disclosed no evidence of, and Samsung knows of no viable evidence to suggest:

- **The alleged invention's commercial success.** Indeed, no products are known to practice the Asserted Claims. Headwater stated in its Infringement Contentions that it “is unaware of any devices which may incorporate or reflect the claims of the Asserted Patents.” To the extent Headwater asserts that Samsung's products practice the Asserted Patents, Samsung denies that assertion and incorporates its responses to date and any future contentions, expert reports, and testimony. Further, Samsung knows of no nexus between any commercial success and the Asserted Claims. *See, e.g., Windsurfing Int'l Inc. v. AMF, Inc.*, 782 F.2d 995, 999–1000 (Fed. Cir. 1986) (considerations such as intervening, non-covered technological innovations, popularity of accessories, and advertising expense are all relevant to the nexus determination). If any commercial success is due to any of the concepts discussed in the Asserted Patents, those concepts

are also present in the prior art, as described above, and thus do not support any commercial success that is relevant to the question of obviousness. *See Tokai Corp. v. Easton Enters., Inc.*, 632 F.3d 1358, 1369–70 (Fed. Cir. 2011) (“If commercial success is due to an element in the prior art, no nexus exists.”); *In re Huai-Hung Kao*, 639 F.3d 1057, 1068 (Fed. Cir. 2011) (“Where the offered secondary consideration actually results from something other than what is both claimed and *novel* in the claim, there is no nexus to the merits of the claimed invention.”); *Ormco Corp. v. Align Tech., Inc.*, 463 F.3d 1299, 1312 (Fed. Cir. 2006) (“[I]f the feature that creates the commercial success was known in the prior art, the success is not pertinent.”).

- **Alleged commercial success via licensing.** Headwater has presented no evidence of commercial success via a licensing program.
- **Long felt but unresolved needs.** Headwater has presented no evidence of any long felt and unresolved need.
- **No industry praise.** There is also no evidence of industry praise for the alleged invention of the Asserted Patents or any functionality that allegedly practices the Asserted Patents. To the extent any praise is related to any functionality that allegedly practices the Asserted Patents, that praise is not due to the allegedly novel features of the Asserted Patents, but instead only to features present in the prior art, which is not a sufficient nexus to be relevant to the question of industry praise for purposes of obviousness. *See Muniauction, Inc. v. Thomson Corp.*, 532 F.3d 1318, 1328 (Fed. Cir. 2008). Praise of Samsung’s mobile phones or of certain Google Android features is not praise of the Asserted Patents.

- **Unexpected results.** No evidence of any such unexpected results is known. As discussed above, the concepts contained in the Asserted Claims were already combined in the same manner in the prior art. These prior art systems, as described in the above-referenced exhibits, disclosed the same combination of elements, and the same result of that combination, that are recited in the claims. Thus, there were no unexpected results that arose from combining the well-known elements in the Asserted Claims.
- **The failure of others.** No evidence of any such failure is known.
- **Skepticism by experts.** No experts or person of skill expressed skepticism about implementing the alleged inventions.
- **Teaching away by others.** No evidence of any such teaching is known.
- **Recognition of a problem.** As discussed above, the industry recognized the problem and had already discussed multiple approaches that implemented the Asserted Claims to solve that problem.
- **Copying of the alleged invention by competitors.** No evidence of any such copying is known. *See Amazon.com, Inc. v. Barnesandnoble.com, Inc.*, 239 F.3d 1343, 1366 (Fed. Cir. 2001) (allegedly copied feature must be an embodiment of the patented claims).

V. INVALIDITY UNDER 35 U.S.C. § 112

Headwater has not yet provided a claim construction for many of the terms and phrases that Samsung anticipates will be in dispute. Samsung, therefore, cannot provide a complete list of its § 112 defenses because Samsung does not know whether Headwater will proffer a construction for certain terms and phrases that is broader than, or inconsistent with, the construction that would be supportable by the disclosure set forth in the specification.

Nevertheless, Samsung contends that, at least under Headwater's actual and/or apparent application of the claims, the Asserted Claims are invalid based on inadequate written description and/or a lack of enablement under 35 U.S.C. § 112 ¶ 1, and/or based on indefiniteness under 35 U.S.C. § 112 ¶ 2.

