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.
11/958,279	12/17/2007	Peter Malcolm	063170.9370	1846

106095 7590 09/30/2019

Baker Botts LLP/CA Technologies
2001 Ross Avenue
SUITE 900
Dallas, TX 75201

EXAMINER	
ZELASKIEWICZ, CHRYSTINA E	

ART UNIT	PAPER NUMBER
3621	

NOTIFICATION DATE	DELIVERY MODE
09/30/2019	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):

PTOmail1@bakerbotts.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte PETER MALCOLM

Appeal 2017-011454[1]
Application 11/958,279[2]
Technology Center 3600

Before ANTON W. FETTING, MICHAEL C. ASTORINO, and TARA L. HUTCHINGS, *Administrative Patent Judges*.

HUTCHINGS, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellant appeals under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1–42 and 64. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.

---

[1] Our Decision references Appellant's Appeal Brief ("App. Br.," filed May 22, 2017) and Reply Brief ("Reply Br.," filed Sept. 12, 2017), and the Examiner's Answer ("Ans.," mailed July 12, 2017) and Final Office Action ("Final Act.," mailed Dec. 21, 2016).

[2] Appellant identifies CA, Inc. as the real party in interest. App. Br. 3.

CLAIMED INVENTION

Appellant's claimed invention "relates to the provision of extended management functionality for Internet applications, particularly in the areas of information security, transaction auditing and reporting, centralized policy, and application connectivity." Spec. ¶ 2.

Claims 1 and 22 are the independent claims on appeal. Claim 22, reproduced below with bracketed notations added, is illustrative of the subject matter on appeal:

> 22. A method of managing information comprising the steps of:
>
> [(a)] providing an application stored in a memory of a workstation for receiving at least inbound data from a computer network;
>
> [(b)] providing policy data, containing rules which define whether or not a validation check is required for a digital certificate used to digitally sign signed data received in said inbound data;
>
> [(c)] identifying, by the workstation, in at least said inbound data, a transaction and the signed data that has been digitally signed with the digital certificate;
>
> [(d)] extracting, by the workstation, one or more details of said signed data;
>
> [(e)] accessing a database to obtain information associated with a history of transmissions signed by said digital certificate;
>
> [(f)] determining, by the workstation, whether or not to request a validation check for said digital certificate, the determining based on the information associated with the history of transmissions signed by said digital certificate and the policy data containing rules which define whether or not a validation check is required for said digital certificate;
>
> [(g)] determining that the validation check for said digital certificate is not required;

> [(h)] accepting, by the workstation, the signed data in response to a determination that the validation check for said digital certificate is not required;
>
> [(i)] allowing the transaction to occur in response to accepting the signed data; and
>
> [(j)] updating the database by updating the history of transmissions signed by said digital certificate to include the transaction.

REJECTIONS

I. Claims 1–42 and 64 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as unpatentable over claims 1–46 of Application No. 11/958,291.

II. Claims 1–42 and 64 are rejected under 35 U.S.C. § 101 as directed to a judicial exception without significantly more.

III. Claims 1–4, 7–17, 19, 21–25, 28–38, 40, 42, and 64 are rejected under 35 U.S.C. § 103(a) as unpatentable over Asay (US 5,903,882, iss. May 11, 1999) and Butt (US 6,754,829 B1, iss. June 22, 2004).

IV. Claims 5, 6, 18, 20, 26, 27, 39, and 41 are rejected under 35 U.S.C. § 103(a) as unpatentable over Asay, Butt, and Cooper (US 2009/0037388 A1, pub. Feb. 5, 2009).

ANALYSIS

Rejection I

We note that Application No. 11/958,291 is now abandoned. Therefore, we dismiss as moot the provisional rejection of claims 1–42 and 64 on the ground of nonstatutory obviousness-type double patenting.

Rejection II

Appellant argues claims 1–42 and 64 together. App. Br. 8–28. We select claim 22 as representative. Claims 1–21, 23–42, and 64 stand or fall with claim 22. *See* 37 C.F.R. §41.37(c)(1)(iv).

