UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

APPLE INC.
Petitioner

v.

UNILOC LUXEMBOURG S.A.
Patent Owner

---

Case No. IPR2018-00884
U.S. Patent No. 8,539,552

---

**PETITION FOR *INTER PARTES* REVIEW**
**OF U.S. PATENT NO. 8,539,552**

# TABLE OF CONTENTS

# I. INTRODUCTION

Petitioner Apple Inc. ("Apple" or "Petitioner") requests an *Inter Partes* Review ("IPR") of claims 1-25 (collectively, the "Challenged Claims") of U.S. Patent No. 8,539,552 ("the '552 Patent"). (EX1001).

The '552 Patent discloses a telephony system in which endpoints request certain services and features in call signaling messages. To ensure only authorized services and features are permitted, signaling messages are received and analyzed by non-endpoint network components to ensure the users have subscribed to the requested services and features. As demonstrated by Petitioner below, the purportedly distinguishing feature of the '552 Patent of intercepting signaling messages to authorize requested services and features was present in the prior art.

# II. SUMMARY OF THE '552 PATENT

## A. Description of the Alleged Invention of the '552 Patent

The '552 Patent discloses a telephony network 100, which "support[s] packet-based telephony and multimedia sessions and services. The network 100 includes a core packet network 102, and two local packet networks 104 and 106, as well as intelligent end-user clients 104a-d and 106a-e associated with the local packet networks 104 and 106." '552 Patent (EX1001) at 3:48-54, FIG. 1. The '552 Patent also describes a specific example of the packet-based network, namely IP

network 200, which implements session initiation protocol (SIP) signaling. *Id*. at 4:46-49.

As explained in the '552 Patent, intelligent end-user clients can handle telephony services and features such as signaling and call-control functionality. *Id*. at 1:23-25. This leaves "the carriers and service provider network's responsib[le for] little more than providing data pipes." *Id*. at 1:23-30.

The use of intelligent end-user clients presents the problem, however, that services "may be signaled, controlled, and/or delivered by intelligent end-user clients that are not owned or controlled by the network providers, thereby enabling potential bypassing by the end user of service agreements or other subscription accounting mechanisms." *Id*. at 1:48-55. Thus, the intelligent end-user clients may bypass authorization by the network and provide a service to a subscriber not authorized to receive the service. *Id*. at 2:61–3:7.

To address this problem, the '552 Patent describes a "policy enforcement point" within the network, which "control[s] access to, and invocation of, features and services which may otherwise be delivered to subscribers without the knowledge or authorization of the network." *Id.* at 1:59-60, 3:20-36, 12:50-13:5 (identifying caller ID as a service), 13:6-28 (identifying call waiting and multi-line service as services), 13:66–14:5 (providing additional listing of services that may be authorized in a user (subscriber) profile), Abstract. The subscriber is authorized

to receive certain services, which are documented in the subscriber's profile. *Id*. at 2:8-14, 7:2-7, 13:36-51.

At call setup, the policy enforcement point receives signaling messages and analyzes them to identify services requested in the message. *Id.* at 8:56-58, 11:55-64 (signaling matched against database to identify requested services). Requested services are authenticated and network resources are allocated accordingly, as illustrated in FIG. 3 below:

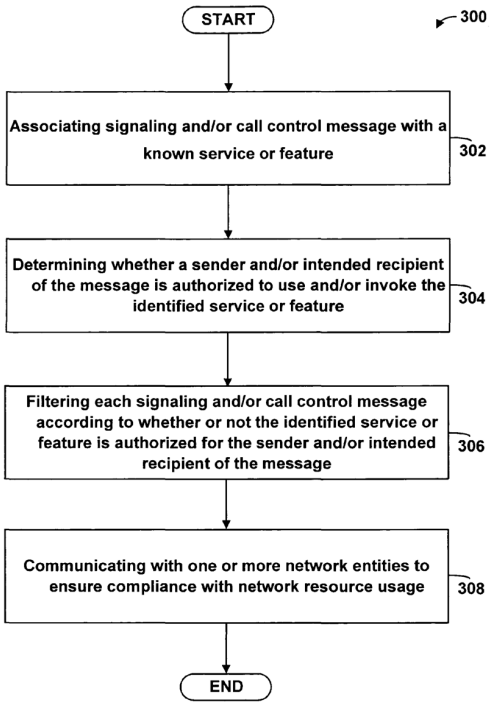


***FIGURE 3***

*See also id*. at 8:60–9:8.

Although the policy enforcement point can be a single physical network component, the '552 Patent explains that "the term policy enforcement point is a

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.