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.
11/872,330	10/15/2007	Yuecel Karabulut	13913-0611001/2007P00360	8637

32864 7590 08/09/2017
FISH & RICHARDSON, P.C. (SAP)
PO BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
OUELLETTE, JONATHAN P	

ART UNIT	PAPER NUMBER
3629	

NOTIFICATION DATE	DELIVERY MODE
08/09/2017	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):

PATDOCTC@fr.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte YUECEL KARABULUT, MURRAY SPORK, and
MING-CHIEN SHAN

Appeal 2016-007487
Application 11/872,330[1]
Technology Center 3600

Before JUSTIN BUSCH, CATHERINE SHIANG, and
CARL L. SILVERMAN, *Administrative Patent Judges.*

SILVERMAN, *Administrative Patent Judge.*

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 1–20, which are the only claims pending. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

[1] The real party in interest is identified as SAP SE. App. Br. 4.

STATEMENT OF THE CASE

The invention relates to secured computing employing composite applications. Abstract; Spec. ¶¶ 1–3. Claim 1, reproduced below, is exemplary of the subject matter on appeal:

> 1. A computer-implemented method executed using one or more processors, the method comprising:
>
> accessing, by the one or more processors, a specification for a composite application corresponding to a business process, the composite application comprising local application logic to control interaction of a plurality of external services, the specification being stored in a computer-readable storage medium and comprising:
>
> a security annotation that defines a security intention comprising security policies and security capabilities of the composite application, and
>
> a plurality of tasks that define at least a portion of the business process, each task of the plurality of tasks requiring invocation of a respective external service of the plurality of external services;
>
> invoking, by the one or more processors, a security pattern that is stored in a pattern repository and that is selected from a plurality of customizable security patterns based on the security annotation, the security pattern defining entry points that automatically trigger enforcement of the security intention; and
>
> for each task of the plurality of tasks:
>
> matching, using a service broker of the enterprise, security policies and security capabilities of each of a plurality of service providers to the security policies and security capabilities of the composite application to provide a set of identified qualified service providers, and
>
> identifying, from the set of identified qualified service providers, a service provider associated with the external service associated with a respective task and that

> satisfies the security intention based on the invoked security pattern, the service provider providing a web-based service and communicating with the enterprise over a network; and
>
> invoking, by the one or more processors, the business process using identified service providers.

App. Br. 19–20 (Claims Appendix).

THE REJECTIONS

Claims 1–20 stand rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1–13 of U.S. Patent Application No. 11/872,358. Final Act. 3.

Claims 1–20 stand rejected under 35 U.S.C. § 101 as ineligible subject matter. Ans. 2.

Claims 1–20 stand rejected under 35 U.S.C. § 102(b) as being unpatentable over Anderson et al. (US 2006/0206440 Al; pub. Sept. 14, 2006) ("Anderson"). Final Act. 3–7.

ANALYSIS

The double patenting rejection

The Examiner finds, although claims 1–20 of the instant application are not identical to claims 1–13 or U.S. Application 11/872,358, the claims are not patentably distinct from each other because both inventions disclose equivalent elements creating a composite application. Final Act. 3. Appellants present no arguments regarding Examiner error and, therefore, we *pro forma* sustain the rejection.

The §101 rejection

The Examiner finds claims 1–20 are directed to an abstract idea and, therefore, directed to ineligible subject matter. Ans. 2–4 (New Ground). In particular, the Examiner finds the claims are "Equivalent to Judicial Example of Abstract idea: Certain methods of . . . Comparing new and stored information and using rules to identify options (*SmartGene*)." *Id.* at 3. The Examiner finds:

