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.
10/880,301	06/28/2004	Paul D. Needham	50277-2432	7760

42425 7590 02/28/2018

HICKMAN PALERMO BECKER BINGHAM/ORACLE
1 Almaden Boulevard
Floor 12
SAN JOSE, CA 95113

EXAMINER	
GORTAYO, DANGELINO N	

ART UNIT	PAPER NUMBER
2168	

NOTIFICATION DATE	DELIVERY MODE
02/28/2018	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):

usdocket@h35g.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte PAUL D. NEEDHAM and VIKRAM R. PESATI

Appeal 2017-008312
Application 10/880,301[1]
Technology Center 2100

Before MAHSHID D. SAADAT, JEFFREY S. SMITH, and ERIC B. CHEN, *Administrative Patent Judges*.

CHEN, *Administrative Patent Judge*.

DECISION ON APPEAL

This is an appeal under 35 U.S.C. § 134(a) from the final rejection of claims 1, 5–17, and 21–32. Claims 2–4, 18–20, and 33–37 have been cancelled. (App. Br. 2.) We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.

---

[1] Appellants identify Oracle International Corporation as the real party in interest. (App. Br. 1.)

STATEMENT OF THE CASE

Appellants' invention relates to regulating access to data in a database, in particular, binding data sensitivity labels to database table columns so that security policies can be applied at the column level rather than at the row level. (Abstract.)

Claim 1 below is exemplary, with disputed limitations in italics.

> 1. A method for regulating access to data, the method comprising the computer-implemented steps of:
>
> storing metadata that specifies one or more columns and one or more *security labels* bound to the one or more columns;
>
> receiving, from a user, *a request for access to data* stored in a column of a data table, said column belonging to said one or more columns;
>
> based on said metadata, looking up a security label bound to said column, wherein said security label belongs to said one or more security labels;
>
> accessing a user security clearance of the user;
>
> *determining whether said user is permitted* to access said data in said column by comparing said user security clearance to said security label bound to said column; and
>
> restricting or permitting access to said data in said column to said user based on said comparing.

Claims 1, 5–17, and 21–32 stand rejected under 35 U.S.C. § 102(e) as anticipated by Bird (US 2005/0246338 A1; pub. Nov. 3, 2005).

Claims 1, 5, 6, 12–17, 21, 22, and 28–32 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Cotner et al. (US 7,240,046 B2; iss. July 3, 2007) and Iyengar (US 7,024,409 B2; iss. Apr. 4, 2006).

Claims 7–11 and 23–27 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Cotner, Iyengar, and Flyntz (US 7,134,022 B2; iss. Nov. 7, 2006).[2]

ANALYSIS

§103 Rejection—Cotner and Iyengar

First, we are unpersuaded by Appellants' arguments (App. Br. 12; *see also* Reply Br. 3) that the combination of Cotner and Iyengar would not have rendered obvious independent claim 1, which includes the limitation "security labels."

The Examiner found that the user table of Cotner, which includes a security label (SECLABEL) column, as illustrated in Figure 2A, corresponds to the limitation "security labels." (Final Act. 13.) We agree with the Examiner's findings.

Cotner relates to "providing security in database management systems." (Col. 1, ll. 8–9.) Figure 2A of Cotner illustrates a conventional user table in a database management system. (Col. 4, ll. 15–16.) Cotner explains that "[t]he table contains various columns of data, labeled Col**1**, Col**2**, and Col**3**" and "also includes a security label (SECLABEL) column." (Col. 4, ll. 17–18.) In particular, Cotner explains that "the security labels are the names of various colors such as red, blue, yellow, green" and "[e]ach color name represents a particular set of security privileges associated with

[2] Appellants do not present any arguments with respect to the rejection of claims 7–11 and 23–27 under 35 U.S.C. § 103(a). Thus, any such arguments are deemed to be waived and we summarily sustain the Examiner's rejection.

the user table row." (Col. 4, ll. 20–24.) Because Cotner explains that security labels are associated with the user table row, as illustrated in Figure 2A, Cotner teaches the limitation "security labels."

Appellants argue that "[t]he privacy metadata of Iyengar is not a security label" and "[a] security label does not specify a transform." (App. Br. 12; *see also* Reply Br. 3.) However, the Examiner cited to Cotner, rather than Iyengar, for teaching the limitation "security labels." (Final Act. 13.) Thus, we agree with the Examiner that the combination of Cotner and Iyengar would have rendered obvious independent claim 1, which includes the limitation "security labels."

Second, we are unpersuaded by Appellants' arguments (App. Br. 13–14) that the combination of Cotner and Iyengar would not have rendered obvious independent claim 1, which includes the limitation "determining whether said user is permitted."

The Examiner found that the read mandatory security unit of Cotner, which compares the user's security label to the row's security label, corresponds to the limitation "determining whether said user is permitted." (Final Act. 14.) We agree with the Examiner's findings.

Figure 3 of Cotner illustrates database management systems (DBMS) 18, which includes data manager 22 and read mandatory security unit 36. (Col. 6, ll. 43–47.) Cotner explains that when "data manager **22** attempts to read a row of data from the data storage unit **24**, the request is directed through the read mandatory security unit **36**" such "[t]hat security unit compares a user's security label passed by the data manager with a security label associated with the requested row of data in the data storage unit **24.**" (Col. 6, ll. 56–62.) Because read mandatory security unit 36 of Cotner

compares the user's security label with the requested row of data from data storage unit 24, Cotner teaches the limitation "determining whether said user is permitted."

