UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

INFORMATICA CORPORATION,
Petitioner,

v.

PROTEGRITY CORPORATION,
Patent Owner.

_____

CBM2015-00010
Patent 8,402,281 B2

Before KEVIN F. TURNER, MEREDITH C. PETRAVICK, and
GREGG I. ANDERSON, *Administrative Patent Judges.*

PETRAVICK, *Administrative Patent Judge.*

DECISION
Institution of Covered Business Method Patent Review
37 C.F.R. § 42.308

I. INTRODUCTION

A. Background

On October 14, 2014, Informatica Corporation ("Petitioner") filed a
Petition (Paper 1, "Pet.") requesting a review under the transitional program
for covered business method patents of U.S. Patent No. 8,402,281 B2 (Ex.
1001, "the '281 patent"). On February 13, 2015, Protegrity Corporation

("Patent Owner") filed a Preliminary Response (Paper 6, "Prelim. Resp.").
We have jurisdiction under 35 U.S.C. § 324.

The standard for instituting a covered business method patent review
is set forth in 35 U.S.C. § 324(a), which provides as follows:

> THRESHOLD.—The Director may not authorize a post-grant
> review to be instituted unless the Director determines that the
> information presented in the petition filed under section 321, if
> such information is not rebutted, would demonstrate that it is
> more likely than not that at least 1 of the claims challenged in
> the petition is unpatentable.

Petitioner challenges the patentability of claims 1–60 ("the challenged
claims") of the '281 patent under 35 U.S.C. §§ 101, 102, and 103. Taking
into account Patent Owner's Preliminary Response, we determine that the
Petition demonstrates that it is more likely than not that at least one of the
challenged claims is unpatentable. Pursuant to 35 U.S.C. § 324, we institute
a covered business method patent review of all of the challenged claims of
the '281 patent.

B. Related Matters

Petitioner identifies *Protegrity Corporation v. Informatica
Corporation*, No. 3:14-cv-02588 (N.D. Cal.) as a related district court
proceeding. Pet. 8; Paper 4, 3. Patent Owner identifies numerous other
related district court matters that would be affected by a decision in this
proceeding. *See* Paper 4, 3–5.

The '281 patent was the subject of terminated proceedings CBM2014-
00024 and CBM2014-00121. Those proceedings terminated due to
settlement between the parties. The '281 patent is also the subject of
pending proceedings CBM2015-00006 and CBM2014-00182.

The '281 patent is a continuation of U.S. Patent No. 6,321,201 B1 (Ex. 1009, "the '201 patent"). The '201 patent is the subject of pending proceedings CBM2015-00002, CBM2015-00014, and CBM2015-00030. The '201 patent was also the subject of Reexamination No. 90/011,364, with some originally issued claims confirmed, some cancelled, one claim amended, and several claims added.

C. The '281 Patent

The '281 patent, titled "Data Security System for a Database," issued on March 19, 2013, based on Application No. 12/916,274, filed on October 29, 2010. Ex. 1001, 1. The '281 patent claims priority through a chain of continuation applications to the '201 patent, filed on June 18, 1997. *Id*.

The '281 patent is concerned with protecting data against unauthorized access. *Id*. at col. 2, ll. 30–33. The '281 patent states that "in . . . fields, such as industry, defen[s]e, banking, insurance, etc[.], improved protection is desired against unauthori[z]ed access to the tools, databases, applications[,] etc.[,] that are used for administration and storing of sensitive information." *Id*. at col. 1, ll. 35–39. Figure 4 is reproduced below.
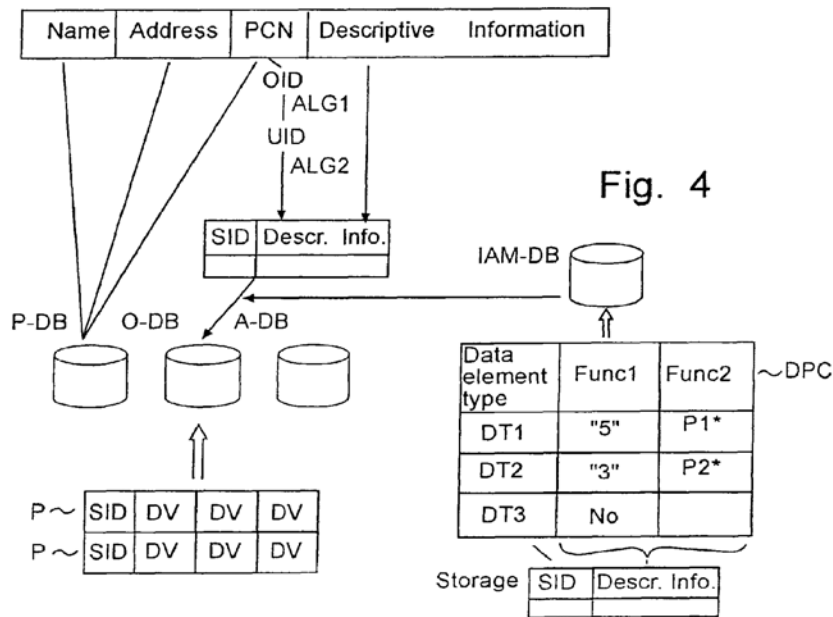
Fig. 4

Figure 4 depicts the '281 patent's system

The system shown in Figure 4 includes an operative database (O-DB) and another database, IAM-DB. O-DB database contains data element values DV that are to be protected. *Id.* at col. 5, ll. 62–67. IAM-DB database contains a data protection catalogue (DPC), which stores protection attributes (e.g., P1*) for data element types (e.g., DT1) that are associated with data element values DV. *Id.* at col. 6, ll. 6–11. The protection attributes state rules for processing the corresponding data element values DV. *Id.* at col. 3, ll. 58–59. For example, a protection attribute indicates the degree to which data element value DV is encrypted (*id.* at col. 7, l. 66–col. 8, l. 3) or indicates that only accepted, or certified, programs are allowed to process data element value DV (*id.* at col. 9, ll. 26–33). *See id.* at col. 4, l. 51–col. 5, l. 6. When a user initiates an attempt to process a certain data element value DV, a compelling calling is created to data protection catalogue DPC to obtain the protection attributes associated with the data element type for data element value DV. *Id.* at col. 2, l. 65–col. 3, l. 4. The

4

processing of data element value DV is then controlled in conformity with the protection attributes. *Id.* at col. 3, ll. 3–5; *see id.* at col. 3, l. 61–col. 4, l. 6. Thus, the individual data element or data element type becomes the controlling unit for determining the level of protection. *Id.* at col. 4, ll. 42–47.

Claims 1 and 33 of the '281 patent are illustrative of the claims at issue and read as follows:

> 1. A computer-implemented data processing method comprising:
>
> maintaining a database comprising a plurality of data portions;
>
> maintaining a separate data protection table comprising, for each of one or more data portions, a plurality of data processing rules associated with the data portion that must each be satisfied before the data portion can be accessed;
>
> receiving a request to access a data portion;
>
> determining whether each of the one or more data processing rules associated with the requested data portion are satisfied; and
>
> granting access to the requested data portion responsive to each of the one or more data processing rules associated with the requested data portion being satisfied.

> 33. A computer-implemented data processing method comprising:
>
> maintaining a database comprising a plurality of data portions, each data portion associated with a data category;
>
> maintaining a separate data protection table comprising, for at least one data category, one or more data processing rules associated with the data category that must each be satisfied before a data portion associated with the data category can be accessed;

DOCKET ALARM

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.