> Claims 1-20 is/are directed to Accessing saved data (Specification for a composite application, Security annotation, and Tasks that define a portion of the business process), Receiving data (service provider security policies and security capabilities), and Correlating/Matching the received data with the saved data (Image Verification), Identifying/ Transmitting/ Displaying the matched data, and Processing further data based on the identified results. . . . The claims do not recite additional elements that are sufficient to amount to significantly more than the judicial exception because (A) the additional elements or combination of elements in the independent claims are recitation of generic computer structure (i.e. a processor to execute instructions to perform the method), which serves to perform generic computer functions that are well-understood, routine, and conventional activities previously known to the pertinent industry, and do not add a meaningful limitation to the abstract idea because they would be routine in any computer implementation. The processor system in the instant application merely receives, processes and stores data. The functions of the computer are well-understood and conventional activities known in the employment and social network art. (B) because the claims do not recite an improvement to another technology or technical field, an improvement to the functioning of the computer itself, or meaningful limitations beyond generally linking the use of an abstract idea to a particular technological environment. The limitations are merely instructions to implement the abstract idea on a computer and require no more than a generic computer to

> perform generic computer functions that are well understood, routine and conventional activities previously known to the industry. Therefore, the claim(s) are rejected under 35 U.S.C. [§] 101 as being directed to nonstatutory subject matter. See Federal Register notice title 2014 Interim Guidance on Patent Subject Eligibility (79 FR 74618) issued Tuesday December 16, 2014.
>
> Furthermore, the claims have been fully analyzed to determine whether there are any additional limitations recited that amount to significantly more than the abstract idea. However, all of the claimed limitations are simply generic computer (i.e. processor, application server, network) functionality, claimed to perform the basic computer functions of: obtaining data, processing data, and transmitting data - through the program that enables the steps of the claimed invention. Taking the additional claimed elements individually and in combination, the computer components at each step of the process perform purely generic computer functions. As such, there is no inventive concept sufficient to transform the claimed subject matter into a patent-eligible application. The claim does not amount to significantly more than the abstract idea itself. Accordingly, the claim is not patent eligible.
>
> Moreover, claims to an apparatus are held ineligible for the same reason, e.g., the generically-recited computers add nothing of substance to the underlying abstract idea.

Id. at 3–4.

Appellants argue the subject matter of claims 1–20 is not directed to an abstract idea and, instead, is directed to "add[ing] high-level security intentions or objectives to the business process specification, where the security framework facilitates the automatic generation of the security configuration and enforcement processes." Reply Br. 1–2 (citing Spec. ¶ 37). According to Appellants, the Examiner over generalizes the subject matter as "organizing human activities, . . . and/or Using categories to organize, store, and transmit information" because the subject matter is directed toward integration of security objectives in composite applications and addresses that security is one of the major concerns when developing mission critical service oriented composite applications. *Id.* at 3–4.

Appellants further argue independent claims 1, 19, and 20 recite sufficiently concrete features to set them outside the broad definition of abstract idea as set forth in *Alice*:

> "accessing[, by the one or more processors,] a specification for a composite application corresponding to a business process, the composite application comprising local application logic to control interaction of a plurality of external services, the specification being stored in a computer-readable storage medium and comprising: a security annotation that defines a security intention comprising security policies and security capabilities of the composite application" and "invoking[, by the one or more processors,] a security pattern that is stored in a pattern repository and that is selected from a plurality of customizable security patterns based on the security annotation, the security pattern defining entry points that automatically trigger enforcement of the security intention" necessitates an underlying computing device.

Id. at 4.

Appellants further argue, *assuming arguendo*, the claims are directed to an abstract idea, the subject matter of the claims is rooted in computer technology in order to overcome problems specifically arising in the realm of composite application development, including integration of security objectives, which qualifies claims 1, 19, and 20 as patent-eligible subject matter. *Id.* (citing *DDR Holdings, LLC v. Hotels.com, LP*, 773 F.3d 1245 (Fed. Cir. 2014)). According to Appellants, the claims are directed to a problem that is unique to composite application development, and the solution provided by claims 1, 19, and 20 "is tethered to the technology that created the problem." *Id.* at 4–5 (citing *DDR Holdings,* 773 F.3d 1245; *Messaging Gateway Sols., LLC v. Amdocs, Inc.*, No. CV 14-732-RGA, 2015 WL 1744343 (D. Del. Apr. 15, 2015)).

Appellants further refer to PTAB decisions and contend these decisions "illustrate that claimed subject matter fundamentally rooted in computer technology, and claims covering more than mere nominal recitation of a computer and requiring input from physical devices are patent-eligible." *Id.* at 5 (citing *Ex Parte Steve Bush*, Appeal 2013-001110 (Feb. 27, 2015); *T. Rowe Price v. Secure Axcess*, CBM2015-00027 (June 22, 2015). According to Appellants, the claims amount to significantly more than an abstract idea itself. *Id.*

We are not persuaded by Appellants' arguments. The Supreme Court in *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014) reiterated the framework set out in *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 132 S. Ct. 1289 (2012) for "distinguishing patents that claim . . . abstract ideas from those that claim patent-eligible applications of those concepts." *Alice*, 134 S. Ct. at 2355. The first step in the analysis is to determine if the claim is directed toward a patent-ineligible concept and, if so, the second step is to determine whether there are additional elements that transform the nature of the claim into a patent eligible application. *Id.* (citing *Mayo*, 132 S. Ct. at 1297, 1298). The second step searches for an inventive concept that is sufficient to ensure that the patent amounts to significantly more than a patent on the patent-ineligible concept. *Id.* (citing *Mayo*, 132 S. Ct. at 1294).

Applying the first step, we are not persuaded by Appellants' arguments that claims 1–20 are not directed to abstract ideas and agree, instead, with the Examiner's conclusions. In addition, we agree the Examiner has considered the abstract ideas in the aggregate. Accordingly, we find that the claims are directed to a patent-ineligible concept.

Step 2 of the analysis considers whether the claims contain an inventive concept such as additional limitations that narrow, confine or otherwise tie down the claims so that it does not fully cover the abstract idea itself. *See Alice*, 134 S. Ct. at 2357. Here, we agree with the Examiner that no inventive concept is present. In particular, the hardware features are the type of generic element that has been determined to be insufficient by the Supreme Court to transform a patent-ineligible claim into one that is patent-eligible. *See id.* The claims include no limitations that prevent it from covering the abstract idea itself.

Appellants challenge the Examiner's articulation of what the claims are directed to, but the challenge is unfounded. *See* Reply Br. 2–5. For example, the fact that the claims are drafted to include a computing environment is not dispositive. The question is not whether claims mention a computing environment but what they are "directed to." [T]he "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." *Internet Patents Corp. v. Active Network, Inc.*, 790 F.3d 1343, 1346 (Fed. Cir. 2015); *see Genetic Techs. Ltd. v. Merial L.L.C.*, 818 F.3d 1369, 1375, 2016 WL 1393573, at *5 (Fed. Cir. 2016) (inquiring into "the focus of the claimed advance over the prior art");

Enfish, LLC v. Microsoft Corp., 822 F.3d 1327, 1335 (Fed. Cir. 2016). "The 'abstract idea' step of the inquiry calls upon us to 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 Texas v. DirectTV, LLC*, 838 F.3d 1253, 1257 (Fed. Cir. 2016) (quoting *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016)). "In determining the eligibility of respondents' claimed process for patent protection under § 101, their claims must be considered as a whole." *Diamond v. Diehr*, 450 U.S. 175, 188 (1981).

For example, claim 1 includes: accessing a specification for a composite application for a business process; invoking a security pattern that automatically triggers enforcement of a security intention; matching security capabilities to provide a set of identified service providers; identifying a service provider from the set; and invoking the business process using identified service providers. While the claim may additionally recite computer related elements (e.g., "composite application, computer-readable storage medium, automatically trigger, processors, network"), we agree with the Examiner that the claim is directed to "Comparing new and stored information and using rules to identify options."

