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.
14/683,964	04/10/2015	Skyler J. Bingham	0436-US-I1	3191

83579 7590 03/10/2020

LEVEL 3 COMMUNICATIONS, LLC
Attn: Patent Docketing
1025 Eldorado Blvd.
Broomfield, CO 80021

EXAMINER	
WILCOX, JAMES J	

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
03/10/2020	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):

patent.docketing@level3.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte SKYLER J. BINGHAM, MAHENDRA K. CHANDRAKAR, LAWRENCE W. GOWIN, and RYAN T. KORTE

Appeal 2018-006696[1]
Application 14/683,964
Technology Center 2400

Before ERIC B. CHEN, NORMAN H. BEAMER, and JOYCE CRAIG, *Administrative Patent Judges*.

BEAMER, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant[2] appeals under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 1–5, 8–13, 15, 18, and 20. Claims 6, 7, 14, 16, 17, and 19 are cancelled. We have jurisdiction over the pending rejected claims under 35 U.S.C. § 6(b).

We affirm.

---

[1] An oral hearing was held February 19, 2020.

[2] We use the word "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42. Appellant identifies the real party in interest as Level 3 Communications, LLC. (Appeal Br. 2.)

THE INVENTION

Appellant's disclosed and claimed invention is directed to generating threat intelligence based on network security data. (Abstract.)

Independent claim 1, reproduced below, is illustrative of the subject matter on appeal:

> 1. A method for identifying network threats, the method comprising:
>
> obtaining a network traffic dataset representative of network traffic for an Internet Protocol address across one or more ports of a primary network, the primary network in communication with a content distribution network, the Internet Protocol address corresponding to a computing device;
>
> obtaining a content distribution network log associated with the content distribution network, the content distribution network log including a history of content requests by the Internet Protocol address;
>
> correlating the network traffic dataset with the content distribution network log based on the Internet Protocol address to obtain network security data;
>
> identifying one or more threat attributes representative of malicious activity from the network security data;
>
> weighting the one or more threat attributes; and
>
> generating network threat intelligence, including a reputation score for the Internet Protocol address, based on the weighted threat attributes using a processing cluster, wherein the reputation score is normalized based on one or more neighborhood scores, each neighborhood score corresponding to an Internet neighborhood of the Internet Protocol address.

REJECTION

The Examiner rejected claims 1–5, 8–13, 15, 18, and 20 under 35 U.S.C. § 101 as being directed to patent-ineligible subject matter. (Final Act. 2–4.)

ISSUE ON APPEAL

Appellant's arguments present the following dispositive issue:[3]

Whether the Examiner erred in concluding claims 1–5, 8–13, 15, 18, and 20 are directed to patent-ineligible subject matter. (Appeal Br. 5–38.)

ANALYSIS

Relying on *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089 (Fed. Cir. 2016), the Examiner concludes claims 1–5, 8–13, 15, 18, and 20 are patent-ineligible under 35 U.S.C. § 101 because the claims are directed to the abstract idea of "generating network threat intelligence based on network security data, i.e. collecting and analyzing information to detect misuse . . . ." (Final Act. 2.) The Examiner notes the claims "recit[e] the steps of 'obtaining a network traffic dataset,' 'obtaining a content distribution network log,' 'correlating the network traffic with the content distribution network log,' 'identifying threat attributes,' 'weighting threat attributes,' and 'generating threat intelligence including a reputation score,'" which the Examiner concludes "are directed to data gathering, analysis and generating threat intelligence which the courts have identified as abstract ideas." (Ans. 2–3; Final Act. 7.)

[3] Rather than reiterate the arguments of Appellant and the positions of the Examiner, we refer to the Appeal Brief (filed Dec. 5, 2017); the Reply Brief (filed June 18, 2018); the Final Office Action (mailed Sept. 22, 2017); and the Examiner's Answer (mailed Apr. 17, 2018) for the respective details.

