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.
14/738,006	06/12/2015	Asheley S. Lee	170111-1081	7270

71247 7590 11/13/2018

Client 170101 c/o
THOMAS HORSTEMEYER, LLP
3200 WINDY HILL RD SE
SUITE 1600E
ATLANTA, GA 30339

EXAMINER
REAGAN, JAMES A

ART UNIT	PAPER NUMBER
3688	

NOTIFICATION DATE	DELIVERY MODE
11/13/2018	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):

uspatents@tkhr.com
docketing@thomashorstemeyer.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte ASHELEY S. LEE, SAFFET G. OZDEMIR, CHRISTOPHER A. WEISS, MARK G. MADEJ, and DAVID B. BAILEY

Appeal 2017-009929[1]
Application 14/738,006
Technology Center 3600

Before ELENI MANTIS MERCADER, NORMAN H. BEAMER, and ADAM J. PYONIN, *Administrative Patent Judges*.

PYONIN, *Administrative Patent Judge*.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 1–20. App. Br. 4. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.

---

[1] "The real party in interest is Zappos IP, Inc., a Nevada corporation, the assignee of record, which is a subsidiary of Amazon.com, Inc." App. Br. 2.

STATEMENT OF THE CASE

Appellants' disclosure relates to an "an end-to-end encryption scheme" protecting "sensitive form data." Spec. ¶ 12. Claims 1, 8, and 15 are independent. Claim 1 is reproduced below for reference:

> 1. A non-transitory computer-readable medium embodying a program executable in at least one computing device, wherein when executed the program causes the at least one computing device to at least:
>
> send a network page to a client, the network page including executable encryption code configured to encrypt a form data item when executed by a browser,
>
> wherein the client is configured to receive the form data item via a form field of the network page;
>
> in response to receiving the form data item from the client over a separately encrypted channel, determine whether the form data item that has been received has been encrypted in the client by the executable encryption code executed by the browser; and
>
> encrypt the form data item in response to determining that the form data item that has been received has not been encrypted in the client by the executable encryption code, wherein the program is configured to refrain from encrypting the form data item in response to determining that the form data item that has been received has been encrypted in the client by the executable encryption code executed by the browser so that the form data item continues to be encrypted.

The Examiner's Rejection

Claims 1–20 stand rejected under 35 U.S.C. § 101 as being directed to a judicial exception to patent eligibility. Final Act. 7.

ANALYSIS

We have reviewed the Examiner's rejections in light of Appellants' arguments. We have considered in this Decision only those arguments Appellants actually raised in the Briefs. Any other arguments Appellants could have made but chose not to make in the Briefs are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(iv). We adopt the Examiner's findings and conclusions as our own, to the extent consistent with our analysis herein.

Alice Corp. Pty. Ltd. v. CLS Bank Int'l, 134 S.Ct. 2347 (2014), identifies a two-step framework for determining whether claimed subject matter is judicially excepted from patent eligibility under 35 U.S.C. § 101. In the first step, "[w]e must first determine whether the claims at issue are directed to a patent-ineligible concept." *Alice*, 134 S.Ct. at 2355. In the second step of the *Alice* analysis, we "consider the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." *Alice*, 134 S.Ct. at 2355 (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 78–79 (2012)). In other words, the second step is to "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.* (alteration in original) (quoting *Mayo*, 566 U.S. at 72–73).

Regarding step one of the *Alice* framework, the Examiner determines the claims are abstract, as they are directed to "the concept of analyzing storing data in the form of digital data, comparing/categorizing data, and displaying the data." Ans. 6. Regarding step two of the *Alice* framework,

the Examiner determines that taking the claim elements separately or considered as an ordered combination, the "claims simply recite the concept of analyzing storing data in the form of digital data, comparing/categorizing data, and displaying the data" as the claims comprise "an instruction to apply the abstract idea of organizing and analyzing data using some unspecified, generic computer." Ans. 6.

Appellants argue that the claims are not directed to "the abstract idea of 'protecting sensitive information,'" because the Examiner "oversimplifies the claims and ignores meaningful claim elements." App. Br. 9, citing *Alice* at 2354 and *Diamond v. Diehr,* 450 U.S. 175, 189 n.12 (1981).

We agree with the Examiner that the claims are directed to an abstract concept. *See* Final Act. 9, Ans. 6. The claims require "executable encryption code configured to encrypt a form data item when executed by a browser" with a backup encryption of the form data item "in response to determining that the form data item that has been received has not been encrypted in the client by the executable encryption code." We are not persuaded the Examiner errs in determining the claims "collect, store, display, and compare data to optimize an encryption objective on a generic computer." Final Act. 5. Further, data encryption or decryption is an abstract mathematical algorithm. *See, e.g.*, *Personalized Media Commc'ns, LLC v. Amazon.com, Inc.*, 161 F.Supp.3d 325, 337 (D. Del. 2015), aff'd, 671 Fed.Appx. 777 (Mem) (Fed. Cir. 2016) ("decryption" is an abstract idea). The claims are, thus, comparable to claims found to be directed to abstract ideas. "Without additional limitations, a process that employs mathematical algorithms to manipulate existing information to generate additional information is not patent eligible." *Digitech Image Techs., LLC v. Elecs. for*

Imaging, Inc., 758 F.3d 1344, 1351 (Fed. Cir. 2014); *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1353–54 (Fed. Cir. 2016)("collecting information, analyzing it, and displaying certain results of the collection and analysis" are "abstract-idea processes").

We are unpersuaded by Appellants' argument that "*Enfish* [*Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327 (Fed. Cir. 2016)] is applicable" because the "present claims are directed to a technological improvement in the security of computer systems" (Reply Br. 5) with a similar argument made with respect to *Bascom Global Internet Services, Inc. v. AT&T Mobility LLC*, 827 F.3d 1341 (Fed. Cir. 2016) (Reply Br. 8–9). We agree with the Examiner that "the focus of the claims is not on the improvement in computers as tools, but on certain independently abstract ideas that use computers as tools." Ans. 7.

We further agree with the Examiner that the claims do not resemble those of *McRO, Inc. v. Bandai Namco Games America Inc.*, 837 F.3d 1299 (Fed. Cir. 2016), because the claims "simply us[e] existing technology to encrypt data, which was ubiquitous at the time the invention was filed." Ans. 7. The Examiner's findings are supported by Appellants' disclosure, which states that "network page server 124," "encryption application 127," "encryption code 133," and "decryption application 148" are "commercially available." *See* Spec. ¶¶ 18, 19, 27. The claims address a problem which does not specifically arise in the operation of computer software, nor does the invention amount to an improvement to technology. *See, e.g.*, Spec. ¶ 2 ("Safeguarding payment data is of paramount importance to network sites that accept payment online"); *cf. FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1095 (Fed. Cir. 2016) ("These are the same questions

(though perhaps phrased with different words) that humans in analogous situations detecting fraud have asked for decades, if not centuries."); *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1373 (Fed. Cir. 2011) (the abstract idea of verifying credit card transactions).

Accordingly, we are not persuaded the Examiner errs. We sustain the Examiner's 35 U.S.C. § 101 rejection of claims 1–20.

DECISION

The Examiner's decision rejecting claims 1–20 under 35 U.S.C. § 101 is affirmed.

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