UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/710,050	05/12/2015	Thorsten SCHWEPP	BOSC.P9246US/11604276	1873

24972 7590 03/11/2019
NORTON ROSE FULBRIGHT US LLP
1301 Avenue of the Americas
NEW YORK, NY 10019-6022

EXAMINER	
JHA, ABDHESH K	

ART UNIT	PAPER NUMBER
3665	

NOTIFICATION DATE	DELIVERY MODE
03/11/2019	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):

nyipdocket@nortonrosefulbright.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte THORSTEN SCHWEPP, INGO OPFERKUCH, MARKUS IHLE,
and HOLGER EGELER

Appeal 2017-011732
Application 14/710,050[1]
Technology Center 3600

Before JOSEPH A. FISCHETTI, BRUCE T. WIEDER, and
BART A. GERSTENBLITH, *Administrative Patent Judges*.

WIEDER, *Administrative Patent Judge*.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134 from the Examiner's rejection of claims 1–10. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM-IN-PART.

CLAIMED SUBJECT MATTER

Appellants' invention "relates to a method for preventing an unauthorized operation of a motor vehicle, to an electronic hardware security

[1] According to Appellants, the real party in interest is ROBERT BOSCH GmbH. (Appeal Br. 1.)

module for implementing the method, and to a control unit including such an electronic hardware security module." (Spec. 1, ll. 2–4.)

Claims 1, 5, and 9 are the independent claims on appeal. Claim 1 is illustrative. It recites:

> 1. A method for preventing an unauthorized operation of a motor vehicle, which uses a vehicle immobilizer software, comprising:
>
> at least partially storing the vehicle immobilizer software in an electronic hardware security module.

REJECTIONS[2]

Claims 1, 5, 6, and 9 are rejected under 35 U.S.C. § 101 as directed to non-statutory subject matter.

Claims 1–3 and 5–9 are rejected under 35 U.S.C. § 103 over Admitted Prior Art and Marco Wolf & Andre Weimerskirch, *Hardware Security Modules for Protecting Embedded Systems*, https://www.escrypt.com/fileadmin/escrypt/pdf/WP-Embedded-HSM.pdf (last visited June 6, 2016) (hereinafter "Wolf").

Claims 4 and 10 are rejected under 35 U.S.C. § 103 over Admitted Prior Art, Wolf, and Official Notice.

ANALYSIS

The § 101 rejection

Claims 1, 5, 6, and 9 are rejected under § 101. Appellants do not separately argue the claims. (*See* Appeal Br. 4–6.) We select claim 1 as

[2] The rejection of claims 2, 3, 4, 7, 8, and 10 under 35 U.S.C. § 112(a) was withdrawn. (*See* Answer 2.)

representative. Claims 5, 6, and 9 will stand or fall with claim 1. *See* 37 C.F.R. § 41.37(c)(1)(iv).

"Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title." 35 U.S.C. § 101. Section 101, however, "'contains an important implicit exception: Laws of nature, natural phenomena, and abstract ideas are not patentable.'" *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 216 (2014) (quoting *Assoc. for Molecular Pathology v. Myriad Genetics, Inc.*, 569 U.S. 576, 589 (2013)).

Alice applies a two-step framework, earlier set out 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*, 573 U.S. at 217.

Under the two-step framework, it must first be determined if "the claims at issue are directed to a patent-ineligible concept." *Id.* If the claims are determined to be directed to a patent-ineligible concept, then the second step of the framework is applied to determine if "the elements of the claim . . . contain[] an 'inventive concept' sufficient to 'transform' the claimed abstract idea into a patent-eligible application." *Id.* at 221 (citing *Mayo*, 566 U.S. at 72–73, 79).

With regard to step one of the *Alice* framework, we apply a "directed to" two prong test to: 1) evaluate whether the claim recites a judicial exception, and 2) if the claim recites a judicial exception, evaluate whether the claim "appl[ies], rel[ies] on, or use[s] 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." *See 2019 Revised Patent Subject Matter Eligibility Guidance*, 84 Fed. Reg. 50, 54 (Jan. 7, 2019) (hereinafter "2019 Guidance").

The Examiner determines that claim 1 is "directed to the abstract idea [of] storing the vehicle immobilizer software in an electronic security module." (Final Action 5.)