Samsung's aforementioned identification of prior art that anticipates and/or renders obvious particular claim elements, including the attached claim charts, should not be deemed as an admission that any claim element satisfies the requirements of 35 U.S.C. § 112. While Samsung asserts below that a claim is invalid under 35 U.S.C. § 112 (such as because of a failure to particularly point out and distinctly claim the alleged invention, failure to provide written description support in the specification, and/or failure to enable one of ordinary skill in the art to make and use the alleged invention), Samsung has nonetheless provided prior art disclosures that anticipate or render obvious the claim on the assumption that Headwater will contend those claims are definite, are supported by an adequate written description, and are adequately enabled.

A. Lack of Written Description and Enablement Under 35 U.S.C. § 112 ¶ 1

Certain claims in the Asserted Patents are invalid for lack of written description. Section 112 requires that a patent specification "contain a written description . . . of the manner and process of making and using [the invention] in such full, clear, concise and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same." 35 U.S.C. § 112 ¶ 1. A patent's written description "must clearly allow persons of ordinary skill in the art to recognize that [the inventor] invented what is claimed." *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (en banc). The disclosure must "convey[] to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date." *Id.* The level of detail required to satisfy the written description requirement varies depending on the nature and scope of the claims and on the complexity and

predictability of the relevant technology, but a “mere wish or plan” for obtaining the alleged invention does not satisfy the written description requirement. *Novozymes A/S v. DuPont Nutrition Biosciences APS*, 723 F.3d 1336, 1344 (Fed. Cir. 2013). Put another way, “a description that merely renders the invention obvious does not satisfy the requirement.” *Ariad*, 598 F.3d at 1352. Instead, “all the limitations must appear in the specification.” *Lockwood v. Am. Airlines, Inc.*, 107 F.3d 1565, 1572 (Fed. Cir. 1997). Samsung contends that, at least under Headwater’s actual and/or apparent application of the claims, the specifications of at least one or more of the Asserted Patents do not include a sufficient written description supporting the claims. Moreover, Samsung contends that Headwater’s actual and/or apparent application of the Asserted Claims covers a broader scope than is justified and/or supported by the written description provided in the specifications of at least one or more of the Asserted Patents. *Tronzo v. Biomet, Inc.*, 156 F.3d 1154, 1159 (Fed. Cir. 1998); *LizardTech, Inc. v. Earth Res. Mapping, Inc.*, 424 F.3d 1336, 1346 (Fed. Cir. 2005); *ICU Med., Inc. v. Alaris Med. Sys., Inc.*, 558 F.3d 1368 (Fed. Cir. 2009).

Section 112 likewise requires that the specification “enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the” alleged invention. 35 U.S.C. § 112 ¶ 1. A claim is not enabled if, “at the effective filing date of the patent, one of ordinary skill in the art could not practice their full scope without undue experimentation.” *Wyeth & Cordis Corp. v. Abbott Lab’ys*, 720 F.3d 1380, 1384 (Fed. Cir. 2013). “This important doctrine prevents both inadequate disclosure of an invention and overbroad claiming that might otherwise attempt to cover more than was actually invented.” *MagSil Corp. v. Hitachi Glob. Storage Techs., Inc.*, 687 F.3d 1377, 1381 (Fed. Cir. 2012). Samsung contends that, at least under Headwater’s actual and/or apparent application of the claims, the specifications of at least one or more of the

Asserted Patents do not enable any person skilled in the relevant art to make and use the alleged inventions of the Asserted Claims without undue experimentation.

Furthermore, under Headwater's actual and/or apparent application of the claims, the specifications of at least one or more of the Asserted Patents do not enable the broad scope of the Asserted Claims as Headwater asserts. Samsung contends that Headwater's actual and/or apparent application of the Asserted Claims covers a broader scope than is justified, and certainly broader than is enabled in the specifications. As explained below, the specifications of at least one or more of the Asserted Patents have not enabled a person of ordinary skill in the art at the time of the alleged invention to perform the full scope of all Asserted Claims.

