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.
11/618,309	12/29/2006	Richendra Khanna	120137.550	5606

500 7590 10/13/2017
SEED INTELLECTUAL PROPERTY LAW GROUP LLP
701 FIFTH AVE
SUITE 5400
SEATTLE, WA 98104

EXAMINER	
KIM, STEVEN S	

ART UNIT	PAPER NUMBER
3685	

MAIL DATE	DELIVERY MODE
10/13/2017	PAPER

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.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte RICHENDRA KHANNA,
EUGENE KALENKOVICH,
and RAJIV CHOPRA

Appeal 2016–000554
Application 11/618,309
Technology Center 3600

Before ANTON W. FETTING, NINA L. MEDLOCK, and BRADLEY B. BAYAT, *Administrative Patent Judges.*

FETTING, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE[1]

Richendra Khanna, Eugene Kalenkovich, and Rajiv Chopra (Appellants) seek review under 35 U.S.C. § 134 of a final rejection of claims, the only claims pending in the application on appeal. We have jurisdiction over the appeal pursuant to 35 U.S.C. § 6(b).

[1] Our decision will make reference to the Appellants' Appeal Brief ("App. Br.," filed May 5, 2015) and Reply Brief ("Reply Br.," filed October 5, 2015), and the Examiner's Answer ("Ans.," mailed August 6, 2015), and Final Action ("Final Act.," mailed January 5, 2015).

The Appellants invented techniques for detecting inappropriate activity, such as to detect users engaged in inappropriate activities based on their interactions with a Web site or other electronic information service. Spec., para. 1.

An understanding of the invention can be derived from a reading of exemplary claim 1, which is reproduced below (bracketed matter and some paragraphing added).

> 1. A computer-implemented method for an electronic marketplace to automatically inhibit inappropriate interactions of users with the electronic marketplace, the method comprising:
>
> [1] receiving, by one or more configured computing systems of the electronic marketplace,
>
>> information describing a sequence of multiple interactions of a user with the electronic marketplace,
>>
>> the sequence of multiple user interactions being related to a single potential transaction within the electronic marketplace that involves the user and one or more items and including a path of multiple information resources being accessed by the user;
>
> [2] automatically determining, by the one or more configured computing systems,
>
>> whether the user is suspected of being engaged in fraudulent activity with respect to the electronic marketplace by applying multiple assessment tests to the received information to assess multiple factors related to the sequence of multiple interactions;
>
> [3] determining, by the one or more configured computing systems,
>
>> that the user is suspected of being engaged in fraudulent activity based on the applying of the multiple assessment tests,

> the applying of the multiple assessment tests including determining whether the path of multiple information resources accessed by the user is associated with a distinct other user previously engaged in fraudulent activities; and
>
> [4] taking, by the one or more configured computing systems, one or more actions to inhibit the fraudulent activity by the user.

The Examiner relies upon the following prior art:

McNair	US 5,375,244	Dec. 20, 1994
Johnson	US 5,615,408	Mar. 25, 1997
Ronning	US 7,165,051 B2	Jan. 16, 2007
O'Connell	US 2007/0239604 A1	Oct. 11, 2007

Claims 1, 4–7, 12–16, 19, 21–23, 25–31, 38, and 42 stand rejected under 35 U.S.C. § 101 as directed to non–statutory subject matter.

Claims 1, 4–7, 12–16, 19, 21–23, 25–31, 38, and 42 stand rejected under 35 U.S.C. § 112(a) as lacking a supporting written description within the original disclosure.

Claims 1, 6, 7, 15, 16, 19, 21–23, 25–31, 38, and 42 stand rejected under 35 U.S.C. § 103(a) as unpatentable over O'Connell, Ronning, and McNair.

Claims 4, 5, and 12–14 stand rejected under 35 U.S.C. § 103(a) as unpatentable over O'Connell, Ronning, McNair, and Johnson.

ISSUES

The issues of eligible subject matter turn primarily on whether the claims recite more than conceptual fraud protection advice for computer implementation. The issues of written description turn primarily on whether the Specification supports the claims. The issues of obviousness turn primarily on whether a description of collecting individual statistics followed by collective analysis is substantial evidence that it was at least predictable to also use those individual statistics in the analysis in any manner.

FACTS PERTINENT TO THE ISSUES

The following enumerated Findings of Fact (FF) are believed to be supported by a preponderance of the evidence.

Facts Related to the Prior Art

O'Connell

01. O'Connell is directed to detecting fraudulent behavior based on analysis of user-browser interaction, such as during an Internet or e-commerce session. O'Connell, para. 1.

02. O'Connell's fraud detection server determines fraud detection results based on the user-browser interaction during the current session and known fraudulent behavioral patterns and returns the fraud detection results to the user. Based on the fraud detection results and in response to a request by the user for an action, the e-commerce application may perform an action such as allowing the requested transaction, requesting additional authentication information, or rejecting the requested action. The e-commerce

application uses the fraud detection results to detect suspicious or fraudulent behavior and help prevent fraudulent transactions from occurring. *Id.* at para. 24.

03. O'Connell's client computer system transmits indications of the user's interaction with the browser to the incoming interaction server via a network to facilitate determination of fraud detection results. The user-browser interaction data transmitted by the client computer system may include both indications of the user-browser interaction as well as identification information. *Id.* at para. 26.

04. O'Connell's user interactions with a browser may be classified into general categories such as keyboard interactions, movement device interactions, and navigation/selection tendencies. Keyboard interactions may include interactions of a user with the keyboard, including key-down time (how long a particular key is pressed), typing rate, time or pauses between keystrokes, numeric keypad usage, capitalization keystroke sequences, common typing errors, etc. A particular user, for example, may typically hold down the 'o' key for milliseconds less time than she holds down the 'k' key, a pattern that may emerge consistently over continued data entry. This particular difference may reflect both hardware differences (e.g., the keyboard spring for each key on a particular keyboard) as well as the user's natural or learned typing pattern. A different user may have a larger gap between the two letters, a smaller gap, no gap, or a reversal of the longer hold time, providing a characteristic that potentially distinguishes the two

users. While one such characteristic may generally be insufficient for authentication purposes, an aggregation of different behaviors provides increasing authentication strength as more data is collected and more factors are considered. Keyboard interactions may include the particular keys selected for tasks, the pauses in between actuations or the length of actuations, etc. *Id.* at para. 27.

05. O'Connell describes how the details of a user's interaction while using a website using their browser may provide an indication of fraudulent behavior by that user. *Id.* at para. 28.

06. O'Connell describes how its fraud detection server may determine fraud detection results based on the user's interaction with a browser during the current session and known fraudulent behavior patterns. Upon receiving a request for fraud detection results for a particular user from an e-commerce application, the fraud detection server may access the stored user-browser interaction data for that user and a fraud detection module may analyze the stored data and compare the user-browser interaction data for the current session with known human or automated program fraudulent behavior. The user-browser interaction data for the current session may, in some embodiments, be stored in the user-browser interaction database. The fraud detection results may include an indication of the likelihood that the person (or entity) acting as the user of the current session is in fact the actual user or is actually a different user or automated program instead engaging in fraudulent behavior. The fraud detection results may be a final result (i.e., it is fraudulent behavior or it is not), a fraud

detection score that provides an indication of the degree of likelihood of fraudulent behavior evidenced by the user, or any other representation of the results. *Id.* at para. 34.

07. O'Connell describes how its fraud detection server may transmit the determined fraud detection results to the requesting e-commerce application, which may in turn determine its course of action based at least in part on the fraud detection results. Once the e-commerce application determines its course of action based on the fraud detection results, any requested actions of the user, and its own internal criteria, the e-commerce may perform the selected action. *Id.*at para. 35.

Ronning

08. Ronning is directed to performing adaptive fraud screening for electronic commerce transactions in order to detect and prevent attempted fraud in conjunction with the transactions. Ronning 1:18–21.

09. Ronning describes a fraud detection mechanism active during electronic commerce transactions. The fraud detection mechanism determines a likelihood that the electronic purchase order is attempted fraud based upon (i) information associated with the user-entered information and (ii) factors relating to a user's real-time interaction with the server during a transaction to process the electronic purchase order. *Id.* at 1:63–2:1.

10. Ronning describes generating the cumulative fraud ranking by analyzing page/order movement/history of an electronic commerce transaction. This processing generally involves

recording how a user progressed through the transaction, and comparing that progression with known profiles indicating fraudulent transactions and known profiles indicating normal (non-fraudulent) transactions. Ronning stores the known profiles for use in the comparison, and the known profiles may be updated as Ronning records additional profiles and associates them with attempted fraudulent or normal transactions. For example, a progression of pages for a normal transaction may include a user accessing welcome page, search page, product information page, and then check out page. A progression of pages for an attempted fraudulent transaction may include, for example, a user repeatedly accessing the shopping basket page and then the check out page several times in a row. In addition, Ronning may include files, known and referred to as "cookies," written to a user's machine to identify the machine in order to detect particular events from the same machine such as, for example, repeated submission of orders from the same machine with potentially different names or other information. *Id.* at 11:20–44.

McNair

11. McNair is directed to controlling access to a resource, such as a telecommunications network or a computer, so that access by unauthorized persons is disallowed. McNair 1:6–10.

12. McNair describes how data obtained from transactions involving both valid and fraudulent users are clustered in a multidimensional attribute space, with each of the clusters representing an attribute profile of similar user behaviors. Next,

> the similarity between the attributes of an access attempt and the attribute profiles represented by the clusters is evaluated, to identify the profiles of valid and fraudulent users that most closely resemble the attributes of the access attempt. If desired, an access decision can then be made simply based upon which type of user (valid or fraudulent) the access attempt most closely resembles. If desired, the history of previous access attempts by particular users may be stored and used subsequently in the access decision process. *Id.* at 1:54–2:10.

ANALYSIS

Claims 1, 4–7, 12–16, 19, 21–23, 25–31, 38, and 42 rejected under 35 U.S.C. § 101 as directed to non–statutory subject matter

The Supreme Court

> set forth a framework for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts. First, . . . determine whether the claims at issue are directed to one of those patent-ineligible concepts. If so, we then ask, "[w]hat else is there in the claims before us? To answer that question, . . . 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. [The Court] described step two of this analysis 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 Corp. Pty. Ltd. v CLS Bank Intl, 134 S. Ct. 2347, 2355 (2014) (citing *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 132 S. Ct. 1289 (2012)).

To perform this test, we must first determine whether the claims at issue are directed to a patent-ineligible concept. The Examiner finds the claims directed to determining whether a user is suspected of being engaged in fraudulent activity. Final Act. 5.

Although the Court, in *Alice*, made a direct finding as to what the claims were directed to, we find that this case's claims themselves and the Specification provide enough information to inform one as to what they are directed to.

The preamble to claim 1 recites that it is a method to inhibit inappropriate interactions of users with the marketplace. The steps in claim 1 result in determining suspected fraud and taking appropriate action. The Specification at paragraph 1 recites that the invention relates to detecting inappropriate activity. Thus, all this evidence shows that claim 1 is directed to fraud detection.

It follows from prior Supreme Court cases, and *Bilski v Kappos*, 561 U.S. 593 (2010) in particular, that the claims at issue here are directed to an abstract idea. Like the risk hedging in *Bilski*, the concept of fraud detection is a fundamental business practice long prevalent in our system of commerce. The use of fraud detection is also a building block of any credit system. Thus, fraud detection, like hedging, is an "abstract idea" beyond the scope of § 101. *See Alice*, 134 S. Ct. at 2356.

As in *Alice*, we need not labor to delimit the precise contours of the "abstract ideas" category in this case. It is enough to recognize that there is no meaningful distinction in the level of abstraction between the concept of risk hedging in *Bilski* and the concept of fraud detection at issue here. Both are squarely within the realm of "abstract ideas" as the Court has used that term. *See Alice*, 134 S. Ct. at 2357.

The remaining claims merely describe parameters and generalized techniques for fraud detection. We conclude that the claims at issue are directed to a patent-ineligible concept.

The introduction of a computer into the claims does not alter the analysis at *Mayo* step two.

> the mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention. Stating an abstract idea "while adding the words 'apply it'" is not enough for patent eligibility. Nor is limiting the use of an abstract idea "'to a particular technological environment.'" Stating an abstract idea while adding the words "apply it with a computer" simply combines those two steps, with the same deficient result. Thus, if a patent's recitation of a computer amounts to a mere instruction to "implement[t]" an abstract idea "on . . . a computer," that addition cannot impart patent eligibility. This conclusion accords with the preemption concern that undergirds our §101 jurisprudence. Given the ubiquity of computers, wholly generic computer implementation is not generally the sort of "additional feature[e]" that provides any "practical assurance that the process is more than a drafting effort designed to monopolize the [abstract idea] itself."

Alice, 134 S. Ct. at 2358 (citations omitted).

"[T]he relevant question is whether the claims here do more than simply instruct the practitioner to implement the abstract idea . . . on a generic computer." *Alice*, 134 S. Ct. at 2359. They do not.

Taking the claim elements separately, the function performed by the computer at each step of the process is purely conventional. Using a computer to receive data and make determinations about such data amounts to electronic data query and retrieval—one of the most basic functions of a computer. All of these computer functions are well-understood, routine, conventional activities previously known to the industry. In short, each step does no more than require a generic computer to perform generic computer functions.

Considered as an ordered combination, the computer components of Appellants' method add nothing that is not already present when the steps are considered separately. Viewed as a whole, Appellants' method claims simply recite the concept of fraud detection as performed by a generic computer. The method claims do not, for example, purport to improve the functioning of the computer itself. Nor do they effect an improvement in any other technology or technical field. Instead, the claims at issue amount to nothing significantly more than an instruction to apply the abstract idea of fraud detection using some unspecified, generic computer. Under our precedents, that is not enough to transform an abstract idea into a patent-eligible invention. *See Alice*, 134 S. Ct. at 2360.

As to the structural claims, they

> are no different from the method claims in substance. The method claims recite the abstract idea implemented on a generic computer; the system claims recite a handful of generic computer components configured to implement the same idea. This Court has long "warn[ed] ... against" interpreting § 101"in ways that make patent eligibility 'depend simply on the draftsman's art.'"

Id.

We further adopt the Examiner's findings and analysis from the Final Office Action at page 5 and the Answer at pages 3–11 and reach similar legal conclusions. We now turn to the Reply Brief arguments.

We are not persuaded by Appellants' argument that the particular claim limitations remove the claims from being a mere abstract idea under part one of the two-part test. Reply Br. 17. Appellants conflate parts 1 and 2 of the *Alice* test. The first part asks whether the claim is directed to an abstract idea, not whether all of the limitations are non-specific. As we find *supra*, the claims themselves and the Specification provide evidence that the claims are directed to fraud detection, which is a generalized abstract concept.

As to the second part of the *Alice* test, the limitations Appellants point to recite the use of a computer network, which itself is generic; data characteristics, such as what the data are related to; the use of plural generic assessment tests; and comparing the path the user took to other paths by at least one other particular user, which amounts to comparing the modus operandi of users. None of these limitations recites any particular implementation for doing so. As such, these amount to no more than conceptual advice on how to detect fraud in a generic computer network.

We are not persuaded by Appellants' argument that the additional data recited in claim 4 amount to more than an abstract idea. Reply Br. 18–19. This is essentially the same argument as in support of claim 1, but contending that further data details make a difference. Simply adding to the data receiving and analysis inputs does not alter what the claim is directed to and does not show that receiving and using any amount of data is not a conventional computer activity. There is no numeric threshold beyond which data entry turns from being conventional to being inventive.

We are not persuaded by Appellants' argument that independent claim 7 is patent-eligible. *Id.* at 20–21. Independent claim 7 is essentially a broader form of claim 1 to which additional data inputs are added. As we find with claim 4 *supra*, simply adding data inputs does not alter the analysis.

We are not persuaded by Appellants' argument that dependent claim 25 is patent-eligible. *Id.* at 21–22. Dependent claim 25 adds the purpose – but not the implementation of the tests – characterizes the outputs, and combines the test results. Combining data is another conventional computer activity and describing the character and purpose of a limitation alone without implementation does not show invention.

We are not persuaded by Appellants' argument that independent claims 38 and 42 are patent-eligible. *Id.* at 22–25. Claims 38 and 42 are computer instructions and device variants of claim 1 and the arguments here are unpersuasive for the same reasons as with claim 1.

We are not persuaded by Appellants' argument that the claims are non-abstract when viewed as a whole. *Id.* at 25–29. As we find *supra*, each of the claims recites conceptual advice on generic fraud detection and adds that it be implemented on a computer, but with no implementation details.

Appellants further argue that the asserted claims are akin to the claims found patent-eligible in *DDR Holdings, LLC v. Hotels.com, L.P.* 773 F.3d 1245 (Fed. Cir. 2014). In *DDR Holdings*, the court evaluated the eligibility of claims "address[ing] the problem of retaining website visitors that, if adhering to the routine, conventional functioning of

Internet hyperlink protocol, would be instantly transported away from a host's website after 'clicking' on an advertisement and activating a hyperlink." *Id.* at 1257. There, the court found that the claims were patent-eligible because they transformed the manner in which a hyperlink typically functions to resolve a problem that had no "pre-Internet analog." *Id.* at 1258. The court cautioned, however, "that not all claims purporting to address Internet-centric challenges are eligible for patent." *Id.* For example, in *DDR Holdings*, the Court distinguished the patent-eligible claims at issue from claims found patent-ineligible in *Ultramercial*. *See id.* at 1258–59 (citing *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 715–16 (Fed. Cir. 2014). As noted there, the *Ultramercial* claims were "directed to a specific method of advertising and content distribution that was previously unknown and never employed on the Internet before." *Id.* at 1258 (quoting *Ultramercial*, 772 F.3d at 715–16). Nevertheless, those claims were patent-ineligible because they "merely recite[d] the abstract idea of 'offering media content in exchange for viewing an advertisement,' along with 'routine additional steps such as updating an activity log, requiring a request from the consumer to view the ad, restrictions on public access, and use of the Internet.'" *Id.*

Similarly, Appellants' asserted claims recite, receiving, determining, and taking action. This is precisely the type of network activity found ineligible in *Ultramercial*. To the extent Appellants may be arguing that "a path of multiple information resources being accessed" is or creates a technological problem, we find that this is no more than the electronic equivalent of conventional transactional paths commercial transactions have traversed through financial and mercantile intermediaries for centuries. Indeed it is the electronic equivalent of a stapled sheaf of paper resulting along such a path, and to instruct one to review it is no more than to review transactional history in general.

Claims 1, 4–7, 12–16, 19, 21–23, 25–31, 38, and 42 rejected under 35 U.S.C. § 112(a) as lacking a supporting written description within the original disclosure

As to claim 1, this turns on whether a "distinct other user" in the recited limitation "determining whether . . . accessed by the user is associated with a distinct other user" is supported by the Specification. Final Act. 6–7. We are persuaded by Appellants' argument that it is. Appellants transcribe Specification paragraphs 15, 19, 20, and 34 and underline several limitations as support for such an other user. App. Br. 31–32; Reply Br. 31–33. This is consistent with the support pointed to in the Appeal Brief at page 5. The Examiner tellingly finds that the Appellants relied on Specification paragraphs 15, 19, 20, and 30 (not 34). Ans. 15. The paragraph the Examiner omits, paragraph 34, describes "a particular interaction sequence may be selected for heightened scrutiny for various reasons, such as an associated user being previously identified as being potentially suspect and/or the interaction sequence including one or more interactions previously identified as particularly suspect." Such an associated user would be a distinct other user.

The remaining independent claims have the same issue. Appellants' arguments are similarly persuasive.

As to claim 5, reciting "the path of multiple information resources is consecutively accessed by the user," we are persuaded by Appellants' argument that the Specification supports this at paragraph 12, reciting "embodiments the assessment tests may analyze information about a sequence of multiple related interactions." App. Br. 37. In any event, Examiner withdraws this rejection. Ans. 19.

Claims 1, 6, 7, 15, 16, 19, 21–23, 25–31, 38, and 42 rejected under 35 U.S.C. § 103(a) as unpatentable over O'Connell, Ronning, and McNair

We are not persuaded by Appellants' argument that the prior art applied fails to describe limitation 3, "determining whether the path of multiple information resources accessed by the user is associated with a distinct other user previously engaged in fraudulent activities," as recited in claim 1. App. Br. 42–45. The Examiner cites McNair as describing collecting individual access attempts by individual users as part of the history used for fraud detection.

The Examiner finds "it certainly would be within the realm of obviousness to one having ordinary skill in the art to include any known data, e.g. profile created from a distinct other user previously engaged in fraudulent activities, in known profile." Ans. 24. We agree McNair presents substantial evidence that it was known to those of ordinary skill to collect such data for distinct other users. The issue is then whether it was predictable to use, in any way, this data on its individual basis in addition to any collective basis further described by the art.

Again, no implementation is recited, so no particular technological use of this individual data is recited. The issue is simply whether it was predictable to use individual as well as collective data, even for the purpose of pattern comparison. It would seem inconsistent for McNair to collect individual data with no intent of using it somehow. So McNair at minimum suggests using such individual data for some purpose, and as McNair is directed to fraud detection, that purpose would encompass fraud detection. We further find that using individual data as exemplary representations of outliers or canonical forms is widespread in data analysis generally, and that fraud is not an especially individual activity, but is frequently practiced by associates. As a result, it was at least predictable for those practicing O'Connell, on seeing how McNair relies on individual as well as collective user data for fraud detection, to extend its analysis to similarly include individual other users.

We are not persuaded by Appellants' argument that adding individual data to collective data still results in only collective data. Reply Br. 10. The issue is not whether it was predictable to add individual data to collective data, but to use both individual and collective data in fraud analysis.

As to the remaining claims, we adopt the Examiner's findings and analysis and reach similar legal conclusions.

Claims 4, 5, and 12–14 rejected under 35 U.S.C. § 103(a) as unpatentable over O'Connell, Ronning, McNair, and Johnson

Appellants rely on their arguments in support of claim 1.

CONCLUSIONS OF LAW

The rejection of claims 1, 4–7, 12–16, 19, 21–23, 25–31, 38, and 42 under 35 U.S.C. § 101 as directed to non–statutory subject matter is proper.

The rejection of claims 1, 4–7, 12–16, 19, 21–23, 25–31, 38, and 42 under 35 U.S.C. § 112(a) as lacking a supporting written description within the original disclosure is improper.

The rejection of claims 1, 6, 7, 15, 16, 19, 21–23, 25–31, 38, and 42 under 35 U.S.C. § 103(a) as unpatentable over O'Connell, Ronning, and McNair is proper.

The rejection of claims 4, 5, and 12–14 under 35 U.S.C. § 103(a) as unpatentable over O'Connell, Ronning, McNair, and Johnson is proper.

DECISION

The decision to reject claims 1, 4–7, 12–16, 19, 21–23, 25–31, 38, and 42 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). *See* 37 C.F.R. § 1.136(a)(1)(iv) (2011).

AFFIRMED