Additionally relying on *Gottschalk v. Ben*son, 409 U.S. 63 (1972), the Examiner further concludes the claims "are also directed to calculating a reputation score which could also constitute a mathematical relationship or formula (an algorithm that calculates a number, without more)." (Final Act. 3.)

The Examiner further concludes that there is nothing in the claims that is significantly more than this abstract idea, given that "the limitations are merely instructions to implement the abstract idea on a computer," and make use of "[g]eneric computers performing generic computer functions." (Final Act. 3.)

Appellant argues the Examiner "oversimplifies" the claims, and argues that the claims at issue are "rooted in network computing" as distinguished from those of *FairWarning* which operate in a "computer environment" but are not rooted in software technology. (Appeal Br. 7–9.) Appellant argues:

> [C]laim 1 of the current application recites "network traffic for an Internet Protocol address across one or more ports of a primary network," "the primary network in communication with a content distribution network," "the Internet Protocol address corresponding to a computing device," "an Internet neighborhood of the Internet Protocol address," and the like. Such features do not exist separate and apart from the computer networking technology and cannot be performed in the conventional sense by a human with pen and paper.

(Appeal Br. 10.) Citing *McRO, Inc. v. Bandai Namco Games America Inc.*, 837 F.3d 1299 (Fed. Cir. 2016), Appellant argues claim 1 "in no way improperly preempts the use of an abstract idea or any purported 'mathematical formula.'" (*Id.*)

Appellant also disputes the Examiner's conclusion that there is nothing additional in the claims that is significantly more than these abstract ideas, and relies on *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245 (Fed. Cir. 2014) to argue "[t]he claimed technology results in improvements to the functioning of the network." (Appeal Br. 13.) Appellant submits that the claims at issue are analogous to those of *Amdocs (Isr.) Ltd. v. Openet Telecom, Inc.*, 841 F.3d 1288 (Fed. Cir. 2016) and *Finjan Inc. v. Blue Coat Systems, Inc.*, 879 F.3d 1299 (Fed. Cir. 2018), in which the Federal Circuit concluded that the subject matter of the claims was patentable under Section 101.[4] (Appeal Br. 14–15; Reply Br. 24.) In addition, citing the April 19, 2018 USPTO "*Berkheimer*" guidance, Appellant argues the Examiner failed to support the finding that the claims merely make use of "[g]eneric computers performing generic computer functions." (Reply Br. 6–8.)

We are not persuaded the Examiner errs. An invention is patent-eligible if it claims a "new and useful process, machine, manufacture, or composition of matter." 35 U.S. C. § 101. Here, independent claim 1 and its dependent claims relate to a method, independent claim 13 and its dependent claim relate to non-transitory computer-readable storage media; and independent claim 18 and its dependent claim relate to a system — *i.e.*, a process, manufacture, or machine, respectively. However, the Supreme Court has long held that "[l]aws of nature, natural phenomena, and abstract ideas are not patentable." *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 216 (2014) (quoting *Assoc. for Molecular Pathology v. Myriad Genetics, Inc.*,

[4] During the Oral Hearing, Appellant also argued *SRI Int'l, Inc. v. Cisco Sys., Inc.*, 930 F.3d 1295 (Fed. Cir. 2019) to like effect. (2/19/20 Hearing Tr. 5, 15–15.)

569 U.S. 576, 598–99 (2013)). The "abstract ideas" category embodies the longstanding rule that an idea, by itself, is not patentable. *Alice*, 573 U.S. at 216–17.

In determining whether a claim falls within an excluded category, we are guided by the Court's two-part framework, described in *Mayo* and *Alice*. *Id.* at 217–18 (citing *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 75–77 (2012)). In accordance with that framework, we first determine what concept the claim is "directed to." *See Alice*, 573 U.S. at 219 ("On their face, the claims before us are drawn to the concept of intermediated settlement, *i.e.,* the use of a third party to mitigate settlement risk."); *see also Bilski v. Kappos*, 561 U.S. 593, 611 (2010) ("Claims 1 and 4 in petitioners' application explain the basic concept of hedging, or protecting against risk.").

