UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INTERNATIONAL BUSINESS MACHINES CORPORATION
Petitioner

v.

DIGITAL DOORS, INC.
Patent Owner

IPR2023-00972
U.S. Patent No. 7,958,268
PETITION FOR *INTER PARTES* REVIEW
UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104

TABLE OF CONTENTS

Page

I. Introduction....1

II. Grounds For Standing....2

III. Summary Of The '268 Patent....2

A. Overview....2

B. Prosecution History....4

C. Priority Date Of The '268 Patent....5

IV. Level Of Ordinary Skill In The Art....6

V. Claim Construction....6

VI. Relief Requested And The Reasons For The Requested Relief....6

A. Challenged Claims And Statutory Grounds For Challenge....6

1. Merenda....7

2. Bossemeyer....9

B. Ground 1: Claims 31, 36, and 41 Are Obvious Over Merenda....14

1. Claim 31, 36, and 41 Preambles....14

2. [31/36/41a] extracting said security sensitive [content/words, characters or icons] from said [input] data to obtain extracted data for respective security levels [and remainder data therefrom];....31

3. [31/36/41b] facilitating the storage of said extracted data in respective ones of said extract stores; and....33

4. [31/36/41c] forwarding [any/said] remainder [input] data to a target[ed] destination in said distributed computer system....35

5. [31/36/41d] and requiring [a respective] predetermined security clearance[s] [for/to] access [to/said corresponding] extract stores. 38

C. Grounds 2-3: Claims 31, 36, and 41 Are Obvious Over Bossemeyer (Ground 2) Or Bossemeyer With Merenda (Ground 3) 40

1. Claim 31, 36, and 41 Preambles 40

2. [31/36/41a] extracting said security sensitive [content / words, characters or icons] from said [input] data to obtain extracted data for respective security levels [and remainder data therefrom]; 59

3. [31/36/41b] facilitating the storage of said extracted data in respective ones of said extract stores; and 64

4. [31/36/41c] forwarding [any / said] remainder [input] data to a target[ed] destination in said distributed computer system 66

5. [31/36/41d] and requiring [a respective] predetermined security clearance[s] [for / to] access [to / said corresponding] extract stores. 69

6. Reasons to Combine Bossemeyer with Merenda 73

VII. Discretionary Denial Would Be Inappropriate 82

A. Discretionary Denial Under The *Fintiv* Factors Is Not Appropriate 82

1. No evidence regarding a stay 82

2. Parallel proceeding trial date 83

3. Investment in the parallel proceeding 84

4. Overlapping issues with the parallel proceeding 84

5. Identity of parties 85

6. Other circumstances 85

B. Discretionary Denial Under 35 U.S.C. § 325(d) Is Not Appropriate 86

VIII. Conclusion 86

IX. Mandatory Notices 87

A. Real Party-in-Interest 87

B. Related Matters 87

C. Lead and Back-up Counsel and Service Information 87

TABLE OF AUTHORITIES

Pages(s)

Cases

Apple Inc. v. Fintiv, Inc.,
IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) 82, 84

Dish Network L.L.C. v. Broadband iTV, Inc.,
IPR2020-01359, Paper 15 (Feb. 12, 2021) 82

Georgetown Rail Equip. Co. v. Holland L.P.,
867 F.3d 1229 (Fed. Cir. 2017) 41

Intel Corp. v. PACT XPP Schweiz AG,
61 F.4th 1373 (Fed. Cir. 2023) 75, 76

KSR Int'l Co. v. Teleflex Inc.,
550 U.S. 398 (2007) 73, 76, 77

Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.,
868 F.3d 1013 (Fed. Cir. 2017) 6

PEAG LLC v. Varta Microbattery GmbH,
IPR2020-01214, Paper 8 (Jan. 6, 2021) 84

Phillips v. AWH Corp.,
415 F.3d 1303 (Fed. Cir. 2005) 6

Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC,
IPR2019-01393, Paper 24 (PTAB June 16, 2020) 82, 85

Statutes

35 U.S.C. § 102(e) 7, 9

35 U.S.C. § 103 6

35 U.S.C. § 311 1

35 U.S.C. § 314(a) 1, 7

35 U.S.C. § 325(d) 86

Rules

37 C.F.R. § 42.100 1

37 C.F.R. § 42.100(b) 6

C.F.R. § 42.104(a).....2

EXHIBIT LIST

Exhibit No.	DESCRIPTION
1001	U.S. Patent No. 7,958,268 to Redlich et al.
1002	Prosecution History of U.S. Patent No. 7,958,268
1003	Declaration of Dr. Erez Zadok
1004	*Curriculum Vitae* of Dr. Erez Zadok
1005	U.S. Patent No. 7,010,701 to Bossemeyer et al.
1006	U.S. Publication No. 2004/0148290 to Merenda et al.
1007	Amended Docket Control Order, *DigitalDoors, Inc. v. Int'l Bus. Machs. Corp.*, Civil Action No. 2:22-cv-00457-JRG-RSP (E.D. Tex. Apr. 5, 2023).
1008	Scheduling Order, *DigitalDoors, Inc. v. Int'l Bus. Machs. Corp.*, Civil Action No. 2:22-cv-00457-JRG-RSP (E.D. Tex. Feb. 7, 2023).
1009	Federal Case Management Statistics for the Eastern District of Texas, as of June 30, 2022
1010	Plaintiff DigitalDoors, Inc.'s Disclosure of Asserted Claims and Initial Infringement Contentions, *DigitalDoors, Inc. v. Int'l Bus. Machs. Corp.*, Civil Action No. 2:22-cv-00457-JRG-RSP (E.D. Tex. Feb. 28, 2023).
1011	U.S. Provisional Application No. 60/247,242
1012	U.S. Provisional Application No. 60/247,232
1013	Director of Central Intelligence Directive No. 1/16, Security of Compartmented Computer Operations ("CIA")
1014	Cheswick et al., Firewalls and Internet Security, Copyright 1994, p. 163
1015	Director's June 21, 2022 Memorandum on Discretionary Denials
1016	Microsoft Computer Dictionary, Fourth Edition, Copyright 1999, Excerpts
1017	Beck et al., Linux Kernel Internals, 2nd Ed., Copyright 1998, pp. 148-187
1018	DOD Standard, Department of Defense Trusted Computer System Evaluation Criteria, December 26, 1985 ("Orange Book")
1019	U.S. Patent No. 8,819,251 to Lenz et al.
1020	U.S. Patent No. 7,356,533 to Schneiter et al.

IBM citations to specific pages of exhibits follow the pagination added to those exhibits per 37 C.F.R. § 42.63(d)(2)(i).

All emphasis has been added unless noted otherwise.

All annotations in Figures have been added unless noted otherwise.

I. Introduction

Pursuant to 35 U.S.C. §§ 311, 314(a), and 37 C.F.R. § 42.100, International Business Machines Corporation ("IBM" or "Petitioner") respectfully requests that the Board cancel as unpatentable claims 31, 36, and 41 (the "Challenged Claims") of U.S. Patent No. 7,958,268 ("'268 Patent," EX1001).

The Challenged Claims cover methods for securing data passing through a browser by separating and securing sensitive portions of the data and then controlling access to the sensitive data.

This Petition demonstrates that separating and securing sensitive data passing through a browser was known. *See e.g.,* EX1006, ¶7 ("[D]ata entered by a consumer into a Web form is separated into related records in a public and private data set. The public records would be available without restriction for read access by a population of merchants. The private records would be available only per the indication of the consumer to the merchant in the population.").

This Petition also demonstrates that controlling access to security sensitive data based on a corresponding security level was known. *See e.g.*, EX1006, ¶29 ("[P]rovision of access to the data elements in the private data set may be made on an element-by-element basis, that is to say, that the merchant may be provided with access to certain select pieces of private data within the single data record…such as the contact information (name, address, phone number, e-mail) but not to other

sensitive data such as revenue, credit card etc..”); *and* EX1005, 2:40-49 (“The information contained within the central database server…can be classified as public information available to all the world; limited access information available to persons or selected groups with a user authentication code; or proprietary information accessible only by the owner of the information or a group with privileges to that directory information.”).

The Petition, supported by the declaration of Dr. Erez Zadok, demonstrates that the combination of the known elements of the Challenged Claims described in the prior art was nothing more than an obvious application of known technologies to address a known problem.

II. Grounds For Standing

Petitioner certifies that the ’268 Patent is eligible for IPR and that Petitioner is not barred or estopped from requesting IPR challenging the patent claims. 37 C.F.R. § 42.104(a).

III. Summary Of The ’268 Patent

A. Overview

The ’268 Patent relates to “a process, program and system which is adjunct or additive to a browser program or a telecommunications program or an encryption process.” EX1001, 1:19-22. Figure 1A illustrates the disclosed data security system:

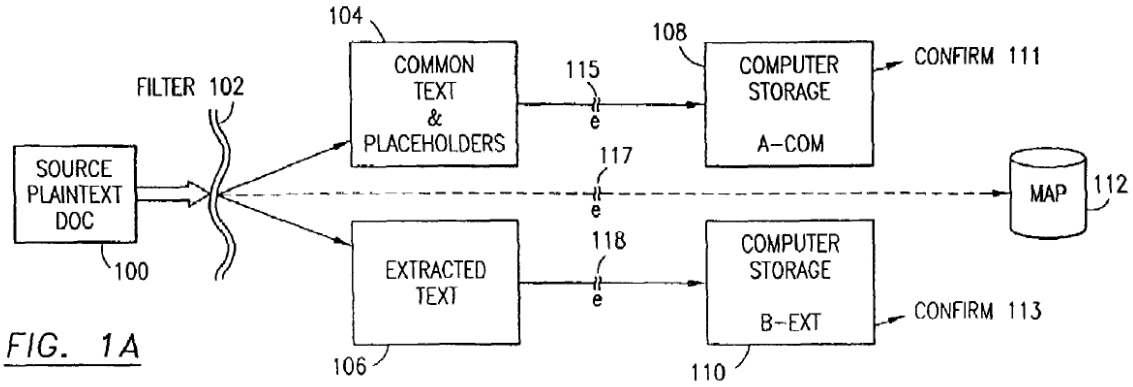


FIG. 1A

EX1001, Figure 1A. As shown, source document 100 is passed through filter 102. EX1001, 18:18-19. "Filter 102…separates out common text or remainder data 104 from uncommon text, words, characters, icons or data objects." EX1001, 18:19-21. The common data objects are then placed into remainder document or common datafile 104, and the uncommon words (or security sensitive words) are placed into a separate extracted text or extracted data file 106. EX1001, 18:31-36. The remainder and extracted data are then stored separately, with the remainder data stored in common storage memory 108, and the extracted data file 106 stored in a different memory computer storage 110. EX1001, 19:18-19, 19:25-26. EX1003, ¶¶79-84.

The data security method may operate in an email or browser environment (EX1001, 9:44-45), for example, using a "user's email device [to] extract[] the security sensitive data, facilitate[] storage of the extracted data in said extract store and, email[] the remainder data to the addressee." EX1001, 9:58-61. "Rather than

extracting security data, the method and program may ***parse*** the data." EX1001, 9:62-63. EX1003, ¶¶82-84.

B. Prosecution History

The '268 Patent was filed on March 7, 2007. EX1001, 1. The Examiner rejected all claims on the ground of nonstatutory obviousness-type double patenting EX1002, 204-206. To overcome the double patenting rejection, Applicant submitted a couple terminal disclaimers, and—in response—the application was allowed. EX1002, 230-233, 253, 261-263, 267. EX1003, ¶¶86-89.

The Examiner's reasons for allowance related to claim 1's encrypting/decrypting limitations:

> Such prior at fails to disclose, among other limitations, in combination the steps of ***encrypting*** said extracted data for each said security level and one of appending, adding or inserting said ***encrypted extracted data*** with remainder input data to form a composite; responsive to a data request, reconstructing fully or partially said input data from said composite with ***decryption*** of said extracted data only in the presence of a respective predetermined security clearance, required for each said security level.

EX1002, 273. EX1003, ¶90.

But these limitations are absent from the Challenged Claims, which are focused on storing sensitive data in extract stores based on the security level, storing non-sensitive data in a separate store, and allowing access based on a security

clearance. As this Petition illustrates, these features were known. For example, Merenda—not considered by the Examiner—discloses securing data passing through a browser (*e.g.*, a web form (EX1006, ¶7)), storing data in extract stores based on different security levels (*e.g.*, "authorizing a viewer" to "access [] certain select pieces of private data" (EX1006, ¶¶27, 29)), and storing non-sensitive data in a separate store. (EX1006, Figure 2, Claim 1). Further, Bossemeyer—also not considered by the Examiner—discloses storing only extracted data for each security level in corresponding extract stores (*e.g.*, limited-access and restricted data (EX1005, 2:17-27)) and storing remainder data in a separate remainder store (*e.g.*, separate stores 210, 212 (EX1005, Figure 3, 5:6-22)). EX1003, ¶¶91-93.

C. Priority Date Of The '268 Patent

The earliest claimed priority date of the Challenged Claims is November 13, 2000, the filing date of two provisional applications which the '268 Patent claims priority to. *See* EX1001, 1; EX1011; EX1012. Petitioner does not concede that the Challenged Claims are entitled to a priority date of November 13, 2000. However, because the prior art references discussed in this Petition qualify as prior art under the earliest claimed priority date of the '268 Patent, Petitioner does not challenge the priority date of the Challenged Claims in this Petition but reserves the right to do so in other proceedings.

IV. Level Of Ordinary Skill In The Art

A Person Of Ordinary Skill In The Art ("POSITA") would have had a bachelor's degree in computer science, computer engineering, electrical engineering, or equivalent, and approximately two years of experience working in the field of data storage systems and data security as of November 13, 2000. Less professional experience can be substituted by additional education, and vice versa. EX1003, ¶¶114-115.

V. Claim Construction

Claim terms in IPRs are construed according to their "ordinary and customary meaning" to those of skill in the art. 37 C.F.R. §42.100(b); *Phillips v. AWH Corp*., 415 F.3d 1303 (Fed. Cir. 2005) (*en banc*). Petitioner submits that, for the purposes of this proceeding and the grounds presented herein, no claim term requires express construction. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). EX1003, ¶¶116-117.

VI. Relief Requested And The Reasons For The Requested Relief

Petitioner asks that the Board institute a trial for *inter partes* review and cancel the Challenged Claims in view of the analysis below.

A. Challenged Claims And Statutory Grounds For Challenge

Petitioner requests cancellation of the Challenged Claims under 35 U.S.C. §103. This Petition, supported by Dr. Erez Zadok's Declaration (EX1003),

demonstrates that there is reasonable likelihood that Petitioner will prevail with respect to the Challenged Claims. *See* 35 U.S.C. § 314(a).

Grounds	Claims	Basis
#1	31, 36, and 41	(§103)-Merenda
#2	31, 36, and 41	(§103)-Bossemeyer
#3	31, 36, and 41	(§103)-Bossemeyer and Merenda

1. Merenda

US Publication No. 2004/0148290 (EX1006, "Merenda"), filed on January, 14, 2004, is a divisional application of US Ser. No. 10/390,954, filed on Mar. 17, 2003, which is a divisional application of US Ser. No 09/563,639, filed on May 2, 2000. Merenda published on July 29, 2004, and is prior art under at least 35 U.S.C. §102(e). EX1003, ¶94.

Merenda describes "a method…for allowing the viewer of a public data set to access related records in a private data set based upon a link which may be selectively provided to the viewer to authorize such access." EX1006, ¶2. Specifically, Merenda describes that "data entered by a consumer into a Web form is separated into related records in a public and private data set. The public records would be available without restriction for read access by a population of merchants.

The private records would be available only per the indication of the consumer to the merchant in the population." *Id.*, ¶7. EX1003, ¶¶95-96.

Merenda discloses that "[u]pon entering the data the consumer may be prompted to indicate whether they wish to provide merchants with access to their private data…The consumer may be offered [an] opportunity to choose among the population of merchant the select merchant to whom they wish their private data to be provided." EX1006, ¶8. "Once selected…the merchants may be provided with a pass code…With the pass code the merchants are provided with the ability to view the particular consumers private data record in the private data set. *Id*., ¶9. For example, a user of Merenda's system requesting information, *e.g*., a merchant, can have access only to certain portions of the private information. That is, a merchant can access certain selected private data sets (*e.g*., private data sets having a first security level, such as ***name, address, phone number, e-mail***), but cannot access other private data sets (*e.g*., private data sets having a second (higher) security level, such as ***revenue, credit card***).

> [T]he merchant may be provided with ***access to certain select pieces of private data*** within the single data record…such as the contact information (***name, address, phone number, e-mail***) but not to other sensitive data such as ***revenue, credit card*** etc.

EX1006, ¶29. EX1003, ¶¶97-98.

A consumer enters data into a web form and data is then separated into public and private data sets. EX1006, ¶7. The data is then collected into tables and, when desired, assembled into an output web page that can be accessed by a merchant for whom access has been authorized. EX1006, ¶10. EX1003, ¶99.

2. Bossemeyer

US Patent No. 7,010,701 (EX1005, "Bossemeyer"), filed on October 19, 1999, and issued on March 7, 2006, is prior art under at least 35 U.S.C. §102(e).

Bossemeyer describes "a network arrangement to provide access to an architecture that supports a variety of advanced smart card applications." EX1005, 1:9-11. Smart cards are electronic devices that "can hold much more information [than data cards] and often include some 'intelligence' such as a microprocessor or the like." EX1005, 1:34-37, 3:28-31 ("Smart card 12… contains circuitry 40 which includes a microprocessor and memory including random access memory (RAM) and read only memory (ROM)."). EX1003, ¶¶100-101.

Bossemeyer's network arrangement includes "a centralized server architecture [where] data related to an individual can be accessed by an individual smart card, predefined groups of smart card users, or the general public." EX1005, 1:49-52. EX1003, ¶¶102-104.

Figure 1 of Bossemeyer, reproduced below, shows a network arrangement including a central database server:

> The network arrangement makes use of a central database server 10 that supports many different smart card applications, and supports many users within a given application. A smart card 12, in combination with a smart card terminal 14, is used to access the central database server 10 through the network central office 16….

EX1005, 2:6-12.

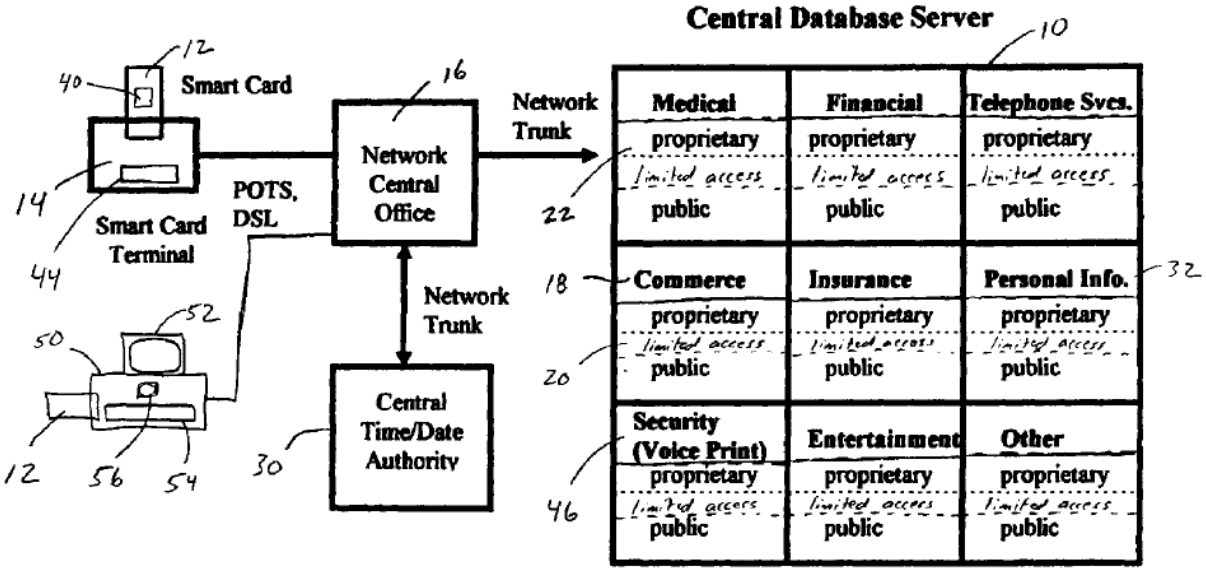


Figure 1

EX1005, Figure 1. EX1003, ¶¶103-105.

Bossemeyer discloses that multiple servers can make up the central database server. EX1005, 3:3-5 ("Although the central database server 10 is shown as a single server, ***it is to be understood that multiple servers may comprise the central database server 10***.") Bossemeyer describes storing different types of information (*e.g.*, financial, insurance, medical information) in databases monitored by appropriate institutions. EX1005, 3:5-16 ("[I]n the merchant transaction discussed

above, the purchaser's credit files are more likely to be stored in a database monitored by the credit reporting companies such as TransUnion or Equifax, as opposed to the central database server 10…. In the same way, insurance information would ultimately reside with the insurer, medical records with the health provider, financial records with the bank or broker, and so on."). EX1003, ¶105.

Bossemeyer's system also includes "advance smart card terminals 50," and "[a] smart card 12 coupled with such a terminal 50 having an established connection through the network central office 16 to the central database server 10 has the power of a typical networked computer." EX1005, 4:9-15. EX1003, ¶106.

Bossemeyer further discloses controlling access to private or proprietary information. EX1005, 2:28-36 ("***Private or proprietary information*** is partitioned such that ***the owner of the information has control over how the information is transferred and used***. Thus, for example, medical information 22 provided to a health professional may be considered private and only available by way of special authorization from the owner of the information. In this way, ***the owner of the information contained within the central database server has control over how the information is transferred and used***."). EX1003, ¶107.

Bossemeyer discloses providing access to data from different partitions of the central database server using a user identification/authentication code or authorization/access code:

> ***Once the user's authorization has been verified, data pointers on the smart card 12 provide access to the relevant partitioned memory portions of the central database server 10***. Routing circuitry controlled by the microprocessor within the central database server 10 routes the data pointer to appropriate memory locations or database of the information keeper relating to the application at issue such as medical, financial, etc. ***Data from these various locations is supplied back to the smart card terminal 14***, and if appropriate, the data stored on the smart card 12 is updated.

EX1005, 3:63-4:6. *See also* EX1005, 4:50-65, Figure 2. EX1003, ¶108.

In Bossemeyer, the information stored in the centralized database server is partitioned according to its security level, *e.g.*, proprietary/restricted, limited access, or public/unrestricted:

> The central database server 10 is a centralized partitioned database server which ***partitions information*** both ***in terms of*** the smart card application as well as ***the accessibility of the information***. The information is stored by category (medical, financial, etc.) as well as ***level of security (unrestricted, or public limited access, restricted)***….

EX1005, 2:13-27. EX1003, ¶109.

Figure 3 discloses examples of the type of information that is accessible using Bossemeyer's networked system.

> [I]nformation is stored in three levels of security: unrestricted, limited access, and restricted. In the pharmacy example,…the pharmacist may have access to the user's digital wallet 210, medical alerts 212, and

> insurance and prescription information 214. Without further authorization,…the pharmacy would not have access to the user's medical history 216.

EX1005, 5:6-15.

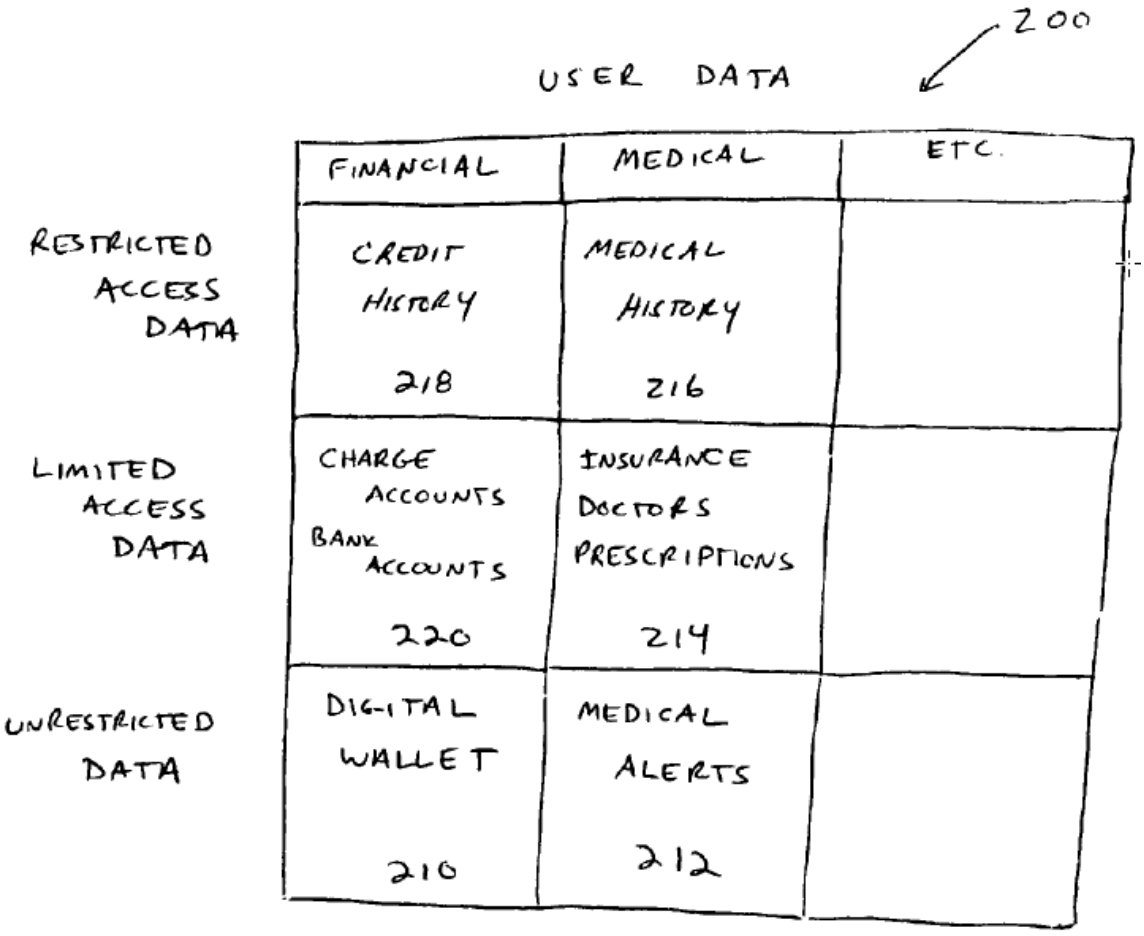


FIG. 3

EX1005, Figure 3. EX1003, ¶110.

Bossemeyer explains that different merchants may have access to information with different levels of security. For example, "a grocer may have access to the

user's digital wallet 210 and medical alerts 212 which may be necessary in the event of a medical emergency, but probably not be allowed to access any other user information." EX1005, 5:16-19. "In contrast, a loan officer at a bank or automotive dealership would be allowed to access to the user's credit history 218 as well as the user's financial account balances 220." EX1006, 5:20-22. EX1003, ¶¶111-113.

B. Ground 1: Claims 31, 36, and 41 Are Obvious Over Merenda

1. Claim 31, 36, and 41 Preambles

To the extent the preamble is limiting, Merenda discloses and/or renders obvious the preambles of independent claims 31, 36, and 41, as explained below. EX1003, ¶118.

i. [31pre-i] A method of securing [input] data passing through a browser,

As discussed in Section VI.C.1.i below, the term "browser" is not limiting. Nevertheless, Merenda discloses and/or renders obvious this limitation. Merenda discloses a method of securing ***input data*** (data entered by a user/consumer). For example, Merenda discloses that "***data entered by a consumer*** into a Web form is separated into related records in a public and private data set." EX1006, ¶7, Title. EX1003, ¶¶119-121, 135.

Specifically, Merenda discloses parsing ***data*** into ***private*** and ***non-private*** elements, for example, by identifying input fields on a ***web page*** that represent sensitive data input versus non-sensitive information:

> [A] set of data may be parsed into ***private*** and ***non-private*** elements. At the most simplistic level this might entail, for example, identifying input fields on a ***Web page*** as requiring ***sensitive data input*** such as an address, credit card or social security number, versus ***non-sensitive information*** such as the name of the item being purchased, the date, time etc...

EX1006, ¶23. EX1003, ¶¶122-125.

Merenda discloses that such input data passes through a ***browser***. Specifically, Merenda discloses "web page 100," with fields where the customer can enter their input. EX1006, ¶24 ("…***data which may emanate from a customer input source*** such as common gateway interface (CGI) fields on a ***Web page 100***."). As Dr. Zadok explains, a POSITA would have recognized that the webpage would be displayed on a ***web browser***. *See* EX1006, ¶¶10, 23; *see also*, US 8,819,251 ("EX1019"), 7:37-39 ("[A] web browser displays a web page that starts a persistent session and contains various web form fields"); Figure 5. EX1003, ¶¶126-128.

Merenda discloses that the input data is entered by a user (*e.g.*, "inputting" the data into a ***browser*** on the input side) to be viewed by a merchant (*e.g.*, viewable via a browser on the output side)—thus "passing through" a ***browser***. Accordingly, the ***input data*** in Merenda passes through a ***browser***, *e.g.*, when the user enters the data in the fields (webform) on Web page 100 and received by Merenda's system. EX1003, ¶129.

Merenda's method secures ***input data*** because "[t]he private records would be available only per the indication of the consumer to the merchant in the population." EX1006, ¶7. Merenda further discloses restricting access to (securing) data:

> Upon ***entering the data*** the consumer may be prompted to indicate whether they wish ***to provide merchants with access to their private data***. This may…take the form of a box on the Web form which may be checked to indicate that the consumer wishes to be contacted.

EX1006, ¶8. EX1003, ¶¶130-131.

Merenda discloses that "a ***web form*** may generate a number of data sets 301*a-d* including demographics 301*a*, server data 301*b*, user data 301*c*, and cost data 301*d*." EX1006, ¶31. Merenda further discloses that "[e]ach time a new ***customer enters web form data***, a record is created in the respective DB2 tables 302*a-d* associated with the segmented data 301*a-d*." EX1006, ¶31. Merenda discloses providing a merchant access to these tables:

> The consumers [sic] ***information will be made accessible to a merchant*** with whom the designated contact is designated, for example, ***by way of an e-mail 305*** provided to the merchant and ***including a hyperlink to the key-coded URL. Via the key-coded URL the merchant may access the query page 306***….

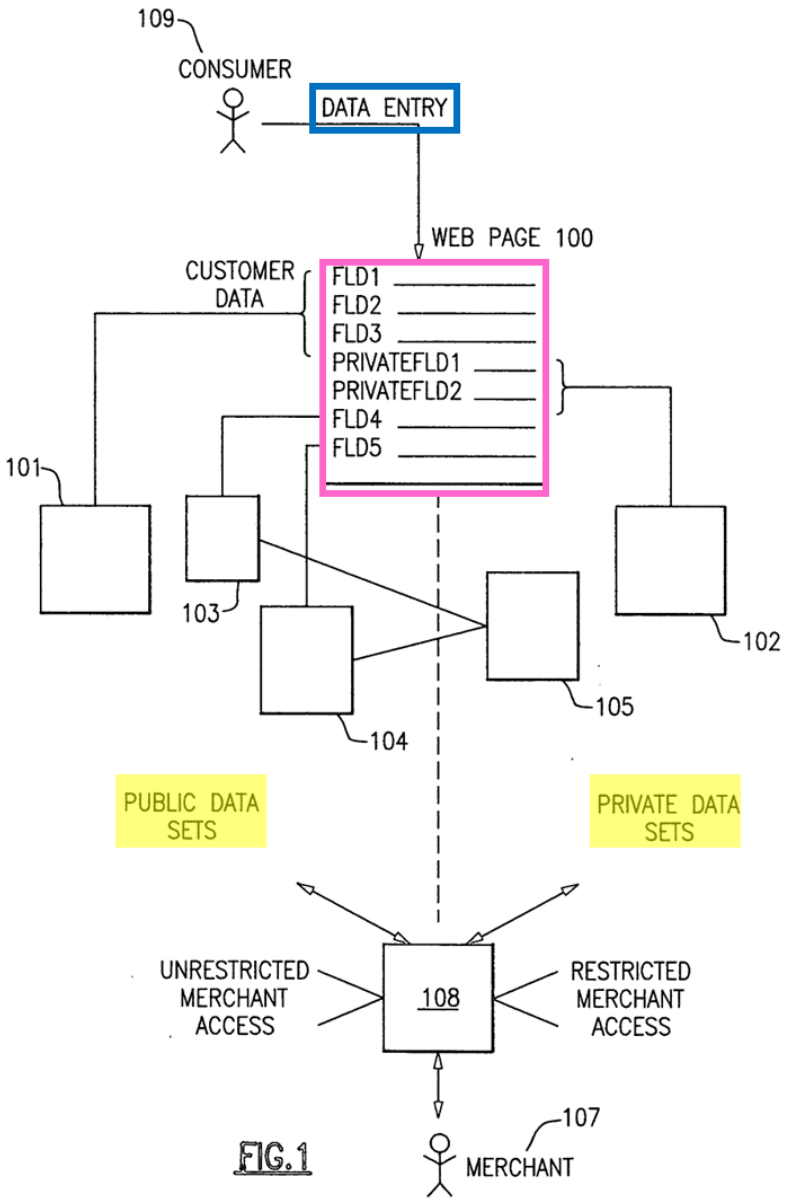
EX1006, ¶32. EX1003, ¶131.

A merchant may be provided with access to a user's data via a webpage assembled for the merchant:

> [U]pon designation by the consumer, the various logically linked records in public and private ***tables for that consumer may be collected and assembled into an output Web page***. The Web page is provided at a uniform resource locator (URL) which has been coded with the common key value linking the related records or with another pass code. The merchant for whom access has been indicated is ***provided either via e-mail or otherwise, with a hyperlink to the coded URL*** thereby enabling the selected merchant to access both the public and private **data**.

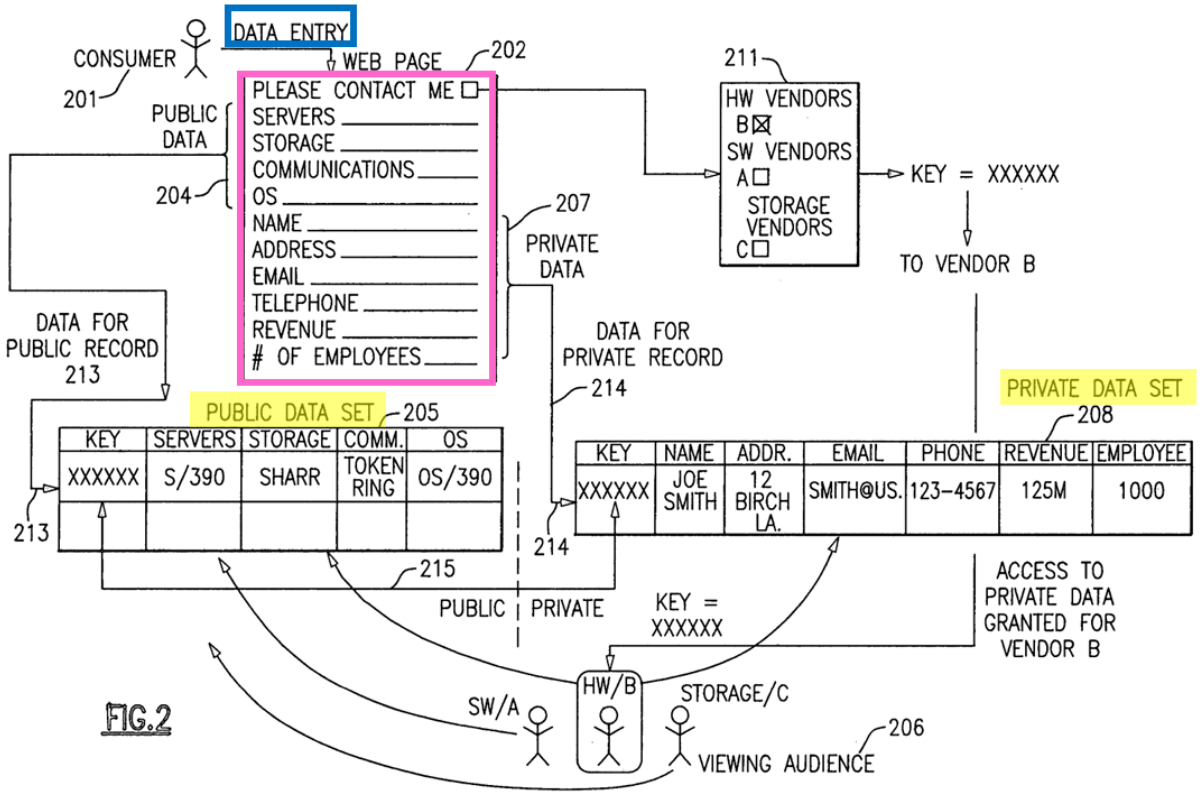
EX1006, ¶10. EX1003, ¶132.

Accordingly, Merenda discloses providing a merchant with access to a consumer's data entered via a web page and where the merchant's access is enabled through the use of a URL. Figure 1 illustrates the customer's data is entered through web page 100 displayed on a ***web browser***, to then be viewed by a merchant:



EX1006, Fig. 1. EX1003, ¶133.

The ***input data*** is secured by separating it into public and private data sets, as shown in Figure 2:



EX1006, Figure 2. EX1003, ¶134.

ii. [36/41pre-i] A non-transitory computer readable medium containing programming instructions for securing [input] data passing through a browser,

Merenda discloses and/or renders obvious this limitation. As discussed in Section VI.B.1.i, Merenda discloses and/or renders obvious "securing input data passing through a browser." EX1003, ¶¶136-137, 140.

Merenda also discloses "[a] non-transitory computer readable medium containing programming instructions." Specifically, Merenda discloses "at least one ***program storage device readable by a machine***, tangibly embodying at least one

program of instructions executable by the machine to perform the capabilities of the present invention can be provided." EX1006, ¶50. Merenda further discloses "programming instructions," *e.g.*, "computer readable program code means":

> The present invention can be included in an article of manufacture (*e.g.*, one or more computer program products) having, for instance, ***computer usable media***. The media has embodied therein, for instance, ***computer readable program code means*** for providing and facilitating the capabilities of the present invention.

