UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION
Petitioner

v.

UNILOC 2017 LLC
Patent Owner

IPR2020-00101
U.S. PATENT NO. 8,495,359

PATENT OWNER PRELIMINARY RESPONSE TO PETITION PURSUANT TO 37 C.F.R. § 42.107(a)

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

Table of Contents

I. INTRODUCTION 1
II. The '359 Patent 1
A. Effective Filing Date of the '359 Patent 1
B. Overview of the '359 Patent 2
C. Prosecution History of the '359 Patent 8
III. RELATED PROCEEDINGS 10
IV. LEVEL OF ORDINARY SKILL IN THE ART 10
V. PETITIONER DOES NOT PROVE A REASONABLE LIKELIHOOD OF UNPATENTABILITY FOR ANY CHALLENGED CLAIM 11
A. Claim Construction Standard 11
B. Overview of Olkin (Ex. 1003) and Kim (Ex. 1004). 12
1. Overview of Olkin (Ex. 1003). 12
2. Overview of Kim (Ex. 1004). 14
C. No proof that sufficient motivation exists to combine the teachings of Olkin (Ex. 1003) with those of Kim (Ex. 1004) 17
D. The Petition does not establish that Olkin (Ex. 1003), Kim (Ex. 1004), or any combination thereof teaches or suggests " a gateway server configured to: … derive an encryption key from the device identifier for the first computing device; [and] send the encryption key to the second computing device" as recited in Claims 1 and 6. 21
E. The Petition does not establish that Olkin (Ex. 1003), Kim (Ex. 1004), or any combination thereof teaches or suggests "a gateway server configured to: … confirm to the first computing device that the encryption key was requested by the second computing device and was sent to the second computing device" as recited in Claims 1 and 6. 25
F. The Petition does not establish that Olkin (Ex. 1003), Kim (Ex. 1004), or any combination thereof teaches or suggests "receiving at the recipient computing device the secured electronic communication, wherein the secured electronic

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

communication is encrypted by a sending computing device with a first encryption key derived from the device identifier by the gateway server" of Claim 11. 30

G. The Petition does not establish that Olkin (Ex. 1003), Kim (Ex. 1004), or any combination thereof teaches or suggests "querying, by the recipient computing device, the gateway server for confirmation that the sending computing device requested the first encryption key" of Claim 11. 31

H. The Petition fails to establish prima facie obviousness of the challenged dependent Claims 2-5, 7-10, and 12-15. 32

VI. CONCLUSION 32

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

I. INTRODUCTION

Pursuant to 35 U.S.C. §313 and 37 C.F.R. §42.107(a), Uniloc 2017 LLC (the "Patent Owner" or "Uniloc") submits its Preliminary Response to the Petition for *Inter Partes* Review ("Pet." or "Petition") of United States Patent No. 8,495,359 ("the '359 Patent" or "Ex. 1001") filed by Microsoft Corporation ("Petitioner") in IPR2020-00101.

In view of the reasons presented herein, the Petition should be denied in its entirety as failing to meet the threshold burden of proving there is a reasonable likelihood that at least one challenged claim is unpatentable.

Uniloc addresses each ground and provides specific examples of how Petitioner failed to establish that it is more likely than not that it would prevail with respect to at least one of the challenged '359 Patent claims.

Accordingly, Uniloc respectfully requests that the Board decline institution of trial on Claims 1-15 of the '359 Patent.

II. THE '359 PATENT

A. Effective Filing Date of the '359 Patent

The '359 Patent is entitled "System and Method For Securing an Electronic Communication." The '359 Patent issued on July 23, 2013, from U.S. Patent Application No. 12/792,249 filed on June 2, 2010, and claiming priority to provisional application 61/219,062, filed on June 22, 2009.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

B. Overview of the '359 Patent

The '359 Patent is directed to a system and method for securing an electronic communication sent to a first computing device from a second computing device using a gateway server. ('359 Patent, column 1, lines 33-37). Generally speaking, the system uses characteristics of a computing device to derive a device identifier (i.e., fingerprint) that uniquely identifies that computing device from among other computing devices on a network. (Id, column 3, line 36 – column 4, line 23). The device identifier is then stored on the computing device as well as on a server, which may be separate from the computing device and is accessible by other computing devices. (Id, column 3, lines 8-10, column 7, lines 20-23). When another computing device desires to send a message to the subject computing device, that other computing device may access an encryption key derived from the device identifier stored on the server, encrypt the message, and transmit the encrypted message to the subject computing device. (Id, column 6, line 61 – column 6, line 13). Due to the strong level of uniqueness provided by the device identifier, the subject computing device can use its internally stored device identifier to decrypt the message. (Id column 4, lines 6-23).

Fig. 3B of the '359 Patent, which illustrates a process that may be used, by the gateway server, to store and distribute device identifiers that can be used to facilitate transmission of an encrypted message from a second computing device to a first computing device is reproduced herein below:

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

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.