Concepts determined to be abstract ideas, and thus patent ineligible, include certain methods of organizing human activity, such as fundamental economic practices (*Alice*, 573 U.S. at 219–20; *Bilski*, 561 U.S. at 611); mathematical formulas (*Parker v. Flook*, 437 U.S. 584, 594–95 (1978)); and mental processes (*Gottschalk v. Benson*, 409 U.S. 63, 67 (1972)). Concepts determined to be patent eligible include physical and chemical processes, such as "molding rubber products" (*Diamond v. Diehr*, 450 U.S. 175, 191 (1981)); "tanning, dyeing, making waterproof cloth, vulcanizing India rubber, smelting ores" (*id.* at 182 n.7 (quoting *Corning v. Burden*, 56 U.S. 252, 267–68 (1854))); and manufacturing flour (*Benson*, 409 U.S. at 69 (citing *Cochrane v. Deener*, 94 U.S. 780, 785 (1876))).

In *Diehr*, the claim at issue recited a mathematical formula, but the Court held that "a claim drawn to subject matter otherwise statutory does not

become nonstatutory simply because it uses a mathematical formula." *Diehr*, 450 U.S. at 187; *see also id.* at 191 ("We view respondents' claims as nothing more than a process for molding rubber products and not as an attempt to patent a mathematical formula."). Having said that, the Court also indicated that a claim "seeking patent protection for that formula in the abstract . . . is not accorded the protection of our patent laws, and this principle cannot be circumvented by attempting to limit the use of the formula to a particular technological environment." *Id.* (citation omitted) (citing *Benson* and *Flook*); *see, e.g.*, *id.* at 187 ("It is now commonplace that an *application* of a law of nature or mathematical formula to a known structure or process may well be deserving of patent protection.").

If the claim is "directed to" an abstract idea, we turn to the second step of the *Alice* and *Mayo* framework, where "we must examine the elements of the claim to determine whether it contains an 'inventive concept' sufficient to 'transform' the claimed abstract idea into a patent-eligible application." *Alice*, 573 U.S. at 221 (quotation marks omitted). "A claim that recites an abstract idea must include 'additional features' to ensure 'that the [claim] is more than a drafting effort designed to monopolize the [abstract idea].'" *Id.* (alterations in original) (quoting *Mayo*, 566 U.S. at 77). "[M]erely requir[ing] generic computer implementation[] fail[s] to transform that abstract idea into a patent-eligible invention." *Id.*

Further to the *Alice/Mayo* analytical framework, after the mailing of the Answer and the filing of the Briefs in this case, in January 2019, the U.S. Patent and Trademark Office (USPTO) published revised guidance on the application of § 101. 2019 Revised Patent Subject Matter Eligibility

Guidance, 84 Fed. Reg. 50 (Jan. 7, 2019) ("2019 Revised Guidance").[5] "All USPTO personnel are, as a matter of internal agency management, expected to follow the guidance." *Id.* at 51; *see also* October 2019 Update at 1.

Under the 2019 Revised Guidance and the October 2019 Update, we first look to whether the claim recites:

> (1) any judicial exceptions, including certain groupings of abstract ideas (i.e., mathematical concepts, certain methods of organizing human activity such as a fundamental economic practice, or mental processes) ("Step 2A, Prong One"); and
>
> (2) additional elements that integrate the judicial exception into a practical application (*see* MPEP § 2106.05(a)–(c), (e)–(h) (9th ed. Rev. 08.2017, Jan. 2018)) ("Step 2A, Prong Two").[6]

2019 Revised Guidance, 84 Fed. Reg. at 52–55.

Only if a claim (1) recites a judicial exception and (2) does not integrate that exception into a practical application, do we then look, under Step 2B, to whether the claim:

---

[5] In response to received public comments, the Office issued further guidance on October 17, 2019, clarifying the 2019 Revised Guidance. USPTO, *October 2019 Update: Subject Matter Eligibility* (the "October 2019 Update") (available at https://www.uspto.gov/sites/default/files/documents/peg_oct_2019_update.pdf).

