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.
13/156,737	06/09/2011	Adam Ratica	8223-1710615	5708

144885 7590 01/03/2019
The Webb Law Firm / Visa International
ONE GATEWAY CENTER
420 FT. DUQUESNE BLVD, SUITE 1200
PITTSBURGH, PA 15222

EXAMINER	
ZELASKIEWICZ, CHRYSTINA E	

ART UNIT	PAPER NUMBER
3621	

NOTIFICATION DATE	DELIVERY MODE
01/03/2019	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):

patents@webblaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte ADAM RATICA

Appeal 2017-008725
Application 13/156,737[1]
Technology Center 3600

Before ANTON W. FETTING, JOSEPH A. FISCHETTI, and ROBERT J. SILVERMAN, *Administrative Patent Judges*.

SILVERMAN, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

The Appellant appeals under 35 U.S.C. § 134(a) from the Examiner's decision rejecting claims 1–3, 5–11, and 13–20. We have jurisdiction under 35 U.S.C. § 6(b).

We REVERSE.

[1] "The real party in interest for this appeal and the present application is CARDINALCOMMERCE CORPORATION." Appeal Br. 1.

ILLUSTRATIVE CLAIM

> 1. A computer-implemented method of segmented processing of order management system data, the method comprising:
>
> using a front end interface of an apparatus to receive unencrypted payment information and unencrypted personal information relating to at least one customer order and return encrypted payment information and encrypted personal information relating to the at least one customer order;
>
> using a middle tier interface of the apparatus to receive encrypted payment information and encrypted personal information relating to at least one customer order and return decrypted personal information only; and
>
> using a back end interface of the apparatus to receive encrypted payment information and encrypted personal information relating to at least one customer order and return decrypted payment information and decrypted personal information relating to the at least one customer order;
>
> wherein the interfaces comprise separate Ethernet ports.

CITED REFERENCES

The Examiner relies upon the following references:

Oskari	US 2006/0072755 A1	Apr. 6, 2006
Bykov et al. (hereinafter "Bykov")	US 2008/0109372 A1	May 8, 2008
Barfield et al. (hereinafter "Barfield")	US 2010/0275005 A1	Oct. 28, 2010

REJECTIONS

I. Claims 1–3, 5–11, and 13–20 are rejected under 35 U.S.C. § 101 as ineligible subject matter.

II. Claims 1–3, 5–11, and 13–20 are rejected under 35 U.S.C. § 103(a) as unpatentable over Bykov, Oskari, and Barfield.

FINDINGS OF FACT

The findings of fact relied upon, which are supported by a preponderance of the evidence, appear in the following Analysis.

ANALYSIS

Subject-Matter Eligibility

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. Yet, subject matter belonging to any of the statutory categories may, nevertheless, be ineligible for patenting. The Supreme Court has interpreted § 101 to exclude laws of nature, natural phenomena, and abstract ideas, because they are regarded as the basic tools of scientific and technological work, such that including them within the domain of patent protection would risk inhibiting future innovation premised upon them. *Ass'n for Molecular Pathology v. Myriad Genetics, Inc.*, 569 U.S. 576, 589 (2013).

Of course, "[a]t some level, 'all inventions . . . embody, use, reflect, rest upon, or apply'" these basic tools of scientific and technological work. *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2354 (2014) (internal citation omitted). Accordingly, evaluating ineligible subject matter, under this judicial exclusion, involves a two-step framework for "distinguish[ing] between patents that claim the buildin[g] block[s] of human ingenuity and those that integrate the building blocks into something more, thereby transform[ing] them into a patent-eligible invention." *Id.* (internal quotation marks and citation omitted). The first step determines whether the claim is directed to judicially excluded subject matter (such as a so-called "abstract idea"); the second step determines whether there are any "additional elements" recited in the claim that (either individually or as an "ordered combination") amount to "significantly more" than the identified judicially excepted subject matter itself. *Id.* at 2355.

According to the Federal Circuit, the first step of the *Alice* framework "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, LLC v. DIRECTV, LLC*, 838 F.3d 1253, 1257 (Fed. Cir. 2016) (citing *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016)). Notably, the Federal Circuit warns that describing the claims at an excessively "high level of abstraction and untethered from the language of the claims all but ensures that the exceptions to § 101 swallow the rule." *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1337 (Fed. Cir. 2016).

The Examiner characterizes all the claims in the Appeal as "directed to an abstract idea of manipulating data via encryption and decryption, which is a mathematical relationship/formula and an idea of itself." Final Action 3.

