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.
13/928,464	06/27/2013	Amnon Perlmutter	1893/181	2477

44696   7590   12/16/2019

Dr. Mark M. Friedman
Moshe Aviv Tower, 54th floor
7 Jabotinsky St.
Ramat Gan, 5252007
ISRAEL

EXAMINER
DESROSIERS, EVANS

ART UNIT	PAPER NUMBER
2491	

NOTIFICATION DATE	DELIVERY MODE
12/16/2019	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):

friedpat.uspto@gmail.com
patents@friedpat.com
rivka_f@friedpat.com

PTOL-90A (Rev. 04/07)

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte AMNON PERLMUTTER and LIOR DRIHEM

Appeal 2018-000294
Application 13/928,464
Technology Center 2400

Before THU A. DANG, ERIC S. FRAHM, and MATTHEW J. McNEILL,
Administrative Patent Judges.

DANG, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE

Pursuant to 35 U.S.C. § 134(a), Appellants[1] appeal from the
Examiner's decision to reject claims 26–52. Claims 1–25 were previously
canceled. App. Br. 5. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.

---

[1] We use the word "Appellants" to refer to "Applicant" as defined in 37
C.F.R. § 1.42. Appellants identify the real party in interest as Check Point
Software Technologies Ltd. Appeal Br. 1.

CLAIMED SUBJECT MATTER

According to Appellants, the claimed invention "relates to enterprise data security and, more particularly, to a method of enabling, for an employee of an enterprise, secure and convenient use of enterprise applications on a personal device of the employee." Spec. 1:11–13.

Claim 26, reproduced below, is illustrative of the claimed subject matter:

26. A method of providing security, comprising the steps of:
(a) providing a long secret with associated identification information;
(b) providing a short secret;
(c) providing a key;
(d) initiating generating of an encrypted key by encrypting said key using said long secret; and
(e) initiating storing of:
      (i) said key;
      (ii) said identification information; and
      (iii) said short secret,
wherein said storing of said key is in association with said identification information and said short secret.

REFERENCES

The prior art relied upon by the Examiner is:

Name	Reference	Date
Verma	US 2012/0114118 A1	May 10, 2012
Rouse	US 2010/0266127 A1	Oct. 21, 2010

REJECTIONS

Claims 26–52 stand rejected under 35 U.S.C. § 101 as being directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea); and not directed to significantly more than the abstract idea itself.

Claims 26–52 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Verma and Rouse. App. Br. 5

ANALYSIS

Except where indicated, we adopt the Examiner's findings in the Answer and Final Office Action and we add the following primarily for emphasis. We note that if Appellants failed to present arguments on a particular rejection, we decline to review unilaterally those uncontested aspects of the rejection. *See Ex parte Frye*, 94 USPQ2d 1072, 1075 (BPAI 2010) (precedential); *Hyatt v. Dudas*, 551 F.3d 1307, 1313–14 (Fed. Cir. 2008) (the Board may treat arguments Appellant failed to make for a given ground of rejection as waived).

Rejection of claims 26–52 under 35 U.S.C. § 101

In determining whether a claim falls within an excluded category, we are guided by the Supreme Court's two-step framework, described in *Mayo* and *Alice*. *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 216–218 (2014) (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, 69 (1972)).

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 (internal citation 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.* (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.*

The PTO recently published revised guidance on the application of § 101. USPTO's January 7, 2019 Memorandum, *2019 Revised Patent Subject Matter Eligibility Guidance* ("Memorandum"). Under that guidance, 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); and
> (2) additional elements that integrate the judicial exception into a practical application (*see* Manual of Patent Examining Procedure (MPEP) § 2106.05(a)–(c), (e)–(h) (9th Ed., Rev. 08.2017, Jan. 2018)).

Only if a 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:

(3) adds a specific limitation beyond the judicial exception that are 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.

See Revised Guidance, 84 Fed. Reg. 56.

