United States District Court
For the Northern District of California

1

2

3

4

5   UNITED STATES DISTRICT COURT

6   NORTHERN DISTRICT OF CALIFORNIA

7

8   FORTINET, INC.,   No. C-13-5831 EMC

9   Plaintiff,

                                                   CLAIM CONSTRUCTION ORDER
10   v.

11   SOPHOS, INC., *et al.*,

12   Defendants.
      _____/

13

14

15   **I.   INTRODUCTION**

16   Plaintiff, Fortinet, Inc. ("Fortinet") has filed this action against Defendants, Sophos Inc. and

17   Sophos LTD ("Sophos"). Currently pending before the Court are the parties' claim construction

18   briefs.

19   **II.   FACTUAL & PROCEDURAL BACKGROUND**

20   Fortinet is a company that specializes in providing "network security appliances and unified

21   threat management solutions." Fortinet, Inc.'s First Amended Complaint ("FAC"), Docket No. 9 ¶

22   23. Sophos is a company that provides a variety of technology security services, including network

23   security and "threat intelligence." *See* Sophos's Amended Answer ("AA"), Docket No. 71 ¶13. In

24   its complaint, Fortinet set out several claims of patent infringement against Sophos, including

25   allegations that Sophos infringed a number of their patents, including the '430 and '125 patents.

26   FAC ¶¶103, 130. Both of those patents relate to network security solutions, including application

27   "whitelisting" and protecting computer systems from harmful software. Mot. at 1. Sophos counter-

28

1 claims that Fortinet is infringing seven of its patents, including the '587, '852, '050 and '344

2 patents. AA at 30-44.

3   All of the patents involved in this dispute relate to online security systems. At bottom, each

4 side is accusing the other of practicing their inventions in the online and network security space.

5   **III.   DISCUSSION**

6 A.   Legal Standard

7   Claim construction is a question of law to be determined by the Court. *See Markman v.*

8 *Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) ("hold[ing] that in a case tried to a

9 jury, the court has the power and obligation to construe as a matter of law the meaning of language

10 used in the patent claim"). "The purpose of claim construction is to determine the meaning and

11 scope of the patent claims asserted to be infringed." *O2 Micro Int'l Ltd. v. Beyond Innovation Tech.*

12 *Co.*, 521 F.3d 1351, 1360 (Fed. Cir. 2008) (citation and quotation marks omitted). Words of a patent

13 are generally given the "ordinary and customary meaning" they would have to a person of ordinary

14 skill in the art who had reviewed the intrinsic record at the time of the invention. *Phillips v. AWH*

15 *Corp.*, 415 F.3d 1303, 1312-13 (Fed. Cir. 2005) (*en banc*). "In some cases, the ordinary meaning of

16 claim language . . . may be readily apparent even to lay judges, and claim construction in such cases

17 involves little more than the application of the widely accepted meaning of commonly understood

18 words." Moreover, elements that are not technical terms of art may not need to be construed at all.

19 *Brown v. 3M*, 265 F.3d 1349, 1352 (Fed. Cir. 2001).

20   However, in many cases, the meaning of a claim term as understood by persons of skill in the

21 art is not readily apparent. In those cases, the court looks to "sources available to the public that

22 show what a person of skill in the art would have understood disputed claim language to mean."

23 *Phillips*, 415 F.3d at 1313. Those sources include intrinsic evidence (the claims, specification, and

24 prosecution history) and extrinsic evidence (*e.g.*, dictionary definitions and treatises) concerning

25 relevant scientific principles and the meaning of technical terms. *Id.* at 1314; *Vitronics Corp. v.*

26 *Conceptronic, Inc.*, 90 F.3d 1576, 1582-83 (Fed. Cir. 1996).

27   "[I]ntrinsic evidence is the most significant source of the legally operative meaning of

28 disputed claim language." *Id*. Extrinsic evidence should be considered, but is less reliable and

2

less significant than intrinsic evidence. *Id.* at 1317-18. As such, a "court should look first to the intrinsic evidence of record" before consulting any extrinsic evidence. *Liquid Dynamics Corp. v. Vaughan Co., Inc.*, 355 F.3d 1361, 1367 (Fed. Cir. 2004) (quoting *Vitrionics*, 90 F.3d at 1582).

Generally, embodiments from the specification should not be imported into the claims as limitations. *Toshiba Corp. v. Imation Corp.,* 681 F.3d 1358, 1369 (Fed. Cir. 2012) ("We do not read limitations from the specification into claims."). "There are only two exceptions to this general rule: (1) when a patentee sets out a definition and acts as his own lexicographer, or (2) when the patentee disavows the full scope of the 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).

B.   "worker module"

Fortinet	Sophos	Court
Plain and ordinary meaning	A module having at least two data ports and a switch port	Plain and ordinary meaning

"Worker module" appears in claims 1, 5, 8, 11, 14, 15, 27, and 30 of the '430 patent. Those claims provide:

Claim 1:   A method for processing network traffic data, comprising: receiving network traffic data; and passing the network traffic data to one of a plurality of **worker modules** for processing the network traffic data;

Claim 5:   The method of claim 1, further comprising using the one of the plurality of **worker modules** to perform stateful inspection, intrusion detection, or antivirus.