The Appellant argues that the independent claims are not directed to an abstract idea, because the recited physical structure and functionality (i.e., the three "interface[s]" that perform different encryption and decryption functions) accomplish a specific technical improvement. *See* Appeal Br. 12–13; Reply Br. 6–8. The nature of the claimed improvement, the Appellant contends, is discussed in paragraph 41 of the Specification, which states:

> The Web servers in the DMZ ["demilitarized zone" — an expression that refers to a network's exposure to public access] could physically be connected only to the front end interface.

> Without connecting a new physical cable, it would not be possible to decrypt the data, since the front end interface 104 does not return decrypted data. This principal [sic] is also applied to the middle tier, where more trust is present but payment information would not be returned.

Appeal Br. 12 (quoting Spec. ¶ 41)

Indeed, the Examiner's characterization, of what the claims are directed to, omits the fundamental aspects of the functionality of the ordered combination. The Appellant's contention that the Examiner appears to have over-generalized the claim language is reinforced by the Federal Circuit's decision in *Ancora Techs., Inc. v. HTC America, Inc.*, 908 F.3d 1343 (Fed. Cir. 2018) in which another type of computer-security technology was deemed *not* to be directed to an abstract idea. In *Ancora*, the Federal Circuit explained: "Improving security . . . can be a non-abstract computer-functionality improvement if done by a specific technique that departs from earlier approaches to solve a specific computer problem. *Ancora*, 908 F.3d at 1348 (citing *Finjan, Inc. v. Blue Coat System, Inc.*, 879 F.3d 1299, 1304–05 (Fed. Cir. 2018)).

In view of the foregoing, we are persuaded that the Examiner has not adequately shown that the claims are directed to judicially excluded subject matter, under the first step of the *Alice* framework. Accordingly, we do not address the second *Alice* step. *See Enfish*, 822 F.3d at 1339. We do not sustain the rejection of claims 1–3, 5–11, and 13–20 under 35 U.S.C. § 101.

Obviousness

Among the arguments presented, in regard to the obviousness rejection, the Appellant submits that the rejection fails to teach or suggest features of claim 1's "middle tier interface" "to receive encrypted payment information and encrypted personal information relating to at least one customer order and return decrypted personal information only." *See* Appeal Br. 7–8, Reply Br. 2–3.

The Examiner relies upon a combination of Bykov and Oskari for this limitation. *See* Answer 3–5. Oskari discloses a wireless "key" device that exchanges information with a "lock" device (this could be a tangible, three-dimensional lock — such as a building door — or a virtual lock that provides access to certain computer functionality), where the interaction between the key and lock comprises encrypted/decrypted communications. *See* Oskari ¶¶ 38, 43. According to the Examiner, Oskari teaches the recited "return[ing] decrypted personal information only," explaining:

> a key device requests access to a lock device by encrypting a random code with a secret key, and sending the result to the lock device (i.e. receiving encrypted data). The lock device decrypts the encrypted data, and if the decrypted code is the same that the lock device originally sent, then the lock opens (i.e. returns decrypted data).

Answer 3 (citing Oskari ¶ 38).

The Appellant contends, in part, that Oskari fails to teach "return[ing] decrypted personal information only," because Oskari's key device receives non-encrypted data (random code) from the lock and returns an encrypted response to the lock — the opposite of what the claims require (*see* Appeal Br. 7–8 (citing Oskari ¶ 73, 76–78); Reply Br. 2 (citing Oskari ¶ 38)), and because opening a lock (per Oskari) is fundamentally and qualitatively different from "return[ing] decrypted personal information only" (*see* Reply Br. 2 (citing Oskari ¶ 38)).

Both of the Appellant's points are reasonable. The exchange of encrypted and decrypted information directly between the key and lock devices in Oskari (¶ 38) is contrary to what the claims require of the "middle tier interface." *See* Oskari ¶ 38. Furthermore, Oskari's unlocking a material structure (or a virtual one), to provide access thereto (*see id.* ¶ 43), does not teach the claimed "return[ing] decrypted personal information only."

The foregoing argument applies to independent claims 9 and 18, as well as independent claim 1. Therefore, we do not sustain the rejection of claims –3, 5–11, and 13–20 are rejected under 35 U.S.C. § 103(a).

DECISION

We REVERSE the Examiner's decision rejecting claims 1–3, 5–11, and 13–20 under 35 U.S.C. § 101.

We REVERSE the Examiner's decision rejecting claims 1–3, 5–11, and 13–20 are rejected under 35 U.S.C. § 103(a).

REVERSED