



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.
11/137,684	05/24/2005	Ju Wu	34874-721002US	6460
64280	7590	04/16/2012	EXAMINER	
MINTZ, LEVIN, COHN, FERRIS, GLOVSKY & POPEO, P.C. ONE FINANCIAL CENTER BOSTON, MA 02111			NOFAL, CHRISTOPHER P	
			ART UNIT	PAPER NUMBER
			2156	
			MAIL DATE	DELIVERY MODE
			04/16/2012	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 BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte JU WU and QIAN WU

Appeal 2010-006221
Application 11/137,684
Technology Center 2100

Before JOHN A. JEFFERY, BRADLEY W. BAUMEISTER, and
JENNIFER S. BISK, *Administrative Patent Judges*.

JEFFERY, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1 and 7-9. We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

STATEMENT OF THE CASE

Appellants' invention delivers specific sections of electronic reports by (1) augmenting a selected report section with security metadata, and

Appeal 2010-006221
Application 11/137,684

(2) inserting the section within an electronic document. *See generally* Abstract; Spec. ¶¶ 0011-13. Claim 1 is illustrative:

1. A computer storage product with a computer-readable medium, comprising executable instructions to:

select a report including information automatically retrieved from a data source, where the information is structured in accordance with a report schema specifying the form in which the information is presented;

select a section of the report;

augment the section of the report with security metadata;

insert the section of the report into an electronic document, wherein the metadata maintains contextual report and data source information, including data security settings for data source and report source information.

RELATED APPEALS

This appeal is said to be related to three appeals in connection with the following applications: (1) 11/166,039; (2) 11/318,074 (Appeal No. 2010-002378); and (3) 11/137,710 (Appeal No. 2010-001624). Br. 4; Ans. 2. The '039 application, however, was allowed and issued as U.S. Patent 7,580,928.

THE REJECTIONS¹

1. The Examiner provisionally rejected claim 1 on the ground of obviousness-type double patenting over claim 1 of Application No. 11/137,710 and Houser (US 5,606,609; Feb. 25, 1997). Ans. 5-7.²

2. The Examiner rejected claim 1 under 35 U.S.C. § 103(a) as unpatentable over Tracy (US 2002/0042687 A1; Apr. 11, 2002) and Houser. Ans. 7-13.

3. The Examiner rejected claims 7 and 8 under 35 U.S.C. § 103(a) as unpatentable over Tracy, Houser, and Weissman (US 6,212,524 B1; Apr. 3, 2001). Ans. 13-16.

4. The Examiner rejected claim 9 under 35 U.S.C. § 103(a) as unpatentable over Tracy, Houser, and Levine (US 6,073,129; June 6, 2000). Ans. 16-18.

THE DOUBLE PATENTING REJECTION

Since Appellants present no arguments pertaining to the Examiner's provisional double patenting rejection (Ans. 5-7), we summarily sustain that rejection. *See* MPEP § 1205.02, 8th ed., Rev. 8, July 2010 ("If a ground of

¹ The Examiner's entry of amendments filed after final rejection overcame rejections under §§ 101 and 112. *See* Br. 5; Ans. 2. Accordingly, those rejections are not before us.

² Throughout this opinion, we refer to the Appeal Brief filed August 11, 2009 and the Examiner's Answer mailed November 20, 2009 (supplemented December 28, 2009).

rejection stated by the examiner is not addressed in the appellant's brief, that ground of rejection will be summarily sustained by the Board.”).

THE OBVIOUSNESS REJECTION OVER TRACY AND HOUSER

The Examiner finds that Tracy discloses every recited feature of representative claim 1 including:

(1) selecting a “report” (network scan file 708 or host profile file 710) including automatically-retrieved information structured according to a report schema;

(2) augmenting a selected report section (the network scan file's “Host” section) with “security metadata” (e.g., metadata involving IP addresses, patch levels, and secret operating environment) via profile integrator 706; and

(3) inserting the report section within an electronic Certification and Accreditation (C&A) document. Ans. 9-12, 22-28.

Although the Examiner acknowledges that Tracy does not explicitly illustrate a finished C&A document containing a “Host” section of the network scan “report,” the Examiner nonetheless concludes that inserting this “report” section in an electronic document would have been obvious in view of Tracy's “customizable” publishing process. *Id.* The Examiner adds that since both Tracy and Houser's metadata provide data security settings for data source and report source information as claimed, this feature would

have been obvious either over Tracy alone or, alternatively, Tracy and Houser collectively. Ans. 11-13, 26-28.

Appellants argue that neither Tracy nor Houser discloses a “report” as claimed and defined in the Specification, namely information that is (1) automatically retrieved from a data source, and (2) structured according to a report schema specifying the form in which the information is presented. Br. 6-9. Appellants add that Tracy and Houser do not augment a selected report section with security metadata as claimed, let alone that the metadata includes data security settings for data source and report source information as claimed. Br. 9-11. The issue before us, then, is as follows:

ISSUE

Under § 103, has the Examiner erred in rejecting claim 1 by finding that Tracy and Houser collectively would have taught or suggested (1) selecting a report including automatically-retrieved information structured according to a report schema specifying the form in which the information is presented; (2) augmenting a selected report section with security metadata including data security settings for data source and report source information; and (3) inserting the report section within an electronic document?

