Trials@uspto.gov
571-272-7822

Paper 41
Date: May 11, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

---

Case IPR2014-00237
Patent 8,504,697 B2

---

Before MICHAEL P. TIERNEY, KARL D. EASTHOM, and STEPHEN C. SIU, *Administrative Patent Judges.*

EASTHOM, *Administrative Patent Judge*.

# FINAL WRITTEN DECISION
*35 U.S.C. § 318(a) and 37 C.F.R. § 42.73*

# I. BACKGROUND

Petitioner, Apple Inc., filed a Petition (Paper 1,"Pet.") seeking an *inter partes* review of claims 1–11, 14–25, and 28–30 of U.S. Patent No. 8,504,697 B2 (Ex. 1001, "the '697 patent") pursuant to 35 U.S.C. §§ 311–319. After VirnetX, Patent Owner, filed a Preliminary Response (Paper 12), we instituted an *inter partes* review of claims 1–11, 14–25, and 28–30 (Paper 15, "Institution Decision" or "Inst. Dec.").

Subsequent to institution, Patent Owner filed a Patent Owner Response (Paper 30) ("PO Resp."), and Petitioner filed a Reply (Paper 33) ("Pet. Reply") thereto. An Oral Hearing was conducted on February 9, 2015, and then transcribed. *See* Paper 40.

The Board has jurisdiction under 35 U.S.C. § 6(c). This Final Written Decision issues pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73.

For the reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–11, 14–25, and 28–30 of the '697 patent are unpatentable.

## *A. The '697 Patent (Ex. 1001)*

The '697 patent describes secure methods for communicating over the internet. Ex. 1001, 10:7–8. To provide a secure network, the '697 patent system employs proxy domain name servers (DNS). The '697 patent describes conventional DNSs as follows:

> Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP [Internet Protocol] address of a requested computer or host. For example, when a computer user types in the web name "Yahoo.com," the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser

> and then used by the browser to contact the destination web site.

Ex. 1001, 39:32–38.

To set up the secure network or Virtual Private Network ("VPN"), a proxy DNS determines whether the user has requested access to a secure site and may determine whether the user has sufficient security privileges to access that site. Ex. 1001, 40:31–37, 41:6–64. To make both determinations, the proxy DNS provides DNS look-up functions for secure hosts. *Id*. at 40:31–37. The proxy DNS may use a domain name extension or an internal table of sites, or may request security information about the user. *Id*. at 40:31–37, 41:14–27. If the user has requested access and has sufficient security privileges, the proxy DNS requests a gatekeeper to set up a secure communication link by passing a "resolved" address or "hopblocks" for the user and target addresses. *See* Ex. 1001, 40:37–65, Fig. 27. Any of various packet fields can be "hopped," for example, "IP source/destination addresses" or "a field in the header." Ex. 1001, 41:38–39. If the user lacks sufficient security privileges, the system returns a "HOST UNKNOWN" error message. Ex. 1001, Fig. 27.

In essence, the system provides security through anonymity of IP addresses—the proxy server does not send back the true IP address of the target computer. *See* Ex. 1001, 40:1–20. For example, the proxy server may receive the client's DNS request, which forwards it to a gatekeeper, which returns a "resolved" destination address to the proxy based on a "resolved" name, which then forwards the "resolved address" back to the client "in a secure administrative VPN." *See* Ex. 1001, 41:49–56.

*B. Illustrative Claim*

Claim 1 of the '697 patent is reproduced below:

> 1. A method of connecting a first network device and a second network device, the method comprising:
>
> intercepting, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device;
>
> determining, in response to the request, whether the second network device is available for a secure communications service; and
>
> initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service;
>
> wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

*C. Prior Art*

Beser US 6,496,867 B1 Dec. 17, 2002 (Ex. 1009)

S. Kent and R. Atkinson, *Security Architecture for the Internet Protocol*, Request for Comments: 2401, BBN Corp., November 1998 ("RFC 2401") (Ex. 1010).

*D. Instituted Grounds of Unpatentability*

We instituted an *inter partes* review on the following grounds and claims.

| **References** | **Basis** | **Claims Challenged** |
|---|---|---|
| Beser | § 102 | 1–11, 14–25, and 28–30 |
| Beser and RFC 2401 | § 103 | 1–11, 14–25, and 28–30 |

*E. Claim Interpretation*

In an *inter partes* review, the Board construes claim terms in an unexpired patent under their broadest reasonable construction in light of the specification of the patent in which they appear. *In re Cuozzo Speed Techs., LLC*, 778 F.3d 1271, 1281 (Fed. Cir. 2015); 37 C.F.R. § 42.100(b); *Office Patent Trial Practice Guide*, 77 Fed. Reg. 48,756, 48,766 (Aug. 14, 2012). With the exception of slight modifications to some of the terms discussed below, we adopt and incorporate the claim constructions set forth in the Institution Decision. *See* Inst. Dec. 7–15.

*i. Secure Communication Link*

In the Institution Decision, we determined, under the broadest reasonable construction standard, that a "secure communication link," as recited in claims 1 and 16, is "a transmission path that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping." Inst. Dec. 10. Patent Owner argues that the term "secure communication link" must include encryption. *See, e.g.*, PO Resp. 10–19.

Notwithstanding Patent Owner's arguments that security requires encryption, the '697 patent Specification states that "[a] *tremendous variety* of methods have been proposed and implemented to provide security and anonymity for communications over the Internet." Ex. 1001, 1:35–37 (emphasis added). The '697 patent Specification also describes data security and anonymity as counterpart safeguards against eavesdropping that may occur while two computer terminals communicate over the Internet. *See id.* at 1:38–54. Security, in one context, may refer to protection of the data

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.