Trials@uspto.gov
Tel: 571-272-7822

Paper 11
Date: October 22, 2020

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

SEVEN NETWORKS, LLC,
Patent Owner.

IPR2020-00707
Patent 9,712,476 B2

Before THU A. DANG, KARL D. EASTHOM, and JONI Y. CHANG, *Administrative Patent Judges.*

DANG, *Administrative Patent Judge*.

DECISION
Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background

Apple Inc. ("Petitioner") filed a Petition requesting an *inter partes* review of claims 13–18, and 23–28 (the "challenged claims") of U.S. Patent No. 9,712,476 B2 (Ex. 1001, "the '476 patent"). Paper 2 ("Pet."). SEVEN Networks, LLC ("Patent Owner") filed a Preliminary Response. Paper 7 ("Prelim. Resp.").

Under 37 C.F.R. § 42.4(a), the Board has authority to determine whether to institute an *inter partes* review. Applying the standard set forth in 35 U.S.C. § 314(a), which requires demonstration of a reasonable likelihood that Petitioner would prevail with respect to at least one challenged claim, we grant Petitioner's request and institute an *inter partes* review of all challenged claims.

B. Related Proceedings

Petitioner identifies the '476 patent as the subject of *SEVEN Networks, LLC v. Apple Inc.*, 2:19-cv-00115 (E.D. Tex.). Pet. 72.

C. The '476 Patent

The '476 patent, titled "Secure End-to-End Transport Through Intermediary Nodes," issued on July 18, 2017, from Application No. 15/140,284 filed on April 27, 2016, which is a continuation of Application No. 14/043,772 ("the '772 application") filed on October 1, 2013, now U.S. Patent No. 9,344,393 ("the '393 patent"), which in turn is a continuation of Application No. 13/396,464 ("the '464 application") filed on February 14, 2012, now U.S. Patent No. 8,549,587 ("the '587 patent"), which in turn is a continuation of Application No. 12/889,252 ("the '252 application") filed on September 23, 2010, now U.S. Patent No. 8,127,342 ("the '342 patent"),

which in turn is a continuation of Application No. 11/875,785 ("the '785 application") filed on October 19, 2007, now U.S. Patent No. 7,827,597 ("the '597 patent"), which then in turn is a continuation of Application No. 10/339,369 ("the '369 application") filed on January 8, 2003, now U.S. Patent No. 7,305,700 ("the '700 patent"). Ex. 1001, codes (54), (45), (22), (63). The '476 patent acknowledges security concerns when information is transferred over the Internet, as an eavesdropper may be able to access the data after decryption at intermediary network processing nodes. *See id.* at 1:33–47. Accordingly, the '476 patent addresses this problem. *Id.*

An illustration of one embodiment of the '476 patent's communication network is depicted in Figure 1, reproduced below:

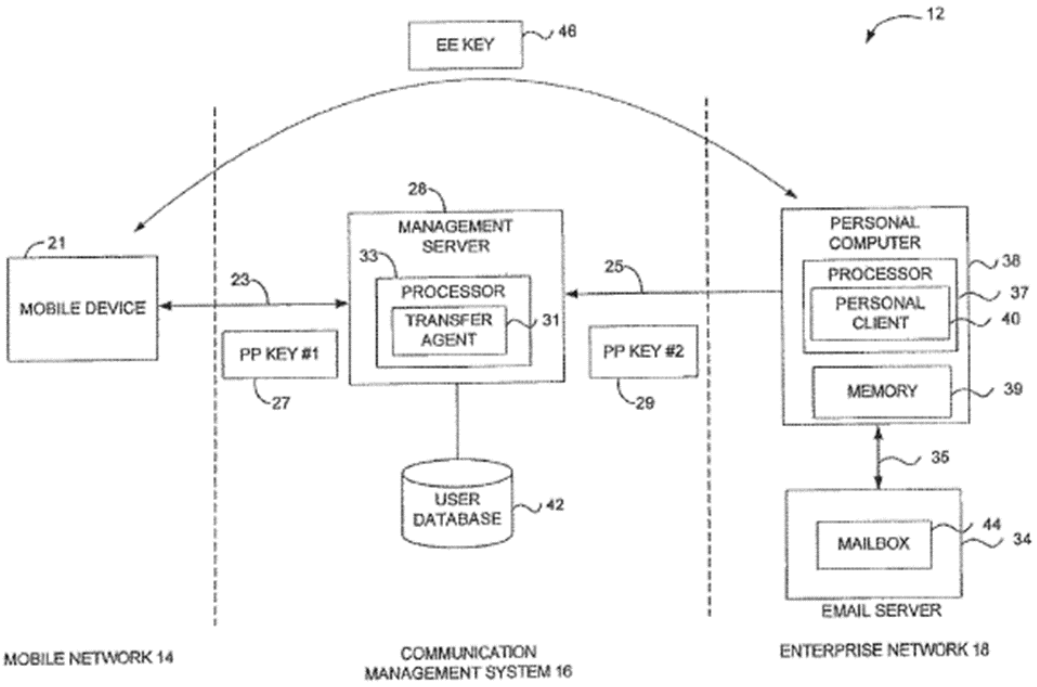

FIG. 1

Figure 1 shows communication network 12 that includes mobile network 14, enterprise network 18, and communication management system 16 that manages communications between mobile network 14 and enterprise network 18. *Id.* at 2:23–27. Mobile network 14 includes mobile devices 21 that communicate with an internet protocol (IP) infrastructure through a wireless or landline service provider, while enterprise network 18 includes email server 34 containing user mailbox 44 accessible using personal computer (PC) 38. *Id.* at 2:27–43. Communication management system 16 includes management server 28 that includes processor 33 operating transfer agent 31, which in turn manages the transactions between mobile devices 21 and enterprise network 18. User database 42 includes configuration information for different users of a mobile communication server. *Id.* at 2:52–59.

As shown in Figure 1, personal client 40 makes outbound connection 25 to management server 28, registers the presence of a particular user to management server 28, and negotiates a security association specifying a cryptographic ciphersuite and unique, secret point-to-point encryption key 29 over connection 25. *Id.* at 2:64–3:3. Further, mobile device 21 negotiates a point-to-point security association, specifying a cryptographic ciphersuite and a unique encryption key 27, with management server 28. *Id.* at 3:10–12.

D. The '785 Application (also "the '597 Patent" or "the Great Great Grandparent Application") (Ex. 2010)

Like the '476 patent, the great great grandparent application addresses security concerns with eavesdroppers being able to access data after decryption at intermediary network processing nodes. *See* Ex. 2010, 1:7–17.

An illustration of an encryption schema of the great great grandparent application is depicted in Figure 5, reproduced below:

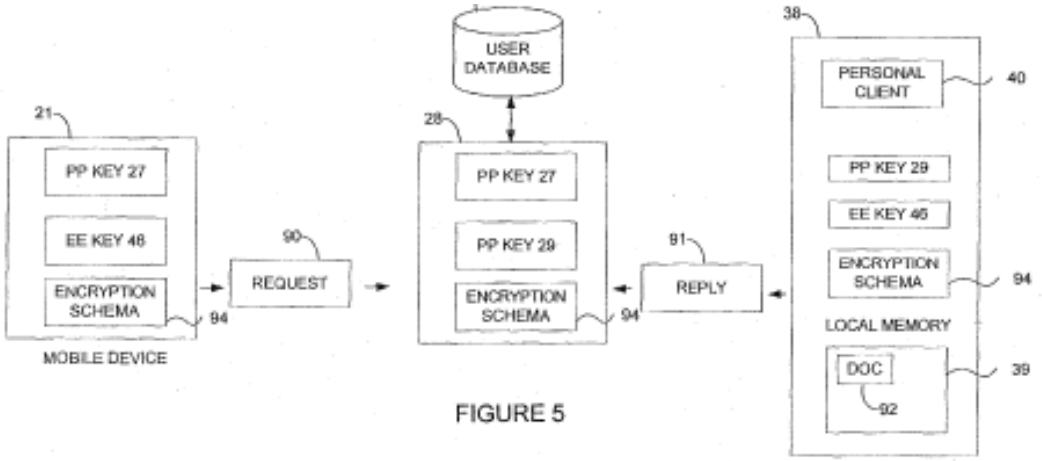

FIGURE 5

Figure 5 shows an encryption schema used by mobile device 21, management server 28, and personal client 40 when processing transactions between a source and a target device. *Id.* at 8:20–22. As shown in Figure 5, mobile device 21 operates as a source for sending transaction 90 requesting personal client 40 to send document 92 located in local memory 39, personal client 40 operates as a target for transaction 90, and management server 28 operates as the transfer agent for transferring transaction 90 from mobile device 21 to personal client 40. *Id.* at 8:22–9:2. Any device can operate as a source or target for the transaction, wherein personal client 40 can operate as a source, and mobile device 21 can operate as a target when transaction 91 is sent as a reply to request 90. *Id.* at 9:6–8.

Mobile device 21 attaches an "auth_token" to a transaction sent to management server 28, wherein mobile device 21 may be required to authenticate to management server 28 by transmitting a username and password, and server 28 issues mobile device 21 an "auth_token" after successfully validating the username and password against information in user database 42. *Id.* at 9:23–10:4. Mobile device 21 then attaches the

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.