Exhibit P

Trials@uspto.gov
571-272-7822

Paper 62
Entered: March 15, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC. and SYMANTEC CORP.,
Petitioner,

v.

FINJAN, INC.,
Patent Owner.

Case IPR2015-01979[1]
Patent 8,141,154 B2

Before, THOMAS L. GIANNETTI, RICHARD E. RICE, and MIRIAM L. QUINN, *Administrative Patent Judges.*

QUINN, *Administrative Patent Judge.*

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

[1] This case is joined with IPR2016-00919. Paper 28 ("Decision on Institution of *Inter Partes* Review and Grant of Motion for Joinder," filed by Symantec Corp.).

lexicographer," and "2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution." *See Thorner v. Sony Computer Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012).

If an inventor acts as his or her own lexicographer, the definition must be set forth in the specification with reasonable clarity, deliberateness, and precision. *Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1249 (Fed. Cir. 1998) (citing *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994)). Although it is improper to read a limitation from the specification into the claims, *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993), claims still must be read in view of the specification of which they are a part. *Microsoft Corp. v. Multi-Tech Sys., Inc.*, 357 F.3d 1340, 1347 (Fed. Cir. 2004).

"content"

In our Decision on Institution, we did not construe expressly any claim terms. Dec. 5. During trial, however, Patent Owner proposed a construction of the term "content" as "a data container that can be rendered by a client web browser." PO Resp. 5. Petitioner challenges this construction as unduly narrow in view of the Specification. Reply 6. In particular, Petitioner argues that the Specification does not define the term and provides no "clear disavowal" of claim scope. *Id.* 6–7. According to Petitioner, the Specification and extrinsic evidence support a broader construction of "content" to mean "code." *Id.* at 7–8 (citing Ex. 1001, 12:49–52; Ex. 2005, 80:11–23).

Because they are not consistent with the broadest reasonable interpretation in light of the specification, and as discussed further below, we

do not adopt either of the parties' proposed constructions. Our reasoning follows.

The '154 patent is titled "System and Method for Inspecting Dynamically Generated Executable Code." Ex. 1001, [54]. Although the title refers to "executable code," the term "content" is used elsewhere in the patent when describing the invention. The Abstract further clarifies that a "method for protecting a client computer from dynamically generated malicious *content*, includ[es] receiving at a gateway computer *content* being sent to a client computer for processing, the *content* including a call to an original function[.]" *Id.* Abstract (emphasis added). The gateway computer modifies the "content," which is then transmitted to the client computer for processing there. *Id.*

By way of background, the '154 patent explains that the "ability to run executable code such as scripts within Internet browsers" has caused a new form of viruses "embedded within web pages and other web content, and[, which] begin executing within an Internet browser as soon as they enter a computer." *Id.* at 1:34–40. In particular, the '154 patent describes these new "dynamically generated viruses" as "taking advantage of features of dynamic HTML generation, such as executable code or scripts that are embedded within HTML pages, to generate themselves on the fly at runtime." *Id.* at 3:31–39. Therefore, according to the '154 patent "dynamically generated malicious code cannot be detected by conventional reactive content inspection and conventional gateway level behavioral analysis content inspection, since the malicious JavaScript is not present in the content prior to run-time." *Id.* at 3:65–4:2. The invention, therefore, seeks to protect against "dynamically generated malicious code, in addition

to conventional computer viruses that are statically generated." *Id.* at 4:30–34.

To accomplish this objective, the '154 patent describes the gateway computer receiving "content from a network, such as the Internet, over a communication channel." *Id.* at 8:47–48. The "content may be in the form of HTML pages, XML documents, Java applets and other such web content that is generally rendered by a web browser." *Id.* at 8:48–51; *see also id.* at 13:49–52 ("Such content may be in the form of an HTML web page, an XML document, a Java applet, an EXE file, JavaScript, VBScript, an Active X Control, or any such data container that can be rendered by a client web browser."); 13:49–52. A "content modifier 265" at the gateway modifies "original content received" by the gateway computer and produces modified "content, which includes a layer of protection to combat dynamically generated malicious code." *Id.* at 9:13–16. It does this by scanning the "original content" and identifying certain function calls. *Id.* at 9:16–20. Selected function calls are then replaced with a corresponding substitute function call. *Id.* at 9:21–26.

One example of a function call in the original content is identified as "Document.write ('content that is dynamically generated at run-time')." *Id.* at 11:55–12:2. The original content is modified by replacing the original function call Document.write() with a substitute function call Substitute_document.write(). *Id.* at 10:31–36. The client computer then receives the "content, as modified by the gateway computer." *Id.* at 11:63–64. And it is this modified content that the client computer processes,

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.