<div align="center">Revised Guidance Step 1</div>

Step 1 of the Revised Guidance asks whether the claimed subject matter falls within the four statutory categories of patentable subject matter identified by 35 U.S.C. § 101: process, machine, manufacture, or composition of matter. Independent claim 26 recites a "method of providing security." Independent claim 44 recites a "user device" comprising a "processing system." Appellants do not argue the Examiner erred in concluding claims 26 and 44 fall within the four statutory categories of patentable subject matter. We agree with the Examiner's conclusion because claim 26 falls within the process category and claim 44 falls within the machine category.

<div align="center">Revised Guidance Step 2A, Prong 1</div>

Under Step 2A, Prong 1 of the Revised Guidance, we determine whether the claims recite 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). *See* Revised Guidance.

The Examiner concludes "[t]he claim(s) is/are directed to the abstract idea of itself of 'Data recognition and storage.'" Final Act. 4; Ans. 9 (emphasis omitted). However, Appellants contend that the claims are not "an abstract idea," because the claims are "not directed to data recognition,

<div align="center">5</div>

but rather, to providing and generating cyber security elements." App. Br. 10.

Independent claim 26 recites, in relevant part, (1) "providing a long secret with associated identification information;" (2) "providing a short secret;" (3) "providing a key;" (4) "initiating generating of an encrypted key . . . using said long secret;" and (5) "initiating storing" of the key, information and short secret, wherein the storing is "in association" with the identification information. Independent claim 44 recites a "user device" comprising a "processing system" being configured to perform steps similar to those in claim 26. That is, claims 26 and 44 merely recite the steps (or a processing system performing the steps) of providing data, initiating the generating of data based on the provided data, and then initiating the storing of the generated data in association with the provided data.

We agree with the Examiner that these limitations, under their broadest reasonable interpretation, recite "Data recognition and storage." That is, these limitations merely comprise steps of "providing," "generating . . . using," and at least one step of "storing . . . in association with" various recognized data, constituting an evaluation or judgment, identified as an exemplary mental process in the Revised Guidance. *See* Revised Guidance, 84 Fed. Reg. at 52. As the Examiner explains, "[t]he claims, as a whole, . . . can be performed entirely by a human . . . as a person can use a pen and a piece of paper to write down random numbers." Ans. 9.

In particular, these steps of storing and recognizing data constitute mental steps because they involve merely making a mental observation of data and evaluating/judging the data, which can be carried out either in the human mind (e.g., in the form of noting an observation) or with the aid of

6

pencil and paper. *See* 2019 Guidance 52 n.14; *see* also *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016) ("[W]e have treated collecting information, including when limited to particular content (which does not change its character as information), as within the realm of abstract ideas."). Acts that can be performed in the human mind fall within the abstract idea exception subgrouping of mental processes.

Thus, under the broadest reasonable interpretation, we conclude claims 26 and 44 recite an evaluation or judgment, which falls within the mental processes category of abstract ideas identified in the Revised Guidance.

<div align="center">Revised Guidance Step 2A, Prong 2</div>

Under Step 2A, Prong 2 of the Revised Guidance, we next determine whether the claims recite additional elements that integrate the judicial exception into a practical application (see MPEP §§ 2106.05(a)–(c), (e)–(h)).

Appellants contend that "[t]he claimed invention is directed to providing several elements . . ., then these provided elements are used to generate an additional element (an encrypted key) with an innovative combination of elements stored in associated with each other." App. Br. 10. Thus, according to Appellants, "the claimed invention is not directed to data recognition, but rather, to providing and generating cyber security elements." *Id.* We are not persuaded by Appellants' arguments.

Notably, Appellants have not persuasively explained how claim 26 and/or claim 44 recites improvements to any technology or technical field (see MPEP § 2106.05(a)), improves a particular machine (see MPEP § 2106.05(b)), transforms or reduces a particular article to a different state or thing (see MPEP § 2106.05(c)), or describes a process or product that

applies the exception in a meaningful way, such that it is more than a drafting effort designed to monopolize the exception (see MPEP § 2106.05(e)). *See* App. Br. 10–12. Instead, as Appellants concede, the claimed invention is merely directed to providing several elements, i.e., data, wherein then these provided elements/data are used to generate an additional element, i.e., additional data. App. Br. 10. As the Examiner explains, "key generation does not necessarily require a machine as a person can use a pen and a piece of paper to write down random numbers." Ans. 9.