[6] This evaluation is performed by (a) identifying whether there are any additional elements recited in the claim beyond the judicial exception, and (b) evaluating those additional elements individually and in combination to determine whether the claim as a whole integrates the exception into a practical application. *See* 2019 Revised Guidance — Section III(A)(2), 84 Fed. Reg. 54–55.

(3) adds a specific limitation beyond the judicial exception that is not "well-understood, routine, conventional" in the field (*see* MPEP § 2106.05(d)); or

(4) simply appends well-understood, routine, conventional activities previously known to the industry, specified at a high level of generality, to the judicial exception.

2019 Revised Guidance, 84 Fed. Reg. at 52–56.

In evaluating the claims at issue here, we consider claim 1 as representative, consistent with how Appellant and the Examiner analyze the claims. *See* 37 C.F.R. § 41.37(c)(1)(iv)(2016). Significantly, the claim is directed to a method for identifying network threats where each step involves collecting information, analyzing that information, or generating weighted and normalized scores relating to the results of the analysis — each of these steps is capable of being performed by a human being: [7]

(i) "obtaining a network traffic dataset representative of network traffic for an Internet Protocol address across one or more ports of a primary network, the primary network in communication with a content distribution network, the Internet Protocol address corresponding to a computing device" — this requirement is directed exclusively to data gathering, which a

[7] The Examiner appropriately paraphrased these claim requirements: "'obtaining a network traffic dataset,' 'obtaining a content distribution network log,' 'correlating the network traffic with the content distribution network log,' 'identifying threat attributes,' 'weighting threat attributes,' and 'generating network threat intelligence including a reputation score.'" (Ans. 4.)

human being is capable of doing.[8] Although network technology is referred to ("network traffic"; "Internet Protocol address"; "ports of a primary network"; "content distribution network"; "computing device"), it is in the context of identifying the source of information — a dataset — that is to be obtained. The claim is not directed to the network technology itself, but rather to obtaining information obtained during the operation of that technology.

(ii) "obtaining a content distribution network log associated with the content distribution network, the content distribution network log including a history of content requests by the Internet Protocol address" — again, this requirement is directed exclusively to data gathering, in this instance obtaining a content distribution network log, which a human being is capable of doing.

(iii) "correlating the network traffic dataset with the content distribution network log based on the Internet Protocol address to obtain network security data" — a human being is capable of the mental process of correlating the specified information to obtain network security data.

(iv) "identifying one or more threat attributes representative of malicious activity from the network security data" — a human

[8] "[M]ere '[data-gathering] step[s] cannot make an otherwise nonstatutory claim statutory.'" *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1370 (Fed. Cir. 2011); *see* 2019 Revised Guidance, 84 Fed. Reg. at 55 n.31.

being is capable of the mental process of identifying such threat attributes.

(v) "weighting the one or more threat attributes" — assigning weight to threat attributes is a mathematical concept, and can be performed by a human being.

(vi) "generating network threat intelligence, including a reputation score, for the Internet Protocol address based on the weighted threat attributes using a processing cluster, wherein the reputation score is normalized based on one or more neighborhood scores, each neighborhood score corresponding to an Internet neighborhood of the Internet Protocol address" — a human being can calculate scores based on the specified weighting and normalizing, which are mathematical concepts.

As stated in the Revised Guidance, abstract ideas include mathematical concepts and mental processes. (Revised Guidance, 84 Fed. Reg. at 52). The claim 1 subject matter of obtaining information about network traffic and content distribution, correlating that information, identify network threats, and weighting and normalizing reputation scores involves mental processes, as well as mathematical concepts of weighting and normalizing. *FairWarning*, cited by the Examiner, is instructive. That case involved claims directed to "ways to detect fraud and misuse by identifying unusual patterns in users' access of sensitive data." 839 F.3d at 1091–92. The court affirmed the conclusion that the subject matter "is directed to or drawn to the concept of analyzing records of human activity to detect suspicious behavior." 839 F.3d at 1093. In detecting suspicious behavior, the court held that the subject matter involved "the same questions

(though perhaps phrased with different words) that humans in analogous situations detecting fraud have asked for decades . . . ." 839 F.3d at 1095. The Specification of the present application acknowledges network threats as a long-standing problem. (Spec. ¶ 3.)