Appellants argue that "[t]he choice of the HSM [hardware security module] module [sic] as the storage location is a concrete innovation, and therefore not abstract, because the step of storing in an HSM involves a new place, a new component, in which to store the immobilizer software." (Appeal Br. 5.)

The Specification provides evidence as to what the invention is directed. In this case, the Specification discloses that the invention "relates to a method for preventing an unauthorized operation of a motor vehicle, to an electronic hardware security module for implementing the method, and to a control unit including such an electronic hardware security module." (Spec. 1, ll. 2–4.) The Specification further discloses "that the vehicle immobilizer software as part of the control unit software authenticates its counterpart via a question-answer method or a challenge/response method" and that "[t]he hardware security module is utilized for the cryptographic calculations." (*Id.* at 2, ll. 18–20.) Claim 1, however, does not recite vehicle immobilizer software authenticating its counterpart, nor does it recite any utilization of cryptographic calculations. Rather, claim 1 merely recites storing some unspecified part of certain software (i.e., the vehicle immobilizer software) in an HSM. This is simply the idea of storing information in a particular location which, under the 2019 Guidelines, is categorized as a mental process, similar to the idea of storing information by remembering it or writing it down.

Although we and the Examiner describe, at different levels of abstraction, to what the claims are directed, it is recognized that "[a]n abstract idea can generally be described at different levels of abstraction." *Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229, 1240 (Fed. Cir. 2016). That need not and, in this case does not, "impact the patentability analysis." *See id.* at 1241.

We contrast the present claim 1 with claim 1 in *Ancora Technologies, Inc. v. HTC America, Inc.*, 908 F.3d 1343 (Fed. Cir. 2018). In *Ancora*, claim 1 recited:

> 1. A method of restricting software operation within a license for use with a computer including an erasable, non-volatile memory area of a BIOS of the computer, and a volatile memory area; the method comprising the steps of:
>
> selecting a program residing in the volatile memory,
>
> using an agent to set up a verification structure in the erasable, non-volatile memory of the BIOS, the verification structure accommodating data that includes at least one license record,
>
> verifying the program using at least the verification structure from the erasable non-volatile memory of the BIOS, and
>
> acting on the program according to the verification.

Id. at 1345–46. In *Ancora*, the Federal Circuit determined that claim 1 was not directed to an abstract idea because

> [t]he claimed method here [(1)] specifically identifies how that functionality improvement is effectuated in an assertedly unexpected way: a structure containing a license record is stored in a particular, modifiable, non-volatile portion of the computer's

> BIOS, and [(2)] the structure in that memory location is used for verification by interacting with the distinct computer memory that contains the program to be verified.

Id. at 1348–49. Unlike claim 1 in *Ancora*, Appellants' claim 1 does not recite how the structure in the memory location is used.[3] Nor does Appellants' claim 1 recite any characteristics of the hardware security module into which the portion of the vehicle immobilizer software is to be stored.

The Federal Circuit contrasted the claimed invention in *Ancora* with that in *Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307 (Fed. Cir. 2016). Although *Symantec* was a step two case under the *Alice* framework, the Federal Circuit, recognizing the "overlap[] between some step one and step two considerations," determined that one of the claimed inventions in *Symantec*

> required the installation of virus screening software on a telephone network. But because the claim at issue did not "recite[] any improvement to conventional virus screening software, nor . . . solve any problem associated with situating such virus screening on the telephone network," we held that the patent did not identify a sufficient inventive concept under *Alice* to transform the claimed abstract idea into something patentable.

Ancora Techs, Inc., 908 F.3d at 1349–50. Like *Symantec*, the claimed invention here merely stores certain software in a certain location. Appellants do not identify any known problem in storing software, e.g., vehicle immobilizer software, in an HSM.

[3] We note that, e.g., claim 2, which the Examiner does not reject under § 101, generally recites a use of the vehicle immobilizer software stored in the HSM.

Appellants do not argue that they invented vehicle immobilizer software or a hardware security module. Claim 1 is simply directed to the idea of storing some unspecified part of the vehicle immobilizer software in the HSM. We do not see how the mere recitation of a hardware security module, even in conjunction with the recited storing function, "ensure[s] 'that the [claim] is more than a drafting effort designed to monopolize the [abstract idea]." *Alice*, 573 U.S. at 221 (brackets in original) (quoting *Mayo*, 566 U.S. at 77.) Moreover, the limitations of claim 1 do not recite implementation details. Rather, "the recited physical components merely provide a generic environment in which to carry out the abstract idea." *In re TLI Commc'ns LLC Patent Litig.*, 823 F.3d 607, 611 (Fed. Cir. 2016).