Because these claimed steps of claim 26 set forth an abstract idea, we do not identify any other additional element(s) sufficient to integrate the abstract idea into a patent-eligible practical application. Similarly, we do not identify any other additional element(s) in claim 44, reciting a "processing system" being configured to perform steps similar to those in claim 26, sufficient to integrate the abstract idea into a patent-eligible practical application.

Accordingly, we conclude claims 26 and 44 do not integrate the judicial exception into a practical application because claims 26 and 44 recite a method that could be performed mentally without integrating that mental process into a particular application.

<div align="center">Revised Guidance Step 2B</div>

Under Step 2B of the Revised Guidance, we next determine whether the elements in the claims both individually and "as an ordered combination" recite an "inventive concept" that "must be significantly more than the abstract idea itself, and cannot simply be an instruction to implement or apply the abstract idea on a computer." *BASCOM Global Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1349 (Fed. Cir.

<div align="center">8</div>

2016). There must be more than "computer functions [that] are 'well-understood, routine, conventional activit[ies]' previously known to the industry." *Alice*, 573 U.S. at 225 (quoting *Mayo*, 566 U.S. at 73).

Here, the Examiner concludes the claims "as a whole, require generic computer implementation or can be performed entirely by a human." Ans. 9. That is, "providing security using and storing different types of keys . . . does not [even] require machine implementation." *Id.*

In response, Appellants contend "[s]ecrets and keys [as claimed] are elements of cyber security, directed to the way computers operate, as they improve the functioning of computers and computer networks." App. Br. 10. According to Appellants, the claim's "method of providing security thus does recite an improvement to the functioning of the computer itself, qualifies as 'significantly more', and is proper under U.S.C. §101." *Id.* at 11. However, we are not persuaded by Appellants' argument.

To the extent Appellants contend that the recited limitations add significantly more than the abstract idea to provide an inventive concept under *Alice/Mayo* (*see* Appeal Br. 10), generating keys/data is not an additional element beyond the abstract idea, but rather is part of the abstract idea itself. *See BSG Tech LLC v. BuySeasons, Inc.*, 899 F.3d 1281, 1290 (Fed. Cir. 2018) (explaining that the Supreme Court in *Alice* "only assessed whether the claim limitations other than the invention's use of the ineligible concept to which it was directed were well understood, routine and conventional").

We briefly look to whether any additional limitations in claim 26 and 44 include an inventive concept. Here, limitations of "providing" secrets and keys, "initiating generating" of keys, and "initiating storing" of keys,

information and secrets, as set forth in claims 26 and 44, individually or as an ordered combination, do not define ways of providing, generating, or storing data that is different than any of the myriad conventional ways in which a computer can provide, generate, or store data, and thus do not provide an inventive concept. *See, e.g., buySAFE, Inc. v. Google, Inc.*, 765 F.3d 1350, 1355 (Fed. Cir. 2014) ("That a computer receives and sends the information over a network—with no further specification—is not even arguably inventive."). The focus of claims 26 and 44 is not on an improvement in computer processors as tools, but on certain independently abstract ideas that use conventional computing components as tools. *See FairWarning IP, LLC v. IA*, 839 F.3d 1089, 1095 (Fed. Cir. 2016). As with the ineligible claimed invention in *BSG*, the claimed invention does not improve a computer's functionality or that of its associated components, but rather the benefits flow from performing the abstract idea in conjunction with those conventional computer components. *See BSG*, 899 F.3d at 1288 ("While the presentation of summary comparison usage information to users improves the quality of the information added to the database, an improvement [in] . . . the information stored by a database is not equivalent to an improvement in the database's functionality.").

Therefore, claims 26 and 44 do not recite an inventive concept. Accordingly, we agree with the Examiner that independent claims 26 and 44, and claims depending respectively therefrom and not specifically argued separately, are directed to patent-ineligible subject matter.

Rejection of claims 26–52 under 35 U.S.C. § 103(a) as being unpatentable over Verma and Rouse.