Appellant argues that "claim 1 is rooted in network computing while claim 1 [considered in *FairWarning*] is not rooted in any software technology." However, as demonstrated above, the network technology referred to in the claims at issue are not claimed subject matter, but rather is identified as the peripheral source of the data that is subjected to the claimed mental processes and mathematical concepts. "[T]he prohibition against patenting abstract ideas 'cannot be circumvented by attempting to limit the use of the formula to a particular technological environment'. . . ." *Bilski v. Kappos*, 561 U.S. 593, 610–11 (2010), (quoting *Diamond v. Diehr*, 450 U.S. 175, 191–92 (1981)). Therefore, we agree with the Examiner that the subject matter of claim 1 recites an abstract idea, as do the remaining claims.[9]

Appellant additionally contends the claims "in no way improperly preempt[] the use of an abstract idea or any purported 'mathematical formula.'" (Appeal Br. 10) However, "questions on preemption are inherent in and resolved by the § 101 analysis," and, although "preemption

[9] Although Appellant does not focus on independent claim 18, we note that system claim does require network hardware components: "primary network"; "content distribution network"; "router interfaces"; and "processing cluster." (Appeal Br. 42 (Appendix A).) Nonetheless, this claim also limits the use of claimed abstract ideas to a particular technological environment, rather than being directed to patent-eligible subject matter.

may signal patent ineligible subject matter, the absence of complete preemption does not demonstrate patent eligibility." *Ariosa Diagnostics, Inc. v. Sequenom, Inc.*, 788 F.3d 1371, 1379 (Fed. Cir. 2015); *cf. OIP Techs., Inc. v. Amazon.com, Inc.*, 788 F.3d 1359, 1362–63 (Fed. Cir. 2015) (citations omitted) ("[T]hat the claims do not preempt all price optimization or may be limited to price optimization in the e-commerce setting do not make them any less abstract.").

Further pursuant to the Revised Guidance, we consider whether there are additional elements set forth in claim 1 that integrate the judicial exception into a practical application. Revised Guidance, 84 Fed. Reg. at 54–55. Here, the abstract idea of claim 1 involves gathering data from "network traffic for an Internet Protocol address across one or more ports of a primary network, the primary network in communication with a content distribution network, the Internet Protocol address corresponding to a computing device," and a "content distribution network." (Appeal Br. 40 (Appendix A).) As discussed above, this network technology is peripheral to the claims (as opposed to an "additional element" thereof), merely specifying the technological environment of the claimed method.[10] This does not integrate the judicial exception into a practical application. Rather, unlike *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1337 (Fed. Cir. 2016), on which Appellant relies, there is no improvement to technology, but rather application of preexisting technology to implement the abstract idea.

[10] The required network hardware components of claim 18 — "primary network"; "content distribution network"; "router interfaces"; and "processing cluster" — similarly define a technological environment of the claim rather than integrating the judicial exception into a practical application.

"[M]erely requir[ing] generic computer implementation[] fail[s] to transform that abstract idea into a patent-eligible invention." *Alice*, 573 U.S. at 221.

As discussed above, Appellant argues that claim 1 is rooted in network computing and improves the functioning of the network, relying on *McRO*, *Amdocs*, *and Finjan*. (Appeal Br. 9–11, 15–16; Reply Br. 2–4.) Those cases are inapposite. In *McRO*, the claimed process used a combined order of specific rules that rendered information in a specific format that was applied to create a sequence of synchronized, animated characters. 837 F.3d at 1315. Notably, the recited process *automatically animated characters* using particular information and techniques—an improvement over manual three-dimensional animation techniques that was not directed to an abstract idea. *Id.* at 1316.

But, unlike the claimed invention in *McRO* that improved how the physical display operated to produce better quality images, the claimed invention here merely obtains information from generic network technology to identify network threats. The claimed subject matter is directed to mental processes and mathematical concepts, and does not improve technology as was the case in *McRO*. *See SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1168 (Fed. Cir. 2018) ("[E]ven if a process of collecting and analyzing information is 'limited to particular content' or a particular 'source,' that limitation does not make the collection and analysis other than abstract")).

In *Amdocs*, the court relied heavily on a claim construction issue: the claim required "the first network accounting record is correlated to *enhance* the first network accounting record" (emphasis added), and the court explained:

> In [a prior holding], we construed "enhance" as being dependent upon the invention's distributed architecture. . . . We construed "enhance" as meaning "to apply a number of field enhancements in a distributed fashion" . . . . We took care to note how the district court explained that "[i]n this context, 'distributed' means that the network usage records are processed close to their sources before being transmitted to a centralized manager" . . . . And we specifically approved of the district court's "reading the 'in a distributed fashion' and the 'close to the source' of network information requirements into the term 'enhance.'"

841 F.3d at 1300 (internal citations omitted). The court held that the claims "purposefully arrange[] the components in a distributed architecture to achieve a technological solution to a technological problem specific to computer networks." 841 F.3d at 1301. Nothing like that is present here. The claims at issue use information obtained from network operations, but it is the way the information is used, rather than the manner that it is obtained, that arguably lends novelty to the subject matter. The fact that the abstract ideas of the claims may be novel does not render them patent eligible. *Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1315 (Fed. Cir. 2016) (citation omitted) ("[T]he 'novelty' of any element or steps in a process, or even of the process itself, is of no *relevance* in determining whether the subject matter of a claim falls within the § 101 categories of possibly patentable subject matter").

Likewise, in *Finjan*, the result hinged on the construction of "downloadable" and "identif[y] suspicious code" claim limitations, which invoked non-traditional, and immediate, detection of "all potentially hostile or suspicious code operations that may be attempted." 879 F.3d at 1303–04. The subject matter of *Finjin* was not merely a mental process, and thus

properly was characterized as an improvement to computer technology. 879 F.3d at 1304–05.[11]

Nor does the subject matter of claim 1 contain additional elements that implement the judicial exception with a "particular machine," because the claims do not specify any details in regard to the email delivery environment. *See* MPEP § 2106.05 (b). Further, the method does not transform matter; at best it transforms information. *See* MPEP § 2106.05(c). Nor does claim 1 have any other meaningful limitations (MPEP § 2106.05 (e)), or any of the other considerations set forth in the Revised Guidance regarding a determination of whether additional elements integrate the judicial exception into a practical application. *See* Revised Guidance, 84 Fed. Reg. at 55. Accordingly, we conclude that the subject matter of claim 1 (and the remaining claims) is directed to mathematical concepts and mental processes for identifying network threats, and thus an abstract idea, and there are no additional elements recited therein that would integrate the abstract idea into a practical application.

Turning to the second step of the *Alice* inquiry, we consider the elements of the claims "individually and 'as an ordered combination"' to

---

[11] *SRI*, cited during the Oral Hearing, is to like effect. Unlike the mental processes amenable to human implementation in the present claims, in *SRI* the "'focus of the claims is on the specific asserted improvement in computer capabilities' — that is, providing a network defense system that monitors network traffic in *real-time* to automatically detect large-scale attacks." 930 F.3d at 1303 (emphasis added) (citation omitted). Thus, unlike the present claims, the realtime requirements of the claims in *SRI* led to the conclusion that "the human mind is not equipped to detect suspicious activity by using network monitors and analyzing network packets as recited by the claims." 930 F.3d at 1304. No such realtime requirement is present here.

determine whether there are additional elements that "'transform the nature of the claim' into a patent-eligible application." 573 U.S. at 217 (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 79, 78 (2012)). We do not agree with Appellant that there are any additional elements of claim 1, whether taken individually or in combination, that would add "significantly more" to the basic abstract idea encompassed by the claim sufficient to transform the claimed abstract idea into a patent-eligible application. *Alice*, 573 U.S. at 223 ("[T]he mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention."). Appellant argues, "[m]uch like in *DDR*, the present claims are directed to improving operations of a computing network by detecting network computing threats. (Appeal Br. 13.) In *DDR*, instead of a computer network operating in its normal, expected manner by sending a website visitor to a third-party website apparently connected with a clicked advertisement, the claimed invention in *DDR* generated and directed the visitor to a hybrid page that presented: (1) product information from the third party, and (2) the visual "look and feel" elements from the host website. 773 F.3d at 1258–59. Given this particular Internet-based solution, the court held that the claimed invention did not merely use the Internet to perform a business practice known from the pre-Internet world, but rather was necessarily rooted in computer technology to overcome a problem specifically arising in computer networks. 773 F.3d at 1257.

That is not the case here. Other than using generic network technology, the claimed improvement consists of the mathematical concepts and mental processes of the claimed abstract idea itself. "It is clear from *Mayo* that the 'inventive concept' cannot be the abstract idea itself." *Aatrix*

Software, Inc. v. Green Shades Software, Inc., 890 F.3d 1354, 1359 (Fed. Cir. 2018). Moreover, "[p]atent law does not protect claims to an 'asserted advance in the realm of abstract ideas . . . no matter how groundbreaking the advance.'" 890 F.3d at 1359.

Appellant's reliance on *BASCOM Global Internet Services, Inc. v. AT&T Mobility LLC*, 827 F.3d 1341 (Fed. Cir. 2016) is unavailing. (Appeal Br. 12–13.) There, the court held eligible claims directed to a technology-based solution to filter Internet content that overcame existing problems with other Internet filtering systems by making a known filtering solution — namely a "one-size-fits-all" filter at an Internet Service Provider (ISP) — more dynamic and efficient via individualized filtering at the ISP. 827 F.3d at 1351. Notably, this customizable filtering solution improved the computer system's performance and, therefore, was patent-eligible. *See id.* But unlike the filtering system improvements in *BASCOM* that added significantly more to the abstract idea in that case, the claimed invention here uses generic network components to implement an abstract idea as noted previously.

Consistent with the USPTO "*Berkheimer*" guidance, the record supports the Examiner's finding that the network technology components referred to in the claims are well-understood, routine, conventional, and specified at a high level of generality. *See* Revised Guidance, 84 Fed. Reg. at 56. Figure 5 of the Specification depicts "an example computing system 500 having one or more computing units that may implement various systems and methods discussed herein." (Spec. ¶ 62.) Furthermore, "[t]he computer system 500 may be a general computing system is capable of executing a computer program product to execute a computer process."

(Spec. ¶ 63.) Nothing regarding any aspect of the "ordered combination" of the claim elements provides significantly more than the abstract idea that claim 1 is directed to.

Accordingly, we sustain the Examiner's 35 U.S.C. § 101 rejection of claim 1. Appellant provides no arguments that would differentiate the remaining claims from claim 1. Thus, the foregoing analysis of claim 1 is exemplary of that for claims 2–5, 8–13, 15, 18, 20. *See* 37 C.F.R. § 41.37(c)(1)(iv) (2016). Therefore, we also sustain the Examiner's 35 U.S.C. § 101 rejection of those claims.

DECISION SUMMARY

In summary:

Claims Rejected	**35 U.S.C. §**	**Basis**	**Affirmed**	**Reversed**
1–5, 8–13, 15, 18, 20	101	Eligibility	1–5, 8–13, 15, 18, 20	

TIME PERIOD FOR RESPONSE

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED