LANDO & ANASTASI

L&A

Date	November 28, 2017	**Number of pages** (including cover): 3	

To: Examiner Immanuel (P# 469-295-9094)

Email: Isidora.Immanuel@USPTO.gov

From: John Spangenberger (P#: 617-395-7030)
John Anastasi (P#: 617-395-7001)

Application No.: 14/071,126

Our Docket No.: W0537-701321

ORIGINAL DOCUMENTS WILL NOT BE MAILED.

Message: Below is a proposed Agenda for the Telephone Interview for Wednesday, November 29th, 2017 at 1:00 p.m. EST:

Applicant's representatives would like to discuss the rejections made in the most recent Office Action under 35 U.S.C. §§ 101, 103, and 112. In particular, Applicant's representatives would like to discuss the following:

- Rejections under 35 U.S.C. § 101

  - Applicant's representative is unaware of any precedent which has held encryption-related claims patent-ineligible. To the contrary, Applicant's representative referred in its response to the most recent Office Action two decisions[1, 2] which held encryption-related claims to be patent-eligible. Applicant's representative would like to review the claims and discuss further why the claims as previously presented are patent-eligible in view of the remarks made in the cited decisions, which emphasized that encryption-related claims are patent-eligible.

  - Applicant's representative would like to discuss why the claims are directed to an abstract idea in view of <u>DDR Holdings, LLC v. Hotels.com, L.P.</u>, which found the claims at issue to be patent-eligible in part because "the claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks." 773 F.3d at 1257. Similarly, the claims are directed to a problem which arises specifically in the realm of computer networks and are therefore patent-eligible.

  - Applicant's representative would like to discuss that even if the claims are considered to be directed to an abstract idea, the arrangement of elements recited in the claims renders the claims patent-eligible. As discussed in <u>BASCOM Global Internet v. AT&T Mobility LLC</u>[3], even though the high-level concept of content filtering was known, the elements were arranged to address problems specific to an Internet context. Similarly, the present application details how the arrangement of elements provides a system which is resistant to malicious actors who attempt to fraudulently access remotely-transmitted data.

- Rejections under 35 U.S.C. § 103

  - The Applicant's representative would like to discuss the Examiner's assertions that Gullman teaches the claimed element of "a user interface configured to receive a user input including authentication information known to the user and information indicative

- Applicant's representative would like to discuss the cited portions of Gullman, which refer to a biometric security apparatus 14 which includes a biometric sensor, an on/off switch, and a display, none of which are "configured to receive…. authentication information **known to the user**" or "information **indicative of a secure operation to be executed**."

- Rejections under 35 U.S.C. § 112

  - Applicant's representative would appreciate clarification of the rejection made in section 48 on page 18 of the Office Action.

Tentative Participants:
John Anastasi (Reg. No.: 37,765)
John Spangenberger (Reg. No.: 76,607)
Examiner Immanuel

REFERENCES

[1]On pages 12-13 of the most recent response, Applicant's representative cited <u>Paone v. Broadcom Corp.</u>, which held that "it would require an overly broad view of the Supreme Court's § 101 jurisprudence to find that a patent directed at a method of encryption does not claim eligible subject matter *per se*, as long as it is specific enough… [I]n <u>TQP</u>, Judge Bryson *rejected the notion that the claimed encryption method was a 'mental process' ineligible under [Gottschalk]*, because 'the invention involves a several-step manipulation of data that, except perhaps in its most simplistic form, *could not conceivably be performed in the human mind or with pencil and paper*." 2015 U.S. Dist. LEXIS 109725 (2015), citing <u>TQP Dev., LLC v. Intuit Inc.</u>, 2014 U.S. Dist. LEXIS 20077 (2014).

[2]On page 13 of the most recent response, Applicant's representative cited <u>TQP Dev., LLC v. Intuit Inc.</u>, which held that "that "[t]ypically, transforming data from one form to another does not qualify as the kind of transformation that the Supreme Court in <u>Bilski</u> regarded as an important indicator of patent eligibility… *In the case of an invention in the field of encryption, however, the entire object of the invention is to transform data from one form into another* that will be recognizable by the intended recipient but secure against decryption by unintended recipients. In that setting, *it does not make sense to say that the transformation of data from one form to another cannot qualify as a patent-eligible invention, because that is what the field of cryptology is all about*." 2014 U.S. Dist. LEXIS 20077 (2014).

[3]"…the claims [do not] preempt all ways of filtering content on the Internet; rather, they recite **a specific, discrete implementation of the abstract idea of filtering content**. Filtering content on the Internet was already a known concept, and the patent describes how its particular arrangement of elements is **a technical improvement over prior art ways of filtering such content**. As explained earlier, prior art filters were either **susceptible to hacking** and dependent on local hardware and software, or confined to an inflexible one-size-fits-all scheme…. [T]he claims may [therefore] be read to '**improve[] an existing technological process**.' […] [A]lthough the invention in the '606 patent is engineered in the content of filtering content, the invention is **not claiming the idea of filtering content simply applied to the Internet**. The '606 patent is instead claiming **a technology-based solution** (not an abstract-idea-based solution implemented with generic technical components in a conventional way) to filter content on the Internet that **overcomes existing problems with other Internet filtering systems**…. [T]he claimed invention represents a 'software-based invention[] that improve[s] the performance of the computer system itself." <u>BASCOM Global Internet v. AT&T Mobility LLC</u>, 827 F.3d at 1350-51 (Fed. Cir. 2016).

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/071,126	11/04/2013	Kenneth P. Weiss	W0537-701321	3814

37462   7590   12/05/2017

LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

EXAMINER
IMMANUEL, ISIDORA I

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
12/05/2017	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):

docketing@LALaw.com
CKent@LALaw.com

	Application No. 14/071,126	Applicant(s) Weiss, Kenneth P.			
Applicant-Initiated Interview Summary	**Examiner** ISIDORA I IMMANUEL	**Art Unit** 3685	**AIA (First Inventor to File) Status** No	**Page** **1 of** 2	

All participants (applicant, applicants representative, PTO personnel):

1. ISIDORA I IMMANUEL(Examiner); Telephonic   2. JOHN SPANGENBERGER(Attorney); Telephonic

3. JOHN ANASTASI(Attorney); Telephonic

Date of Interview: <u>29 November 2017</u>

Claims Discussed: Discussed claim 40, 101 rejection, overall claimed idea and claim language.

Brief Description of the main topic(s) of discussion: Discussed 101 and the use of encryptions in 101 rejections . Discussed case law and Applicant's argument for encryption overcoming the 101 rejection. No agreements reached.

Issues Discussed:

Item(s) under 35 U.S.C. 101:
Discussed case law and encrypting

Attachment(s): Agenda,

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.