Appellants contend that "Verma teaches in paragraph [0010] (cited by the Examiner) that the long-term key identifier is used for locating a long-term key, and the long-term key is used for encrypting a short-term key," whereas "the current claims recite encrypting a 'key' using a 'long secret.'" Appeal Br. 13. According to Appellants, "Verma has no need for a 'key' in addition to the 'short term key', as Verma encrypts the short-term key." *Id.* at 14.

Similarly, Appellants contend that "Rouse teaches in paragraph [0009]-[0010] (cited by the Examiner) that the encrypted Long Term Key is used on the Originator with the Session Key," whereas "the current claims store the key in association with the identification information and the short secret." *Id.* That is, "Rouse has no need for a short secret, as the Session Key is associated directly with an encrypted Long Term Key." *Id.*

We have considered all of Appellants' arguments and evidence presented. We agree with Appellants that the preponderance of evidence on this record does not support the Examiner's legal conclusion that claims 26 and 52 would have been obvious over Verma and Rouse.

As Appellants argue, Verma discloses a "memory component" that stores a "long-term key identifier for locating a long-term key used for encrypting a short-term key." *See* Verma ¶ 10. In particular, Verma discloses providing a long-term key with associated identification information, providing a short-term key, and encrypting the short-term key using the long-term key. *Id.* Thus, Verma does not disclose <u>both</u> a "short secret" <u>as well as</u> a "key," wherein the "key" is encrypted and then stored "in association with" the "short secret." *See* claim 26. Instead, Verma only

discloses a single "short-term key" that is encrypted by the long-term key but is not stored in association with any short secret. Verma ¶ 10.

Further, Rouse discloses "encrypt[ing] the Session Key using a Long Term Key" (Rouse ¶ 10), wherein the Long Term Keys "are stored in a Long Term Key File and each is associated with a Long Term Key version number." Rouse ¶ 36. In particular Rouse discloses providing a Long-Term Key with associated identification information, providing a Session Key, and encrypting the Session Key using the Long Term Key. *Id.* at ¶¶ 10, 36. Thus, like Verma, Rouse does not disclose both a "short secret" as well as a "key," wherein the "key" is encrypted and then stored "in association with" the "short secret." *See* claim 26. Instead, Verma only discloses a single "Session Key" that is encrypted by the Long Term Key but is not stored in association with any short secret. Rouse ¶¶ 10, 36.

Thus, contrary to the Examiner's findings (Ans. 11–19), neither Verma nor Rouse, alone or in combination, teaches or suggests both a "short secret" as well as a "key," wherein the "key" is encrypted by a "long secret" and then stored "in association with" the "short secret." Claim 26.

In such case, we would have to engage in some degree of speculation regarding the Examiner's finding and conclusion that the references teaches and suggests these recited limitations. Ans. 11–19. We decline to engage in speculation.

Accordingly, we are persuaded by Appellants' contentions that Verma and Rouse fail to teach or suggest the contested limitations recited in independent claim 26, and similarly recited in independent claim 44. Because we find at least these errors with respect to the Examiner's rejections, we need not and do not make any findings with respect to the

other contested limitations. Rather, we confine our findings to these argued features, which are dispositive of this appeal.

Consequently, we are constrained by the record before us to find that the Examiner erred in finding the combination of Verma and Rouse teaches or suggests Appellants' claims 26 and 44. We also do not sustain the Examiner's obviousness rejection of dependent claims 27–43, and 45–52 depending respectively from claims 26 and 44 but not separately argued, over Verma and Rouse.

CONCLUSION

The Examiner's rejection of claims 26–52 under 35 U.S.C. § 101 as being directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea); and not directed to significantly more than the abstract idea itself is affirmed.

However, the Examiner's rejection of claims 26–52 under 35 U.S.C. § 103(a) as being unpatentable over Verma and Rouse is reversed.

Because we affirm at least one ground of rejection with respect to each claim on appeal, the Examiner's decision is affirmed.

DECISION SUMMARY

Claims Rejected	35 U.S.C. §	Basis	Affirmed	Reversed
26–52	101	Eligibility	26–52	
26–52	103(a)	Verman, Rouse		26–52
Overall Outcome:			26–52	

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). *See* 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED