Trials@uspto.gov
571-272-7822

Paper 7
Entered: April 29, 2019

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

JUNIPER NETWORKS, INC.,
Petitioner,

v.

FINJAN, INC.,
Patent Owner.

Case IPR2019-00060
Patent 7,647,633 B2

Before THOMAS L. GIANNETTI, MIRIAM L. QUINN, and PATRICK M. BOUCHER, *Administrative Patent Judges.*

QUINN, *Administrative Patent Judge.*

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

I. INTRODUCTION

Juniper Networks, Inc. ("Petitioner") filed a Petition to institute *inter partes* review of claims 1, 8, 14, and 19 of U.S. Patent No. 7,647,633 B2 (Ex. 1001, "the '633 patent"). Paper 2 ("Pet."). Finjan, Inc. ("Patent Owner") timely filed a Preliminary Response. Paper 6 ("Prelim. Resp.").

We have jurisdiction under 35 U.S.C. § 314. For the reasons discussed below, we do not institute *inter partes* review of claims 1, 8, 14, and 19 of the '633 patent.

A. Related Matters

The parties indicate that the '633 patent is involved in *Finjan, Inc. v. Juniper Networks, Inc.*, Case No. 3:17-cv-05659-WHA (N.D. Cal.) and other litigations. Pet. 1–2; Paper 3, 1. The '633 patent is also the subject of IPR2018-00391 (the "391 case"), in which a Final Written Decision is pending.

B. The '633 Patent (Ex. 1001)

The '633 patent relates to a system and a method for protecting network-connectable devices from undesirable downloadable operation. Ex. 1001, 1:30–33. The patent describes that "Downloadable information comprising program code can include distributable components (e.g. Java™ applets and JavaScript scripts, ActiveX™ controls, Visual Basic, add-ins and/or others)." *Id.* at 1:60–63. Protecting against only some distributable components does not protect against application programs, Trojan horses, or zip or meta files, which are other types of "Downloadable information." *Id.* at 1:63–2:2. The '633 patent "enables more reliable protection." *Id.* at

2:27–28. According to the Summary of the Invention,

> In one aspect, embodiments of the invention provide for determining, within one or more network "servers" (e.g. firewalls, resources, gateways, email relays or other devices/processes that are capable of receiving-and-transferring a Downloadable) whether received information includes executable code (and is a "Downloadable"). Embodiments also provide for delivering static, configurable and/or extensible remotely operable protection policies to a Downloadable-destination, more typically as a sandboxed package including the mobile protection code, downloadable policies and one or more received Downloadables. Further client-based or remote protection code/policies can also be utilized in a distributed manner. Embodiments also provide for causing the mobile protection code to be executed within a Downloadable-destination in a manner that enables various Downloadable operations to be detected, intercepted or further responded to via protection operations. Additional server/information-destination device security or other protection is also enabled, among still further aspects.

Id. at 2:39–57.

C. Illustrative Claim

Challenged claims 1, 8, and 14 of the '633 patent are independent. Illustrative claim 1 is reproduced below.

> 1. A computer processor-based method, comprising:
>
> receiving, by a computer, downloadable-information;
>
> determining, by the computer, whether the downloadable-information includes executable code; and
>
> based upon the determination, transmitting from the computer mobile protection code to at least one information-destination of the downloadable-information, if the downloadable-information is determined to include executable code.

Id. at 20:54–62.

D. Asserted Prior Art and Grounds of Unpatentability

The Petition identifies the following references in connection with Petitioner's challenge of unpatentability (Pet. 4):

a) *Sonnenberg*: U.S. Patent No. 7,076,650 B1, filed in the record as Exhibit 1005;

b) *Jensen*: *Protection Wrappers: A Simple and Portable Sandbox for Untrusted Applications*, Proceedings on the 8th ACM SIGOPS European Workshop on Support for Composing Distributed Applications, filed in the record as Exhibit 1006;

c) *Hanson*: PCT Application No. WO 98/31124, filed in the record as Exhibit 1008; and

d) *Lemay*: *Teach Yourself Java™ in 21 Days, Professional Reference Edition*, filed in the record as Exhibit 1009.

Petitioner asserts the following grounds of unpatentability based on the aforementioned references (Pet. 4):

Challenged Claim	Basis	References
1, 8, 14, and 19	§ 103(a)	Sonnenberg and Jensen
1 and 8	§ 103(a)	Hanson and Lemay
1, 8, 14, and 19	§ 103(a)	Hanson

Petitioner also relies on a declaration of Seth Nielson, Ph.D., filed as Exhibit 1004 ("Nielson Decl.").

II. DISCUSSION

A. Claim Construction

In an *inter partes* review, claim terms in an unexpired patent are given their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b) (2017);[1] *see Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016). We presume a claim term carries its plain meaning, which is the meaning customarily used by those of skill in the relevant art at the time of the invention. *Trivascular, Inc. v. Samuels*, 812 F.3d 1056, 1062 (Fed. Cir. 2016).

1. "Mobile protection code"

Petitioner asserts that the broadest reasonable interpretation of "mobile protection code" is "code for causing one or more predetermined malicious operations or operation combinations of a Downloadable to be monitored or otherwise intercepted." Pet. 9. Patent Owner asserts that "mobile protection code" means "code that, at runtime, monitors or intercepts actually or potentially malicious code operations without modifying the executable code." Prelim. Resp. 6. According to Patent Owner, the difference between Petitioner and Patent Owner's constructions is that Petitioner's broader construction does not specify that the mobile protection code monitors and intercepts operations *without modifying the executable code*. Prelim. Resp. 7–8.

---

[1] A recent amendment to this rule does not apply here because the Petition was filed before November 13, 2018. *See* Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board, 83 Fed. Reg. 51340 (Oct. 11, 2018) (to be codified at 37 C.F.R. pt. 42).

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.