Each of the asserted claims below are invalid because, at least to the extent Headwater contends any of the following limitations should be construed to encompass Samsung's accused instrumentalities, the specifications fail to provide written description and/or an enabling disclosure of at least the following limitations:

1. '144 patent

- **Claims 1-18:** "kernel execution partition"
- **Claims 1-18:** "application execution partition"
- **Claims 1-18:** "protected execution partition"
- **Claims 1-18:** "an operating system packet network stack to pass Internet data packet traffic between the WWAN modem and one or more applications executing in the application execution partition"
- **Claims 1-18:** "an application identification agent to classify individual flows of the Internet data packet traffic passing through the stack according to which of the one or more applications is associated with a particular individual flow"
- **Claims 1-18:** "a service measurement agent to measure, for classified individual flows, an amount of the Internet data packet traffic associated with each of the one or more applications"

- **Claims 1-18:** “a policy control agent to apply application-specific traffic policy controls to classified individual flows”
- **Claims 1-18:** “device agents with limited privileges to access processes executing in the kernel execution partition”
- **Claims 1-18:** “privilege to configure application-specific traffic policy controls of the policy control agent”
- **Claims 1-18:** “privilege to receive at least one of internet data packet traffic passing between the operating system packet network stack and the WWAN modem”
- **Claims 1-18:** “traffic information including the measured amount of the Internet data packet traffic associated with each of the one or more applications.”
- **Claims 2, 18:** “device-assisted-services agent to communicate with at least one device agent executed in the protected execution partition”
- **Claims 3, 4, 6-10:** “one or more memory partitions to store program code for the respective processes of the operating system packet network stack, the application identification agent, the service measurement agent, the policy control agent, and the one or more device agents”
- **Claims 3, 4, 6-10:** “one or more processors configured to retrieve the stored program code from the one or more memory partitions to execute the respective processes”
- **Claims 4-5:** “separately protected device-assisted services partition to store the program code for the one or more device agents”
- **Claims 4-5:** “access control integrity agent having exclusive permission to update program code stored in the separately protected device-assisted services partition”
- **Claim 5:** “access control integrity agent further configured to validate the program code for the one or more device agents”
- **Claims 6-10:** “a device-assisted services partition to store device service state information”
- **Claims 6-10:** “device service state information only modifiable by the one or more device agents”
- **Claims 7-10:** “one or more device agents further comprising a service control link configured to securely communicate with a network service controller”
- **Claims 8-10:** “service control link is further configured to receive at least one of the application-specific traffic policy controls from the network service controller”

- **Claims 9-10:** “the service control link is further configured to transmit at least some of the device service state information to the network service controller”
- **Claim 10:** “one or more device agents are further configured to retain the transmitted device service state information until after an instruction is received from the network service controller acknowledging that the device service state information can be deleted”
- **Claim 11:** “one or more device agents further configured to, based on the application-specific traffic policy controls, configure application settings for the one or more applications”
- **Claim 12:** “one or more device agents further configured to calculate, separate from the traffic information, a service usage measurement for the Internet data packet traffic passing between the operating system packet network stack and the WWAN modem”
- **Claim 13:** “one or more device agents further configured to encrypt Internet data packet traffic passing from the operating system packet network stack to the WWAN modem”
- **Claim 14:** “the protected execution partition comprises a secure virtual execution environment”
- **Claim 15:** “the privilege to configure the application-specific traffic policy controls of the policy control agent is an exclusive privilege for one or more of the device agents executed in the protected execution partition”
- **Claims 16-17:** “the WWAN modem comprising a modem execution partition configured to calculate, separate from the traffic information, a service usage measurement for the Internet data packet traffic passing between the operating system packet network stack and the WWAN modem”
- **Claim 17:** “the modem execution partition further comprising a modem control link to communicate the calculated service usage measure to at least one of a network service controller and at least one device agent executed in the protected execution partition”
- **Claim 18:** “a user interface”
- **Claim 18:** “at least one device-assisted-services agent comprising a user-interface agent to display to a user, and allow modification to, at least one policy setting affecting at least one of the application-specific policy controls”

2. '250 patent

- **Claim 1:** “secure policy information”
- **Claim 1:** “application-specific execution environment policy”