Claim 8:   The method of claim 7, further comprising mapping an IO port from which the network traffic data is received with a logical interface of the one of the plurality of **worker modules**.

Claim 11:   The method of claim 10, wherein the step of passing the network traffic data from the one of the plurality of **worker modules** to another one of the plurality of **worker modules** is performed based on the value.

Claim 14:   A system for processing network traffic data, comprising: The method of claim 16, wherein the step of passing is performed by the IO module.
means for receiving network traffic data; and means for passing the network traffic data to one of a plurality of **worker modules** for processing the network traffic data; wherein the means for passing is configured to perform the step of passing based at least in part on a quantity of the **worker modules**; and wherein each of the **worker modules** has an identification number, and the means for passing passes the network traffic data based on a matching between a value and the identification number of one

3

of the **worker modules**, the value obtained using an IP address associated with a receiver of the network traffic data. A computer product having a set of stored.

Claim 15: A computer product having a set of stored instructions, an execution of which causes a process to be performed, the process comprising: receiving network traffic data; and passing the network traffic data to one of a plurality of **worker modules** for processing the network traffic data; wherein the step of passing is performed based at least in part on a quantity of the **worker modules**; and wherein each of the **worker modules** has an identification number, and the network traffic data is passed based on a matching between a value and the identification number of one of the **worker modules**, the value obtained using an IP address associated with a receiver of the network traffic data.

Claim 27: A system for processing network traffic data, comprising:
a first IO module; a second IO module; a first **worker module** coupled to the first and second IO modules; a second **worker module** coupled to the first and second IO modules; and a switch module coupled to the first IO module, the second IO module, the first **worker module**, and the second **worker module**; wherein the first IO module comprises a first IO port, and a first distribution port communicatively coupled to the first **worker module**; and wherein the first **worker module** comprises a first data port and a second data port, the first distribution port of the first IO module communicatively coupled to the first data port of the first **worker module**, and the second data port of the first **worker module** communicatively coupled to a distribution port of the second IO module.

Claim 30: The system of claim 27, wherein the first IO module is configured to pass network traffic data to the first or the second **worker module** based on a number associated with an IP address.

The parties' basic dispute is whether the term "worker"[1] should be construed to mean "having at least two data ports".[2] Sophos argues that it should; Fortinet argues that the plain meaning is sufficient.

The Court finds that the term "worker," as used to modify a module in the '430 patent does not have a special or technical meaning. Neither party, in their papers nor at the hearing, provided a definition for this term that goes beyond designating a module. Moreover, having reviewed the claims and specification, the Court does not find any indication that the term "worker" does more than designate a particular module, among other modules; no peculiarized task is evident from the claims and specifications. Thus, the Court declines to construe a term which effectively functions as a generic descriptor.

---

[1] The term "module" is undisputed.

[2] The parties do not dispute that a "worker module" has a switch port.

4

1   Sophos's attempt to clarify the meaning of "worker" is unhelpful. The thrust of Sophos's

2   argument is that because worker modules are modules that must have two data ports, the term

3   "worker module" must mean "module with at least two data ports." In particular, Sophos argues that

4   a "worker module" should be construed as having two data ports because (1) the specification

5   indicates such; and (2) the function of the worker module necessitates at least two ports. Both

6   arguments lack merit.

7   First, Sophos points to a portion of the specification that provides: "[i]n further

8   embodiments, worker modules can each have more than two data ports." '403 at 3:56-58.

9   According to Sophos, this statement evidences an expectation that a worker module have *at least*

10   two data ports. However, as noted above, statements in the specification should not be read to limit

11   the claim language unless a patentee (1) sets out a definition and acts as his own lexicographer; or

12   (2) clearly disavows the full scope of the claim term in the specification. *Thorner,* 669 F.3d at 1365;

13   *see also SciMed Life Sys., Inc. v. Advanced Cardiovascular Sys., Inc.*, 242 F.3d 1337, 1341

14   (Fed.Cir.2001). Neither exceptions apply here. Sophos does not contend that the patentee was

15   acting as a lexicographer, but seems to argue that the above cited language constitutes a "clear

16   disavowal" of a worker module with one port. The Court disagrees. Far from mandating a

17   minimum of two ports, the specification only says each worker module "can" have more than two

18   ports. This language at best evidences a mere expectation that a worker module will have two data

19   ports. An expectation is not a "clear disavowal" of the full scope of the claims and thus the Court

20   will not import that expectation into a claims limitation.

21   Sophos's second argument is that the Court should construe a worker module to have two

22   data ports because two data ports are required to carry out the described function of a worker

23   module. Specifically, Sophos argues that because the worker module must handle both inbound and

24   outbound data traffic, it must have two different data ports. The problem with this implied-by-

25   necessity argument is that it ignores the possibility of bi-directional data ports – *i.e. one* data port

26   that can handle both inbound and outbound data traffic. Sophos fails to provide any evidence that

27   bi-directional ports were unknown or even uncommon at the time that the '403 patent's issuance.