Appellants argue that "Iyengar may disclose privacy metadata" but "the mechanism that Iyengar proposes is not used to decide, at the time a request arrives, whether to allow access." (App. Br. 13.) However, the Examiner cited to Cotner, rather than Iyengar, for teaching the limitation "determining whether said user is permitted." (Final Act. 14.) Thus, we agree with the Examiner that the combination of Cotner and Iyengar would have rendered obvious independent claim 1, which includes the limitation "determining whether said user is permitted."

Third, we are unpersuaded by Appellants' arguments (App. Br. 14–15) that the combination of Cotner and Iyengar would not have rendered obvious independent claim 1, which includes the limitation "a request for access to data."

The Examiner found that the query processor of Cotner, which controls the interaction of the data manager with the data repository, corresponds to the limitation "a request for access to data." (Final Act. 13.) We agree with the Examiner's findings.

Cotner explains that "query processor **20** processes requests containing queries received at a web site from a client" and that "[b]ased on the query, the query processor **20** controls the data manager **22** to interact with the data repository **24** to handle the appropriate data satisfying the query." (Col. 4, ll. 7–14.) Because query processor 20 of Cotner processes requests containing queries received from the client, Cotner teaches the limitation "a request for access to data."

Appellants argue that "the mechanism that Iyengar proposes regards imagined future querying and is not used to decide, when a query arrives, whether to allow access" (App. Br. 14) and "[s]uch imaginary usage is insufficient, because it does not enable determining whether to permit access to particular data identified by a particular request" (*id.* at 14–15). However, the Examiner cited to Cotner, rather than Iyengar, for teaching the limitation "a request for access to data." (Final Act. 13.) Thus, we agree with the Examiner that the combination of Cotner and Iyengar would have rendered obvious independent claim 1, which includes the limitation "a request for access to data."

Last, we are not persuaded by Appellants' arguments (App. Br. 15–16) that the Examiner improperly combined Cotner and Iyengar.

The Examiner found that the metadata of Iyengar, which includes information about data in the columns that should be suppressed due to privacy concerns, corresponds to the limitation "storing metadata that specifies one or more columns." (Final Act. 14–15.) The Examiner concluded that "[i]t would have been obvious . . . to combine Cotner's method of providing secure access to data stored in table utilizing security labels with Iyengar's ability to utilize metadata comprising information about columns and the privacy constraints associated with columns to abstract or suppress access to column data." (*Id.* at 15.) We agree with the Examiner's findings and conclusions.

Iyengar relates to managing data, in particular, "transforming data in a manner that satisfies predetermined privacy constraints." (Col. 1, ll. 17–19.) Figure 2 of Iyengar illustrates two components of data 20, which include meta-data 21 and tabular data 22. (Col. 4, ll. 10–12.) Iyengar explains that

"meta-data 21 comprises information about the input data" that "includes the name and type of information in each column" (col. 4, ll. 49–51) and "meta-data also comprises information on which columns are potentially identifying and need to be abstracted or suppressed according to privacy constraints" (col. 4, l. 67 to col. 5, l. 3). Iyengar also explains that "in tabular data where each row represents an individual, and one or more columns comprise explicitly identifying information (e.g., social security numbers), the identifying information can be suppressed." (Col. 1, ll. 54–57.)

A person of ordinary skill in the art would have recognized that incorporating the metadata of Iyengar for providing the type of information in each column, with the user table of Cotner, would improve Cotner by identifying information subject to privacy constraints. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007). Thus, we agree with the Examiner (Final Act. 15) that modifying Cotner to incorporate the metadata of Iyengar would have been obvious.

Appellants argue that "[t]he combination of Cotner and Iyengar would compare a user security clearance to a transform that replaces characters, which is an invalid comparison" (App. Br. 15–16) and "[a]s combined, *Cotner* would decide access based on an invalid comparison, which would not achieve the intended purpose of *Cotner*" (*id.* at 16). However, the Examiner's articulated rationale for combining Cotner and Iyengar is based upon modifying the user table Cotner by incorporating the metadata of Iyengar, rather than incorporating the feature of data transformation to mask privacy. (Final Act. 14–15.) Therefore, the Examiner has properly

combined Cotner and Iyengar to reject independent claim 1 under 35 U.S.C. § 103(a).

Accordingly, we sustain the rejection of independent claim 1 under 35 U.S.C. § 103(a). Claims 5, 6, and 12–16 depend from claim 1, and Appellants have not presented any additional substantive arguments with respect to these claims. Therefore, we sustain the rejection of claims 5, 6, and 12–16 under 35 U.S.C. § 103(a), for the same reasons discussed with respect to independent claim 1.

Independent claim 17 recite limitations similar to those discussed with respect to independent claim 1, and Appellants have not presented any additional substantive arguments with respect to these claims. We sustain the rejection of claim 17, as well as dependent claims 21, 22, and 28–32, for the same reasons discussed with respect to claim 1.

§102 Rejection—Bird

We do not reach the rejection of claims 1, 5–17, and 21–32 under 35 U.S.C. § 102(e) as anticipated by Bird. Affirmance of the rejection discussed previously renders it unnecessary to reach the remaining rejections, as all of pending claims have been addressed and found unpatentable. *Cf. In re Gleave*, 560 F.3d 1331, 1338 (Fed. Cir. 2009) (not reaching additional obviousness rejections).

DECISION

The Examiner's decision rejecting claims 1, 5–17, and 21–32 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