The Specification supports this view. Spec. Abstract, ¶¶ 2–6. Also, the Specification presents insufficient support that the computer related elements are anything other than conventional and generic. *See, e.g.,* Spec. ¶¶ 152, 154–173.

Appellants also assert the claims are directed to "adding a security annotation to a composite application," but fail to address how that idea is more than the abstract idea of storing information and comparing that information when identifying and selecting web service providers. Reply Br. 2–3. Thus, Appellants have not demonstrated error in the Examiner's conclusion that the claims are directed to an abstract idea. *See* Ans. 3 (stating the claims are directed to "Comparing new and stored information and using rules to identify options").

Moreover, we conclude each of Appellants' claims on appeal is distinguishable from the type of claim recently considered by the court in *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327. We conclude none of Appellants' claims is "directed to an improvement in the functioning of a computer," as was found by the court regarding the subject claim in *Enfish*, 822 F.3d at 1338, because the claims recite conventional computer elements without addressing improvements to the functioning of a computer. To the extent that the recited steps or acts may be performed faster or more efficiently using a computer, our reviewing court provides applicable guidance:

> While the claimed system and method certainly purport to accelerate the process of analyzing audit log data, *the speed increase comes from the capabilities of a general-purpose computer, rather than the patented method itself. See Bancorp Servs., L.L.C. v. Sun Life Assurance Co. of Can. (U.S.)*, 687 F.3d 1266, 1278 (Fed. Cir. 2012) ("[T]he fact that the required calculations could be performed *more efficiently* via a computer does not materially alter the patent eligibility of the claimed subject matter.").

FairWarning IP, LLC v. Iatric Sys., Inc., 839 F.3d 1089, 1095 (Fed. Cir. 2016) (emphasis added).

Applying this reasoning to Appellants' claims on appeal, we similarly find any purported faster or more efficient performance of the claimed steps or acts merely comes from the capabilities of conventional computer processing and/or computer related elements, rather than from Appellants' claimed steps or functions.

With respect to Appellants' arguments that the claims are patent eligible under step two of the *Alice/Mayo* test, Reply Br. 4–5, we are similarly unpersuaded. As discussed above, Appellants have characterized their claim as directed to "add[ing] high-level security intentions or objectives to the business process specification, where the security framework facilitates the automatic generation of the security configuration and enforcement processes." Analyzing the claim limitations, both individually and as an ordered combination, Appellants have not sufficiently demonstrated how the claims are significantly more than the abstract idea of comparing new and stored information and using rules to identify options.

Appellants claims store information, including a security annotation, in a business process (a specification for a composite application) and execute the business process (i.e., set of steps or tasks) after identifying service providers who match the requirements (rules) in the specification. We find the claims here are similar to those in *Accenture Glob. Servs., GmbH v. Guidewire Software, Inc.,* 728 F.3d 1336, 1338–39 (Fed. Cir. 2013), which involved insurance tasks, including rules for determining which tasks to be completed and triggered by specific occurrence of events. Appellants' reliance on *DDR* and other cited cases is misplaced. For example, in *DDR*, the claims at issue involved, *inter alia*, "web pages displays [with] at least one active link associated with a commerce object associated with a buying opportunity of a selected one of a plurality of merchants" (claim 1 of US 7,818,399). The Federal Circuit found the claims in *DDR* to be patent eligible under step two of the *Mayo/Alice* test because "the claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks." *DDR Holdings,* 773 F.3d at 1257. Specifically, the Federal Circuit found the claims addressed the "challenge of retaining control over the attention of the customer in the context of the Internet." *Id.* at 1258. The claims before us are analogous to the claims in *Accenture, and are dissimilar to DDR*'s web page with an active link. Furthermore, as discussed *supra,* the Specification does not support the view that the computer related claim elements are unconventional.

Accordingly, in view of the forgoing, we sustain the 35 U.S.C. § 101 rejection of claim 1 and independent claims 19 and 20 which are of commensurate scope. We also sustain the rejection of dependent claims 2–18 as these claims are not argued separately.

The §102(b) rejections

Appellants argue Anderson is silent as to "composite application" and "security annotation" as recited in claims 1, 19, and. 20. App. Br. 14–15 (citing Anderson ¶¶ 57, 58, 66–78). According to Appellants, "the application of Anderson may be written to understand standard policy statements exported by services and to communicate with other processes or applications, which is different than the composite application including local application logic to control interaction of a plurality of external services." *Id.* at 15. Regarding "security intentions," Appellants argue:

> Anderson provides that preferences among vocabulary items, vocabulary item values, policy constraints, and other elements of a policy may be specified and automatically taken into account by a policy-processing engine (Anderson, ¶ [0023]). That is the policy constraints and preferences of Anderson policy may be specified and automatically taken into account

> by a policy-processing engine, which is different than a security annotation that defines a security intention including security policies and security capabilities of the composite application, as recited in claims 1, 19, and 20.

Id.

Appellants further argue Anderson does not disclose the limitation "invoking, by the one or more processors, a security pattern that is stored in a pattern repository and that is selected from a plurality of customizable security patterns based on the security annotation, the security pattern defining entry points that automatically trigger enforcement of the security intention" because "Anderson [is] silent as to a security pattern as defined in claims 1, 19 and 20." *Id.* According to Appellants, Anderson provides automated matching of policy constraints and this is different than a security pattern defining entry points that automatically trigger enforcement of the security intention. *Id.* (citing Anderson ¶¶ 66–78, 167–175, 23, 70).

Appellants argue Anderson does not disclose the claim limitation:

> for each task of the plurality of tasks:
> matching, using a service broker of the enterprise, security policies and security capabilities of each of a plurality of service providers to the security policies and security capabilities of the composite application to provide a set of identified qualified service providers, and
>
> identifying, from the set of identified qualified service providers, a service provider associated with the external service associated with a respective task and that satisfies the security intention based on the invoked security pattern, the service provider providing a web-based service and communicating with the enterprise over a network.

Id. at. 16.

Appellants argue the policy intersection of Anderson is used to identify vocabulary item values that satisfy the intersection of both policies and also to identify a specific preferred policy set, and this is different than matching, using a service broker of the enterprise, security policies and security capabilities of each of a plurality of service providers to the security policies and security capabilities of the composite application to provide a set of identified qualified service providers, as recited in each of claims. *Id.* According to Appellants, Anderson does not disclose identifying, from the set of identified qualified service providers, a service provider associated with the external service associated with a respective task and that satisfies the security intention based on the invoked security pattern, the service provider providing a web-based service and communicating with the enterprise over a network, as recited in each of claims. *Id.* (citing Anderson ¶¶ 81–92, 100–103, 81).

We are persuaded by Appellants' arguments as, on the record before us, the Examiner presents insufficient factual findings regarding these limitations as required for anticipation. In particular, the Examiner does not sufficiently address the specific identified differences, *supra*, argued by Appellants. For example, Anderson provides automated matching of policy constraints and, on the record before us, this is different than a security pattern defining entry points that automatically trigger enforcement of the security intention. App. Br. 15. A claim is anticipated only if each and every element as set forth in the claims is found, either expressly or inherently described in a single prior art reference, and arranged as required by the claim. *Verdegaal Bros., Inc. v. Union Oil Co. of Cal.*, 814 F.2d 628, 631 (Fed. Cir. 1987).

In view of the above, we do not sustain the rejection of claim 1, and independent claims 19 and 20, which are commensurate in scope and are argued together with claim 1. We also do not sustain the rejection of dependent claims 2–18.

DECISION

We affirm the Examiner's double patenting rejection of claims 1–20.

We affirm the Examiner's decision rejecting claims 1–20 under 35 U.S.C. § 101.

We reverse the Examiner's decision rejecting claims 1–20 under 35 U.S.C. § 102(b).

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

AFFIRMED