UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/466,806	08/22/2014	Neeraj Thakar	P68155 (920-0360US)	6257

149052 7590 07/09/2018

HANLEY, FLIGHT & ZIMMERMAN, LLC (McAfee)
150 S. WACKER DRIVE
SUITE 2200
CHICAGO, IL 60606

EXAMINER
LE, CANH

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
07/09/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@hfzlaw.com
jflight@hfzlaw.com
pcesarz@hfzlaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte NEERAJ THAKAR, PRAVEEN KUMAR AMRITALURU, and VIKAS TANEJA

Appeal 2017-011033
Application 14/466,806[1]
Technology Center 2400

Before ROBERT E. NAPPI, JOHN P. PINKERTON, and JAMES W. DEJMEK, *Administrative Patent Judges*.

DEJMEK, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134(a) from a Final Rejection of claims 1–9 and 15–20. Appellants have canceled claims 10–14. App. Br. 30. We have jurisdiction over the remaining pending claims under 35 U.S.C. § 6(b).

We reverse.

---

[1] Appellants identify McAfee, Inc. as the real party in interest. App. Br. 3.

STATEMENT OF THE CASE

Introduction

Appellants' disclosed and claimed invention generally relates to network security management and, more particularly, to "detecting malwares that use domain generation algorithms and identifying systems that are infected by such malware." Spec. ¶ 1. According to the Specification, a type of malware relies on a domain generation algorithm (DGA) to create thousands of domain names that contact a Command and Control (C&C) channel. Spec. ¶ 2. Many of the randomly generated domain names are not valid (i.e., referred to as non-existent, or NX, domains). Spec. ¶ 2. However, if a valid domain named is generated, the C&C server is found and contacted. Spec. ¶ 2. In a disclosed embodiment, a process is used to examine domain name server (DNS) queries for NX domains. Various aspects of the NX domain name are analyzed to determine if the name is likely to be part of a DGA malware. Spec. ¶ 11; *see also* Figs. 4A, 4B.

Claim 1 is illustrative of the subject matter on appeal and is reproduced below with the disputed limitations emphasized in *italics*:

> 1. At least one non-transitory computer readable medium on which are stored instructions comprising instructions that when executed cause a programmable device to:
>
> identify a domain name by monitoring network activity;
>
> *determine a length of a First Level Domain (FLD) of the domain name;*
>
> *compare the length against a specified threshold;*
>
> *remove, responsive to the comparing, the FLD from the domain name;*

identify, responsive to the removing, a name as a remainder of the domain name;

calculate a lexical complexity score for the name; and

determine if the domain name is Domain Generated Algorithm (DGA) generated, based on at least the lexical complexity score.

The Examiner's Rejections

1. Claims 1–9 and 15–20 stand rejected under 35 U.S.C. § 101 as being directed to patent-ineligible subject matter. Final Act. 5–7.

2. Claims 1–6 and 17–19 stand rejected under 35 U.S.C. § 103 as being unpatentable over Stefano Schiavoni et al., *Tracking and Characterizing Botnets Using Automatically Generated Domains*, arXiv:1311.5612v1, (Cornell University, Nov. 21, 2013) ("Schiavoni") and Antonakakis et al. (US 2013/0191915 A1; July 25, 2013) ("Antonakakis"). Final Act. 8–15.

3. Claims 7–9 stand rejected under 35 U.S.C. § 103 as being unpatentable over Schiavoni, Antonakakis, and Srinivas Krishnan et al., *Crossing the Threshold: Detecting Network Malfeasance via Sequential Hypothesis Testing*, 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 10.1109/DSN.2013.6575364 (2013) ("Krishnan"). Final Act. 15–17.

ANALYSIS[2]

Rejection under 35 U.S.C. § 101

Appellants dispute the Examiner's conclusion that the claims are directed to patent-ineligible subject matter under 35 U.S.C. § 101. App. Br. 7–14; Reply Br. 2–4. In particular, Appellants contend the claims are directed to an improvement in computer-related technology by improving the manner of determining whether domain names are algorithmically generated. App. Br. 7–14; Reply Br. 2–3. As discussed below, we are persuaded by Appellants' arguments.