Appellants argue that "storing the immobilizer software in an HSM . . . represents a technological innovation in that the particular storage location . . . is an unconventional storage location for this software." (Appeal Br. 5.) As discussed above, Appellants do not identify any known problem in storing software in an HSM. Nor do Appellants persuasively argue why merely using an allegedly novel storage location constitutes a technological innovation that transforms the claim into patent-eligible subject matter. It is well established that "[t]he 'novelty' of any element or steps in a process, [i.e., the asserted unconventional storage location,] or even of the process itself, is of no relevance in determining whether the subject matter of a claim falls within the § 101 categories of possibly patentable subject matter." *Diamond v. Diehr*, 450 U.S. 175, 188–89 (1981). Moreover, "the claim language here provides only a result-oriented solution, with insufficient detail for how [it would be accomplished]."

Intellectual Ventures I LLC v. Capital One Fin. Corp., 850 F.3d 1332, 1342 (Fed. Cir. 2017).

Appellants also argue that "[t]he claims do not preempt all ways of securing the immobilizer." (Appeal Br. 5.) We do not find this argument persuasive of error. Preemption is not a separate test.

"Where a patent's claims are deemed only to disclose patent ineligible subject matter under the *Mayo* framework, as they are in this case, preemption concerns are fully addressed and made moot." *Ariosa Diagnostics, Inc. v. Sequenom, Inc.*, 788 F.3d 1371, 1379 (Fed. Cir. 2015). In other words, "preemption may signal patent ineligible subject matter, [but] the absence of complete preemption does not demonstrate patent eligibility." *Id.*

In view of the above, we are not persuaded that the Examiner erred in determining that claim 1 is directed to an abstract idea.

Step two of the *Alice* framework has been described "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*, 573 U.S. at 217–18 (citing *Mayo*, 566 U.S. at 72–73).

As discussed above, claim 1 merely recites storing some unspecified part of the vehicle immobilizer software in the HSM. The claim amounts to nothing significantly more than an instruction to apply the abstract idea in an unspecified manner. That is not enough to transform an abstract idea into a patent-eligible invention. *See Alice*, 573 U.S. at 225–26.

In view of the above, we are not persuaded that the Examiner erred in rejecting claim 1. Claims 5, 6, and 9 fall with claim 1. *See* 37 C.F.R. § 41.37(c)(1)(iv).

The § 103 rejection of claims 1, 2, 5–7, and 9

The Examiner finds that the admitted prior art teaches a "method of preventing an unauthorized operation of a motor vehicle which uses a [sic] vehicle immobilizer software." (Answer 7, citing Spec. 2, ll. 3–7.) The Examiner finds that Wolf discloses that "HSMs are also already used to protect vehicular components (e.g., head unit, V2X communication, engine control, anti-theft, tachograph) to prevent unauthorized modifications, theft or exchange, counterfeits, or espionage." (*Id.*, quoting Wolf at 4 (emphasis omitted).) The Examiner further finds that

> it would have been an [sic] obvious to an ordinary person skilled in the art to modify the Admitted prior art to incorporate Wolf to further enhance the security of the vehicle, the integrity of the immobilizer software and to improve the vulnerabilities of immobilizer software by storing it in a Hardware Security Module.

(*Id.* at 8.)

Appellants disagree and argue:

> What is evident from this section in Wolf is that this quote on which the Examiner relies never mentions storing immobilizer (or "anti-theft") software in the HSM itself. Instead, when one considers that this quote appears in a section entitled "Application examples," and when one further considers that in Figure 2 all the boxes labeled "Application" are located outside the HSM and in the software layer, one of ordinary skill in the art would not see in Wolf a teaching, whether in verbatim or "implicitly understood," of storing the immobilizer software in an HSM. Instead, by clearly illustrating in Figure 2 that

> applications like "anti-theft" are stored outside of the HSM, Wolf can only be characterized as practicing the old, and less secure, technique of storing such applications outside of the HSM.

(Reply Br. 5.)

We are not persuaded of error. Figure 2 of Wolf is discussed in section 2 of Wolf. (Wolf at 2.) Section 2 is titled "How [sic] a Typical Hardware Security Modules [sic] Looks Like." (*Id.*) The portion of Wolf relied upon by the Examiner is titled "Hardware Security Modules for Embedded Systems." (*Id.* at 4.) It begins by stating that "[h]ardware security modules are already variously deployed in today's embedded systems and the fields of application will continue to grow rapidly. In the following application examples, a short market overview, HSM evaluations, and certifications are presented." (*Id.*) In other words, section 2 and figure 2 discuss "[t]ypical [h]ardware [s]ecurity [m]odules," while section 5 discloses how HSMs are "deployed in today's embedded systems," and that deployment includes the use of HSMs in vehicle anti-theft systems. Therefore, we agree with the Examiner that Wolf teaches using HSMs in vehicle anti-theft systems.

We do not find persuasive Appellants' argument that Wolf, by itself, "never mentions storing immobilizer (or "anti-theft") software in the HSM itself." (*See* Reply Br. 5.) The Examiner does not rely on the references individually but relies on *the combination* of references. (*See* Answer 8.) "[O]ne cannot show non-obviousness by attacking references individually where, as here, the rejections are based on combinations of references." *In re Keller*, 642 F.2d 413, 426 (CCPA 1981). A reference "must be read, not in isolation, but for what it fairly teaches in combination with the prior art as a whole." *In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986). In short, obviousness is more than what is specifically disclosed in the cited references. "If a person of ordinary skill can implement a predictable variation, § 103 likely bars its patentability." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007). Moreover, "[u]nder the correct analysis, any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *Id.* at 420.

Here, the admitted prior art teaches using vehicle immobilizer software to prevent unauthorized vehicle operation, e.g., theft, and Wolf teaches using HSMs in vehicle anti-theft systems. Appellants do not persuasively argue why the Examiner erred in finding that it would have been obvious to one of ordinary skill in the art to modify the admitted prior art by incorporating "Wolf to further enhance the security of the vehicle, the integrity of the immobilizer software and to improve the vulnerabilities of immobilizer software by storing it in a Hardware Security Module." (*See* Answer 8.)

The § 103 rejection of claims 3 and 8

Claim 3 recites: "The method as recited in claim 1, wherein a portion of the vehicle immobilizer software that is stored in the electronic hardware security module actuates a first switch-off interface."

The Examiner finds that Wolf discloses

> that the HSM is used to protect vehicular components to prevent unauthorized modifications, theft or exchange etc … And it can be interpreted that when the authentication process fails, the HSM will do something (switch off interface) through its hardware layer as disclosed in figure 2 on Page 2) to prevent unauthorized access.

(Final Action 10.) The Examiner also finds that it can be "implicitly understood" that an anti-theft system will actuate a switch-off interface because preventing unauthorized use of a vehicle is the main task of a vehicle immobilizer. (Answer 9.)

Appellants argue that the Examiner merely "hypothesizes a mode of operation for Wolf ('the HSM will do something (switch-off interface)'[)] that has no support in Wolf." (Appeal Br. 8.)

"[T]here must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn,* 441 F.3d 977, 987 (Fed. Cir. 2006). Even assuming that an anti-theft system will actuate a switch-off interface (*see* Answer 9), the Examiner does not sufficiently explain why it would have been obvious to store in the HSM either the entirety of the anti-theft software (including vehicle immobilizer software) or that portion of the vehicle immobilizer software that actuates a first switch-off interface.

Therefore, we will reverse the rejection of claim 3 under § 103. Claim 8 contains similar language and is rejected for similar reasons. We will also reverse the rejection of claim 8 under § 103.

The § 103 rejection of claims 4 and 10

Similar to claim 3, claim 4, which also depends from claim 1, recites "a first portion of the vehicle immobilizer software is stored in the electronic hardware security module" and that "the first portion actuates a first switch-off interface." For the reasons discussed above regarding claim 3, we will reverse the rejection of claim 4 under § 103. Claim 10 contains similar language and is rejected for similar reasons. We will also reverse the rejection of claim 10 under § 103.

DECISION

The Examiner's rejection of claims 1, 5, 6, and 9 under 35 U.S.C. § 101 is affirmed.

The Examiner's rejection of claims 1, 2, 5–7, and 9 under 35 U.S.C. § 103 is affirmed.

The Examiner's rejections of claims 3, 4, 8, and 10 under 35 U.S.C. § 103 are reversed.

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-IN-PART