United States Court of Appeals for the Federal Circuit

THE TRUSTEES OF COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK,
Plaintiff-Appellant

v.

SYMANTEC CORPORATION,
Defendant-Appellee

2015-1146

Appeal from the United States District Court for the Eastern District of Virginia in No. 3:13-cv-00808-JRS, Senior Judge James R. Spencer.

Decided: February 2, 2016

DAVID ISAAC GINDLER, Irell & Manella LLP, Los Angeles, CA, argued for plaintiff-appellant. Also represented by RICHARD BIRNHOLZ, JOSEPH M. LIPNER, JASON SHEASBY, GAVIN SNYDER; AARON MARTIN PANNER, Law Office of Aaron M. Panner, PLLC, Washington, DC.

DAVID A. NELSON, Quinn Emanuel Urquhart & Sullivan, LLP, Chicago, IL, argued for defendant-appellee. Also represented by NATHAN HAMSTRA; RICHARD WOLTER

ERWINE, ALEXANDER RUDIS, New York, NY; ADAM CONRAD, King & Spalding LLP, Charlotte, NC; DARYL JOSEFFER, Washington, DC.

Before PROST, *Chief Judge,* DYK, and HUGHES, *Circuit Judges.*

DYK, Circuit Judge

The Trustees of Columbia University ("Columbia") appeal from a claim construction order and subsequent partial final judgment of non-infringement and invalidity with respect to claims of six patents that it owns: U.S. Patent No. 7,487,544 ("the '544 patent"), U.S. Patent No. 7,979,907 ("the '907 patent"), U.S. Patent No. 7,448,084 ("the '084 patent"), U.S. Patent No. 7,913,306 ("the '306 patent"), U.S. Patent No. 8,074,115 ("the '115 patent"), and U.S. Patent No. 8,601,322 ("the '322 patent").

We find that the district court correctly construed the term "byte sequence feature" in connection with the '544 and '907 patents and the term "probabilistic model of normal computer system usage" in connection with the '084 and '306 patents. Accordingly, we affirm the district court's judgment of non-infringement with respect to the '544 patent, the '907 patent, the '084 patent, and the '306 patent. We also affirm the judgment of the district court finding claims 1 and 16 of the '544 patent indefinite.

However, we find that the district court incorrectly construed the term "anomalous" in the '115 and '322 patent claims by requiring the model of normal computer usage be built only with "typical, attack free data." Because we reverse the district court's claim construction with respect to the '115 and '322 patents, we remand for further proceedings with respect to the asserted claims of those patents.

BACKGROUND

All of the six patents at issue on this appeal involve applying data analytics techniques to computer security to detect and block malware. The patents can be grouped into three families. The '544 and '907 patents share the same specification and relate to detecting malicious email attachments. The '084 and '306 patents share the same specification, and relate to a method for detecting intrusions in the operation of a computer system. The '115 and the '322 patents also share a specification and relate to detecting anomalous program executions.

In December of 2013, Columbia sued Symantec, alleging infringement of claims of these six patents by various Symantec products. In January of 2014, Symantec answered the complaint, asserting, among other things, the affirmative defenses of non-infringement, invalidity, and unenforceability of the asserted patents. After briefing and a hearing, the district court issued a claim construction order on October 7, 2014, and later issued an order clarifying certain constructions.

Based on the district court's claim constructions, the parties filed a joint motion for entry of final judgment on all infringement claims. Specifically, the parties agreed to a judgment of non-infringement on all asserted claims and a finding of invalidity for indefiniteness of claims 1 and 16 of the '544 patent. Columbia reserved the right to appeal the district court's claim constructions. Pursuant to the stipulation, the court entered partial final judgment under Rule 54(b) of the Federal Rules of Civil Procedure, and Columbia now appeals.[1] We have jurisdiction pursuant to 28 U.S.C. § 1295(a)(1).

---

[1] Other claims, including state-law claims, remain pending in the district court.

DISCUSSION

Claim construction is ultimately a question of law that this court reviews *de novo*. *Teva Pharm. USA, Inc. v. Sandoz, Inc.*, 135 S. Ct. 831, 839 (2015). The construction of claim terms based on the claim language, the specification, and the prosecution history are legal determinations. *Id.* However, claim construction may involve subsidiary issues of fact based on the extrinsic record, which this court reviews for clear error. *See id.* at 837–38.