28   Absent such a showing, two data ports are not necessarily implied by a requirement that a module

5

1 handle both inbound and outbound data traffic. Accordingly, Sophos's second argument fails as

2 well.

3   Having found Sophos's proposed construction untenable, and finding no construction helpful

4 in clarifying the meaning of the term "worker module," the Court declines to construe the term

5 beyond its plain and ordinary meaning.

6 C.   "flow-based packet classification"

Fortinet	**Sophos**	**Court**
Plain and ordinary meaning	Classifying a packet based on fields of an LQ header and of the L3/L4 headers	Plain and ordinary meaning

12   "Flow-based packet classification" appears in claims 1, 3 and 5 of the '125 patent. Those

13 claims provide:

Claim 1:   establishing a flow cache having a plurality of entries each identifying one of a plurality of virtual router (VR) flows through a VR-based network device and corresponding forwarding state information; receiving a packet at an input port of a line interface module of the VR-based network device; the line interface module forwarding the packet to a virtual routing engine (VRE); the VRE determining one or more appropriate packet transformations for application to the packet by performing **flow-based packet classification** on the packet; using a result of the **flow-based packet classification** to retrieve an entry of a plurality of entries of the flow cache; on a flow cache hit, determining, based on the corresponding forwarding state information of the retrieved flow cache entry, whether to process the packet with a virtual service engine (VSE) of the VR-based network device; on a packet flow cache miss, identifying the existence of a new VR flow and upon successful allocation of a new entry of the packet flow cache for the new VR flow, forwarding the packet to software on the processor for flow learning.

Claim 3:   An article of manufacture comprising a computer-readable medium encoded with one or more computer programs, which when executed by one or more processors of a virtual router (VR)-based network device cause the one or more processors to perform a method comprising: establishing a flow cache having a plurality of entries each identifying one of a plurality of VR flows through the VR-based network device and corresponding forwarding state information; receiving a packet at an input port of a line interface module of the VR-based network device; the line interface module forwarding the packet to a virtual routing engine (VRE); the VRE determining one or more appropriate packet transformations for application to the packet by performing **flow-based packet classification** on the packet; using a result of the **flow-based packet classification** to retrieve an entry of a plurality of entries of the flow cache; on a flow cache hit, determining, based on the corresponding forwarding state information of the retrieved flow cache entry, whether to process the packet with a virtual service engine (VSE) of the VR-based network device; on a packet flow cache

6

1   miss, identifying the existence of a new VR flow and upon successful allocation of a
2   new entry of the packet flow cache for the new VR flow, forwarding the packet to
     software on the processor for flow learning.

3   **Claim 5:**   A virtual router (VR)-based network device comprising: a means for establishing a
4   flow cache having a plurality of entries each identifying one of a plurality of virtual
     router (VR) flows through a VR-based network device and corresponding forwarding
5   state information; a means for receiving a packet at an input port of a line interface
     module of the VR-based network device and for forwarding the packet to a virtual
6   routing engine (VRE); a means associated with the VRE for determining one or more
     appropriate packet transformations for application to the packet by performing **flow-
7   based packet classification** on the packet; a means for using a result of the **flow-
     based packet classification** to retrieve an entry of a plurality of entries of the flow
8   cache[.]

9   The parties' dispute is whether the term "flow," in the context of "flow-based packet

10   classification," should be limited to "fields of an LQ header and of the L3/L4 headers." Sophos

11   argues that is should. Fortinet argues to the contrary.

12   Sophos's argument is based on the prosecution history of the '125 patent. Specifically,

13   Sophos contends that the original '125 patent application was rejected on the grounds that it did not

14   provide sufficient support for understanding the term "flow-based packet classification."

15   Subsequently, the applicants for the '125 patent filed an amendment, providing further explication of

16   what was meant by "flow-based packet classification." That amendment provided the examiner with

17   what is now Figure 12 of the '125 patent, and a related disclosure. In its related disclosure, the

18   applicants stated that two forms of "packet classification" exist: (1) "flow-based . . . using various

19   fields of the LQ header along with fields in the L3/L4 headers" and (2) an unnamed type that "uses

20   the upper bits of the IP address or MPLS label to index a table of flow indices." '125 Patent at

21   15:18-20; 15:22-23. Thereafter, the examiner granted the patent.

22   According to Sophos, that amendment is the only "true disclosure" of "flow based packet

23   classification" because the examiner rejected the previous disclosure as insufficient. As such,

24   Sophos contends that the Court should look *exclusively* to the amendment, wherein the patentee

25   explicitly defines what it meant by "flow-based" – *i.e.* "using various fields of the LQ header along

26   with fields in the L3/L4 headers." Sophos contends that, when looking exclusively at that

27

28

7

1 amendment, the Court should disregard the "plain and ordinary meaning" of the term flow,[3] because

2 the patentee provided a different definition and was "acting as their own lexicographer." *See*

3 *Phillips*, 415 F.3d at 1316.

4   A patentee acts as its own lexicographer if it (1) clearly set forth a definition of a claim term

5 other than its plain and ordinary meaning; and (2) "clearly express[ed] an intent" to redefine that

6 claim term. *See Thorner*, 669 F.3d at 1365; *see also Helmsderfer v. Bobrick Washroom Equip., Inc.*,

7 527 F.3d 1379, 1381 (Fed.Cir.2008); *Kara Tech. Inc. v. Stamps.com*, 582 F.3d 1341, 1347–48

8 (Fed.Cir.2009). Thus, here, to show that the patentee of the '125 patent acted as its own

9 lexicographer, Sophos has the burden of showing both prongs are met. The Court finds that Sophos

10 succeeds on the first prong, but fails on the second.

11   The parties do not dispute that the term "flow-based packet classification" means sorting

12 packets on the basis of their header characteristics. As noted, the March 2007 amendment defines

13 "flow-based" packet classification as sorting packets "using various fields of the LQ header along

14 with fields in the L3/L4 headers." '125 Patent at 15:18-20. That definition is different from the

15 plain and ordinary meaning of "flow-based" because it limits classification to particular headers,

16 whereas the plan and ordinary meaning has no such limitation. Therefore, the Court finds that the

17 first prong is satisfied, because the 2007 amendment sets forth a definition of a claim term other than

18 its plain and ordinary meaning. *See Helmsderfer*, 527 F.3d at 1381.

19   As to the second prong, the Court finds that the 2007 amendment, when viewed as a whole,

20 does not evidence the requisite intent to redefine "flow-based." As an initial matter, the definition

21 contained in the 2007 amendment appears in a sentence that begins with "[a]ccording to one

22 embodiment . . .." '125 Patent at 15:18. This preamble indicates that the succeeding definition may

23 have been intended to apply only to "one embodiment," and not the entire patent. Further, the

24 specification reflects a flow-based packet classification that includes L2 classification, even though

25 the definition provided in the amendment limits classification to LQ, L3, and L4 headers.

26

27   [3] At the hearing, the parties agreed that "flow" is a commonly understood term that refers to

28 a grouping of packets that have common characteristics. Thus, if one is sorting packets based on
their common characteristics, they are sorting the packets into "flows."

Taken together, the Court finds that the narrowing preamble of the amendment definition and the contrary descriptions in the specification negate a conclusion that the patentee intended to re-define "flow-based packet classification," by incorporating the limitations referred to in the amendment. As such, Sophos has not met its burden of showing that the applicant for the '125 patent "clearly express[ed] an intent" to redefine "flow-based packet classification," and has thus failed to show an intent to act as its own lexicographer.

For the foregoing reasons the Court declines to construe "flow-based packet classification" any differently than its plain and ordinary meaning.

D.   "stor[ed/ing] for access [by]"

Fortinet	Sophos	Court
Claim 1, preamble: "stored at a first data processor for access [by]" 1(a): "storing at a second data processor for access [by]" 9(a): "stored at a first data processor for access [by]"	No construction necessary or plain and ordinary meaning	No construction necessary or

"Stor[ed/ing] for access [by]" appears in claim 1 and 9 of the '587 patent. Those claims provide:

Claim 1:   a method for checking the validity of an item or data **stored for access by** a first data processor of a data processing network comprising at least two interconnected data processors, the method comprising the steps of:

storing for access by a second data processor a plurality of definitions of forms of data indicative of invalidity of items of data;

causing the first data processor to provide the second data processor with a copy of the item of data;

determining, using the second data processor, whether any of the stored forms of data are present in the item of data and declaring the item of data invalid if any of the stored forms of data are present in the item of data;

reporting to the first data processor on the validity of item of data; and causing the first data processor to prevent access to the item of data if the item of data is declared as invalid.

9

Claim 9:   A data processing system comprising a plurality of data processors interconnected as a network, and comprising:

means in a first data processor of the network for providing a second data processor of the network with a copy of an item of data which is **stored for access by** the first data processor;

storage means for access by the second data processor for storing a set of information defining data of a plurality of characteristic forms that are indicative of invalidity[.]

Sophos's '587 patent describes an invention by which two processors work in tandem to intercept and verify data requests within a computer network. Sophos Opening Claim Construction Brief (SOCC) at 2. The '587 patent describes this invention as a basic three step process. '587 Patent 1:50-54, 2:26-30. The first processor intercepts data requests pending within the network, and relays their characteristics to the second processor. *Id* 1:50-54. The second processor then verifies the validity of the data request by comparing its characteristics to characteristics typically associated with a virus, or other unwanted programs. *Id.* at 1:55-65. After analysis, the second processor responds to the first processor, instructing it to either permit or deny the data request. *Id*. at 2:26-33.

The parties' dispute boils down to this question: when the claims state that data is "stored for access by the first data processor," does that mean the data is stored *on* the first data processor, or may the data be stored anywhere *for access by* the first data processor? Sophos argues for the latter, Fortinet the former.

As the parties agreed at the hearing, this dispute has more to do with grammar than technology. The meaning of the words in the phrase are not in dispute. Rather, what is disputed is what the ordering of the words means. The Court does not see ambiguity in the claim sufficient to deviate from its plain and ordinary meeting.

Generally, the meaning of a written expression flows not just from the meaning of the selected words, but from the ordering of the words in relation to one another. The effect of the ordering of words is comprehended, in part, by reference to the grammatical principals that govern the English language. Claim language is no exception . *See In re Hyatt*, 708 F.2d 712, 714 (Fed.Cir.1983) ("A claim must be read in accordance with the precepts of English grammar."); *see*

10

1 *also SuperGuide Corp. v. DirecTV Enterprises, Inc.*, 358 F.3d 870, 886 (Fed. Cir. 2004) (applying

2 the rules of grammar to interpret claim language) (citing William Strunk, Jr. & E.B. White, *The*

3 *Elements of Style* 27 (4th ed. 2000).

4   Here, Fortinet's construction reads "stored for access by the first data processor" as "stored

5 by the first data processor." This construction is problematic because it defies the general

6 grammatical rule that " [t]he subject of a sentence and the principal verb should not . . . be separated

7 by a phrase or clause that can be transferred to the beginning." William Strunk, Jr. & E.B. White,

8 *The Elements of Style,* 20 (4th ed. 2000). Were Fortinet's construction correct, the subject (the

9 processor) would be separated from its proposed action (storing) by the phrase "for access." Thus, a

10 plain grammatical structure of this language counsels against Fortinet's construction. The claim

11 reads "stored for *access* by the first date processor," not "stored by the first date processor."

12 Fortinet reads out "for access." Thus, the first data processor is *not* necessarily the subject

13 performing the storing as Fortinet contends.

14   Fortinet's construction is further undermined by two portions of the specification. The first

15 provides:"[t]he storage means of each [processor] may be located remotely of the rest of the

16 [processor]." '125 Patent at 3:51-53. The second portion provides: "data to be tested for is stored

17 by, *or* for access by the second data processor." *Id*. at 2:16-18. Both of these provisions evidence

18 an understanding that the data being processed by a data processor can be stored at that data

19 processor, but does not need to be. Thus, Fortinet's requirement that the data be stored at the data

20 processor is at odds with the specification.

21   Nevertheless, Fortinet argues its construction is supported by the testimony of the inventor,

22 Jan Hruska, who testified that "stored for access by" was intended to mean "stored at." Hruska

23 testified that:

24   Q. Where is the item of data referred to in this phrase stored?

25   A. On the first processor, the first data processor.

26

27 Ex. Q, Hruska Dep. at 51:49-52:2. Fortinet argues that under *Gemalto SA v. HTC Corp.*, 754 F. 3d

28 1364 (Fed. Cir. 2014) the Court should consider this testimony in construing the claim language.

11

The Court disagrees. In *Gemalto*, the Federal Circuit considered the testimony of two inventors as representative of persons skilled in the relevant art. *Id*. at 1371. Here, by contrast, the Hruska's testimony is being offered to show his intention in drafting the claim language, not as a representative understanding of one skilled in the relevant art. Thus, *Gemalto* is inapposite. The Court declines to gear its construction around the *post-hoc* statements of an interested party.

For the foregoing reasons, the Court rejects Fortinet's construction, and finds that the plain and ordinary meaning is sufficient.

E.   "forms of data"

Fortinet	Sophos	Court
"instructions that are characteristic of a computer virus such as jump instructions"	No construction necessary	Plain and ordinary meaning

"Forms of data" appears in claims 1 and 4 of the '587 patent. Those claims provide:

Claim 1:   a method for checking the validity of an item or data stored for access by a first data processor of a data processing network comprising at least two interconnected data processors, the method comprising the steps of:

storing for access by a second data processor a plurality of definitions of **forms of data** indicative of invalidity of items of data;

causing the first data processor to provide the second data processor with a copy of the item of data;

determining, using the second data processor, whether any of the stored **forms of data** are present in the item of data and declaring the item of data invalid if any of the stored **forms of data** are present in the item of data;

reporting to the first data processor on the validity of item of data; and causing the first data processor to prevent access to the item of

data if the item of data is declared as invalid.

Claim 4:   A method as claimed in claim 1, wherein the first data processor in response to a command to access the item of data causes the item of data to be checked for the presence of any of the stored **forms of data**.

The parties' dispute concerns the effect of an opinion by the Board of Patent Appeals and Interferences ("BPAI"). The opinion by the BPAI was issued in response to an appeal taken by the

'587 patent applicant, challenging the PTO's rejection of their application. *See* Docket No. 97, Ex.

K. The BPAI opinion confirmed the patentability of the '587 invention. *Id*. However, it also

provided that the BPAI predicated its patentability confirmation on its interpretation of the term

"forms of data" as meaning "instructions that are characteristic of a computer virus." *Id*. at 8-9. The

BPAI went on to distinguish the '587 patent language from prior art on the grounds that the prior art

did not scan for instructions that are characteristic of a virus. *Id*.

Fortinet contends that this BPAI opinion constitutes a disclaimer of the scope of the term

"forms of data," and should therefore limit the Court's interpretation. *See Southwall Tech., Inc. v.*

Cardinal IG Co., 54 F.3d 1570, 1576 (Fed.Cir.1995) ("The prosecution history limits the

interpretation of claim terms so as to exclude any interpretation that was disclaimed during

prosecution."). Additionally, Fortinet argues that even if a disclaimer was not effected, the BPAI's

reasoning should guide this Court's analysis. *See Vitronics*, 90 F.3d at 1582-83 ("the prosecution

history can often inform the meaning of the claim language by demonstrating how the inventor

understood the invention").

In general, when the scope of a claim is disclaimed during prosecution, the matter disclaimed

must guide a future court's interpretation of that claim. *Id*. It is well settled that "it is the applicant,

not the examiner, who must give up or disclaim subject matter that would otherwise fall within the

scope of the claims." *Biogen Idec, Inc. v. GlaxoSmithKline LLC*, 713 F.3d 1090, 1101 (Fed. Cir.

2013) (quoting *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1124

(Fed.Cir.2004)). Thus, even if an examiner interprets the scope of a patent term narrowly during

prosecution, it is not "disclaimed" unless the applicant adopts that narrowed interpretation. *See, e.g.,*

Salazar v. Procter & Gamble Co., 414 F.3d 1342, 1345–47 (Fed.Cir.2005). However, to adopt a

narrowed interpretation an applicant need not "repeat the examiner's language [of limitation]

verbatim et literatim [if] it is clear that they were limiting their invention" as the examiner indicated.

Biogen Idec, 713 F.3d at 1101.

Here, the BPAI opinion does not limit the scope of the claim term "forms of data," nor does

it persuade the Court to do so. First, Fortinet has failed to demonstrate a disclaimer because it has

failed to show that the '587 applicant adopted the BPAI's interpretation – *verbatim et literatim* or

13

1   otherwise. Without such a showing, any argument for disclaimer must fail. *See Salazar*, 414 F.3d

2   1345–47; *see also 3M Innovative Properties Co. v. Avery Dennison Corp.*, 350 F.3d 1365, 1373

3   (Fed. Cir. 2003) ("Prosecution history . . . cannot be used to limit the scope of a claim unless the

4   applicant took a position before the PTO") (quoting *Schwing GmbH v. Putzmeister*

5   *Aktiengesellschaft*, 305 F.3d 1318, 1324–25 (Fed.Cir.2002). Thus, the Court finds that the scope of

6   the claim term was not disclaimed as a result of the BPAI opinion.

7   Moreover, the Court finds the BPAI opinion – limiting the term "forms of data" to

8   "instructions that are characteristic of a computer virus such as jump instructions" – unpersuasive

9   for two reasons. First, the BPAI seemed to support its construction with a portion of the

10   specification that "defines the limitation as follows[:]"

11   Information defining the characteristic forms of data indicative of the
      file's validity or invalidity is stored at the file server. These
12   characteristic forms may indicate whether the file contains unwanted
      data, *such as* a virus, *or whether it has been authorized for or barred*
13   *from use*. For a virus, for example, the characteristics may indicate the
      form of data characteristic of the virus such as instructions found at
14   the start of the file (typically "jump" instructions) or elsewhere in the
      file, which for some viruses may appear in any sequence.

15

16   Docket No. 92-2 Board of Patent Appeals and Interferences opinion ("BPAIO") at 6-7 (quoting '587

17   Patent 4:24-34) (emphasis added). The BPAI interprets this portion of the specification as limiting

18   the "forms of data" construction. However, that reading ignores the explicit language of reservation

19   which makes it clear that the "form of data" indicate unwanted data "such as a virus, or. . .." Thus,

20   the Court finds this excerpt undermines the persuasiveness of BPAI's construction; it demonstrates

21   that the specification reflected an understanding of the term "forms of data" broader than that

22   afforded by the BPAI.

23   Second, although the BPAI opinion suggests that narrowing the claim term is necessary to

24   distinguish the '587 claims from prior art, the opinion goes on to assert that the prior art at issue

25   "does not store forms of data which are indicative of invalidity of data . . . [r]ather . . . the [prior art]

26   uniquely and selectively identif[ies] the submitted program [using electronic indicia]." BPAIO at 7.

27   Thus, the BPAI's own analysis suggests that the "forms of data" in the '587 patent may be construed

28   broadly; the term generally encompasses "data which is indicative of invalidity," and is not limited

14

1 to instructions that are characteristic of a computer virus. Such a construction does not overlap with

2 the prior art at issue. Hence, the Court finds the BPAI's stated reason for narrowing the claim term

3 unpersuasive, because the term "forms of data" may be construed broadly without subjecting the

4 patent to invalidation by the prior art cited.

5 　　In sum, the Court finds that the BPAI opinion did not have the effect of disclaiming the

6 scope of the term "forms of data," and does not present a persuasive basis for the Court to do so

7 now. Accordingly, the Court construes the claim term to comport with its plain and ordinary

8 meaning.

9 F.　　"secondary URL"

Fortinet	Sophos	Court
URL that is a substring of and distinct from the primary URL	URL other than the primary URL	a distinct URL included within a primary URL

15 　　"Secondary URL" appears in claims 1, 20, and 22. Those claims provide, in relevant

16 portion:

17 **Claim 1(D):**　when the URL includes a **secondary URL** with a second network location of a
18 　　　　　website to be accessed using the first network location as a proxy site, accessing the
       　　　　　URL database and determining if the client is restricted from accessing the website
       　　　　　identified by the **secondary URL**;

19 **Claim 20(B):**　analyzing the network location access request to discover if the network location
20 　　　　　request includes a primary URL of a proxy site and a **secondary URL** of a website to
       　　　　　be accessed through the proxy site;

21 **Claim 22:**　　The method of claim 20, wherein the action is blocking access by the client to the
22 　　　　　**secondary URL** through the proxy site.

23 　　At the hearing, the parties agreed that "secondary URL" is properly construed as "a distinct

24 URL included within a primary URL." The Court adopts that construction.

25 ///

26 ///

27 ///

28 ///

15

G.   "sub-deliverables"

Fortinet	Sophos	Court
Separately delivered content that will be stored or processed as a unit	Plain and ordinary meaning	"indicative delivery data"

"Sub-deliverables" appears in claims 1 and 11 of the '050 patent. Those claims provide, in relevant portion:

Claim 1:   a method comprising:

causing contextual information to be attached to data as it passes through a series of computing devices, wherein the data includes a plurality of **sub-deliverables**, wherein the contextual information includes a source address for each one of the plurality of **sub-deliverables**, and wherein the contextual information includes a pattern of changing source addresses for each one of the plurality **of sub-deliverables**;

Claim 11:   A computer program product embodied on a non-transitory computer readable medium that, when executing on one or more computing devices, performs the steps of:

causing contextual information to be attached to data as it passes through a series of computing devices, the contextual information relating to the series of computing devices, wherein the data includes a plurality of **sub-deliverables**, wherein the contextual information includes a source address for each one of the plurality of **sub-deliverables**, and wherein the contextual information includes a pattern of changing source addresses for each one of the plurality of **sub-deliverables**[.]

The parties dispute concerns the effect of "sub-" upon the term "deliverable." Both parties agree[4] that "deliverable" means "content of data to be delivered or provided." Sophos argues the plain and ordinary meaning of the term is sufficient. However, Fortinet contends that when read in the context of the full '050 patent, the term "sub-deliverable" refers exclusively to content which is (1) separately delivered; and (2) stored or processed as a unit.

---

[4] *See* Docket No. 113 at 88-89.

16

1   In support of its first limitation – that sub-deliverables are separately delivered – Fortinet

2 cites the language of claim 1, which indicates that each sub-deliverable has a source address. *See*

3 '050 Patent at 39:6-9. According to Fortinet, if each sub-deliverable has a separate source address,

4 it must be delivered separately. In response, Sophos contends that sub-deliverables often share

5 source addresses, and thus may be delivered together.

6   At the hearing, and in their papers, Fortinet repeatedly asserts that if a piece of data contains

7 a source address it *must* be delivered separately from all other data. Yet, Fortinet does not provide

8 any intrinsic or extrinsic evidence for this proposition. Thus, the Court cannot conclude that the

9 existence of source addresses in each sub-deliverable necessarily indicates that, at all times, each

10 sub-deliverable is delivered separately.

11   The Court also rejects Fortinet's second limitation – that sub-deliverables must be stored and

12 processed as a unit – because it contradicts embodiments within the specification. Specifically, two

13 embodiments are described in these words:

14   Upon reception of the first address in the series, some characteristic
      may be recognized, such as an unusual embedded sequence, a
15   recognized embedded sequence, and the like, and action may be taken
      upon scanning the retrieved content along with this contextual
16   information. '050 Patent at 19:66 - 20:3.

17   Upon reception of the first address in the series some characteristic
      may be recognized, such as an unusual embedded sequence, a
18   recognized embedded sequence, and the like. *Id*. at 25:26-29.

19   Each of these embodiments reflects a single sub-deliverable – in both cases, the first sub-

20 deliverable received – as being processed by itself. Fortinet's construction which requires that all

21 sub-deliverables must be stored or processed together is not consistent with these embodiments. The

22 Court rejects this proposed limitation as well. *See Markman v. Westview Instruments, Inc.*, 52 F.3d

23 967, 979 (Fed. Cir. 1995), aff'd, 517 U.S. 370 (1996) ("[claims] must be read in view of the

24 specification, of which they are a part.").

25   For the foregoing reasons, the Court finds that neither of Fortinet's proposed limitations are

26 appropriate. Instead, the Court agrees with Sophos, that the plain and ordinary meaning of "sub-

27

28

17

deliverable" is sufficient. The prefix "sub" has a widely and generally understood meaning.[5] The

Court does not see any ambiguity in applying the widely accepted meaning of the prefix "sub-" to

the agreed upon meaning of "deliverable." Accordingly, the Court finds that the plain and ordinary

meaning is sufficient.

H.   "gene/genes"

Fortinet	Sophos	Court
"sequence[s] of API's and strings that describe a single piece of functionality or a property of the program"	"a piece of functionality or property of a program"	"sequence[s] of API's and strings that describe a piece of functionality or property of a program"

"Gene/genes" appears in claims 1 and 16 of the '344 patent. Those claims provide, in

relevant portion:

Claim 1:   A method for classifying software, said method comprising;

providing a library of **gene** information including a number of classifications based on groupings of **genes**; identifying at least one functional block and at least one property of the software; identifying one or more **genes** each describing one or more of the at least one functional block and the at least one property of the software as a sequence of APIs and strings; matching the one or more **genes** against one or more of the number of classifications using a processor; classifying the software based on the matching to provide a classification for the software; and notifying a user of the classification of the software.

Claim 16:   A method for generating software classifications for use in classifying software, said method comprising:

providing a library of **gene** information including a number of classifications based on groupings of **genes**;

identifying one or more **genes** each describing a functionality or a property of the software as a sequence of APIs and strings;

combining a plurality of **genes** that describe the software, thereby providing a set of **genes**;

---

[5] For example, one definition provides: "forming a subdivision or subordinate part of a whole." *See* "sub-." *Collins English Dictionary - Complete & Unabridged 10th Edition.* HarperCollins Publishers. http://dictionary.reference.com/browse/sub- (accessed: February 20, 2015).

18

1   testing the set of **genes** for false-positives against one or more reference files using a
2   processor[.]

3   Among the sources of intrinsic evidence, the specification is "the single best guide to the

4   meaning of a disputed term." *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582

5   (Fed.Cir.1996). By expressly defining terms in the specification, an inventor may "choose[ ] to be

6   his or her own lexicographer," thereby limiting the meaning of the disputed term to the definition

7   provided in the specification*. Johnson Worldwide Assocs., Inc. v. Zebco Corp.*, 175 F.3d 985, 990

8   (Fed.Cir.1999).

9   Here, the specification of the '344 patent provides: "[a] gene is [sic] piece of functionality or

10   property of a program." '344 Patent at 5:32-33. The Court finds that this statement constitutes an

11   explicit definition, and thereby limits the meaning of the term "gene" to that definition. *See Anchor*

12   *Wall Sys., Inc. v. Rockwood Retaining Walls, Inc.*, 340 F.3d 1298, 1306 (Fed.Cir.2003) ("[T]he

13   presumption in favor of the ordinary meaning of claim language as understood by one of ordinary

14   skill in the art may be overcome where the patentee chooses to be his or her own lexicographer by

15   clearly setting forth a definition for a claim term in the specification."); *see also Johnson Worldwide*

16   *Associates, Inc. v. Zebco Corp.,* 175 F.3d 985, 990 (Fed. Cir. 1999) (explaining that a patentee

17   demonstrates an intent "to be his or her own lexicographer by clearly setting forth an explicit

18   definition for a claim term.")*; see also Intellicall, Inc. v. Phonometrics, Inc.*, 952 F.2d 1384,

19   1387–88 (Fed.Cir.1992) (same); *Lear Siegler, Inc. v. Aeroquip Corp.*, 733 F.2d 881, 888–89

20   (Fed.Cir.1984) (same).

21   Fortinet's arguments to contrary are unavailing. Primarily, Fortinet contends that the Court

22   should read the definition quoted above to include information from the sentence that comes after it

23   in the specification. That next sentence provides: "[e]ach piece of functionality is described using

24   sequences of APIs and strings, which can be matched against functional blocks." Fortinet requests

25   the Court read that second sentence into the definition to arrive at its preferred construction:

26   "sequence[s] of API's and strings that describe a single piece of functionality or a property of the

27   program."

28

1   The Court declines Fortinet's request for two reasons. First, it is well established that when a

2 patentee acts as its own lexicographer, by defining a disputed claim term, that is sufficient reason to

3 adopt that definition. *See Irdeto Access, Inc. v. Echostar Satellite Corp.*, 383 F.3d 1295, 1300 (Fed.

4 Cir. 2004); *see also In re Paulsen*, 30 F.3d 1475, 1480 (Fed.Cir.1994); *Intellicall, Inc. v.*

5 *Phonometrics, Inc.*, 952 F.2d 1384, 1387–88 (Fed.Cir.1992); *Lear Siegler, Inc. v. Aeroquip Corp.*,

6 733 F.2d 881, 888–89 (Fed.Cir.1984). As discussed, the inventor of the '344 patent chose to act as

7 his own lexicographer in defining the term "gene."

8   Second, the limitations requested by Fortinet already appear in the relevant claims, and thus

9 its requested construction is redundant. In both claim 1 and claim 16, a gene is referred to as

10 "describing a functionality or a property of the software as a sequence of APIs and strings." '344

11 Patent at 7:64-67. Thus, Fortinet's construction – which supplements the inventor's definition by

12 clarifying that a functionality is a sequence of APIs and strings – becomes redundant. Claim terms

13 should not be construed in a manner that results in such redundancies. *See Robotic Vision Sys., Inc.*

14 *v. View Eng'g, Inc.*, 189 F.3d 1370, 1376 (Fed. Cir. 1999) (rejecting a construction on the ground

15 that it "would necessarily be redundant and would add no additional limitations.").

16   For the foregoing reasons, the Court construes the term "gene" as: "a piece of functionality

17 or property of a program," as expressly defined in the specification.

18

19   IT IS SO ORDERED.

20

21 Dated: February 27, 2015

22   _____
                                           EDWARD M. CHEN
23   United States District Judge

24

25

26

27

28