Under 35 U.S.C. § 101, an invention is patent-eligible if it claims a "new and useful process, machine, manufacture, or composition of matter." 35 U.S.C. § 101. The Supreme Court, however, has long interpreted § 101 to include an implicit exception: "[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).

The Supreme Court, in *Alice*, reiterated the two-step framework previously set forth in *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 566 U.S. 66 (2012), "for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts." *Alice Corp.*, 573 U.S. at 217. The first step in that analysis is to "determine whether the claims at issue are directed to one of those patent-ineligible concepts." *Id.* If the claims are not directed to a patent-ineligible concept, e.g., an abstract idea, the inquiry ends. Otherwise, the inquiry proceeds to the second step where the elements of the claims are considered "individually and 'as an ordered combination'" to determine whether there are additional elements that "'transform the nature of the claim' into a patent-eligible application." *Id.* (quoting *Mayo*, 566 U.S. at 79, 78). This is "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.'" *Id.* at 217–18 (alteration in original).

The Court acknowledged in *Mayo*, that "all inventions at some level embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas." *Mayo*, 566 U.S. at 71. Therefore, the Federal Circuit has instructed that claims are to be considered in their entirety to determine "whether their character as a whole is directed to excluded subject matter." *McRO, Inc. v. Bandai Namco Games Am., Inc.*, 837 F.3d 1299, 1312 (Fed. Cir. 2016) (quoting *Internet Patents Corp. v. Active Network, Inc.*, 790 F.3d 1343, 1346 (Fed. Cir. 2015)).

The U.S. Patent and Trademark Office (the "USPTO") published revised guidance on January 7, 2019 for use by USPTO personnel in evaluating subject matter eligibility under 35 U.S.C. § 101. That guidance "extracts and synthesizes key concepts identified by the courts as abstract ideas to explain that the abstract idea exception includes" the following three groupings: (1) mathematical concepts; (2) certain methods of organizing human activity, e.g., fundamental economic principles or practices, commercial or legal interactions; and (3) mental processes. 2019 REVISED PATENT SUBJECT MATTER ELIGIBILITY GUIDANCE, 84 Fed. Reg. 50, 52 (Jan. 7, 2019) (the "2019 Revised Guidance").[3]

Under the 2019 Revised Guidance, in determining whether a claim is patent-eligible, we first look to whether the claim recites a judicial exception, including one of the enumerated groupings of abstract ideas ("Step 2A, Prong One"). *Id.* at 54. If so, we next consider whether the claim includes additional elements, beyond the judicial exception, "that

[3] The Revised Guidance, by its terms, applies to all applications, and to all patents resulting from applications, filed before, on, or after January 7, 2019. 84 Fed. Reg. 50.

integrate the [judicial] exception into a practical application," i.e., apply, rely on, or use the judicial exception in a manner that imposes a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the judicial exception. ("Step 2A, Prong Two"). *Id.* at 54–55.

Only if the claim (1) recites a judicial exception and (2) does not integrate that exception into a practical application do we then look to whether the claim "[a]dds a specific limitation or combination of limitations" that is not "well-understood, routine, conventional activity in the field" or simply "appends well-understood, routine, conventional activities previously known to the industry, specified at a high level of generality, to the judicial exception" ("Step 2B"). *Id.* at 56.

Step One of the Mayo/Alice Framework

The Federal Circuit has explained that "the 'directed to' inquiry applies a stage-one filter to claims, considered in light of the [S]pecification, based on whether 'their character as a whole is directed to excluded subject matter.'" *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335 (Fed. Cir. 2016) (quoting *Internet Patents Corp.*, 790 F.3d at 1346).

We are not persuaded that the Examiner erred in determining that claim 22 is directed to an abstract idea. Here, claim 22 recites a method of "managing information" comprising the steps of: ". . . receiving at least inbound data" (limitation (a)); "providing policy data, containing rules which define whether or not a validation check is required for a [] certificate used to [] sign signed data received in said inbound data" (limitation (b)); "identifying . . . in at least said inbound data, a transaction and the signed data that has been [] signed with the [] certificate" (limitation (c));

extracting, . . . one or more details of said signed data" (limitation (d)); ". . . obtain[ing] information associated with a history of transmissions signed by said [] certificate" (limitation (e)); "determining . . . whether or not to request a validation check for said [] certificate, the determining based on the information associated with the history of transmissions signed by said [] certificate and the policy data containing rules which define whether or not a validation check is required for said [] certificate" (limitation (f)); "determining that the validation check for said [] certificate is not required" (limitation (g)); "accepting . . . the signed data in response to a determination that the validation check for said [] certificate is not required" (limitation (h)); "allowing the transaction to occur in response to accepting the signed data" (limitation (i)); and ". . . updating the history of transmissions signed by said [] certificate to include the transaction" (limitation (k)).

These limitations, when given their broadest reasonable interpretation, recite collecting, processing, and storing data for use in a transaction, i.e., a commercial interaction,[4] which is a certain method of organizing human activity, and, therefore, an abstract idea. *See* 2019 Revised Guidance 52.

Having concluded that claim 1 recites a judicial exception, i.e., an abstract idea (Step 2A, Prong One), we next consider whether the claim recites "additional elements that integrate the exception into a practical

[4] We characterized the abstract idea at a higher level of abstraction than the Examiner. However, we find no error in the Examiner's determination that claim 22 is directed to "determining whether a validation check is required on a digital certificate used to sign transaction data." Final Act. 2. This concept also falls into the grouping of subject matter relating to a commercial transaction, i.e., a method of organizing human activity, which is an abstract idea.

application" (Step 2A, Prong Two). Revised Guidance 54; *see also* MANUAL OF PATENT EXAMINING PROCEDURE ("MPEP") § 2106.05(a)–(c), (e)–(h).

Beyond the abstract idea, claim 1 additionally recites an "application," "memory," "workstation," "computer network," "digital certificate," "digitally sign[ing]," and "database." We find no indication in the Specification, nor does Appellant direct us to any indication, that these additional elements implement the abstract idea with a specialized computer hardware or other inventive computer components, i.e., a particular machine, or that the claimed invention is implemented using other than generic computer components to perform generic computer functions. Instead, these elements are described in the Specification at a high level of generality, i.e., as generic computer components. *See, e.g.*, Spec. ¶¶ 3, 4, 5, 7, 10, 14, 55, 58, 64, 81. And "after *Alice*, there can remain no doubt: recitation of generic computer limitations does not make an otherwise ineligible claim patent-eligible." *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1256 (Fed. Cir. 2014).

Appellant contends that the claims are directed to a computer-centric problem associated with digital certificate verification and, thus, are necessarily rooted in computer technology to overcome a problem that specifically arises with computer-implemented communications. App. Br. 9; *see also id.* at 20–21 (arguing that the claims are analogous to the patent-eligible claims in *DDR Holdings*). Similarly, Appellant asserts that the claims are analogous to the claims in *Enfish* because they "improve an existing technological process" by "using a history of transmissions signed by a digital certificate in combination with policy data to determine whether

[to] request a validation check of the digital certificate in a centralized system." App. Br. 19 (citation omitted). Appellant contends that claim 22's limitation (f) reflects a "specific technological solution that leverages the history of transmissions signed by the digital certificate in a single integrated system to determine whether to request verification of a digital certificate and incur the associated costs." *Id.* at 14.

However, we are not persuaded that claim 22 recites any elements, considered individually and as an ordered combination, that address a problem rooted in technology analogous to the situation in *DDR Holdings* or an improvement in computer functionality analogous to the situation in *Enfish*. Instead, claim 22 improves the abstract idea by implementing it in a centralized system and determining whether to request a validation check based on a history of transaction. In this way, the invention avoids payment of fees for unnecessary validity checks. *See* Spec. ¶¶ 15 (describing that digital certificates are verified by third party services for a fee), 141. Thus, we agree with the Examiner (*see* Ans. 5, 8–9) that claim 22 addresses a financial problem with a business solution that saves costs.

Appellant further asserts that eCommerce differs from traditional commerce in that it requires extra security precautions related to identity and trust. App. Br. 10 (citing Spec. ¶ 27). However, we are not persuaded that concerns regarding identity and trust are unique to eCommerce transactions. To the contrary, these concerns play a role in traditional commerce as well, and result in an entity requesting an individual to verify his identity before allowing a transaction to occur.

Appellant asserts that the distributed nature of computer systems give rise to additional technological problems with digital certificates that

claim 22 addresses. App. Br. 11 (citing Spec. ¶ 142). Appellant argues that a single, integrated system for information exchange is needed for digital certificate validation to avoid incurring unnecessary validation costs. *Id.* at 12 (citing Spec. ¶ 28). The Specification describes, for example, that users of a distributed system operate in isolation from other users, and have no ability to share information, even when at the same location. *See* Spec. ¶ 27. As a result, two users in an organization may independently receive e-mail messages digitally signed by the same sender, each incurring a separate validation charge for validating the same digital certificate. *Id.* Another consequence of this paradigm is that multiple users may request validation of a certificate that has been revoked, incurring unnecessary charged. *Id.* ¶ 141. Yet, we are not persuaded that using an integrated system to process information regarding digital certificate validation reflects an improvement to technology. Instead, the improvement is realized by linking use of the abstract idea in a particular technological environment (i.e., a centralized system).

Appellant alleges that paragraph 143 of the Specification "specifically address[es] the technological solution to which the [c]laims are directed." *Id.* at 13. This paragraph, however, explains that information about the digital certificates that have been received is stored, together with the status of the certificate at the last check and transaction history. Put differently, this paragraph represents the abstract idea to which claim 22 is directed. *See Two-Way Media Ltd. v. Comcast Cable Communications, LLC*, 874 F.3d 1329, 1337 (2017) (a claim that recites the functional results of converting, routing, controlling, monitoring and accumulating records, without

sufficiently describing how to achieve this result, is directed to an abstract idea).

Appellant argues that claim 22 is patent-eligible because it allegedly avoids preemption. *See* App. Br. 16. Appellant's argument is unpersuasive of Examiner error. Although preemption is the concern that drives the exclusion of abstract ideas from patent eligible subject matter (*see Alice*, 573 U.S. at 216), it is not a separate test for patent eligibility. Instead, the proper test for determining whether a claim recites patent eligible subject matter is to apply the two-step framework that the Supreme Court delineated in *Alice* and *Mayo*. "Where a patent's claims are deemed only to disclose patent ineligible subject matter under the *Mayo* framework . . . , preemption concerns are fully addressed and made moot." *Ariosa Diagnostics, Inc. v. Sequenom, Inc.*, 788 F.3d 1371, 1379 (Fed. Cir. 2015). "[P]reemption may signal patent ineligible subject matter, [but] the absence of complete preemption does not demonstrate patent eligibility." *Id.*

We also find no indication in the Specification that the claimed invention effects a transformation or reduction of a particular article to a different state or thing. Nor do we find anything of record, short of attorney argument, that attributes an improvement in technology and/or a technical field to the claimed invention or that otherwise indicates that the claimed invention integrates the abstract idea into a "practical application," as that phrase is used in the 2019 Revised Guidance. *See* Revised Guidance 55.

For example, each of steps (a)–(j) is written as result-based limitations without technological details for how to achieve the desired results. *See Intellectual Ventures I LLC v. Capital One Fin. Corp.*, 850 F.3d 1332, 1342 (Fed. Cir. 2017) (explaining that "[o]ur law demands more" than claim

language that "provides only a result-oriented solution, with insufficient detail for how a computer accomplishes it"). Appellant's Specification also fails to provide any such technological details for each of these steps.