Claim construction requires a determination as to how a person of ordinary skill in the art would understand a claim term "in the context of the entire patent, including the specification." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc). We begin a claim construction analysis by considering the language of the claims themselves. *Id.* at 1314. However, "claims must be read in view of the specification, of which they are a part." *Id.* at 1315 (quoting *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 978 (1995) (en banc) (quotation marks omitted). The specification is the "single best guide to the meaning of a disputed term," *Vitronics Corp. v. Conceptronic, Inc.,* 90 F.3d 1576, 1582 (Fed. Cir. 1996), and "is, thus, the primary basis for construing the claims." *Phillips,* 415 F.3d at 1315 (citation and quotation marks omitted). A court should also consider the patent's prosecution history, *Id.* at 1317, and may rely on dictionary definitions, "so long as the dictionary definition does not contradict any definition found in or ascertained by a reading of the patent documents." *Id.* at 1321–22 (citation and internal quotation marks omitted).

Columbia argues that the district court here erred in departing from the plain meaning of "byte sequence feature" in the '544 and the '907 patents and "probabilistic model of normal computer system usage" in the '084 the '306 patents. It argues that "there is a heavy presump-

tion that claim terms carry their accustomed meaning in the relevant community at the relevant time" which can only be "overcome in only two circumstances: the patentee has *expressly* defined a term or has *expressly* disavowed the full scope of the claim." Appellant's Br. 26 (emphasis added) (citation and quotation marks omitted). For this proposition, it cites to several recent cases including *Thorner v. Sony Computer Entertainment America LLC*, 669 F.3d 1362 (Fed. Cir. 2012), a case where we stated that "[i]t is not enough for a patentee to simply disclose a single embodiment or use a word in the same manner in all embodiments, the patentee must clearly express an intent to redefine the term" and that "the standard for disavowal of claim scope is similarly exacting." *Id.* at 1365.

Our case law does not require explicit redefinition or disavowal. *See, e.g., Aventis Pharma S.A. v. Hospira, Inc.*, 675 F.3d 1324, 1330 (Fed. Cir. 2012) ("This clear expression need not be *in haec verba* but may be inferred from clear limiting descriptions of the invention in the specification or prosecution history."). Indeed, our en banc *Phillips* opinion rejected this very approach. In *Phillips*, we rejected a line of cases following *Texas Digital Systems, Inc. v. Telegenix, Inc.*, where we held that "terms used in the claims bear a 'heavy presumption' that they . . . have the ordinary meaning that would be attributed to those words by persons skilled in the relevant art [and,] unless compelled otherwise, a court will give a claim term the full range of its ordinary meaning." 308 F.3d 1193, 1202 (Fed. Cir. 2002). Specifically, *Phillips* rejected an approach "in which the specification should be consulted only after a determination is made, whether based on a dictionary, treatise, or other source, as to the ordinary meaning or meanings of the claim term in dispute." 415 F.3d at 1320. As *Phillips* carefully explained, such an approach "improperly restricts the role of the specification

in claim construction" to determining "whether the presumption in favor of the dictionary definition of the claim term has been overcome by an explicit definition of the term different from its ordinary meaning, or whether the inventor has disavowed or disclaimed scope of coverage." *Id.* (citations and quotation marks omitted). "[T]he specification is *always* highly relevant to the claim construction analysis" and is, in fact "the single best guide to the meaning of a disputed term." *Id.* (emphasis added) (citation and quotation marks omitted).

Phillips makes clear that "[t]he claims . . . do not stand alone. Rather they are part of a fully integrated written instrument, consisting principally of a specification that concludes with the claims." 415 F.3d at 1315 (internal quotation marks and citations omitted). The only meaning that matters in claim construction is the meaning in the context of the patent. *See id.* at 1316 (citing and quoting *Netword, LLC v. Centraal Corp.,* 242 F.3d 1347, 1352 (Fed. Cir. 2001) ("The claims are directed to the invention that is described in the specification; they do not have meaning removed from the context from which they arose.")).

Thus, we reject Columbia's argument that the presumption of plain and ordinary meaning "can be overcome in only two circumstances: [when] the patentee has *expressly* defined a term or has *expressly* disavowed the full scope of the claim in the specification and the prosecution history." Appellant's Br. at 26 (emphasis added). As our en banc opinion in *Phillips* made clear, "a claim term may be clearly redefined without an explicit statement of redefinition" and "[e]ven when guidance is not provided in explicit definitional format, the specification may define claim terms by implication such that the meaning may be found in or ascertained by a reading of the patent documents." 415 F.3d at 1320–21 (citing and quoting *Bell Atl. Network Servs., Inc. v. Covad Commc'ns Group, Inc.*, 262

F.3d 1258, 1268 (Fed. Cir. 2001), and *Irdeto Access, Inc. v. Echostar Satellite Corp.*, 383 F.3d 1295, 1300 (Fed. Cir. 2004)).[2]

We have previously followed this approach, for example, holding that the claim term "electrochemical sensor" excluded cables and wires based on critical language in the claims and specification, despite there having been no explicit disclaimer of cables or wires. *See In re Abbott Diabetes Care Inc.*, 696 F.3d 1142, 1149–50 (Fed. Cir. 2012); *see also AIA Eng'g Ltd. v. Magotteaux Int'l S/A*, 657 F.3d 1264, 1278 (Fed. Cir. 2011) (where "the specification reveals a special meaning for a term that differs from the meaning it might otherwise possess, that special meaning governs"); *Comput. Docking Station Corp. v. Dell, Inc.*, 519 F.3d 1366, 1374 (Fed. Cir. 2008) ("Occasionally specification explanations may lead one of ordinary skill to interpret a claim term more narrowly than its plain meaning suggests."); *Astrazeneca AB v. Mut. Pharm. Co.*, 384 F.3d 1333, 1339 (Fed. Cir. 2004) (The patentee "seems to suggest that lexicography requires a statement in the form 'I define _____ to mean _____,' but such rigid formalism is not required.").

We have also found that a patent applicant need not expressly state "my invention does not include X" to

---

[2] Absent implied or explicit lexicography or disavowal, we have recognized that the specification plays a more limited role where claim language has so "plain a meaning on an issue" that it "leav[es] no genuine uncertainties on interpretive questions relevant to the case." *Straight Path IP Group, Inc. v. Sipnet EU S.R.O.*, 806 F.3d 1356, 1361 (Fed. Cir. 2015) (stating that "redefinition or disavowal is required where claim language is plain, lacking a range of possible ordinary meanings in context").

indicate his exclusion of X from the scope of his patent because "the patentee's choice of preferred embodiments can shed light on the intended scope of the claims." *Astrazeneca*, 384 F.3d at 1340; *see also On Demand Mach. Corp. v. Ingram Indus., Inc.*, 442 F.3d 1331, 1340 (Fed. Cir. 2006) ("[W]hen the scope of the invention is clearly stated in the specification, and is described as the advantage and distinction of the invention, it is not necessary to disavow explicitly a different scope."); *Edwards Lifesciences LLC v. Cook Inc.*, 582 F.3d 1322, 1333 (Fed. Cir. 2009) (finding disavowal implicitly); *Boss Control, Inc. v. Bombardier Inc.*, 410 F.3d 1372, 1377 (Fed. Cir. 2005) (same).

I

Columbia challenges the district court's construction of "byte sequence feature" as used in claims 1–3, 6, 16–17, 28, 34, and 43 of the '544 patent and claims 1–4, and 10 of the '907 patent. The various claims of both the '544 and '907 patents cover systems and methods for detecting malicious executable attachments at an email processing application of a computer system using data mining techniques. As described in the specification, a computer model is "taught" to distinguish between a malicious file and a non-malicious file by inputting various known malicious and benign files and instructing the computer to examine various aspects, or "byte sequence features," common to these files. The model can then be used to analyze new, unknown programs to see whether they contain byte sequence features that would indicate a program is malicious.

Claim 1 of the '544 patent is representative and reads:

> A method for classifying an executable attachment in an email received at an email processing application of a computer system comprising:

> a) filtering said executable attachment from said email
>
> b) extracting a *byte sequence feature* from said executable attachment; and
>
> c) classifying said executable attachment by comparing said *byte sequence feature* of said executable attachment with a classification rule set derived from *byte sequence features* of a set of executables having a predetermined class in a set of classes to determine the probability whether said executable attachment is malicious, wherein extracting said *byte sequence features* from said executable attachment comprises creating a byte string representative of resources referenced by said executable attachment.

'544 patent, col. 19 ll. 11–26 (emphasis added). The district court construed "byte sequence feature" to mean a "[f]eature that is a representation of machine code instructions of the executable." J.A. 9.

Columbia takes issue with the district court's limiting the construction to only "machine code instructions." Machine code instructions are the parts of a program that instruct a computer's processor to perform certain actions. A program, or "executable," contains machine code instructions, but also contains other information such as "resource information," which contains data that is used by the executable but that does not provide specific instructions. Columbia argues that the term "byte sequence feature" is an umbrella term for the properties or attributes of sequences of bytes that are extracted from any part of an executable, including not only machine code instructions but also other information. It contends that this construction is apparent from a simple examination

of the plain meaning of the claim language and that nothing in the specification limits the broad plain meaning of the claim language. A byte sequence, it argues, is a sequence of bytes according to the plain meaning of these "familiar words." Thus, a "byte sequence feature" must be an attribute of a sequence of any bytes, not just machine code instructions. The district court, it urges, erred in relying on the specification to limit the ordinary meaning.

However, as discussed above and as *Phillips* teaches, "the specification is *always* highly relevant" and "is often the best guide to the meaning of a disputed term." *Phillips*, 415 F.3d at 1315 (emphasis added). In this case, the district court's construction is well supported by the specification. Twice in the specification, the patentee states that the "byte sequence feature" is useful and informative "because it represents the machine code in an executable." '544 patent, col. 6 ll. 12–14; '907 patent, col. 6 ll. 18–20; '544 patent col. 13 ll. 25–26; '907 patent, col. 13 ll. 32–33. These are not simply descriptions of the preferred embodiment but are statements defining "byte sequence feature." Further, the provisional application similarly defined byte sequence feature, stating that "[t]he byte sequence feature is the most informative because it represents the *machine code in an executable instead of resource information*" which is not made of machine code instructions. J.A. 850 (emphasis added); *see Advanced Display Sys., Inc. v. Kent State Univ.*, 212 F.3d 1272, 1282 (Fed. Cir. 2000) (provisional applications incorporated by reference are "effectively part of the" specification as though it was "explicitly contained therein.")

So too if "byte sequence feature" were construed to include information other than machine code instructions, the term "byte sequence feature" would have the same

scope as the general term "feature."[3] The specification makes it clear that a "byte sequence feature" is just one type of "feature" used for developing and later applying the model. The specification states that "a feature is a property or attribute of data (such as 'byte sequence feature')," '544 patent, col. 5 ll. 63–64; '907 patent, col. 6 ll. 1–2, and also states that "[f]eatures . . . are defined as properties extracted from each example program in the data set, e.g., byte sequences." '544 patent, col. 5 ll. 58–60; '907 patent, col. 5 ll. 63–65. The specification describes other embodiments as "additional methods of feature extraction," '544 patent, col. 6 l. 23; '907 patent, col. 6 l. 29, and not another approach to *byte sequence* feature extraction. The provisional application, similarly, shows that "byte sequence feature" extraction is just one type of "feature extraction" and not a general term.

Columbia points to language in the specification that states that, in another embodiment, "extracting the byte sequence features from the executable attachment may comprise creating a byte string representative of resources referenced by said executable attachment," '544 patent, col. 3 ll. 37–40. Resource information is not made up of machine code instructions and thus, it argues, "byte sequence feature" cannot be so limited. This single sentence in the specification cannot overcome the overwhelming evidence in other parts of the specification and the provisional application (described above) demonstrating that the intended definition of this term does not include information other than machine code instructions. The patentee cannot rely on its own use of inconsistent and

---

[3] The district court construed "feature" to mean "a property or attribute of data which may take on a set of values." J.A. 9. Columbia does not challenge this construction on appeal.

confusing language in the specification to support a broad claim construction which is otherwise foreclosed.

As we have previously found, the "construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction." *Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1250 (Fed. Cir. 2003). The district court's construction of "byte sequence feature" is correct.

The parties stipulated to a judgment of non-infringement of all claims of these two patents based on the district court's claim construction because, as Columbia concedes, none of the accused products analyzes an attachment's machine code instructions. Instead, when Symantec's programs analyze the contents of a file, they analyze the attached file's "header," which contains information regarding the organization of the file but does not contain any executable code. Because we have found the district court's construction to be correct, we now affirm that judgment.