- **Claims 1-2:** “configurable communication security policy”
- **Claims 1-2:** “secure stored information”
- **Claim 1:** “first set of multiple device application instances”
- **Claims 1-2:** “first secure application environment”
- **Claims 1-2:** “second set of device application instances”
- **Claims 1-2:** “outside of the first secure application environment”
- **Claims 1-2:** “first secure tunnel”
- **Claim 1:** “network tunnel endpoint”
- **Claims 1-2:** “network data communications to and from device application instances”
- **Claim 2:** “first configuration, which indicates that application instances in the second set of device application instances are not allowed to use the first secure tunnel”
- **Claim 2:** “network path outside of the first secure tunnel”

B. Indefiniteness Under 35 U.S.C. § 112 ¶ 2

35 U.S.C. § 112, ¶ 2 requires that a patent claim “particularly point[] out and distinctly claim[] the subject matter which the applicant regards as his invention.” 35 U.S.C. § 112, ¶ 2. Claim terms that fail to inform those skilled in the art “with reasonable certainty . . . about the scope of the invention” fail the definiteness requirement of 35 U.S.C. § 112, ¶ 2. *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014). Samsung contends that, at least under Headwater’s actual and/or apparent application of the claims, the Asserted Claims of the Asserted Patents fail to distinctly claim what the inventors regard as their alleged invention.

Each of the asserted claims are invalid as indefinite under 35 U.S.C. § 112 because they fail to particularly point out and distinctly claim the subject matter which the applicant regards as his invention. In particular, the following limitations, read in light of the intrinsic evidence, fail to inform those skilled in the art with reasonable certainty about the scope of the claimed inventions:

1. '144 patent

- **Claims 1-18:** “kernel execution partition”
- **Claims 1-18:** “application execution partition”
- **Claims 1-18:** “protected execution partition”
- **Claims 1-18:** “an operating system packet network stack to pass Internet data packet traffic between the WWAN modem and one or more applications executing in the application execution partition”
- **Claims 1-18:** “an application identification agent to classify individual flows of the Internet data packet traffic passing through the stack according to which of the one or more applications is associated with a particular individual flow”
- **Claims 1-18:** “a service measurement agent to measure, for classified individual flows, an amount of the Internet data packet traffic associated with each of the one or more applications”
- **Claims 1-18:** “a policy control agent to apply application-specific traffic policy controls to classified individual flows”
- **Claims 1-18:** “device agents with limited privileges to access processes executing in the kernel execution partition”
- **Claims 1-18:** “privilege to configure application-specific traffic policy controls of the policy control agent”
- **Claims 1-18:** “privilege to receive at least one of internet data packet traffic passing between the operating system packet network stack and the WWAN modem”
- **Claims 1-18:** “traffic information including the measured amount of the Internet data packet traffic associated with each of the one or more applications.”
- **Claims 2, 18:** “device-assisted-services agent to communicate with at least one device agent executed in the protected execution partition”
- **Claims 3, 4, 6-10:** “one or more memory partitions to store program code for the respective processes of the operating system packet network stack, the application identification agent, the service measurement agent, the policy control agent, and the one or more device agents”
- **Claims 3, 4, 6-10:** “one or more processors configured to retrieve the stored program code from the one or more memory partitions to execute the respective processes”

- **Claims 4-5:** “separately protected device-assisted services partition to store the program code for the one or more device agents”
- **Claims 4-5:** “access control integrity agent having exclusive permission to update program code stored in the separately protected device-assisted services partition”
- **Claim 5:** “access control integrity agent further configured to validate the program code for the one or more device agents”
- **Claims 6-10:** “a device-assisted services partition to store device service state information”
- **Claims 6-10:** “device service state information only modifiable by the one or more device agents”
- **Claims 7-10:** “one or more device agents further comprising a service control link configured to securely communicate with a network service controller”
- **Claims 8-10:** “service control link is further configured to receive at least one of the application-specific traffic policy controls from the network service controller”
- **Claims 9-10:** “the service control link is further configured to transmit at least some of the device service state information to the network service controller”
- **Claim 10:** “one or more device agents are further configured to retain the transmitted device service state information until after an instruction is received from the network service controller acknowledging that the device service state information can be deleted”
- **Claim 11:** “one or more device agents further configured to, based on the application-specific traffic policy controls, configure application settings for the one or more applications”
- **Claim 12:** “one or more device agents further configured to calculate, separate from the traffic information, a service usage measurement for the Internet data packet traffic passing between the operating system packet network stack and the WWAN modem”
- **Claim 13:** “one or more device agents further configured to encrypt Internet data packet traffic passing from the operating system packet network stack to the WWAN modem”
- **Claim 14:** “the protected execution partition comprises a secure virtual execution environment”
- **Claim 15:** “the privilege to configure the application-specific traffic policy controls of the policy control agent is an exclusive privilege for one or more of the device agents executed in the protected execution partition”

- **Claims 16-17:** “the WWAN modem comprising a modem execution partition configured to calculate, separate from the traffic information, a service usage measurement for the Internet data packet traffic passing between the operating system packet network stack and the WWAN modem”
- **Claim 17:** “the modem execution partition further comprising a modem control link to communicate the calculated service usage measure to at least one of a network service controller and at least one device agent executed in the protected execution partition”
- **Claim 18:** “a user interface”
- **Claim 18:** “at least one device-assisted-services agent comprising a user-interface agent to display to a user, and allow modification to, at least one policy setting affecting at least one of the application-specific policy controls”

2. '250 patent

- **Claim 1:** “secure policy information”
- **Claim 1:** “application-specific execution environment policy”
- **Claims 1-2:** “configurable communication security policy”
- **Claims 1-2:** “secure stored information”
- **Claim 1:** “first set of multiple device application instances”
- **Claims 1-2:** “first secure application environment”
- **Claims 1-2:** “second set of device application instances”
- **Claims 1-2:** “outside of the first secure application environment”
- **Claims 1-2:** “first secure tunnel”
- **Claim 1:** “network tunnel endpoint”
- **Claims 1-2:** “network data communications to and from device application instances”
- **Claim 2:** “first configuration, which indicates that application instances in the second set of device application instances are not allowed to use the first secure tunnel”
- **Claim 2:** “network path outside of the first secure tunnel”

Samsung’s investigation of grounds of invalidity based upon indefiniteness is ongoing, and Samsung reserves the right to supplement these Contentions.

C. Indefiniteness Under 35 U.S.C. § 112 ¶ 6

Section 112, ¶ 6 allows a patentee to express a claim element “as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof.” 35 U.S.C. § 112, ¶ 6. For such claims, the written description of the patent must disclose with sufficient particularity the corresponding structure for performing the claimed function, and it must clearly link that structure to the claimed function. *Ibormeith IP, LLC v. Mercedes-Benz USA, LLC*, 732 F.3d 1376, 1379 (Fed. Cir. 2013).

Several of the ’144 Patent Asserted Claims are invalid under § 112, ¶ 6 because they contain means-plus-function terms and the ’144 Patent fails to disclose with sufficient particularity the corresponding structure for performing the claimed function.

The following limitations recited in the ’144 Patent Asserted Claims are indefinite in whole, in part or in combination:⁷

Term	Relevant Claim(s)
“application identification agent”	1
“service measurement agent”	1
“policy control agent”	1
“device agents”	1,
“device-assisted-services agent”	2
“access control integrity agent”	4
“user-interface agent”	18

⁷ Listed claims also include all Asserted Claims dependent thereon, even if those claims are not individually listed.

VI. INVALIDITY UNDER 35 U.S.C. § 101

Samsung contends that all claims of the Asserted Patents are invalid under 35 U.S.C. § 101 because the claims are not directed to patent-eligible subject matter. Samsung's contentions that the Asserted Claims are invalid under 35 U.S.C. § 101 do not constitute, and should not be interpreted as, admissions regarding the construction or scope of the claims of the Asserted Patents, or that any of the claims of the Asserted Patents are not anticipated or rendered obvious by prior art.

35 U.S.C. § 101 provides that “[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor[.]” Because abstract ideas form the “basic tools of scientific and technological work,” they are unpatentable subject matter under 35 U.S.C. § 101. *Alice Corp. v. CLS Bank Int’l*, 573 U.S. 208, 216 (2014). The Supreme Court provided a two-part test for assessing patent eligibility under Section 101. *See generally id.*

