



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.
12/625,780	11/25/2009	Michal Aharon	82258277	1895
56436	7590	11/01/2016	EXAMINER	
Hewlett Packard Enterprise 3404 E. Harmony Road Mail Stop 79 Fort Collins, CO 80528			ANDERSON, FOLASHADE	
			ART UNIT	PAPER NUMBER
			3623	
			NOTIFICATION DATE	DELIVERY MODE
			11/01/2016	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):

hpe.ip.mail@hpe.com
mkraft@hpe.com
chris.mania@hpe.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte MICHAL AHARON, HADAS KOGAN,
and ELIAV LEVI

Appeal 2014-004068
Application 12/625,780¹
Technology Center 3600

Before: JOSEPH A. FISCHETTI, MICHAEL C. ASTORINO, and
BRADLEY B. BAYAT, *Administrative Patent Judges*.

FISCHETTI, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellants seek our review under 35 U.S.C. § 134 of the Examiner's
Final rejection of claims 1–20. We have jurisdiction under 35 U.S.C. § 6(b).
We REVERSE (37 C.F.R. § 41.50(b)).

¹ Appellants identify Hewlett-Packard Development Company, LP as the
real party in interest. Appeal Br. 1.

Claim 1 reproduced below, is representative of the subject matter on appeal.

1. A method, comprising:
 - receiving a business service model comprising a description of a topology of interconnections between configuration items that implement a business service, wherein each of the configuration items is associated with a respective vulnerability score and a respective type classification;
 - based on the vulnerability scores and the type classifications, determining for each of the configuration items a respective activity level value indicating a probability of the configuration item being active in the business service, a respective vulnerability probability value indicating a probability of the configuration items being compromised and damaged in the business service, and a respective business service risk value indicating a probability of a failure of the business service resulting from damage of the configuration item; and
 - scoring the business service based on the activity level values, the vulnerability values, and the business service risk values;
 - wherein the receiving, the determining, and the scoring are performed by a computer.

THE REJECTIONS

The following rejections are before us for review.

1. Claims 3 and 11 are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite. (Final Act. 7).
2. Claims 1, and 3–20 are rejected under 35 U.S.C. 103(a) as being unpatentable over R. Ann Miura-Ko et al., (SecureRank: A Risk-

Appeal 2014-004068
Application 12/625,780

Based Vulnerability Management Scheme for Computing Infrastructures, Management Science and Engineering, Stanford University, IEE Communication Society, 2007, hereinafter “Miura-Ko”), and Swiler et al, (US 7,013,395 B1, iss. Mar. 14, 2006, hereinafter “Swiler”). (Final Act. 8).

ANALYSIS

35 U.S.C. § 112 SECOND PARAGRAPH REJECTION

The Examiner rejects claims 3 and 11 because “[c]laim 3 is dependent on claim 1, which does not include the limitation of a ‘risk score.’ The risk score is first introduced in claim 2. It is unclear if [Appellants are] claiming that the equation claimed in claim 3 relates to the vulnerability score or the risk score.” (Answer 2).

Appellants argue on page 8 of their Brief that “neither claim 1 nor claim 3 recites a ‘risk score’ and, therefore, the failure of claim 3 to recite a ‘risk score’ cannot possibly render claim 3 indefinite.” (Appeal Br. 8).

We agree with Appellants for the reasons set forth on page 8, lines 7–13 of the Appeal Brief.

Thus, we will not affirm the rejection of claims 3 and 11 under 35 U.S.C. § 112 second paragraph.

Appeal 2014-004068
Application 12/625,780

35 U.S.C. § 103(a) REJECTION

Independent claims 1, 10, and 16 each requires in one form or another,

based on the vulnerability scores and the type classifications, determining for each of the configuration items a respective activity level value indicating a probability of the configuration item being active in the business service, a respective vulnerability probability value indicating a probability of the configuration items being compromised and damaged in the business service, and a respective business service risk value indicating a probability of a failure of the business service resulting from damage of the configuration item.

(Appeal Br. 17) (emphasis added).

The Examiner finds for this limitation that,

Swiler teaches activity level value (col. 4, lines 38-42, see “Edges represent a change of state caused by a single action”), vulnerability probability value (col. 5, lines 10-14 “edge has a weight representing a system-security metric, such as success probability”) and business service risk (col. 3, lines 49-50 see “high-risk attack paths”). Swiler uses this information of score the business services (col. 9, lines 16-19 where the for example shortest path is a ranking of most cost efficient means of protection i.e. equivalent of the claimed score). Swiler uses modeling to determine where the systems vulnerability to attack and to protect the system from risk of damage by the attackers. The modeling is analogues to the claimed scoring.