The parties also stipulated to a judgment of indefiniteness as to claims 1 and 16 of the '544 patent. As previously discussed, executable files contain machine code instructions and other information, like resource information. Claims 1 and 16 conflate a "byte sequence feature," which is a feature extracted from machine code instructions, with the extraction of "resource information," which is not a machine code instruction. Specifically, the claims describe the step of extracting machine code instructions from something that does not have machine code instructions. *See, e.g.*, '544 patent, col. 19 ll. 23–25 ("extracting said *byte sequence features* from said executable attachment comprises creating *a byte string representative of resources*.") (emphasis added). The claims are nonsensical in the way a claim to extracting

orange juice from apples would be, and are thus indefinite. *See Allen Eng'g Corp. v. Bartell Indus.*, 299 F.3d 1336, 1349 (Fed. Cir. 2002). Columbia conceded at oral argument that it does not argue that claims 1 and 16 of the '544 patent are not indefinite under the district court's claim construction. Because we have affirmed the district court's claim construction, we also affirm the district court's judgment that claims 1 and 16 of the '544 patent are indefinite.

II

Columbia next challenges the district court's construction of "probabilistic model of normal computer system usage," as used in claims 1, 9, and 14 the '084 patent and claims 1 and 7 of the '306 patent. The Microsoft Windows operating system contains a registry, which is a library of common low-level settings for the operating system and for other applications. When programs are executed, they may read from or change the information in this database. The theory underlying the invention in Columbia's patents is that malicious programs access the registry in different ways than normal programs do. Thus, as for email attachments in the '544 and '907 patents, a computer model is "taught" to distinguish between accesses to the registry which indicate a malicious program and normal accesses to the registry. The model then can be used to detect malicious accesses to the database and identify malicious programs.

The claims of these two patents cover systems and methods for detecting intrusions in a computer system by monitoring operating system registry accesses. Claim 1 of the '084 patent is representative and reads:

> A method for detecting intrusions in the operation of a computer system comprising:

> (a) gathering features from records of normal processes that access the operating system registry;
>
> (b) generating a *probabilistic model of normal computer system usage* based on the features and determining the likelihood of observing an event that was not observed during the gathering of features from the records of normal processes; and
>
> (c) analyzing 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.

'084 patent, col. 22 ll. 21–34 (emphasis added). The district court, in its original claim construction order, construed the term to mean a "model of typical attack-free computer system usage that employs probability." J.A. 10. The district court furthered construed the term "normal computer system usage" to mean "typical attack-free computer system usage," relying on the specification. *Id.* After Columbia moved for clarification of the district court's construction of this term, the district court clarified that the model described in the '084 and '306 patents must be generated with "only attack-free data." J.A. 12. Again, contrary to *Phillips*, Columbia argues that the district court erred in departing from the plain and ordinary meaning and instead relied on the specification to erroneously import a negative limitation from the specification despite no "clear and unmistakable" disclaimer of the claim scope.

The district court was correct in finding that, according to the patentee's own words in the specification, the "probabilistic model of normal computer system usage" is

built using only attack-free data. According to the specification, the model is built by "[g]athering features from the records of *normal* processes that access the Windows registry." '084 patent, col. 3 ll. 31–33 (emphasis added); '306 patent, col. 3 ll. 32–33. The invention then takes these features (which were gathered from *normal* processes) and builds "a probabilistic model of normal computer system usage based on records of a plurality of processes that access the Windows registry and that are indicative of normal computer system usage, e.g., free of attacks." '084 patent, col. 4 ll. 3–6 (emphasis added); '306 patent, col. 4 ll. 4–8. The specification consistently describes an implementation where the inventors ran ordinary programs to "generate normal data for building an accurate and complete training model." '084 patent, col. 14 ll. 55–59; '306 patent, col. 14 ll. 55–59; *see also id.* col. 8 ll. 12–14 ("statistics of the values of these features over normal data are used to create the probabilistic model of normal registry behavior"); *id.* col. 10 ll. 33–35 (probability "estimated over the normal data"); *id.* col 11 ll. 17–18 ("From the normal data . . ."). Nothing in the specification describes any embodiment which uses attack data to build the model.[4] The provisional patent application, incorporated by reference into the specification, similarly describes creating the model using only normal data. *See* J.A. 925 ("Statistics . . . over normal data are used to create the model of normal registry behavior.")

The prosecution history also confirms this conclusion. To distinguish some prior art, the patentee said that the

---

[4] Columbia's references to the specification where attack data is used all relate to testing and setting the threshold for determining whether something is an attack rather than creating the model. *See* '084 patent, col. 15 ll. 44–51.

prior art did not suggest "a technique for predicting events which were not observed during training." J.A. 5805. In other words, what distinguished the invention from the prior art is that it could predict whether a registry access was malicious from a model that was built using only normal data. If the model were built on attack data and then subsequently used to predict attacks, it would not be "predicting events which were not observed during training."

Columbia points to an academic paper referenced in the specification and written by one of the inventors wherein a model for detecting network intrusions was built using both attack and attack-free data as support for its construction. However, this reference describes a different invention and is not relevant for construing the claims of these patents. In addition, Columbia points to two patent applications incorporated into the specification describing databases used to store information to build models that have passing references to attack data's being stored in the database. These fleeting references cannot overcome the overwhelming evidence in the specification and the prosecution history, especially given the specification did not "even refer with any detailed particularity" to the passages Columbia now argues support its construction. *See SkinMedica, Inc. v. Histogen Inc.*, 727 F.3d 1187, 1207 (Fed. Cir. 2013). The district court's conclusion that the model of the '084 and '306 patents must be built with only attack-free normal data is correct.

Based on the district court's claim construction, the parties stipulated to a judgment of non-infringement of these two patents by the accused Symantec products. Columbia concedes that none of the Symantec products builds a model based on clean, attack-free data. Rather, these products use known good *and bad* files to classify new unknown files. We therefore affirm the stipulated judgment of non-infringement of these two patents.

III

Lastly, Columbia argues that the district court incorrectly construed the term "anomalous" as used in claims 1, 4–5, 11, 14–15, 21–22, 25–26, 32, 35–36, and 42 of the '115 and claims 1–4, 9–13, 18–21, and 26–27 of the '322 patent. The claims of these two patents cover media, systems, and methods for detecting and classifying anomalous program executions. As is described in the specification, computer programs may anomalously "terminate due to any number of threats, program errors, software faults, attacks, or any other suitable software failure." '115 patent col. 1 ll. 23–25. Thus, a program crash may be the result of a malicious attack or it simply may be the result of a bug in the software. This invention "teaches" a computer model to tell the difference between the two, and then uses that model to predict whether anomalous program executions are the result of a malicious attack.

Claim 1 of the '115 patent is representative and reads:

> A method for detecting anomalous program executions, comprising:
>
> > executing at least a part of a program in an emulator;
> >
> > comparing a function call made in the emulator to a model of function calls for the at least a part of the program;
> >
> > identifying the function call as *anomalous* based on the comparison; and
> >
> > upon identifying the *anomalous* function call, notifying an application community that includes a plurality of computers of the anomalous function call.

'115 patent, col. 20 ll. 37–46 (emphasis added). The district court construed "anomalous" to mean

"[d]eviation/deviating from a model of typical, attack-free computer system usage." J.A. 10. After Columbia moved for clarification, the district court, relying on its construction of "normal computer usage" in the various claims of '084 and '306 patents, as described above, found that the model in '115 and '322 patents also only uses attack-free data. J.A. 11–12.

At the outset, we note that there is no reason why the construction of claim terms in the '115 and '322 patents should be the same as the '084 and '306 patents, contrary to the views expressed by the district court and the parties. We have previously held that where multiple patents "derive from the same parent application and share many common terms, we must interpret the claims consistently across all asserted patents." *NTP, Inc. v. Research in Motion, Ltd.*, 418 F.3d 1282, 1293 (Fed. Cir. 2005); *see also Microsoft Corp. v. Multi-Tech Sys., Inc.*, 357 F.3d 1340, 1349–50 (Fed. Cir. 2004) (finding that statements by the patentee in prosecution of sibling patent were a "representation of its own understanding of the inventions disclosed" in all sibling patents, despite the statement being made *after* the issuance of the patent in which the term being analyzed was used). But here, none of those considerations is present. These four patents comprise two separate families, and these two families of patents claim two different inventions, list only one inventor in common, were filed years apart, and do not result from the same patent application. *See Abbot Labs. V. Dey, L.P.*, 287 F.3d 1097, 1104–05 (Fed. Cir. 2002).

Further, the language of the two terms being construed—"anomalous" in claims of the '115 and '322 patents and "probabilistic model of normal computer system usage" in claims of the '084 and '306 patents—is not the

same, or even similar.[5] Thus, even if they were part of the same family, there would be no reason to construe the terms similarly. *See Ventana Med. Sys., Inc. v. Biogenex Labs., Inc.*, 473 F.3d 1173, 1182 (Fed. Cir. 2006) ("[T]he doctrine of prosecution disclaimer generally does not apply when the claim term in the descendant patent uses different language."); *ResQNet.com, Inc. v. Lansa, Inc.*, 346 F.3d 1374, 1383 (Fed. Cir. 2003) ("Although a parent patent's prosecution history may inform the claim construction of its descendant, the [parent] patent's prosecution history is irrelevant to the meaning of this limitation because the two patents do not share the same claim language."). We see no reason to construe the term "anomalous" in the '115 and '322 patents consistently with the term "probabilistic model of normal computer system usage" in the '084 and '306 patents.

The claims themselves show that the model can be built with both attack-free and attack data. Claim 7 of the '115 patent, which depends on claim 1, claims "[t]he method of claim 1, wherein the model reflects normal activity of the at least a part of the program." '115 patent, col. 20 ll. 61–62. Claim 8 of the '115 patent claims "[t]he method of claim 1, wherein the model reflects attacks against the at least a part of the program." *Id.* at ll. 63–64. Claims 6 and 7 of the '322 patent, similarly depend on independent claim 1 and also refer to model building using normal data and attack data, respectively. *See* '322 patent, col. 20 ll. 64–67. As we have previously held, "each claim in a patent is presumptively different in scope." *RF Del., Inc. v. Pac. Keystone Techs., Inc.*, 326 F.3d 1255, 1263 (Fed. Cir. 2003). Thus, in a situation

---

[5] The specifications of the '084 and '306 patents use the word anomalous, but only in describing the detection phase not the model building phase.

where dependent claims have no meaningful difference other than an added limitation, the independent claim is not restricted by the added limitation in the dependent claim. *Phillips*, 415 F.3d at 1314-15; *Acumed LLC v. Stryker Corp.*, 483 F.3d 800, 806 (Fed. Cir. 2007). In such situations, construing the independent claim to exclude material covered by the dependent claim would be inconsistent. *Andersen Corp. v. Fiber Composites*, LLC, 474 F.3d 1361, 1369–70 (Fed. Cir. 2007). Thus, because the dependent claims in the '115 and '322 patents are presumed to be narrower than the independent claims on which they depend, "anomalous" cannot be read to limit the type of data used to model to only attack-free data in the independent claims in the absence of other evidence rebutting the presumption.

The prosecution histories of the '115 and '322 patents also support Columbia's assertion that the model here can be built with attack-free and attack data. The provisional application describes using "approximately 300,000 records of which approximately 2,000 are labeled attacks" to build the model. J.A. 3649–50. In addition, it states that the data used to build a model "can conceivably include . . . malicious programs" and "harmful data." J.A. 3752; J.A. 3739. No similar statements appear in the provisional application or prosecution histories for the '084 and '306 patents. Thus we conclude that the district court erred in limiting the term "anomalous" to mean that the model here must be built only using attack-free data.

Again based on the district court's claim construction, the parties stipulated to non-infringement of these two patents by the accused Symantec products. Because we reverse the district court's construction of "anomalous," we vacate the stipulated judgment of non-infringement as to all claims of the '115 and the '322 patents and remand for further proceedings consistent with this opinion.

CONCLUSION

In summary, we affirm stipulated judgment of non-infringement of the asserted claims of the '544 patent, the '907 patent, the '084 patent, and the '306 patent. In addition, we affirm the district court's finding of invalidity of claims 1 and 16 of the '544 patent. However, we reverse the stipulated judgment of non-infringement of the asserted claims of the '115 and '322 patents because it was based on an incorrect claim construction, and remand for further proceedings consistent with this opinion.

AFFIRMED-IN-PART, REVERSED-IN-PART, REMANDED-IN-PART

COSTS

Costs to neither party