UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

FINJAN, INC.,

Plaintiff,

v.

PROOFPOINT, INC., et al.,

Defendants.

Case No. 13-cv-05808-HSG

CLAIM CONSTRUCTION ORDER

Plaintiff Finjan, Inc. filed this patent infringement action against Defendants Proofpoint, Inc. and Armorize Technologies, Inc. The parties seek construction of seven claim terms found in six patents: Patent Nos. 6,154,844 ("the '844 Patent"), 7,058,822 ("the '822 Patent"), 7,647,633 ("the '633 Patent"), 7,975,305 ("the '305 Patent"), 8,141,154 ("the '154 Patent"), and 8,225,408 ("the '408 Patent"). This order follows claim construction briefing, a technology tutorial, and a claim construction hearing.

I. LEGAL STANDARD

Claim construction is a question of law to be determined by the Court. *See Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995). "The purpose of claim construction is to determine the meaning and scope of the patent claims asserted to be infringed." *O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1360 (Fed. Cir. 2008) (internal quotation marks omitted).

Generally, claim terms should be given their ordinary and customary meaning—*i.e.*, the meaning that the terms would have to a person of ordinary skill in the art at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-13 (Fed. Cir. 2005) (en banc). There are only two circumstances where a claim is not entitled to its plain and ordinary meaning: "1) when a patentee sets out a definition and acts as his own lexicographer, or 2) when the patentee disavows

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

When construing claim terms, the Federal Circuit emphasizes the importance of intrinsic evidence such as the language of the claims themselves, the specification, and the prosecution history. *Phillips*, 415 F.3d at 1312-17. The claim language can "provide substantial guidance as to the meaning of particular claim terms," both through the context in which the claim terms are used and by considering other claims in the same patent. *Id.* at 1314. The specification is likewise a crucial source of information. Although it is improper to read limitations from the specification into the claims, the specification is "the single best guide to the meaning of a disputed term." *Id.* at 1315 ("[T]he specification is always highly relevant to the claim construction analysis. Usually, it is dispositive.") (internal quotation marks omitted); *see also Merck & Co. v. Teva Pharms. USA, Inc.*, 347 F.3d 1367, 1371 (Fed. Cir. 2003) ("[C]laims must be construed so as to be consistent with the specification.").

Despite the importance of intrinsic evidence, courts may also consider extrinsic evidence—technical dictionaries, learned treatises, expert and inventor testimony, and the like—to help construe the claims. *Phillips*, 415 F.3d at 1317-18. For example, dictionaries may reveal what the ordinary and customary meaning of a term would have been to a person of ordinary skill in the art at the time of the invention. *Frans Nooren Afdichtingssystemen B.V. v. Stopaq Amcorr Inc.*, 744 F.3d 715, 722 (Fed. Cir. 2014) ("Terms generally carry their ordinary and customary meaning in the relevant field at the relevant time, as shown by reliable sources such as dictionaries, but they always must be understood in the context of the whole document—in particular, the specification (along with the prosecution history, if pertinent)."). Extrinsic evidence is, however, "less significant than the intrinsic record in determining the legally operative meaning of claim language." *Phillips*, 415 F.3d at 1317 (internal quotation marks omitted).

II. AGREED TERMS

The parties have agreed to the construction of the following terms:

Claim Term	Agreed Claim Construction

downloadable	an executable application program, which is downloaded from a source computer and run on the destination computer
security context	an environment in which a software application is run, which may limit resources that the application is permitted to access or operations that the application is permitted to perform
CODE-A	potentially malicious executable code
CODE-B	executable wrapper code
CODE-C	combined code

See Dkt. No. 117. In light of the parties' agreement on the construction of these terms, the Court adopts the parties' constructions.

III. DISPUTED TERMS

A. '822 and '633 Patents

The '822 and '633 Patents share the same specification and are titled "Malicious Mobile Code Runtime Monitoring System and Methods." The inventions provide protection from "undesirable downloadable operation." '822 Patent at 1:25-29; '633 Patent at 1:30-33. Embodiments of the invention provide "for receiving downloadable-information and detecting whether the downloadable-information includes one or more instances of executable code." '822 Patent at 5:34-39. Where there is executable code, the invention provides

> **mobile protection code** ("MPC") and downloadable protection policies to be communicated to, installed and executed within one or more received **information destinations** in conjunction with a detected-Downloadable. Embodiments also provide, within an information-destination, for detecting malicious operations of the detected-Downloadable and causing responses thereto in accordance with the protection policies. . . .