Under the first step of *Alice* (“Step One”), a court must decide whether the claims are directed to ineligible subject matter, such as an abstract idea. *RecogniCorp, LLC v. Nintendo Co.*, 855 F.3d 1322, 1326 (Fed. Cir. 2017); *Internet Patents Corp. v. Active Network, Inc.*, 790 F.3d 1343, 1346 (Fed. Cir. 2015). To do so, a court examines the claims to determine whether their “character as a whole,” or their “focus,” is an abstract idea. *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016). This examination entails “identify[ing] and defin[ing] whatever fundamental concept appears wrapped up” in the claims. *Accenture Glob. Servs., GmbH v. Guidewire Software, Inc.*, 728 F.3d 1336, 1341 (Fed. Cir. 2013) (internal quotation marks and citations omitted). Once ascertained, the court then determines whether that character is “directed to excluded subject matter,” such as an abstract idea. *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335 (Fed. Cir. 2016) (internal citation omitted). This inquiry often asks whether the claims’

character is directed to “a specific means or method” for improving technology or whether it is simply directed to an abstract end-result. *RecogniCorp*, 855 F.3d at 1326. If the claims are not directed to an abstract idea, the inquiry ends. *Thales Visionix Inc. v. United States*, 850 F.3d 1343, 1349 (Fed. Cir. 2017). To resolve this question, “it is often helpful to ask whether the claims are directed to ‘an improvement in the functioning of a computer,’ or merely ‘adding conventional computer components to well-known business practices.’” *Affinity Labs. of Texas, LLC v. Amazon.com Inc.*, 838 F.3d 1266, 1270 (Fed. Cir. 2016) (quoting *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1338 (Fed. Cir. 2016)). “Generalized steps to be performed on a computer using conventional computer activity are abstract[.]” *RecogniCorp*, 855 F.3d at 1326 (internal quotation marks omitted). And “[c]laims directed to generalized steps to be performed on a computer using conventional computer activity are not patent eligible.” *Affinity Labs.*, 838 F.3d at 1270 (citing *Internet Patents Corp. v. Active Network, Inc.*, 790 F.3d 1343, 1348-49 (Fed. Cir. 2015)).

If the claims, as here, are directed to one or more abstract ideas, then the court advances to the second step of *Alice* (“Step Two”), where the claim elements must be scrutinized “both individually and ‘as an ordered combination’ to determine whether the additional elements ‘transform the nature of the claim’ into a patent-eligible application.” *Enfish*, 822 F.3d at 1354 (quoting *Alice*, 573 U.S. at 217). At Step Two, the court searches for an “‘inventive concept’ sufficient to ‘transform the nature of the claim into a patent-eligible application.’” *RecogniCorp*, 855 F.3d at 1327 (quoting *Alice*, 573 U.S. at 217). To save a patent at Step Two, an inventive concept must be evident in the claims. See *Alice*, 573 U.S. at 221; *Synopsys, Inc. v. Mentor Graphics Corp.*, 839 F.3d 1138, 1149 (Fed. Cir. 2016). The “inventive concept” must also “involve more than performance of well-understood, routine, and conventional activities previously known to the industry.” *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1367 (Fed. Cir. 2018);

Mayo Collaborative Servs. v. Prometheus Labs., Inc., 566 U.S. 66, 73 (2012); *Certain Elec. Devices*, 2020 WL 6441422 at *4. The Federal Circuit’s “precedent is clear that merely adding computer functionality to increase the speed or efficiency of the process does not confer patent eligibility on an otherwise abstract idea.” *Ericsson Inc. v. TCL Commc’n Tech. Holdings Ltd.*, 955 F.3d 1317, 1330 (Fed. Cir. 2020) (citing *Intell. Ventures I LLC v. Capital One Bank (USA)*, 792 F.3d 1363, 1370 (Fed. Cir. 2015)). In addition, limitations that simply restrict the invention to a single field of use or merely add “token post-solution” requirements also fail to impart patentability. *Bilski v. Kappos*, 561 U.S. 593, 612 (2010).

All Asserted Claims are invalid under 35 U.S.C. § 101 because they fail to claim patent-eligible subject matter, including the following claims:

- Claims 1-18 of the ’144 patent; and
- Claims 1-2 of the ’250 patent.

A. Alice Step One: The Asserted Claims Embody Abstract Concepts

At Step One, the court must “identify and define whatever fundamental concept appears wrapped up in the claim.” *Accenture Glob. Servs.*, 728 F.3d at 1341.

The independent claims of the ’144 and ’250 patents relate to wireless device security. The independent claim of the ’144 patent relates to a device enforcing/implementing a network/security policy (*i.e.*, a service usage policy). The independent claim of the ’250 patent relates to a method of enforcing/implementing security policies.

At the most basic level, the Asserted Claims are linked to the same abstract idea of managing information flow and resource allocation, including by simply applying rules, which is a long prevalent human activity. Because the Asserted Claims fail to offer anything more than using generic pre-existing computer functionality to carry out the abstract idea of prioritizing

information flow and resource allocation, the Asserted Claims are abstract at Step One. Detailed subject matter eligibility contentions for the '144 and '250 patents are set forth in Exhibits C-1 and C-2, respectively.

B. Alice Step Two: The Asserted Claims Do Not Recite an Inventive Concept

For a claim to be patent eligible under *Alice* Step Two, “an inventive concept must be evident in the claims,” *RecogniCorp*, 855 F.3d at 1327, and it must provide “significantly more” than the abstract idea itself, *BSG Tech LLC v. Buyseasons, Inc.*, 899 F.3d 1281, 1289-90 (Fed. Cir. 2018). In performing this analysis, a court must scrutinize the claim elements “both individually and ‘as an ordered combination’ to determine whether the additional elements ‘transform the nature of the claim’ into a patent-eligible application.” *Enfish*, 822 F.3d at 1354 (quoting *Alice*, 573 U.S. at 217). Elements that are “well-understood, routine, conventional,” or “purely functional” cannot confer patent-eligibility. *Alice*, 573 U.S. at 225-26 (citation omitted). The Asserted Claims here are implemented on a “wireless end-user device” described in generic terms in the specification, and the allegedly novel functionality is carried out using a generic processor using well-known techniques. Thus, there is no particularized solution to any problem, and nothing that can pass Step 2 of *Alice*. See Exs. C-1, C-2.

The Asserted Claims recite only conventional, well-known components and functionalities, and do not recite any purportedly novel arrangement of those components. As set forth in Exhibits A-01 through B-21, Exhibits A-A through B-B, and/or through applicant-admitted prior art, individually and/or collectively, these features were well known, routine, and/or conventional, and known in the prior art as set forth herein.

VII. Document Production

Pursuant to Patent Rule 3-4, Samsung is concurrently producing the prior art identified in these Invalidity Contentions, but Samsung is not required to produce the prior art in the file histories of the Asserted Patents.

In addition, based on investigations to date, Samsung is concurrently producing and/or making available for inspection source code, specifications, schematics, flow charts, artwork, formulas, or other documentation sufficient to show the operation of any aspects or elements of the Accused Instrumentalities identified by Headwater in its P.R. 3-1(c) chart.

Samsung reserves the right to supplement these productions with additional documentation, in accordance with the Federal Rules of Civil Procedure, the Local Rules, the Court's orders and other applicable rules and statutes.

Dated: January 16, 2025

Respectfully submitted,

By: /s/ Lawrence R. Jarvis
Ruffin B. Cordell
TX Bar No. 04820550
Michael J. McKeon
DC Bar No. 459780
mckeon@fr.com
FISH & RICHARDSON P.C.
1000 Maine Avenue, SW, Ste 1000
Washington, D.C. 20024
Telephone: (202) 783-5070
Facsimile: (202) 783-2331

Thad C. Kodish
GA Bar No. 427603
tkodish@fr.com
Benjamin K. Thompson
GA Bar No. 633211
bthompson@fr.com
Lawrence R. Jarvis
GA Bar No. 102116
jarvis@fr.com
FISH & RICHARDSON P.C.
1180 Peachtree Street NE, Fl. 21
Atlanta, GA 30309
Telephone: (404) 892-5005
Facsimile: (404) 892-5002

Melissa R. Smith
State Bar No. 24001351
Melissa@gillamsmithlaw.com
GILLAM & SMITH, LLP
303 South Washington Avenue
Marshall, Texas 75670
Telephone: (903) 934-8450

ATTORNEYS FOR DEFENDANTS
SAMSUNG ELECTRONICS CO., LTD. AND
SAMSUNG ELECTRONICS AMERICA, INC.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing was served on counsel of record for Plaintiff via electronic mail on January 16, 2025.

/s/ Lawrence R. Jarvis

Lawrence R. Jarvis