(Answer. 8–9).

Appellants argue:

Regarding the ‘scoring’ element of claim 1, the Examiner has taken the position that Swiler discloses ‘. . . scoring the business service based on the activity level values, the vulnerability values, and the business service risk values . . .’ in col. 9, lines 16-19 (see pages 9-10 of the [F]inal Office action). The cited disclosure of Swiler reads as follows:

Once the attack graph is generated, it is run through the - optimal shortest path algorithm described above to determine a representation of all of the paths with length less than or equal to $(1 + E)$ times the shortest path length. The output of these calculations is then displayed to the user through the graphical user interface.

This disclosure does not teach or suggest anything whatsoever about any of an ‘activity level value’ indicating a probability of the configuration item being active in the business service, a ‘vulnerability probability value’ indicating a probability of the configuration items being compromised and damaged in the business, and a ‘business service risk value’ indicating a probability of a service failure of the business service resulting from damage of the configuration item. Therefore, the Examiner has not shown that Swiler makes up for the failure of Miura-Ko to disclose or suggest the "determining" element of claim 1.

(Appeal Br. 11–12).

We agree with Appellants. The Examiner finds that Miura-Ko does not disclose the claimed “activity level value,” but instead relies on Swiler as disclosing this feature. (Answer 8). So we look to Swiler for a disclosure of an activity level value. The Specification and the claims describe “activity level value” in terms of:

the business services risk management system 10 determines for each of the configuration items a respective activity level value indicating a probability of the configuration item being active in the business service, a respective vulnerability probability value indicating a probability of the configuration items being compromised and damaged in the business service, and a respective business service risk value indicating a probability of a failure of the business service resulting from damage of the configuration item (FIG. 2, block 22).

According to Swiler, each edge (which the Examiner maps to the “activity level value”) has a weight representing a security metric, namely, probability, average time to implement, or a cost/effort level for an attacker. (Column 5, lines 11–13). But, it is not apparent, and the Examiner does not explain how these weights meet the claimed constituent elements of the “activity level value”, namely, *probability of the configuration item being active in the business service, a respective vulnerability probability value indicating a probability of the configuration items being compromised and damaged in the business service, and a respective business service risk value indicating a probability of a failure of the business service resulting from damage of the configuration item.* (Specification ¶ 16) (emphasis added).

Accordingly, we will not sustain the rejection of independent claims 1, 10, and 16.

Because claims 2–9, 13–15 and 17–20 depend from claim 1, 10, and 16 and since we cannot sustain the rejection of claim 1, 10, and 16, the rejection of claims 1–20 likewise cannot be sustained.

NEW GROUNDS OF REJECTION

The following new ground of rejection is entered pursuant to 37 C.F.R. § 41.50(b). Claims 1–20 are rejected under 35 U.S.C. § 101 as directed to non-statutory subject matter.

The Supreme Court

set forth a framework for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts. First, [] determine whether the claims at issue are directed to one of those patent-ineligible concepts. [] If so, we then ask, “[w]hat else is there in the claims before us? [] To answer that question, [] consider the elements of each claim both individually and “as an ordered combination” to determine whether the additional elements “transform the nature of the claim” into a patent-eligible application. [The Court] described step two of this analysis as a search for an “‘inventive concept’”—i.e., an element or combination of elements that is “sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.”

Alice Corp., Pty. Ltd. v CLS Bank Intl, 134 S.Ct. 2347, 2355 (2014) (citing *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 132 S.Ct. 1289 (2012)).

To perform this test, we must first determine whether the claims at issue are directed to a patent-ineligible concept.

We find that the claims and the Specification provide enough information to inform to what they are directed.

Representative claim 1 recites a method for scoring business risk values. It does this by determining, relevant probabilities, i.e., *determining for each of the configuration items a respective activity level value indicating a probability of the configuration item being active in the business service, a respective vulnerability probability value indicating a probability of the configuration items being compromised and damaged in the business service, and a respective business service risk value indicating a probability of a failure of the business service resulting from damage of the configuration item.* (Specification ¶ 16) (emphasis added). It follows from prior Supreme Court cases, and *Bilski* in particular, that the claims at issue here are directed to an abstract idea. Like the risk hedging in *Bilski*, the concept of rating risk values is a fundamental practice long prevalent in human behavior. Thus, rating or scoring risk values based on an assessment of related probabilities, like hedging, is an “abstract idea” beyond the scope of § 101. *See Alice Corp. Pty. Ltd.*, 134 S.Ct. at 2356.

As in *Alice Corp. Pty. Ltd.*, we need not labor to delimit the precise contours of the “abstract ideas” category in this case. It is enough to recognize that there is no meaningful distinction in the level of abstraction between the concept of risk hedging in *Bilski* and the concept assigning a service risk value based on assessed probabilities of related factors. Both are within the realm of “abstract ideas” as the Court has used that term. *See Alice Corp. Pty. Ltd.*, 134 S.Ct. at 2357. We conclude that the claims at issue are directed to a patent-ineligible concept.

The introduction of a computer into the claims does not alter the analysis at Mayo step two.

[T]he mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention. Stating an abstract idea “while adding the words ‘apply it’” is not enough for patent eligibility. Nor is limiting the use of an abstract idea “to a particular technological environment.” Stating an abstract idea while adding the words “apply it with a computer” simply combines those two steps, with the same deficient result. Thus, if a patent’s recitation of a computer amounts to a mere instruction to “implement[t]” an abstract idea “on . . . a computer,” that addition cannot impart patent eligibility. This conclusion accords with the preemption concern that undergirds our §101 jurisprudence. Given the ubiquity of computers, wholly generic computer implementation is not generally the sort of “additional feature[e]” that provides any “practical assurance that the process is more than a drafting effort designed to monopolize the [abstract idea] itself.”

Alice Corp. Pty. Ltd., 134 S.Ct. at 2358 (citations omitted).

“[T]he relevant question is whether the claims here do more than simply instruct the practitioner to implement the abstract idea [] on a generic computer.” *Alice Corp. Pty. Ltd.*, 134 S.Ct. at 2359. They do not.

Taking the claim elements separately, the function performed by the computer at each step of the process is purely conventional. Using a computer to determine and score a value, and/or execute code from a computer readable medium, are computer functions well-understood as routine, conventional activities previously known to the industry. Each step

Appeal 2014-004068
Application 12/625,780

does no more than require a generic computer to perform generic computer functions.

Considered as an ordered combination, the computer components of Appellants' claims add nothing that is not already present when the steps are considered separately. Viewed as a whole, Appellants' method and medium claims simply recite the concept of scoring business related values to arrive at a probability of failure, performed by a generic computer. The method claims do not, for example, purport to improve the functioning of the computer itself. Nor do they effect an improvement in any other technology or technical field. Instead, the claims at issue amount to nothing significantly more than an instruction to apply the abstract idea of scoring a value for a risk on a generic computer. Under our precedents, that is not enough to transform an abstract idea into a patent-eligible invention. *See Alice Corp. Pty. Ltd.* 134 S.Ct. at 2360.

CONCLUSIONS OF LAW

We conclude the Examiner did err in rejecting claims 1–20 under 35 U.S.C. § 103.

We conclude the Examiner did err in rejecting claims 3 and 11 under 35 U.S.C. § 112.

DECISION

The decision of the Examiner to reject claims 1–20 is reversed.

This decision contains a new ground of rejection pursuant to 37 C.F.R. § 41.50(b) (effective September 13, 2004, 69 Fed. Reg. 49960

Appeal 2014-004068
Application 12/625,780

(August 12, 2004), 1286 Off. Gaz. Pat. Office 21 (September 7, 2004)). 37 C.F.R. § 41.50(b) provides “[a] new ground of rejection pursuant to this paragraph shall not be considered final for judicial review.”

37 CFR § 41.50(b) also provides that the appellants, WITHIN TWO MONTHS FROM THE DATE OF THE DECISION, must exercise one of the following two options with respect to the new ground of rejection to avoid termination of the appeal as to the rejected claims:

- (1) Reopen prosecution. Submit an appropriate amendment of the claims so rejected or new evidence relating to the claims so rejected, or both, and have the matter reconsidered by the examiner, in which event the proceeding will be remanded to the examiner
- (2) Request rehearing. Request that the proceeding be reheard under § 41.52 by the Board upon the same record

REVERSED, 37 C.F.R. § 41.50(b)