Having determined under step one of the *Mayo*/*Alice* framework that claim 1 is directed to an abstract idea, we next consider under Step 2B of the 2019 Revised Guidance, the second step of the *Mayo*/*Alice* framework — whether claim 1 recites additional elements that provide an inventive concept (i.e., whether the additional elements amount to significantly more than the judicial exception itself).

Appellant contends that "the use of the history of transmissions in combination with policy data in determining whether or not to request a validation check of a digital certificate" constitutes an inventive concept. App. Br. 14. Yet, this concept is part of the abstract idea, and the inventive concept under step two of the *Mayo*/*Alice* test cannot be the abstract idea itself:

> It is clear from *Mayo* that the "inventive concept" cannot be the abstract idea itself, and *Berkheimer* . . . leave[s] untouched the numerous cases from this court which have held claims ineligible because the only alleged "inventive concept" is the abstract idea.

Berkheimer v. HP Inc., 890 F.3d 1369, 1374 (Fed. Cir. 2018) (Moore, J., concurring).

Appellant additionally argues that the location of the determining step presents an inventive concept. App. Br. 15 (citing Spec., Fig. 5). Specifically, Appellant asserts that "the e-mail is examined before the e-mail is even placed in the Inbox[;]" however, "[if] the user is required to enter a decryption key, the message is examined immediately following decryption, but before viewing." *Id.* (citing Spec. ¶ 94). However, these features are not

recited in claim 22. Instead, claim 22 recites that accepting the signed data occurs in response to a determination that a validation check is not required. There is no indication that the claimed accepting (limitation (h)) entails more than authenticating the digital certificate as valid without performing a validation check, such that the transaction is allowed to proceed (limitation (i)). *See* App. Br. 7 (citing Spec. ¶¶ 143–44 as describing the claimed step of accepting); *see also* Spec. ¶¶ 143–44.

However, even if claim 22 were to recite preventing a message from being placed in an inbox until it was determined that a validation check is not required, it is unclear, and Appellant does not describe, how this change would constitute an inventive concept significantly more than the abstract idea, as opposed to an improvement to a process that is itself abstract.

As we explained above, the only additional recited elements claim 22 recites beyond the abstract idea are an "application," "memory," "workstation," "computer network," "digital certificate," "digitally sign[ing]," and "database," which are described in the Specification at a high level as generic components performing generic functions. Appellant cannot reasonably contend, nor does Appellant, that there is a genuine issue of material fact regarding whether any of these additional elements, considered alone and as an ordered combination, is well-understood, routine, or conventional, where nothing in the Specification indicates that the operations recited in claim 22 are implemented using anything other than generic computer components to perform generic computer functions, e.g., receiving and processing information, and displaying the results.

We are not persuaded, on the present record, that the Examiner erred in rejecting claim 22 under 35 U.S.C. § 101. Therefore, we sustain the

Examiner's rejection of claim 22 and claims 1–21, 23–42, and 46, which fall with claim 22.

Rejection III

Independent Claims 1 and 22, and Dependent Claims 2–4, 7–17, 19, 21, 23–25, 28–38, 40, 42, and 64

We are persuaded by Appellant's argument that the Examiner erred in rejecting claims 1 and 22 under 35 U.S.C. § 103(a) because Butt and Asay, considered alone or in combination, do not teach or suggest "determining . . . whether or not to request a validation check for said digital certificate, the determining based on the information associated with the history of transmissions signed by said digital certificate and the policy data containing rules which define whether or not a validation check is required for said digital certificate," as recited in limitation (f) of claim 22, and similarly recited in claim 1. App. Br. 29–32; *see also* Reply Br. 2–3. The Examiner acknowledges that Asay does not disclose the argued limitation, and relies on Butt to cure the deficiency. Final Act. 6–7 (citing Butt col. 4, ll. 31–51; col. 7, ll. 20–47; col. 10, ll. 53–65).