ANALYSIS

We begin by construing the key disputed limitation of claim 1, which recites, in pertinent part, a “report.” As Appellants indicate (Br. 6-7), the term is expressly defined in the Specification, and refers to information that is (1) *automatically* retrieved from a data source (e.g., a database, data warehouse, and the like), and (2) structured according to a report schema specifying the form in which the information is presented. Spec. ¶ 0008. Automatically-retrieved information is a key aspect of a “report” in Appellants’ parlance that distinguishes it from “non-report” electronic documents, which typically require at least some manual intervention to establish content and formatting. *Compare* Spec. ¶ 0008 *with* ¶ 0009.

Despite the Examiner’s assertion to the contrary (Ans. 20-22), we find Appellants clearly and unambiguously define the term “report” as noted above, notwithstanding using open-ended and exemplary terms in connection with the associated data source. Although broad, this definition hardly lacks “clarity, deliberateness, and precision” as the Examiner alleges (Ans. 21). The Examiner’s assertion in this regard is therefore unavailing.

That said, however, we find no error in the Examiner’s alternative position that interprets the recited “report” in light of this definition. Ans. 22-28. First, even assuming, without deciding, that the recited “electronic document” is a *non-report* electronic document notwithstanding the lack of

the term “non-report” in the claim,³ the distinction between a “report” and a “non-report” is without a structural or functional difference here, for it merely pertains to *how the data is acquired*—not to the data itself. That is, the functions recited in claim 1 pertain to the *data itself* in terms of its selection, augmentation, and insertion, but are not germane to the data’s previous acquisition (i.e., either manually or automatically), which characterizes the data as a “report” or otherwise.

In any event, we see no reason why Tracy’s network scan file 708 cannot constitute a selected “report” as claimed, for it includes automatically-retrieved information structured according to a “report schema,” namely the Microsoft “.INI” file format as the Examiner indicates. *See* Ans. 8-9, 22-24 (citing Tracy, ¶¶ 0056-58, 0063-64); *see also id.*, ¶ 0059 (listing information written to a network scan file); Fig. 8 (illustrating this file). Appellants’ contention that the published document in Tracy’s Paragraph 0143 is not a “report” (Br. 8) is unavailing, for this argument does not squarely address—let alone show error in—the Examiner’s mapping Tracy’s network scan file to the recited “report” noted above. Rather, the Examiner maps the published document in Tracy’s Paragraph 0143 to the recited “electronic document” as noted above. Ans. 11.

Nor do we find error in the Examiner’s position that Tracy’s profile integrator 706 augments a selected report section (the network scan file’s

³ *But see* claim 1 of related application 11/318,074 (Appeal No. 2010-002378) (reciting a “*non-report* electronic document”) (emphasis added).

“Host” section) with “security metadata” including data security settings for data source and report source information. Ans. 9-10, 23-25. As shown in Tracy’s Figure 8, the network scan file’s “Host” section 808 is a subset of the information retrieved from the associated data source, and therefore fully meets a “report section” given the term’s scope and breadth. And this “report section” is augmented with at least information from host profile file 710 by the profile integrator as the Examiner indicates. Ans. 9, 23-25; *see also* Tracy, ¶ 0065; Fig. 8 (“Host” section 810).

We also see no error in the Examiner’s position (Ans. 9-10, 12, 24-25) that this information (e.g., IP addresses, operating environment conditions) also constitutes “security metadata” given the scope and breadth of the limitation. Leaving aside the fact that the metadata’s data security settings for data source and report source information (as well as these two pieces of information) constitute non-functional descriptive material as they merely describe data and therefore do not functionally limit the claimed invention,⁴ we find no error in the Examiner’s position (Ans. 12, 25) that Tracy’s metadata includes data security settings, at least regarding a data source (database) and a report source (network) secure operating environment. Appellants’ arguments regarding Tracy’s shortcomings regarding the recited data security settings (Br. 10) are not commensurate with the scope of the

⁴ *See In re Ngai*, 367 F.3d 1336, 1339 (Fed. Cir. 2004); *see also Ex parte Nehls*, 88 USPQ2d 1883, 1887-89 (BPAI 2008) (precedential) (discussing cases pertaining to non-functional descriptive material).

claim, and, in any event, fail to persuasively rebut the Examiner's position noted above.

Nor are we persuaded of error in the Examiner's alternative position based on Houser. Ans. 10-13, 25-28. The Examiner cites Houser merely to show that providing security information for documents is known, and enhancing Tracy's metadata with such security-based information would have been obvious. *Id.* Not only are the data security settings non-functional descriptive material as noted above, but enhancing Tracy's metadata with Houser's security-based features as the Examiner proposes merely predictably uses prior art elements according to their established functions—an obvious improvement. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007). And even assuming, without deciding, that Houser's documents are not “reports” as Appellants contend (Br. 8-9), where, as here, if a technique (including security information) has been used to improve one device (electronic documents) and an ordinarily skilled artisan would recognize that it would improve similar devices in the same way (e.g., reports), using the technique is obvious unless its actual application is beyond his or her skill. *See id.*

Lastly, we see no error in the Examiner's position that it would have been obvious to insert the selected report part within an electronic C&A document in view of Tracy's customizable publishing process for the reasons indicated by the Examiner. Ans. 11.

Appeal 2010-006221
Application 11/137,684

We are therefore not persuaded that the Examiner erred in rejecting claim 1.

THE OTHER OBVIOUSNESS REJECTIONS

Since Appellants present no arguments pertaining to the Examiner's obviousness rejections of claims 7-9 (Ans. 13-18), we summarily sustain those rejections. *See* MPEP § 1205.02.

CONCLUSION

The Examiner did not err in rejecting (1) claim 1 on the ground of obviousness-type double patenting, and (2) claims 1 and 7-9 under § 103.

ORDER

The Examiner's decision rejecting claims 1 and 7-9 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

rwk