Id. at 5:44-51 (emphases added). The parties dispute the meaning of the two bolded phrases.

1. "mobile protection code"

Finjan's Construction	Proofpoint's Construction

code capable of monitoring or intercepting potentially malicious code	code communicated to at least one information-destination that, at runtime, monitors or intercepts actually or potentially malicious code operations

The parties agree that "mobile protection code" is not a term known in the art. Dkt. No. 142 at 5; Dkt. No. 170 at 57. Accordingly, the intrinsic record is the best evidence of the term's meaning. *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996) ("[A] patentee may choose to be his own lexicographer and use terms in a manner other than their ordinary meaning, as long as the special definition of the term is clearly stated in the patent specification or file history.").

In support of its construction, Plaintiff directs the Court to a portion of the specification indicating that "[t]he sandboxed package includes mobile protection code ("MPC") for causing one or more predetermined malicious operations or operation combinations of a Downloadable to be monitored or otherwise intercepted." '822 Patent at 3:6-10. Plaintiff argues that this passage provides an "explicit definition" of the term MPC, and demonstrates that MPC must merely be capable of monitoring or intercepting potentially malicious code. Dkt. No. 142 at 6.

Defendants' construction adds two limitations: (1) that MPC must monitor or intercept actually or potentially malicious code "at runtime" (*i.e.*, that is, monitoring potentially malicious code as the code is being executed), Dkt. No. 143 at 1-3, and (2) that MPC is "code communicated to at least one information-destination," *id.* at 4-5.

a. "at runtime"

The claims describe the execution of MPC as corresponding to "attempted operations" of the executable code at a downloadable-information destination. *See* '822 Patent at 22:63-67 (Claim 16); *id.* at 23:41-45 (Claim 27); '633 Patent at 22:1-5 (Claim 14); *id.* at 22:17-22 (Claim 20). Claim 28 of the '633 Patent describes the MPC receiving "operations attempted by the Downloadable" and "initiating, by the MPC on the computer, a protection policy corresponding to the attempted operation." '633 Patent at 22:55-63. And Claim 41 of the '633 Patent describes how the MPC initiates a "protection policy corresponding to the attempted operation." *Id.* at

24:30-34.[1] The Court finds that the claims' consistent description of correspondence with "attempted operations" by the downloadable indicates an "at runtime" limitation.

The specifications support this "at runtime" construction. First, the title of the patents is "Malicious Mobile Code **Runtime** Monitoring Systems and Methods." (emphasis added). The reference to "runtime" also is made in the first sentence of the "Detailed Description": "In providing malicious mobile code **runtime** monitoring systems and methods, embodiments of the invention enable actually or potentially undesirable operations of even unknown malicious code to be efficiently and flexibly avoided." '822 Patent at 5:30-31; '633 Patent at 5:30-31 (emphasis added).

Second, the specifications' description of when MPC is generated and initiated provides further support. The action generator generates MPC only when the protection engine determines that received downloadable information includes executable code, *see* '822 Patent at 9:24-26, 30-34; 12:18-65; Figs. 3 and 4. Upon such a determination, the protection engine "causes [MPC] to be communicated to the Downloadable-destination" by way of the transfer engine. *Id.* at 9:63-67; 14:38-43; 16:15-22. Figure 11 is instructive with regard to MPC's protection method within the destination device. MPC installs its elements and policies in the device and "forms an access monitor or 'interceptor' for monitoring or 'intercepting' downloadable destination device access attempts within the destination device." *Id.* at 20:21-30. When the monitored or intercepted information indicates that the downloadable is attempting to access the device in an undesirable way, MPC executes the protection policies. *Id.* at 20:33-40; *see also id.* at 20:54-56 (noting that MPC applies "suitable policies in accordance with an access attempt by a Downloadable"); *id*. at 18:42-47 (discussing MPC's resource access analyzer component "[d]uring downloadable operation").

The exemplary application of a sandbox package is further instructive:

> Upon receipt of sandboxed package by a compatible browser, email or other destination client and activating of the package by a user or

[1] *See also* '822 Patent at 24:5-11 (Claim 28) (describing the execution of MPC as "such that one or more operations of the executable code at the destination, if attempted, will be processed by the [MPC]."); *see also* '822 Patent at 24:39-43; '633 Patent at 22:28-34, 46-51; *Id.* at 23:21-28.

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.