Butt relates to providing remote access to manageable devices using certificates with embedded cryptographic data to validate operator identity and access rights. Butt, col. 1, ll. 7–11. Manageable devices are preconfigured to trust a signing certificate at installation time. *Id.* at col. 7, ll. 3–6. The manageable device agrees to trust any session certificate created by an owner of a signing certificate. *Id.* at col. 7, ll. 7–10. The manageable device maintains a list of trusted signing certificates, allowing it to trust more than one core (i.e., a computer on which management services reside). *Id.* at col. 3, ll. 17–20; col. 7, ll. 24–26. Each certificate contains

information about the issuer, which enables identification of the core's signing certificate in the trusted certificate list. *Id.* at col. 7, ll. 26–31. Further, trusted cores maintain a list of other trusted cores, and instruct the manageable device to add certificates for these other trusted cores to its trusted certificate list. *Id.* at col. 7, ll. 36–40.

The Examiner takes the position that the manageable device's list of trusted signing certificates teaches the claimed "determining based on the information associated with the history of transmissions signed by said digital certificate," as recited in claim 22's limitation (f), and similarly recited in claim 1. Final Act 7 (citing Butt, col. 7, ll. 20–47). Yet, the cited portion of Butt does not describe a history of transmissions signed by the signing certificate, much less that a step of determining whether to request a validation check for a digital certificate is based on information related thereto, as required by limitation (f) of claim 22, and similarly required by claim 1.

In the remarks, the Examiner additionally finds that Asay discloses this aspect of the claim language. *See* Final Act. 21–22 (citing Asay, col. 14, ll. 43–55); *see also* Ans. 10 (citing Asay, col. 14, ll. 43–53; col. 25, ll. 1–7). Asay describes that a certificate validity database includes, for each primary certificate, the following information: validity status; supplemental assurance parameters applicable to secondary certificates based on the primary certificate; and links to account history and periodic reporting information. Asay, col. 14, ll. 43–48. Yet, we find nothing in the cited portion indicating that information associated with a history of transmissions signed by a digital certificate is used in a step of determining.

Asay also provides an example in which Perry is concerned about Susan's ability to pay $10,000 for widgets. *Id.* at col. 24, ll. 64–66. Rather than seeking supplemental certificates (e.g., a letter of credit from Susan's bank), a digital signal is verified. *Id.* at col. 25, ll. 1–5. But this cited portion does not teach or suggest that information associated with a history of transmissions signed by the signing certificate is used to determine whether to request a validation check for a digital certificate, as required by claim 22, limitation (f), and similarly required by claim 1.

In view of the foregoing, we do not sustain the Examiner's rejection under 35 U.S.C. § 103(a) of independent claims 1 and 22, and dependent claims 2–4, 7–17, 19, 21, 23–25, 28–38, 40, 42, and 64.

Rejection IV

Dependent Claims 5, 6, 18, 20, 26, 27, 39, and 41

The Examiner's rejection of dependent claims 5, 6, 18, 20, 26, 27, 39, and 41 under 35 U.S.C. § 103(a) as unpatentable over Asay, Butt, and Cooper does not cure the deficiency in the Examiner's rejection of independent claims 1 and 22 under U.S.C. § 103(a) as unpatentable over Asay and Butt. Therefore, we do not sustain the Examiner's rejection of claims 5, 6, 18, 20, 26, 27, 39, and 41 under 35 U.S.C. § 103(a) for the same reason set forth above with respect to the independent claims.

DECISION

We dismiss the Examiner's provisional rejection of claims 1–42 and 64 on the ground of nonstatutory obviousness-type double patenting.

We affirm the Examiner's rejections of claims 1–42 and 64 under 35 U.S.C. § 101.

We reverse the Examiner's rejections of claims 1–42 and 64 under 35 U.S.C. § 103(a).

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