



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.
10/219,890	08/16/2002	Paul B. Schneck	3059.7080006	6096

26111 7590 12/02/2016
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER

AGWUMEZIE, CHINEDU CHARLES

ART UNIT	PAPER NUMBER
----------	--------------

3685

MAIL DATE	DELIVERY MODE
-----------	---------------

12/02/2016

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 PAUL B. SCHNECK and MARSHALL D. ABRAMS

Appeal 2014-008425
Application 10/219,890
Technology Center 3600

Before HUBERT C. LORIN, ANTON W. FETTING, and
NINA L. MEDLOCK, *Administrative Patent Judges*.

FETTING, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE¹

Paul B. Schneck and Marshall D. Abrams (Appellants) seek review under 35 U.S.C. § 134 of a non-final rejection of claims 2–21, 24–29, and 97–102, 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 February 14, 2014) and Reply Brief (“Reply Br.,” filed July 21, 2014), and the Examiner’s Answer (“Ans.,” mailed May 21, 2014), and Non-Final Action (“Non-Final Act.,” mailed November 14, 2013).

The Appellants invented a way to control distribution and access of digital property and the payment therefor. Specification 1:8–10.

An understanding of the invention can be derived from a reading of exemplary claim 2, which is reproduced below (bracketed matter and some paragraphing added).

2. A method, performed by a computer device having a memory and a processor, of distributing data for subsequent controlled use of the data on at least one apparatus, the method comprising:

[1] protecting portions of the data;

[2] preventing access to the protected portions of the data other than in a non-useable form;

[3] determining, by the processor,

rules concerning access rights to the data,

wherein the rules include validity information and identification information;

[4] protecting the rules including protecting the validity information and identification information;

[5] distributing the protected portions of the data and the protected rules to the at least one apparatus,

wherein the at least one apparatus

comprises a tamper detection mechanism

and

permits only controlled access to the data,

the controlled access being permitted only in accordance with the rules as enforced by the tamper detection mechanism;

and

[6] in response to detecting tampering by the tamper detection mechanism,

destroying the protected rules.

The Examiner relies upon the following prior art:

Rosenow	US 5,128,996	July 7, 1992
Carter '192	US 5,161,192	Nov. 3, 1992
Stefik	US 5,629,980	May 13, 1997
Carter '175	US 5,787,175	July 28, 1998
Koyama	US 6,424,385 B1	July 23, 2002

Claims 2–19 and 24–29 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Carter '175 and Rosenow.

Claims 97, 100, and 102 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Carter '175, Rosenow, and Carter '192.

Claims 20, 21, 98, and 99 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Carter '175, Rosenow, and Stefik.

Claim 101 stands rejected under 35 U.S.C. § 103(a) as unpatentable over Carter '175, Rosenow, Stefik, and Koyama.

ISSUES

The issues of obviousness turn primarily on whether Rosenow describes destroying its rules when tampering is detected.

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 Claim Construction

01. The disclosure contains no lexicographic definition of “rule.”

Facts Related to the Prior Art

Carter '175

02. Carter '175 is directed to controlling a work group document, and more particularly to allowing each member of a specified group to encrypt and/or decrypt a document or to digitally sign and/or authenticate the document by using a key that is unique to the member in question, and to preventing access to the document by persons who are not currently members of the group.
Carter '175, 1:5–13.
03. Carter '175 configures a document as having a data portion and a prefix portion. Carter '175 describes a collaborative encryption method which uses structures in the prefix portion to restrict access to the information stored in the data portion. Users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot. Carter '175, 6:5–15.
04. Carter '175's prefix portion of the work group document includes at least one member definition. The member definitions may be located in the same file as the data portion or in one or

more separate files. The member definitions define a collaborative group of computer system users which have access to the data portion of the work group document. Carter '175 12:25–32.

Rosenow

05. Rosenow is directed to electronic transaction processing, and more specifically, to a microcomputer-based encryption system which provides multiple encryption channels in a single unit. Rosenow 1:5–9.
06. FIG. 12 is a flow diagram of the TAMPER__SWITCH__ INTERRUPT routine. The DS5000 generates an interrupt when the contents of its RAM are being tampered with, as when the encapsulation module has been broken. When this occurs, the tamper switch opens and interrupts the DS5000. This interrupt is referred to as the tamper switch interrupt. The TAMPER__SWITCH__ INTERRUPT routine processes such an interrupt. When the tamper switch interrupt occurs, the routine zeros out the application program and data portions of memory. Rosenow 30:4–23.

ANALYSIS

We are not persuaded by Appellants' argument that the cited references do not disclose the limitation of "in response to detecting tampering by the tamper detection mechanism, destroying the protected rules." App. Br. 7–8. Appellants contend the claim allows targeting of only

the rules allowing the data to be recovered. *Id.* The claim is broader than that. The claim does not recite that the data is left unharmed when the rules are destroyed. Rosenow destroys both the application program and the data upon detecting tampering. Such a self-destruct form of enforcement is within the scope of the limitation as drafted. As the Examiner did not cite this portion of Rosenow, we will afford the Appellants an opportunity to respond by denominating this as a new ground.

We are not persuaded by Appellants' argument that the cited references do not disclose the limitation of rules. App. Br. 8–11. Appellants do not lexicographically define rules, but proffer a dictionary definition as a statement that tells you what is or is not allowed in a particular game, situation, etc.; a statement that tells you what is allowed or what will happen within a particular system. App. Br. 10. We agree this is consistent with most dictionary definitions.

What Appellants omit is that computers store data, not rules. Even a computer program is data. It is this data that is interpreted as various items including rules, and how that interpretation occurs is a matter of implementation. Thus there are many ways of implementing what we perceive to be rules in a computer.

Carter '175 describes adding a prefix to its data that defines which members may access that data. Such a definition is within the scope of a statement that tells you what is allowed or what will happen within a particular system with regard to such access. Presumably Appellants are contending that the logic to implement this is in the program rather than the data. But the implementation is that of a generic rule in the program that is

then instantiated as a specific rule by the criteria in the data. Thus, the prefix data that are distributed are implementations of the specific rules that are actually applied. That they depend on the implementing program for interpretation and execution does not diminish their status as such statements. Indeed any rule that is distributed, as recited in the claims, is data that must rely on the implementing program for interpretation and execution. It is only a matter of how much detail is included in the statement. Carter '175 happens to use a concise implementation. Appellants do not impose any limitation on how the rules are implemented.

CONCLUSIONS OF LAW

The rejection of claims 2–19 and 24–29 under 35 U.S.C. § 103(a) as unpatentable over Carter '175 and Rosenow is proper.

The rejection of claims 97, 100, and 102 under 35 U.S.C. § 103(a) as unpatentable over Carter '175, Rosenow, and Carter '192 is proper.

The rejection of claims 20, 21, 98, and 99 under 35 U.S.C. § 103(a) as unpatentable over Carter '175, Rosenow, and Stefik is proper.

The rejection of claim 101 under 35 U.S.C. § 103(a) as unpatentable over Carter '175, Rosenow, Stefik, and Koyama is proper.

DECISION

The rejection of claims 2–21, 24–29, and 97–102 is affirmed.

This affirmance is denominated as a new ground of rejection.

Our decision is not a final agency action.

This decision contains a new ground of rejection pursuant to 37 C.F.R. § 41.50(b). 37 C.F.R. § 41.50(b) provides “[a] new ground of rejection pursuant to this paragraph shall not be considered final for judicial review.” Section 41.50(b) also provides:

When the Board enters such a non-final decision, the appellant, within two months from the date of the decision, must exercise one of the following two options with respect to the new ground of rejection to avoid termination of the appeal as to the rejected claims:

(1) *Reopen prosecution.* Submit an appropriate amendment of the claims so rejected or new Evidence relating to the claims so rejected, or both, and have the matter reconsidered by the examiner, in which event the prosecution will be remanded to the examiner. The new ground of rejection is binding upon the examiner unless an amendment or new Evidence not previously of Record is made which, in the opinion of the examiner, overcomes the new ground of rejection designated in the decision. Should the examiner reject the claims, appellant may again appeal to the Board pursuant to this subpart.

(2) *Request rehearing.* Request that the proceeding be reheard under § 41.52 by the Board upon the same Record. The request for rehearing must address any new ground of rejection

Appeal 2014-008425
Application 10/219,890

and state with particularity the points believed to have been misapprehended or overlooked in entering the new ground of rejection and also state all other grounds upon which rehearing is sought.

Further guidance on responding to a new ground of rejection can be found in the Manual of Patent Examining Procedure § 1214.01.

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;

37 C.F.R. § 41.50(b)