Under the Supreme Court's two-step framework, if a claim falls within one of the statutory categories of patent eligibility (i.e., a process, machine, manufacture or composition of matter) then the first inquiry is whether the claim is directed to one of the judicially-recognized exceptions (i.e., a law of nature, a natural phenomenon, or an abstract idea). *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2355 (2014). If so, the second step is to determine whether any element, or combination of elements, amounts to significantly more than the judicial exception. As part of the "directed to" inquiry of step one, we must "look at the 'focus of the claimed advance over the prior art' to determine if the claim's 'character as a whole' is directed to excluded subject matter." *Affinity Labs of Tex. v. DirecTV, LLC*, 838 F.3d 1253, 1257 (Fed. Cir. 2016). In *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335–36 (Fed. Cir. 2016), our reviewing

[2] Throughout this Decision, we have considered the Appeal Brief, filed April 3, 2017 ("App. Br."); the Reply Brief, filed August 24, 2017 ("Reply Br."); the Examiner's Answer, mailed June 29, 2017 ("Ans."); and the Final Office Action, mailed September 23, 2016 ("Final Act."), from which this Appeal is taken.

court framed the question as "whether the focus of the claims is on [a] specific asserted improvement in computer capabilities . . . or, instead, on a process that qualifies as an 'abstract idea' for which computers are invoked merely as a tool." If the claims are not directed to an abstract idea, the inquiry ends. *See McRO, Inc. v. Bandai Namco Games Am.*, 837 F.3d 1299, 1312 (Fed. Cir. 2016).

The Examiner concludes the claims are directed to the abstract idea of organizing and manipulating information through mathematical correlations and do not recite significantly more to transform the abstract idea into a patent-eligible application. Final Act. 6; Ans. 2–4. In particular, the Examiner finds the recited steps of determining (a length of a FLD), comparing (the determined FLD length to a threshold), removing (the FLD from the domain name), calculating (a lexical complexity score), and determining (whether the domain name is algorithmically generated) are similar to the process of organizing information through mathematical correlations found to be abstract in *Digitech Image Techs., LLC v. Elec. for Imaging, Inc.*, 758 F.3d 1344, 1350 (Fed. Cir. 2014). Ans. 3.

In *Mayo Collaborative Servs. v. Prometheus Labs., Inc.,* 566 U.S. 66 (2012), the Court cautioned that the "directed to" inquiry not simply ask whether the claims involve a patent-ineligible concept because, "all inventions at some level embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas." Rather, the "directed to" inquiry "applies a stage-one filter to claims, considered in light of the specification, based on whether 'their character as a whole is directed to excluded subject matter.'" *Enfish*, 822 F.3d at 1335 (quoting *Internet*

Patents Corp. v. Active Network, Inc., 790 F.3d 1343, 1346 (Fed. Cir. 2015)).

When considered as a whole, in light of the Specification, we disagree with the Examiner that the claims are directed to the abstract idea of simply organizing information using mathematical correlations. Rather, the focus of Appellants' claims is to improving the detection of DGA malware. *See* Spec. ¶¶ 1, 30–36, Figs. 4A, 4B. The improvement to the detection of algorithmically generated domain names is similar to *McRO*, where the court found the focus of the claims was to an improvement to an existing technological process (i.e., accurate and realistic lip synchronization and facial expressions in animated characters) by applying a limited set of rules having specific characteristics. *McRO*, 837 F.3d at 1313; *see also Enfish*, 822 F.3d at 1336 (concluding the claims were directed to a specific improvement in the way computers operate). Appellants' claims are necessarily rooted in computer technology and recite specific steps for determining whether a domain name is algorithmically generated. Accordingly, we conclude the claims are not directed to an abstract idea.

For the reasons discussed *supra*, we are persuaded of Examiner error. Accordingly, we do not sustain the Examiner's rejection of independent claim 1 under 35 U.S.C. § 101. For similar reasons, we do not sustain the Examiner's rejection under 35 U.S.C. § 101 of independent claim 15, which is similarly directed to improving the determination of whether a domain name is algorithmically generated. Further, we do not sustain the Examiner's rejection of claims 2–9 and 16–20, which depend directly or indirectly therefrom.

Rejections under 35 U.S.C. § 103

a. Claims 1–9

The Examiner rejected independent claim 1, *inter alia*, under 35 U.S.C. § 103 as being unpatentable over Schiavoni and Antonakakis. Final Act. 8–10. The Examiner finds "[Schiavoni] does not explicitly disclose determine a length of a First Level Domain (FLD) of the domain name; compare the length against a specified threshold; and remove, responsive to the comparing, the FLD from the domain name." Final Act. 9. The Examiner finds these limitations "are virtually suggested" by Antonakakis. Final Act. 9–10 (citing Antonakakis ¶¶ 15–33). Similarly, in response to Appellants' arguments disputing the teachings of Antonakakis (*see, e.g.*, App. Br. 16–20), the Examiner again finds the limitations "are nearly/almost suggested by Antonakakis." Ans. 7–8 (citing Antonakakis ¶¶ 15–33).

As an initial matter, the test for obviousness is whether the combination of references, taken as a whole, would have suggested the patentee's invention to a person having ordinary skill in the art. *In re Merck & Co., Inc.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986). It is not enough that the combined teachings "virtually suggest[]" or "almost/nearly suggest" the claimed invention. Nonetheless, we provide a brief overview of Antonakakis.

Antonakakis is generally directed to "detecting a domain generation algorithm (DGA)." Antonakakis, Abstract. As relied on by the Examiner, Antonakakis discloses a DGA Discovery Module. Antonakakis ¶¶ 15–33. As part of the DGA Discovery module, Antonakakis describes a Name-Based Features Clustering Module that clusters vectors composed by α NX

domains sharing similar name-based statistical properties. Antonakakis ¶ 18. "Name-based features may aim to model the statistical properties of domain name strings." Antonakakis ¶ 21. Antonakakis also describes extracting three groups of name-based features from the NX domains observed over a determined period of time: n-Gram features, entropy-based features, and structural domain features. Antonakakis ¶¶ 15–33. Antonakakis further discloses that DGA domains may often have a number of similarities, including similar lengths, levels of randomness, and numbers of domain levels. Antonakakis ¶ 21.

Antonakakis also provides an example domain name (www.example.com) to describe the notation and the domain levels used. Antonakakis ¶ 23. In particular, Antonakakis describes: (i) the top-level domain (TLD) of the example as .com; (ii) the second-level domain (2LD) as example.com; and (iii) the third-level domain (3LD) as www.example.com. Antonakakis ¶ 23.

Referring to the groups of name-based features, the n-Gram feature measures the frequency distribution of n-grams across the entire domain name whereas the entropy of character distribution is computed for separate domain levels (i.e., 2LD and 3LD). Antonakakis ¶¶ 27, 30. The structural domains feature summarizes information about the structure of the NX domains "such as their length, the number of unique TLDs, and the number of domain levels. Antonakakis ¶ 33. Further, Antonakakis describes the average, median, standard deviation, and variance may be computed for the length of the domain names and the number of domain levels for a given set of NX domains. Antonakakis ¶ 33.

Substantively, Appellants argue Antonakakis does not teach or reasonably suggest determining the length of a first level domain (FLD), as claimed. App. Br. 17–18. Rather, Appellants contend Antonakakis teaches performing various statistical analyses on the NX domains, but is silent on determining the length of an FLD. App. Br. 17–18. Further, because Antonakakis does not teach determining the length of an FLD, Appellants assert Antonakakis does not teach comparing the length of an FLD to a threshold or removing, responsive to the comparing, the FLD from the domain name. App. Br. 18–20.

In their Specification, Appellants also provide an example domain name (e.g., abc.com) and describe identifying a top level domain (TLD) as .com (similar to Antonakakis) and a first level domain as "abc." Spec. ¶ 32. As discussed above, the 2LD of Antonakakis includes the TLD. Thus, in these examples, Appellants' FLD is different from Antonakakis' 2LD. We are mindful, however, that limitations are not to be read into the claims from the Specification. *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993).

Although Antonakakis describes determining the length of the *domain name* (*see e.g.*, Antonakakis ¶ 33), the Examiner has not identified how Antonakakis teaches or reasonably suggests determining a length of a *portion* of the domain name (i.e., the FLD). Further, we agree with the Appellants that Antonakakis does not teach or reasonably suggest comparing the determined length to a threshold or removing it from the domain name.

For the reasons discussed *supra*, we are persuaded of Examiner error. Accordingly, we do not sustain the Examiner's rejection of independent claim 1. For similar reasons we do not sustain the Examiner's rejections of claims 2–9, which depend directly or indirectly therefrom.

b. Claims 17–19

Claims 17–19 depend directly from independent claim 15. The Examiner has not rejected claim 15 under either 35 U.S.C. §§ 102, 103. *See generally* Final Act. Rather, the Examiner finds claims 17–19 are similar in scope to claims 4–6, respectively, and rejects them under a similar rationale. Final Act. 14–15. However, claims 4–6 depend from independent claim 1, which was rejected under 35 U.S.C. § 103. Final Act. 8–10.

"Dependent claims are nonobvious under section 103 if the independent claims from which they depend are nonobvious." *In re Fine*, 837 F.2d 1071, 1076. (Fed. Cir. 1988). Accordingly, at least because claims 17–19 depend from a claim that is nonobvious, we do not sustain the Examiner's rejection of claims 17–19 under 35 U.S.C. § 103.

DECISION

We reverse the Examiner's decision rejecting claims 1–9 and 15–20 under 35 U.S.C. § 101.

We reverse the Examiner's decision rejecting claims 1–9 and 17–19 under 35 U.S.C. § 103.

REVERSED