IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

THE TRUSTEES OF COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK,

Plaintiff,

v.

SYMANTEC CORPORATION,

Defendant.

Civil Action No. 3:13-CV-808

JURY TRIAL DEMANDED

MEMORANDUM ORDER

THIS MATTER is before the Court on Plaintiff's Motion for Clarification of Claim Construction Order ("Motion") (ECF No. 128). Defendant filed a brief opposition on October 10, 2014. The parties have waived oral argument on this matter. Therefore, the issue is ripe for disposition. The Motion is hereby GRANTED and the Claim Construction Order issued on October 7, 2014 ("Order") (ECF No. 123) is clarified below.

On October 9, 2010, Columbia filed the instant Motion asking the Court to clarify its Order with respect to the terms "probabilistic model of normal compute system usage" in the '084/'306 patents and "anomalous" in the '115/'322 patents. This Court's Order defined "probabilistic model of normal computer system usage" as a "[m]odel of typical attack-free computer system usage that employs probability." The Court defined "anomalous" as "[d]eviation/deviating from a model of typical, attack-free computer system usage." Specifically, Columbia now seeks clarification on whether the Court intended its construction to mean that the claimed model may be generated with normal data and also attack data or whether the model must be generated with *only* "typical, attack free" data. In the claim construction briefs, Columbia argued the former interpretation, while Symantec argued the latter.

As an initial matter, the Court notes that its Order construed the specific disputed terms that were originally presented in the parties' claim construction briefs. Columbia now seeks a further interpretation of the disputed terms to answer the question Columbia posed at the claim construction hearing, that is, "What information is used to construct the model?" (*See* Tr. Markman Hr'g 75:13–14.) Despite not originally requesting a construction of such issue, the Court chooses to now clarify its ruling with respect to this question. *See U.S. Surgical Corp. v. Ethicon, Inc.*, 103 F.3d 1554, 1568 (Fed. Cir. 1997) (emphasis added) ("Claim construction is a matter of resolution of disputed meanings and technical scope, to *clarify* and when necessary to explain what the patentee covered by the claims, for use in the determination of infringement.").

"Anomaly detectors . . . do not operate by looking for malicious activity directly. Rather, they look for deviations from normal activity." ('084 patent at 7:47–49.) Claim 1 of the '084 patent mirrors this concept: "[A]nalyzing features from a record of a process that accesses the operating system registry *to detect deviations from normal computer system usage to determine whether the access to the operating system registry is an anomaly*." (*Id.* at 22:30–34) (emphasis added). Logically, if the anomaly detection systems detect *deviations* from normal activity, that normal activity must be "attack-free" activity. Applying this logic to the rest of claim 1, which gathers "features from records of *normal* processes" and then *generates* "a probabilistic model of normal computer system usage based on [those] features," it follows that the model is generated with only attack-free data.

Let the Clerk send a copy of this Order to all counsel of record

It is SO ORDERED.

________________/s/________________
James R. Spencer
Senior U. S. District Judge

ENTERED this ___23rd___day of October 2014.