EX1006, ¶49, Claim 31 ("the computer program product comprising a ***computer readable medium*** having ***computer readable program code*** therein."). EX1003, ¶138.

Merenda specifically discloses using the computer readable code (*i.e.*, "the programming instructions") to separate ***data*** into public and private sets (*i.e.*, "securing input data"). EX1006, Claim 31 (disclosing "computer readable program code for separating a data record into a public data record stored in a public data set and a private data record stored in a private data set."). EX1003, ¶139.

iii. [31/36pre-ii] said input data having security sensitive content, represented by one or more security sensitive words, characters, images, data elements or data objects therein,

Merenda discloses and/or renders obvious this limitation. EX1003, ¶¶141, 144. As discussed in Section VI.B.1.i, Merenda discloses ***input data***. Further, Merenda discloses (or at least renders obvious) this limitation. EX1006, ¶23 ("[A]

set of ***data*** may be parsed into private and non-private elements…[T]his might entail, for example, identifying input fields on a Web page as requiring ***sensitive data input*** such as an ***address***, ***credit card*** or ***social security number***, versus non-sensitive information such as the name of the item being purchased, the date, time etc."), ¶24 ("[S]uch separation of data elements may be accomplished using known techniques to any desired level of granularity."); Figures 1-2, 6. EX1003, ¶142.

A POSITA would have recognized that Merenda's "sensitive data input" is sensitive in terms of security, *i.e.*, "security sensitive content." *See* EX1006, ¶¶3-5 (discussing the impacts of "privacy interests" regarding consumer data). A POSITA would have further recognized that such content could be presented in multiple forms, such as words for an address, a data element for a link to a bank account, or an image to a social security card. EX1003, ¶143.

iv. [41pre-ii] said data having one or more security sensitive words, characters or icons,

Merenda discloses and/or renders obvious this limitation for the reasons discussed in Section VI.B.1.iii. EX1003, ¶145.

v. [41pre-iii] used in conjunction with a distributed computer system with a plurality of remote memories respectively designated as corresponding extract stores,

Merenda discloses and/or renders obvious this limitation. EX1003, ¶¶146, 161.

First, Merenda discloses a distributed computer system. For example, Merenda discloses that ***multiple individuals*** can access information stored in Merenda's system, as illustrated in Figure 2:

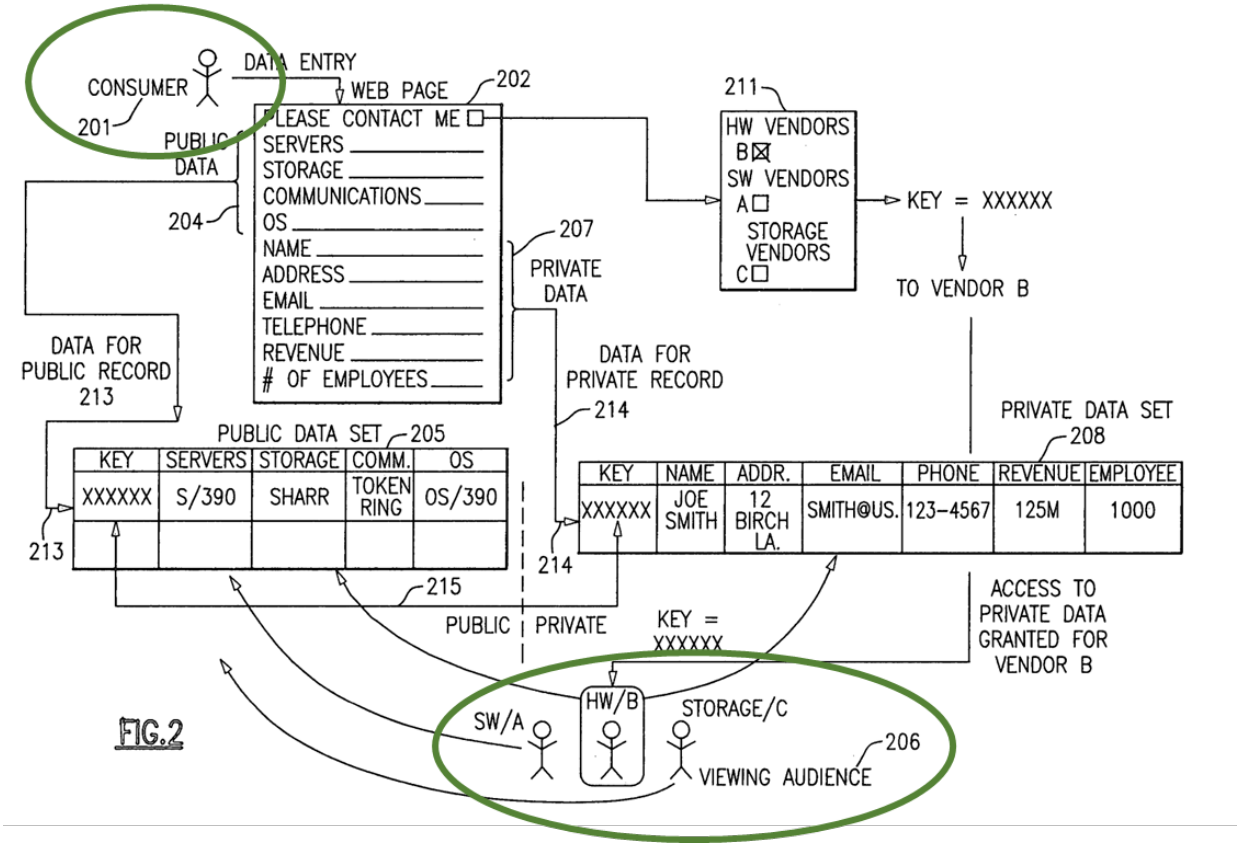


FIG.2

EX1006, Figure 2. EX1003, ¶¶147-51, 160.

Merenda describes a "viewing audience 206," such as including merchants, that access the information stored in Merenda's system. EX1006, ¶26 ("The public data set does not impose any access restrictions to its ***viewing audience 206***. Other items of information…will be stored separately in a private data set 208 which

imposes certain restrictions on access by the ***viewing audience 206***."). A POSITA would have recognized that an "audience" consists of more than one person. A POSITA would have further recognized that multiple merchants would not use the same computer to implement Merenda's computer program, and in fact would use multiple computers. Thus, a POSITA would have recognized that Merenda's "audience" is made possible through a network of computers, i.e., deployed in a distributed computer system. EX1003, ¶¶152-153.

Additionally, as discussed in Sections VI.B.1.i and VI.B.1.ii, a POSITA would have found it obvious to use Merenda's method of entering user data through a web page or web form via a computer. A POSITA would have also found it obvious that multiple users could enter data, using multiple computers, because Merenda supports organization of multiple consumers' data. EX1006, ¶31 ("[T]able 302c includes a record indicating ***the number of users*** for each server type."). EX1003, ¶¶154-156.

Second, Merenda discloses "a plurality of remote memories respectively designated as corresponding ***extract stores***." Specifically, Merenda teaches private data sets and that the "private data sets are…***relational databases*** [plural]" (EX1006, ¶24), *i.e.*, ***extract stores***. These private data sets, which are relational databases, are illustrated in Figure 1:

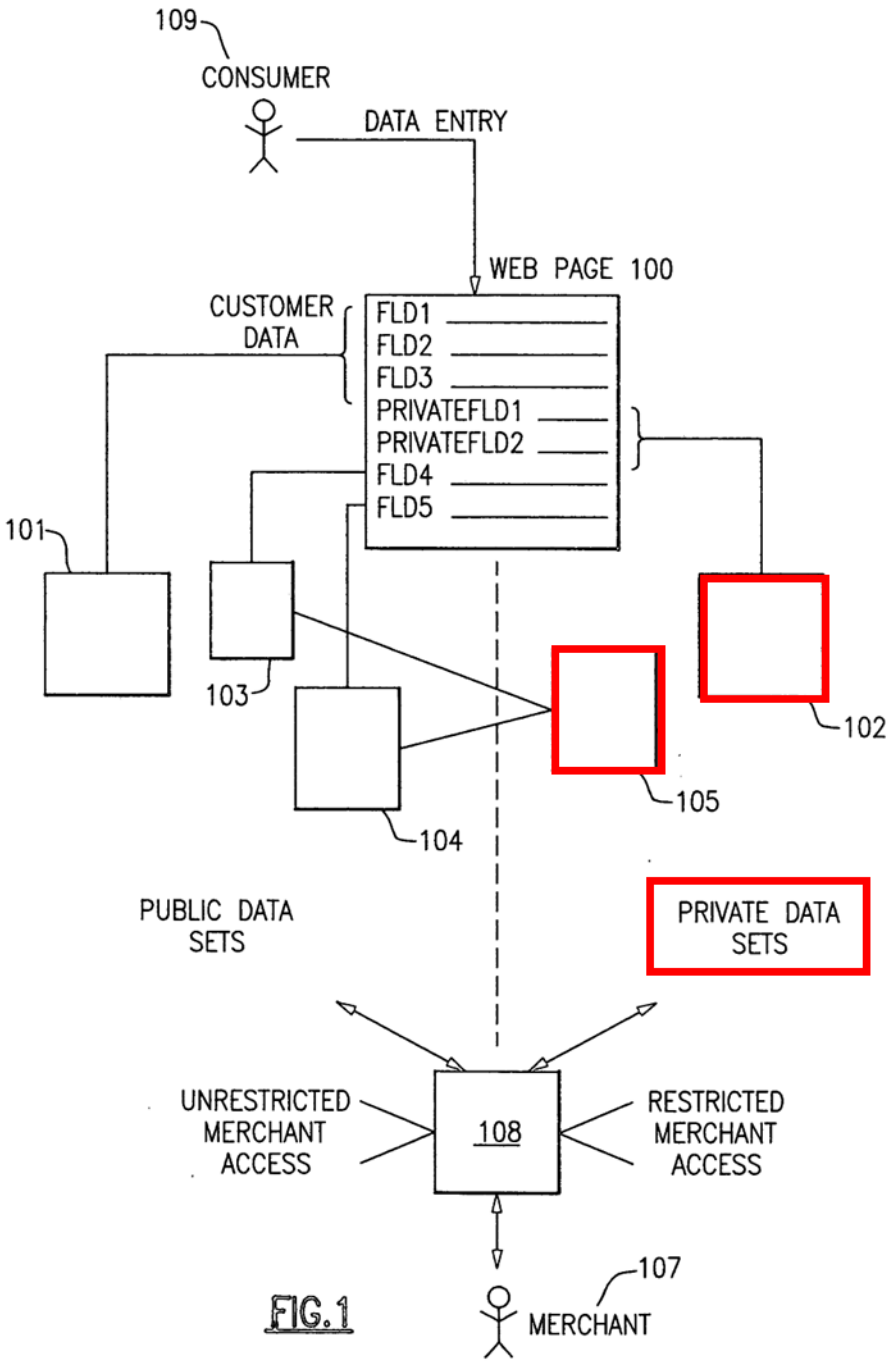


FIG. 1

EX1006, Figure 1.

[S]eparation of data elements may be accomplished using known techniques to any desired level of granularity, resulting potentially in

> ***multiple*** public and ***private data sets*** and in the combination of individually public data sets 103, 104 into a combined private data set 105. The public 101 and ***private 102 data sets*** are, in a preferred embodiment, ***relational databases***….

EX1006, ¶24. EX1003, ¶¶157-158.

To the extent Patent Owner argues that Merenda's private data sets (relational databases) stored in databases are not "a plurality of remote memories," a POSITA would have understood that such private data sets could easily be stored in remote stores (*e.g.*, separate databases) and that these databases could be implemented remotely. For example, a POSITA would have found it obvious to store private datasets in separate, remote databases for better control of the secure data, under specific agencies or organizations that are equipped to monitor them. *See e.g.,* EX1005, 3:5-16 ("[T]he purchaser's credit files are more likely to be stored in a database monitored by the credit reporting companies such as TransUnion or Equifax, as opposed to the central database server 10…. In the same way, insurance information would ultimately reside with the insurer, medical records with the health provider, financial records with the bank or broker, and so on."). A POSITA would have understood that these databases are separate from one another; the '268 Patent admits that "[i]t is ***common knowledge*** that the highest security is delivered through total separation." EX1001, 10:38-39. EX1003, ¶159.

vi. [31/36pre-iii] the [method]/[programming instructions operably] deployed in a distributed computer system with a plurality of extract stores,

Merenda discloses and/or renders obvious this limitation for the reasons discussed in Section VI.B.1.v. EX1003, ¶162.

vii. [31/36/41pre-iv] each having a [respective] security level and clearance [therefor], comprising:

Merenda discloses and/or renders obvious this limitation. EX1003, ¶¶163, 183.

First, Merenda discloses, or at minimum renders obvious, respective ***security levels*** for the private data sets and the extract stores storing them. Merenda discloses providing partial access to data according to different ***security levels***. For example, someone requesting information, *e.g.*, a merchant, ***can have access only to certain portions of the private information***. That is, a merchant can access certain selected private data sets (*e.g.*, private data sets having a ***first security level***, such as ***name, address, phone number, e-mail***), but cannot access other private data sets (*e.g.*, private data sets having a ***second (higher) security level***, such as ***revenue, credit card***), *i.e.*, one merchant can have a different security level than another.

> It is useful to note that the present invention contemplates that provision of ***access to the data elements in the private data*** set may be made on an element-by-element basis, that is to say, that ***the merchant may be provided with access to certain select pieces of private data within the***

> ***single data record 214***, such as the ***contact information (name, address, phone number, e-mail)*** but ***not to other sensitive data*** such as ***revenue, credit card etc***.

EX1006, ¶29. EX1003, ¶¶164-165.

Further, Merenda discloses separating data at any level of granularity resulting in multiple private data sets and providing access to reconstructed data. EX1006, ¶29 ("[A]ccess to the data elements in the private data set may be made on an element-by-element basis..."), ¶¶8-10, 23-26, 29-30, 34-36. EX1003, ¶¶166-169.

Second, Merenda discloses allowing access to the private data sets based on a respective ***clearance*** (*i.e.*, a ***pass code***).

> The Web page is provided at a uniform resource locator ***(URL) which has been coded*** with the common key value linking the related records ***or with another pass code***. The merchant for whom access has been indicated is provided either via e-mail or otherwise, with a hyperlink to the coded URL thereby enabling the selected merchant to access both the public and private data. With the ***pass code*** the merchants are provided with the ability to view the particular consumers private data record in the private data set.

EX1006, ¶¶10, 25 ("As a result of the distribution of data elements among various public and private data sets, it is desirable ***to establish a level of control over access*** to the public and private data stored therein."). Public data may be available without restriction, while private or sensitive data would only be available based on the

clearances indicated, for example, by the consumer (*e.g.*, provider of the data) or the level of control indicated for the data set:

> ***[A] public data set is available, without restriction***…or… to a select subset of merchants 107 who subscribe to a marketing service that accumulates such data....The present invention is directed toward providing the level of control 108 required in keeping the public and private data separate, and ***allowing access to the private data either at the explicit direction of the consumer 109 (the individual that is the subject of the public and private data) or in such a manner as to protect the privacy concerns of the consumer***.

EX1006, ¶25.

> ***The public data set does not impose any access restrictions*** to its viewing audience 206. Other items of information, such as the name, location, phone, e-mail, revenue, number of employees, may for our purposes, be designated as a single record 214 of private data elements 207 and as such will be stored separately in ***a private data set 208 which imposes certain restrictions on access by the viewing audience 206***.

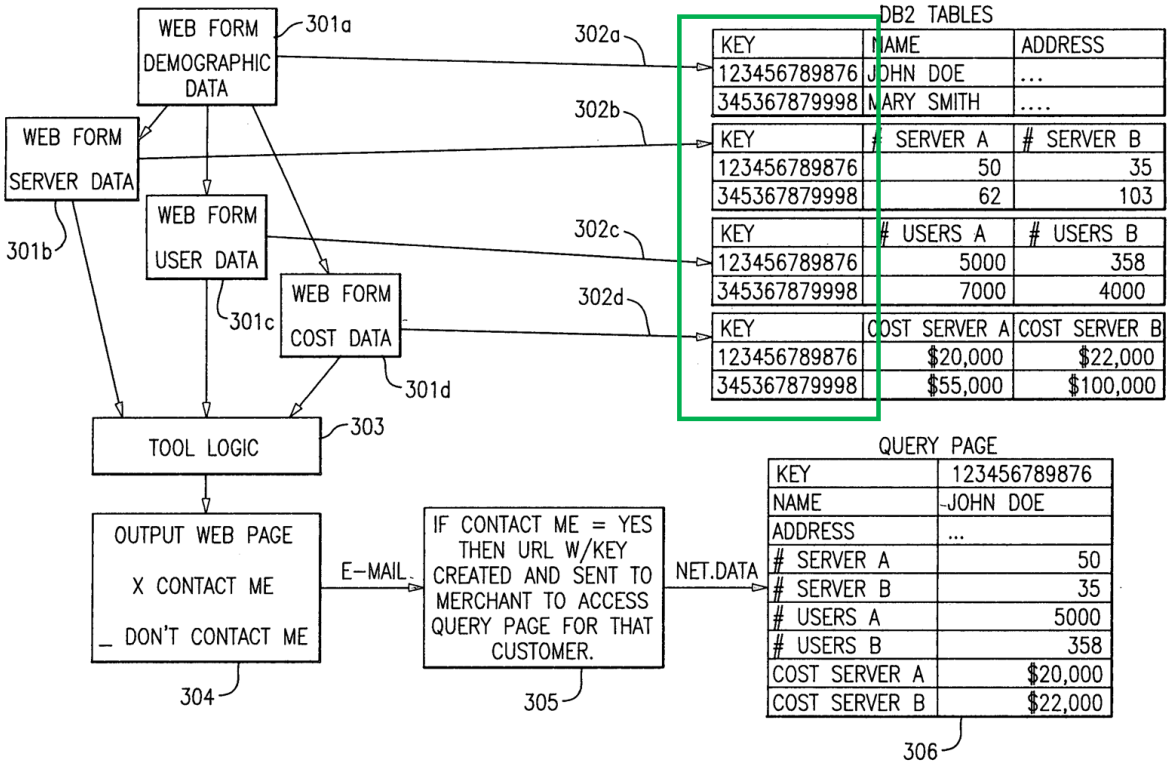
EX1006, ¶26; ¶¶10-13, 23, 34-35. EX1003, ¶¶170-178.

Merenda also discloses customizable access to the private data for the viewing audience (each merchant), with the customer retaining the highest ***clearance***. EX1006, ¶37 ("[T]he selective access 203 to the private data set 208 provides a merchant with consumer-controlled access to private data which prevents massive

unintended access while allowing those selected merchants to benefit from access to the data."). EX1003, ¶179.

To the extent Patent Owner argues that Merenda does not disclose respective ***security levels***, a POSITA would have understood that one merchant is not granted the same access to a consumer's private data compared to another merchant (or even to the actual consumer). Merenda discloses that a consumer may limit the number of merchants who have access to their data, and to what data a merchant has access to. EX1006, ¶28 ("[T]he consumer may be presented with a menu 211 of potential solution providers… [t]his level of control allows the customer to selectively provide his/her contact information to a subset of the viewing audience 206 with whom the customer wishes to interact, without opening up the otherwise private data to the entire viewing audience 206 for uncontrolled public access."), ¶29 ("It is useful to note that the present invention contemplates that provision of access to the data elements in the private data set may be made on an element-by-element basis, that is to say, that the merchant may be provided with access to certain select pieces of private data within the single data record 214, such as the contact information (name, address, phone number, e-mail) but not to other sensitive data such as revenue, credit card etc.."). EX1003, ¶180.

Merenda discloses that the private data may be stored in multiple tables, each with an ***access key*** enabled by the consumer. *See* Figure 3:



EX1006, Figure 3, ¶35 ("The selected merchants are provided with a key which enables them to access the private information…."). EX1003, ¶181.

A POSITA would have understood that one merchant could be granted access to all private data sets, and another merchant could be granted access to only a select data sets, creating respective ***security levels*** for extracted data (*i.e.*, private data sets). This would be a trivial modification, considering that Merenda already discloses multiple private data sets (for different types of private data), multiple access keys (one for each merchant), and limiting merchant access to certain private data sets.

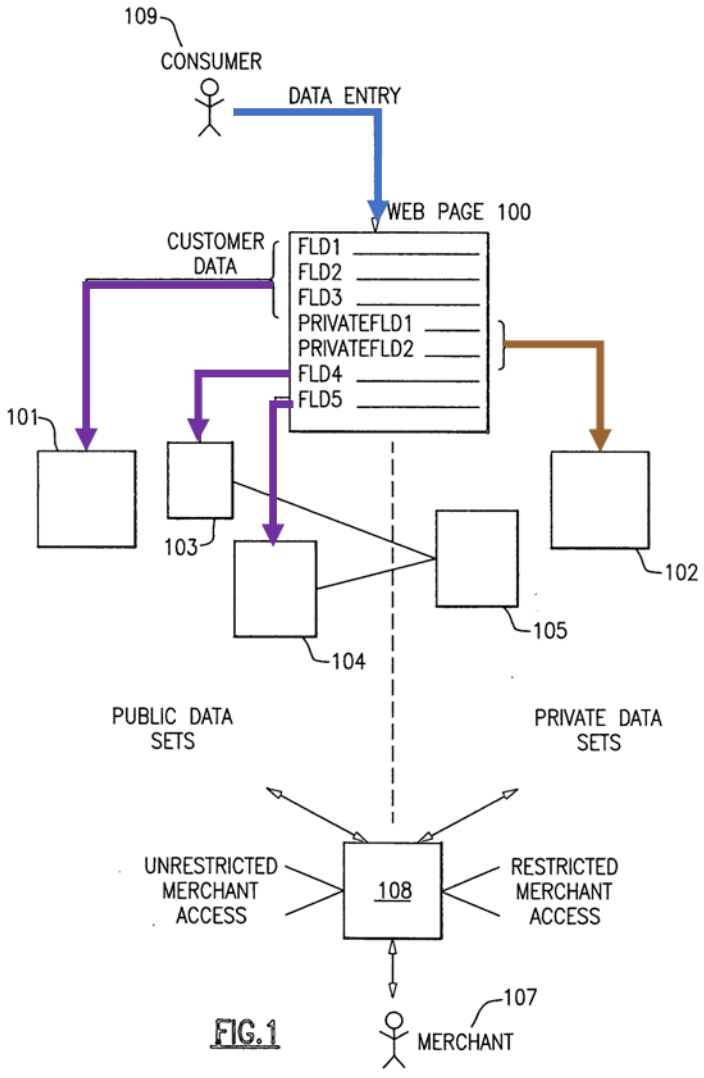
This trivial modification could be performed by permitting some access keys to be limited to certain private data sets, and not others. EX1003, ¶182.

2. [31/36/41a] extracting said security sensitive [content/words, characters or icons] from said [input] data to obtain extracted data for respective security levels [and remainder data therefrom];

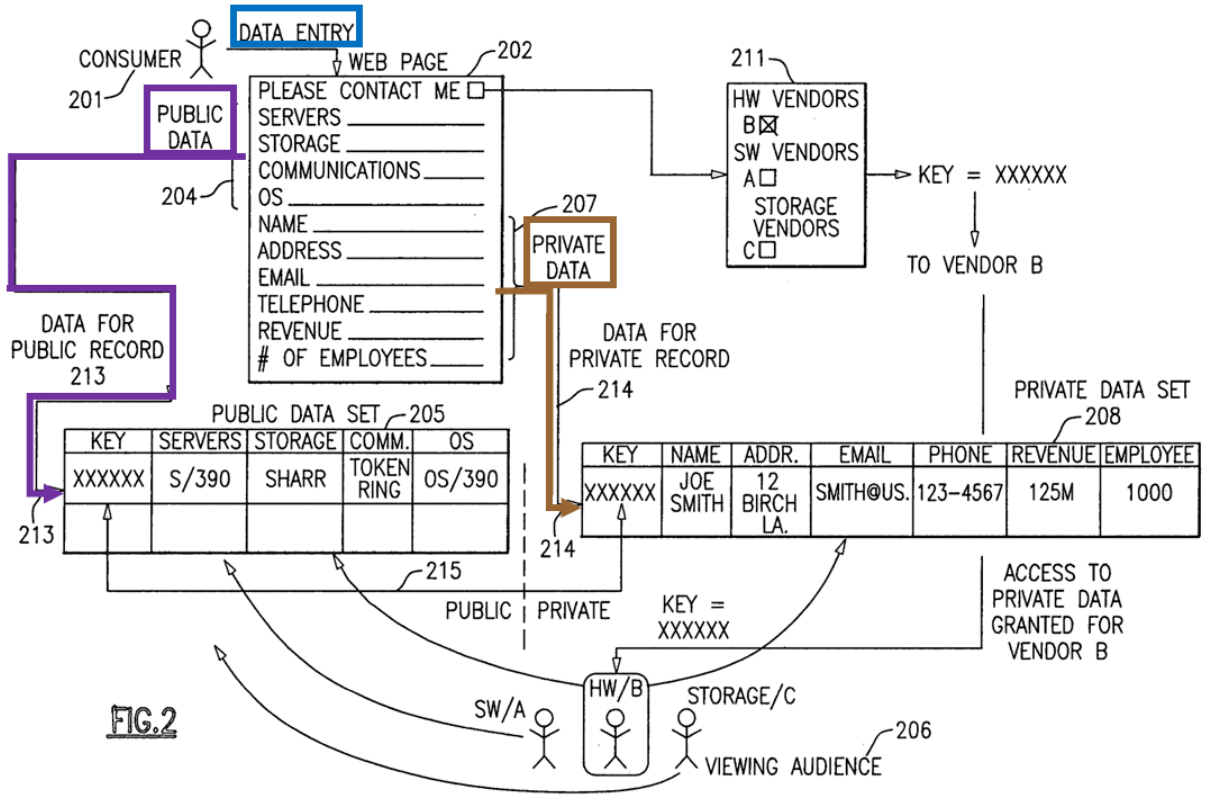
Merenda discloses and/or renders obvious this limitation. As discussed in Sections VI.B.1.v, VI.B.1.vi, and VI.B.1.vii, Merenda discloses multiple extract stores (which store ***extracted data***) for respective ***security levels***. EX1003, ¶184, 191.

Merenda discloses extracting, *e.g.*, parsing, security sensitive content (words, characters or icons), *e.g.*, ***private elements***, from ***user data*** to obtain subsets of ***extracted data***, *e.g.*, ***address***, ***credit card*** or ***social security number*** and ***remainder data***, *e.g.*, ***non-private elements***. EX1006, ¶23 ("[A] set of ***data*** may be ***parsed*** into ***private*** and ***non-private elements***. At the most simplistic level this might entail, for example, identifying input fields on a Web page as requiring sensitive data input such as an ***address***, ***credit card*** or ***social security number***, versus non-sensitive information such as the ***name of the item being purchased***, the ***date***, ***time*** etc."), ¶24 ("[D]ata may come from any number of sources, including…surveys, transactional data, etc. and is not limited to customer interactions over the World Wide Web. …[S]uch separation of data elements may be accomplished using known techniques

to any desired level of granularity, resulting potentially in multiple public and private data sets…."), ¶31 ("Turning to FIG. 3 it is seen that a web form may generate a number of data sets 301*a-d* including demographics 301*a*, server data 301*b*, user data 301*c*, and cost data 301*d*. Any of these data sets may be designated as including private data, and the ***remaining data sets*** include public data."), Figures 1-3.



EX1006, Figure 1.

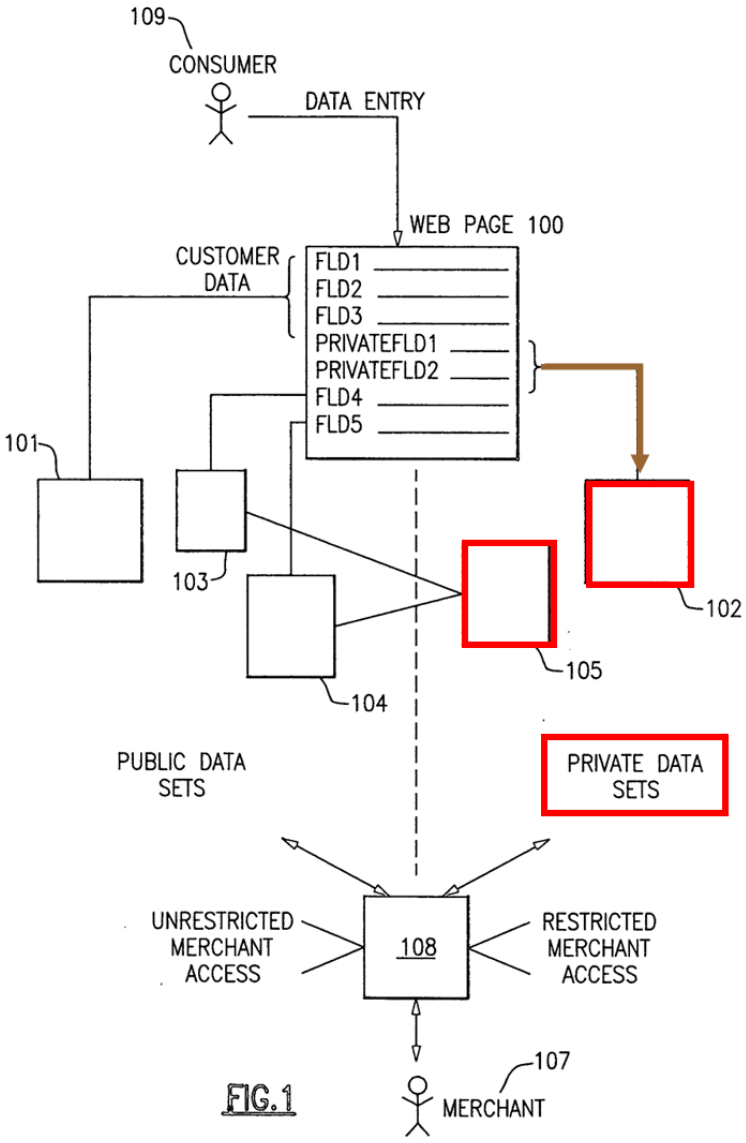


EX1006, Figure 2. EX1003, ¶¶185-190.

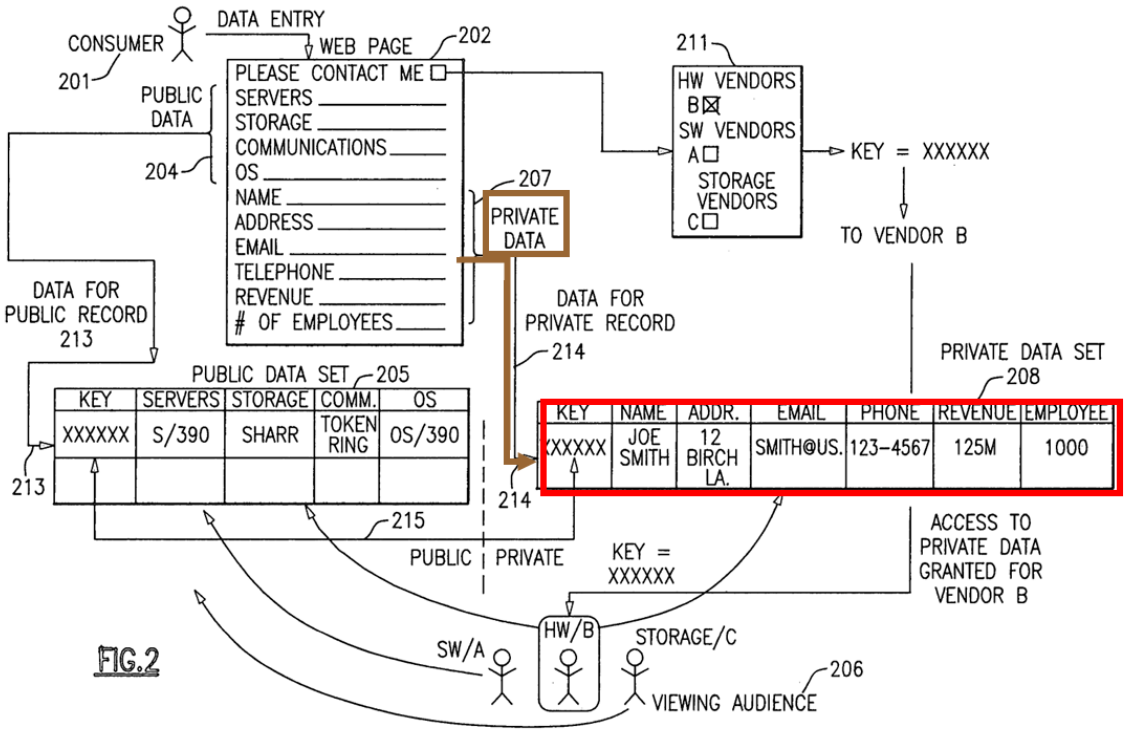
3. [31/36/41b] facilitating the storage of said extracted data in respective ones of said extract stores; and

Merenda discloses and/or renders this limitation. EX1003, ¶¶192, 196.

As discussed in Section VI.B.1.v, Merenda's distributed computer system includes a plurality of remote memories respectively designated as corresponding ***extract stores***. As also disclosed in Section VI.B.2, Merenda discloses parsing data into ***public data*** (*e.g.*, ***remainder data***) and ***private data*** (*e.g.*, ***extracted data***) and storing (facilitating the storage of) the ***extracted data*** as respective private data sets (*e.g.*, in ***databases*** (***extract stores***)). *See e.g.,* Figures 1-2, below:



EX1006, Figure 1.



EX1006, Figure 2; *see also* Section VI.B.1.v. EX1003, ¶¶193-195.

4. [31/36/41c] forwarding [any/said] remainder [input] data to a target[ed] destination in said distributed computer system

Merenda discloses and/or renders obvious this limitation. EX1003, ¶197, 201.

As discussed in Section VI.B.3, Merenda discloses parsing (separating) ***public data*** (*e.g.*, ***remainder data***). Further, Merenda discloses using its method in a distributed computer system. *See* Section VI.B.1.ii. EX1003, ¶198.

Merenda discloses forwarding (storing) ***remainder data*** in ***public data sets***, *e.g.*, a ***targeted destination***, which can be one or more databases. EX1006, Claim 1 ("[S]eparating a data record into a ***public data record*** stored in a ***public data set*** and a private data record stored in a private data set."), Claim 31 ("[C]omputer readable

program code for separating a data record into a ***public data record*** stored in a ***public data set*** and a private data record stored in a private data set."), ¶26 ("The particular responses to theses technical queries…we will designate as being ***public data***. …[T]he particular hardware, software and storage solution responses made by the consumer will be stored as a single record 213 in a ***public data set 205***."), ¶24 ("The ***public 101*** and private 102 ***data sets*** are, in a preferred embodiment, ***relational databases***") Figures 1-2.

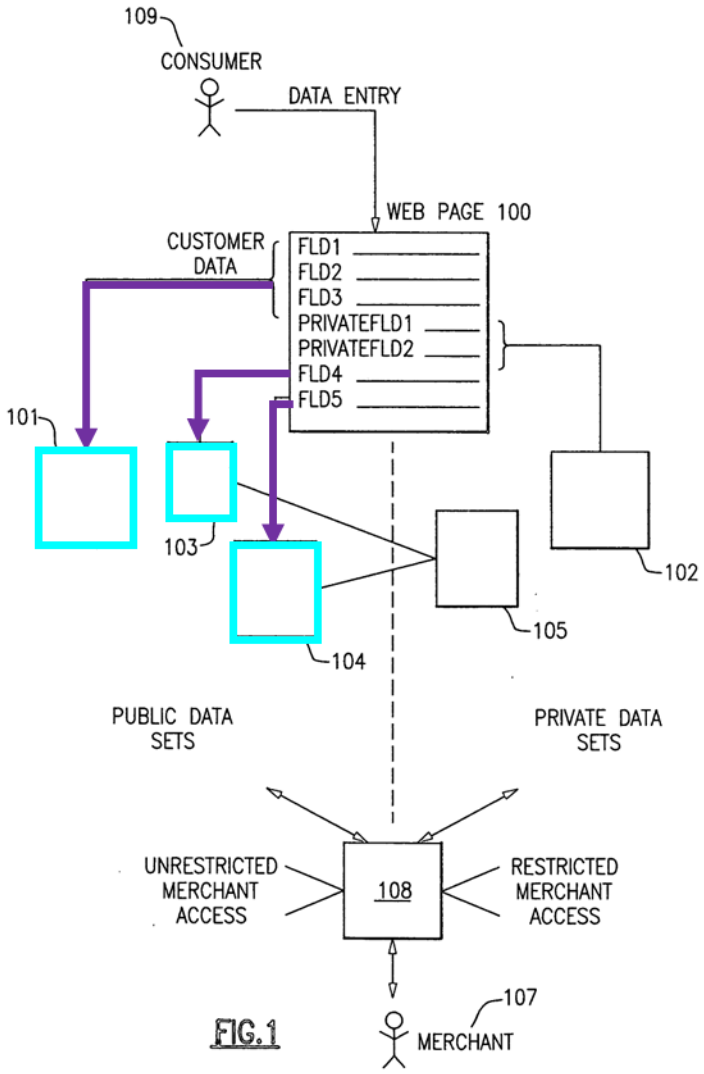


FIG. 1

EX1006, Figure 1.

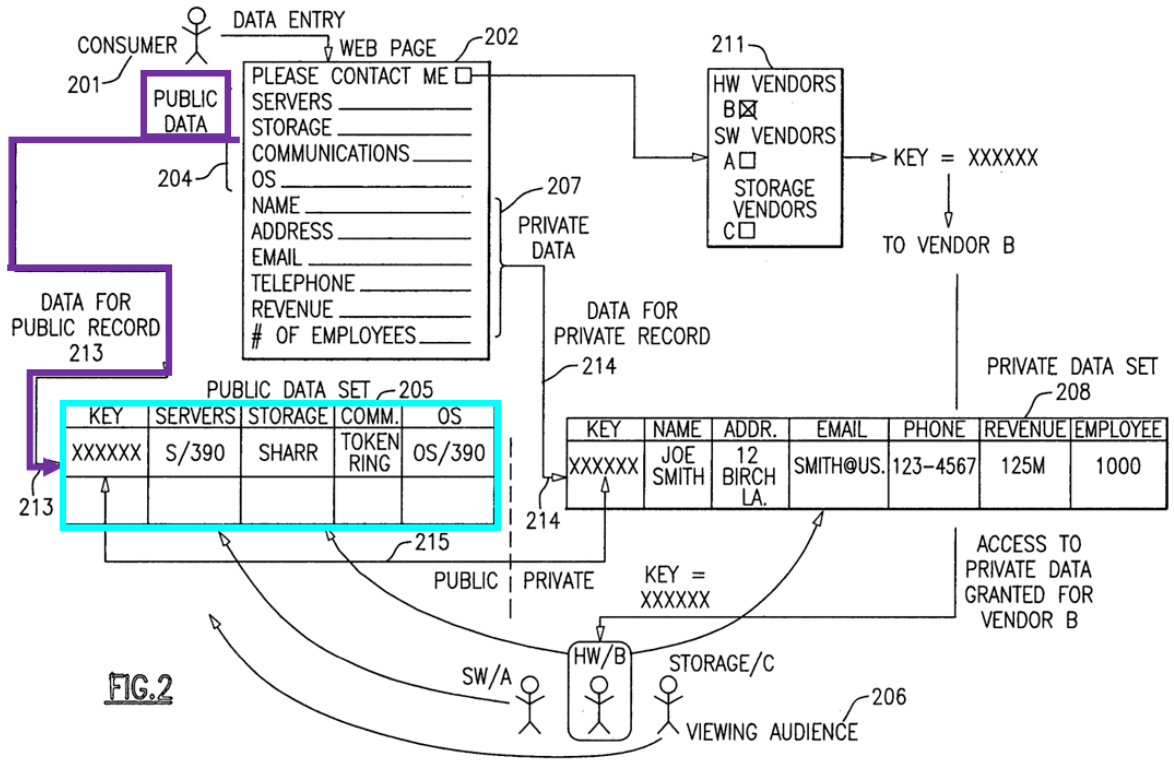


FIG.2

EX1006, Figure 2. EX1003, ¶¶199-200.

5. [31/36/41d] and requiring [a respective] predetermined security clearance[s] [for/to] access [to/said corresponding] extract stores.

Merenda discloses and/or renders obvious this limitation. As discussed in Sections VI.B.1.v and VI.B.1.vii, Merenda discloses and/or renders obvious respective security levels for the private data sets and the ***extract stores*** storing them and allowing access to the private data sets based on respective ***clearances***. EX1003, ¶¶202-203, 215.

Specifically, Merenda discloses accessing data by combining the public and private data, when the requester has the ***predetermined (designated) security***

clearance. *Id.,* ¶7 ("The private records would be ***available only per the indication of the consumer*** to the merchant in the population."), ¶10 ("***[U]pon designation by the consumer***, the various logically linked records in public and private tables for that consumer may be collected and assembled into an output Web page."), ¶25 ("[P]roviding the level of control 108 required in keeping the public and private data separate, and ***allowing access to the private data either at the explicit direction of the consumer*** [] or in such a manner as to protect the privacy concerns of the consumer."), ¶35 ("The selected merchants are provided with a key which enables them to access the private information 406."), ¶36 ("In step 409 those vendors ***for whom access has been indicated by the consumer*** in step 407 are provided with an e-mail including a hyperlink to the key-coded URL through which the merchant may access 410 the results of the combined consumer data."). Merenda discloses that such designation or direction by the consumer is ***predetermined***. EX1006, ¶26 ("***[A] consumer*** 201, ***upon entering information*** to a Web page 202, is ***given an option 203 to designate*** that they wish to be contacted regarding the particular Web transaction."). EX1003, ¶¶204-209.

Further, Merenda discloses accessing the data based on any desired level of granularity. *Id*., ¶29 ("It is useful to note that the present invention contemplates that provision of ***access*** to the data elements in the private data set may be made on an element-by-element basis, that is to say, that the merchant may be ***provided with***

access to certain select pieces of private data within the single data record 214, such as the contact information (name, address, phone number, e-mail) but not to other sensitive data such as revenue, credit card etc."), ¶¶8-10, 23-26, 29-30, 34-36. EX1003, ¶¶205-210.

A POSITA would have understood that to provide access to data, which includes private data sets, Merenda's method would access the respective ***extract stores*** for the corresponding security levels (*e.g.*, highest level for full reconstruction of data), which would suggest using a ***predetermined security clearance*** to access the corresponding ***extract store*** storing the data. EX1003, ¶¶211-214.

C. Grounds 2-3: Claims 31, 36, and 41 Are Obvious Over Bossemeyer (Ground 2) Or Bossemeyer With Merenda (Ground 3)

1. Claim 31, 36, and 41 Preambles

The preambles of claims 31, 36, and 41 include the term "browser," which is not limiting. Bossemeyer discloses the preambles of independent claims 31, 36, and 41, as explained below. To the extent Patent Owner argues that "browser" is limiting, Bossemeyer renders obvious alone (or in combination with Merenda for Ground 3) the preambles of independent claims 31, 36, and 41, as explained below. EX1003, ¶¶216-219, 321.

i. [31pre-i] A method of securing [input] data passing through a browser,

The term "browser" is not limiting. A "browser" is not mentioned in the body of the claim (*e.g.*, no antecedent basis), is not essential to understand the body of the claim, is not an additional step of the method of the claim, and it was not relied on by Patent Owner to distinguish prior art during prosecution. *Georgetown Rail Equip. Co. v. Holland L.P.*, 867 F.3d 1229, 1236 (Fed. Cir. 2017) ("Generally, the preamble does not limit the claims…However, a preamble may be limiting if: it recites essential structure or steps; claims depend on a particular disputed preamble phrase for antecedent basis; the preamble is essential to understand limitations or terms in the claim body; the preamble recites additional structure or steps underscored as important by the specification; or there was clear reliance on the preamble during prosecution to distinguish the claimed invention from the prior art." (quotations and citations omitted)).

Bossemeyer discloses and/or renders obvious a method of securing ***input data***. *First,* Bossemeyer discloses a user ***inputting*** data into its system. EX1005, 5:28-31 ("[T]he user data becomes populated when the user subscribes as part of the smart card activation process. Additional data is created as the user and merchants interact with the system."). EX1003, ¶¶221, 229.

Second, Bossemeyer discloses securing the data that has been **input**. Specifically, Bossemeyer discloses partitioning the ***data*** to control how the data is transferred and used. EX1005, 2:28-30 ("Private or proprietary information is partitioned such that ***the owner of the information has control over how the information is transferred and used***."). Bossemeyer further discloses storing and restricting access to sensitive data ("***limited access information***" and/or "***proprietary information***"):

> The information contained within the central database server is associated with the user identification codes on the smart cards 12 such that it can be classified as public information available to all the world; ***limited access information*** available to persons or selected groups with a user authentication code; or ***proprietary information*** accessible only by the owner of the information or a group with privileges to that directory information. Besides ***restricting others access to a smart card holder's information/data***, the information or data within the server 10 can limit options available to cardholders.

EX1005, 2:40-50; Figures 1, 3:

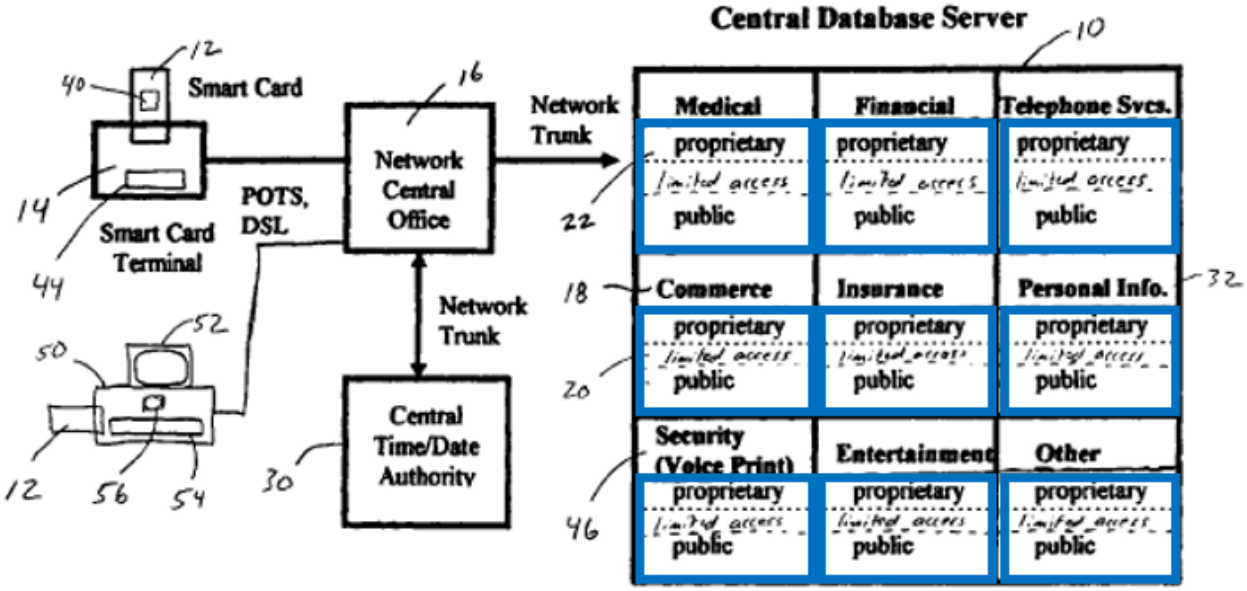


Figure 1

EX1005, Figure 1.

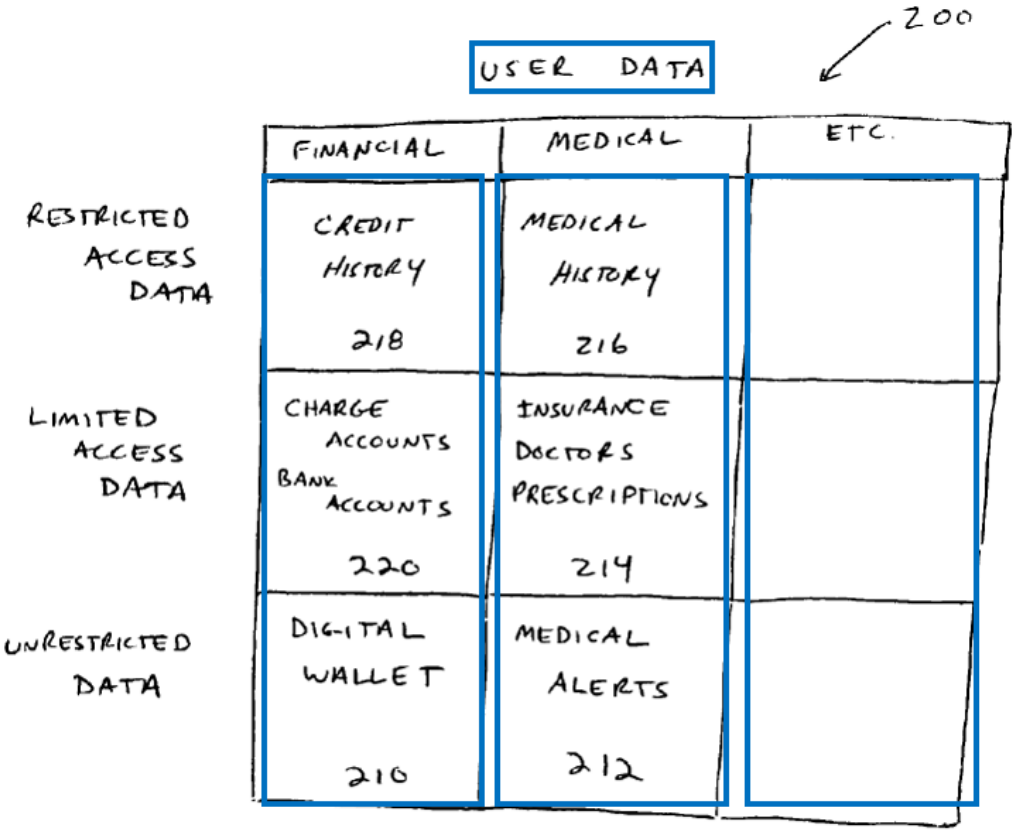


FIG. 3

EX1005, Figure 3. EX1003, ¶¶222-226.

To the extent Patent Owner argues the term "browser" is limiting, Bossemeyer renders obvious "securing input data ***passing through a browser***." For example, a user of the Bossemeyer system using a computer to populate user data, would have used a browser to visit a website associated with smart card services to enter data. As Dr. Zadok explains, a POSITA would have understood that using a website and the Internet was a ubiquitous way of signing up to different services from different providers. Thus, a POSITA would have found it obvious for a user to enter data

through a website running on a browser when a user subscribes to Bossemeyer's smart card services or when the user continues to interact with Bossemeyer's system. And because the user data is entered on the website, the data passes through the browser into Bossemeyer's system. EX1003, ¶¶227-229.

For Ground 3, to the extent the term "browser" is found to be limiting and Patent Owner argues that Bossemeyer fails to render obvious this limitation, Bossemeyer combined with Merenda renders obvious this limitation, because as discussed in Section VI.B.1.i., Merenda itself discloses and/or renders obvious this limitation. For example, a POSITA would have found it obvious to use Merenda's method of inputting user data through a web page or web form via a computer in the combined Bossemeyer/Merenda system, for example, when a user subscribes to Bossemeyer's smart card services. EX1005 (Bossemeyer), 5:28-30 ("the user data becomes populated when the user subscribes as part of the smart card activation process"). A POSITA would have understood that a user would have used a computer, which would allow a web browser running on the computer to present the web page or web form to the user. Further, as discussed in Section VI.C.6, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in combining Bossemeyer with Merenda. EX1003, ¶¶322-329.

ii. [36/41pre-i] A non-transitory computer readable medium containing programming instructions for securing [input] data passing through a browser,

Bossemeyer renders obvious alone (or with Merenda for Ground 3) this limitation. EX1003, ¶¶230, 237.

As discussed in Section VI.C.1.i, Bossemeyer discloses and/or renders obvious a method of securing input data passing through a browser. A POSITA would have understood that Bossemeyer's method would have been implemented using programming instructions and that these programming instructions would be stored in a non-transitory computer readable storage medium. EX1003, ¶231.

Additionally, Bossemeyer's method is performed in a computer system: Bossemeyer's network arrangement for securing data is implemented over an interconnected network of computers. A POSITA would have understood that Bossemeyer's method would have been implemented using programming instructions and that these programming instructions would be stored in a "non-transitory computer readable medium." To implement its computerized method, Bossemeyer's computer system would read the programming instructions from the medium and execute them, for example, in an execution unit. EX1003, ¶¶232-236.

For Ground 3, to the extent Patent Owner argues Bossemeyer does not disclose this limitation, Merenda does for the reasons discussed in Section VI.B.1.ii. For example, Merenda discloses "at least one program storage device readable by a

machine, tangibly embodying at least one program of instructions executable by the machine to perform the capabilities of the present invention can be provided." EX1006, ¶¶49-50. As discussed in Section VI.C.6, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in combining Bossemeyer with Merenda. EX1003, ¶¶330-334.

iii. [31/36pre-ii] said input data having security sensitive content, represented by one or more security sensitive words, characters, images, data elements or data objects therein,

Bossemeyer renders obvious alone (or with Merenda for Ground 3) this limitation. As discussed in Section VI.C.1.i, Bossemeyer stores ***input data*** with "***limited access information***" and/or "***proprietary information***." *See also,* EX1005, 2:40-50; Figures 1, 3. A POSITA would have understood that the "***limited access information***" and/or "***proprietary information***" would include security sensitive content, such as, words, characters, images, data elements or data objects, because Bossemeyer discloses restricting access to such content. Bossemeyer discloses different types of security sensitive content, as shown, for example, in Figure 3, including a user's ***medical history 216***, ***prescription information 214***, ***credit history 218***, and ***bank accounts 220***. A POSITA would have understood that medical history information can include images of medical charts, insurance information can

include icons of the user's insurance card, prescription information can include the names of the drugs prescribed to the user, etc. *See, e.g.,* EX1005, 3:25-27 ("[P]ersonal information 32 such as digitized photograph…can be included as part of a photo identification such as a driver's license.").

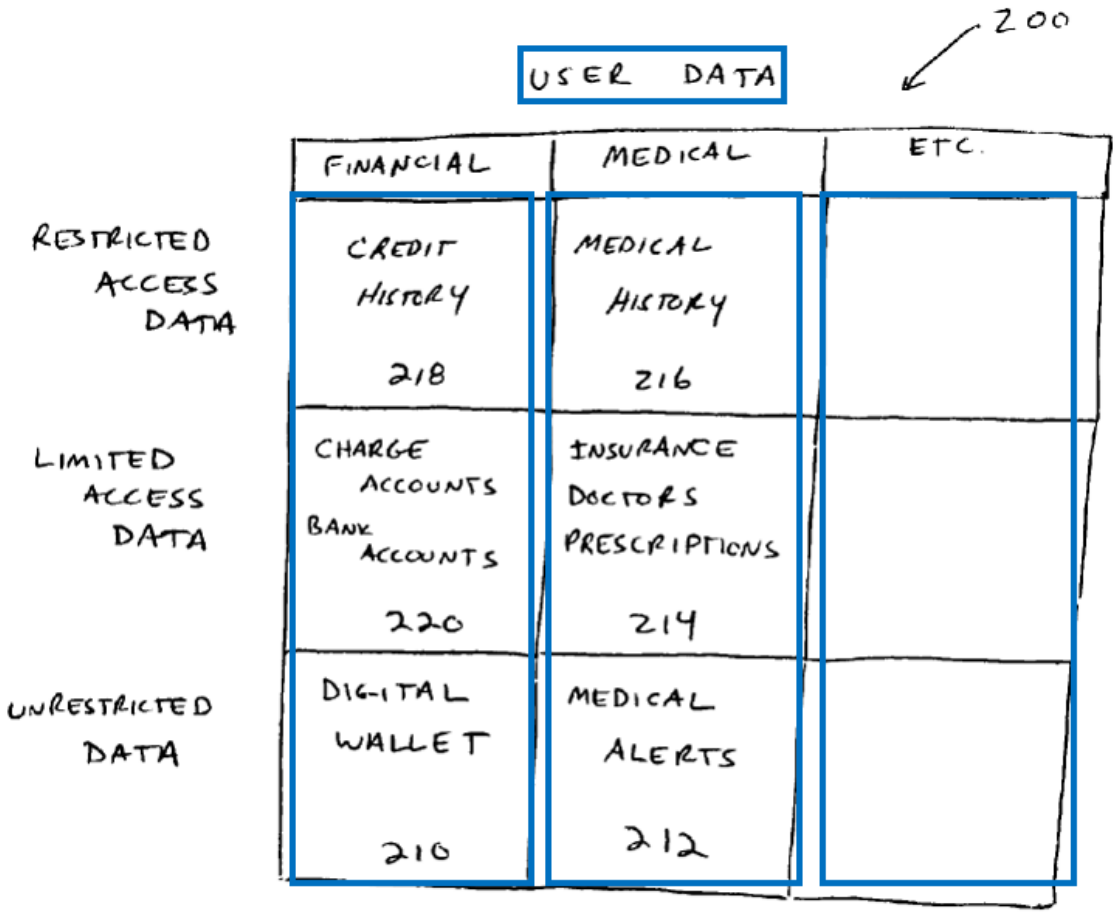


FIG. 3

EX1005, Figure 3. In addition to the types of security sensitive content explicitly disclosed in Bossemeyer, a POSITA would have also found it obvious that Bossemeyer's method secures other types of security sensitive words, characters,

data objects or icons. For example, Figure 3 of Bossemeyer includes additional columns for storing user data with a restricted- or limited-access security level. Similarly, Figure 1 of Bossemeyer shows different types of data that include security sensitive content, *e.g.*, stored as proprietary or limited access data. EX1003, ¶¶238-245.

For Ground 3, as discussed in Section VI.B.1.iii, to the extent Patent Owner argues Bossemeyer does not disclose this limitation, Merenda discloses data that has security sensitive content represented by one or more security sensitive words, characters, images or data objects. A POSITA would have recognized that Merenda's "sensitive data input" and Bossemeyer's "limited access information" and "proprietary information" all contain security sensitive content, such as credit information (EX1005, 5:21-22, Figure 3; EX1006, ¶23). As discussed in Section VI.C.6, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in combining Bossemeyer with Merenda. EX1003, ¶¶335-339.

iv. [41pre-ii] said data having one or more security sensitive words, characters or icons,

Bossemeyer renders obvious alone (or with Merenda for Ground 3) the limitation "said [] data having…one or more security sensitive words, characters,

images, data elements or data objects therein," for the reasons discussed in Section VI.C.1.iii. EX1003, ¶¶246, 345.

v. [41pre-iii] used in conjunction with a distributed computer system with a plurality of remote memories respectively designated as corresponding extract stores,

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 3) this limitation. EX1003, ¶¶247, 267.

First, Bossemeyer discloses an interconnected network of computers, *i.e.*, a distributed computer system having a plurality of computers. EX1005, 1:44-52 ("[A] network arrangement which is readily accessible from different types of smart card terminals supporting various smart card applications. ***The network connections are facilitated by the present telephone network or an interconnected network of computers such as the Internet***."), 4:11-15 ("A smart card 12 coupled with such a terminal 50 having an established connection through the network central office 16 to the central database server 10 has the power of ***a typical networked computer***."), 4:19-22 ("It is contemplated that such smart card 'docking stations' could transform hotel room entertainment centers or airplane seat video screens into ***networked computers*** with the insertion of a user's smart card."), 4:25-28 ("[T]he network arrangement of FIG. 2 is implemented over ***an interconnected network of***

computers such as the Internet 100 as well as or alternatively to the traditional telephone network 102."). EX1003, ¶¶248-58.

Second, Bossemeyer discloses that the central database server includes a plurality of memories (*i.e.*, ***extract stores***). Specifically, Bossemeyer's computer system includes a central database server with a ***memory that is broken into different partitions*** that can be located in different servers/databases, *i.e.*, ***extract stores***. EX1005, 2:13-16 ("The ***central database server 10*** includes ***partitioned memory***, described in further detail below, as well as a microprocessor for processing data received from and transmitted to the smart card terminal 14."). EX1003, ¶¶259-264.

Bossemeyer also discloses that different servers at various locations can collectively make up the central database server, and that a server in a particular location (*e.g.*, remote location) can store sensitive information:

> Although the ***central database server 10*** is shown as a single server, ***it is to be understood that multiple servers may comprise the central database server 10***. For example, in the merchant transaction discussed above, the ***purchaser's credit files*** are more likely to be stored ***in a database monitored by the credit reporting companies*** such as TransUnion or Equifax, as opposed to the central database server 10.

EX1005, 3:3-9. Bossemeyer's memories at various locations, *e.g.*, databases at the credit reporting companies, that store sensitive information also satisfy the claimed

extract stores. A POSITA would have understood that these databases are separate from one another; the '268 Patent admits that "[i]t is ***common knowledge*** that the highest security is delivered through total separation." EX1001, 10:38-39; EX1003, ¶¶265-266.

For Ground 3, to the extent Patent Owner argues that Bossemeyer does not disclose this limitation, Merenda does for the reasons discussed in Section VI.B.1.v. As discussed in Section VI.C.6, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in combining Bossemeyer with Merenda. EX1003, ¶¶341-344.

vi. [31/36pre-iii] the [method]/[programming instructions operably] deployed in a distributed computer system with a plurality of extract stores,

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 3) this limitation for the reasons discussed in Section VI.C.1.v. EX1003, ¶¶268, 345.

vii. [31/36/41pre-iv] each having a [respective] security level and clearance [therefor], comprising:

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 3) this limitation. Bossemeyer discloses partitioning sensitive data to control how the data is transferred and used. EX1005, 2:28-30 ("Private or proprietary information is partitioned such that ***the owner of the information has***

control over how the information is transferred and used.”). EX1003, ¶¶269-270, 279.

First, Bossemeyer discloses securing sensitive data by restricting access to the sensitive data, *e.g.*, limited access data or restricted access data, corresponding to ***respective security/access levels***:

> The information contained within the central database server is associated with the user identification codes on the smart cards 12 such that it can be classified as public information available to all the world; ***limited access information*** available to persons or selected groups with a user authentication code; or ***proprietary information*** accessible only by the owner of the information or a group with privileges to that directory information. Besides ***restricting others access to a smart card holder's information/data***, the information or data within the server 10 can limit options available to cardholders.

EX1005, 2:40-50; EX1003, ¶271.

Bossemeyer's memory partitions are security-controlled because they store data having respective ***levels of security/accessibility***:

> The central database server 10 is a centralized partitioned database server which ***partitions information*** both ***in terms*** of the smart card application as well as ***the accessibility of the information***. The information is stored by category (medical, financial, etc.) as well as ***level of security (unrestricted, or public limited access, restricted)***. Thus, for example, in a retail purchase application 18, a merchant may require access to a user's credit information to determine whether to

accept the user's credit for a particular dollar amount. This information may be partitioned ***in the limited access region 20*** of commercial transaction applications 18.

EX1005, 2:17-27; Figures 1, 3 (reproduced below).

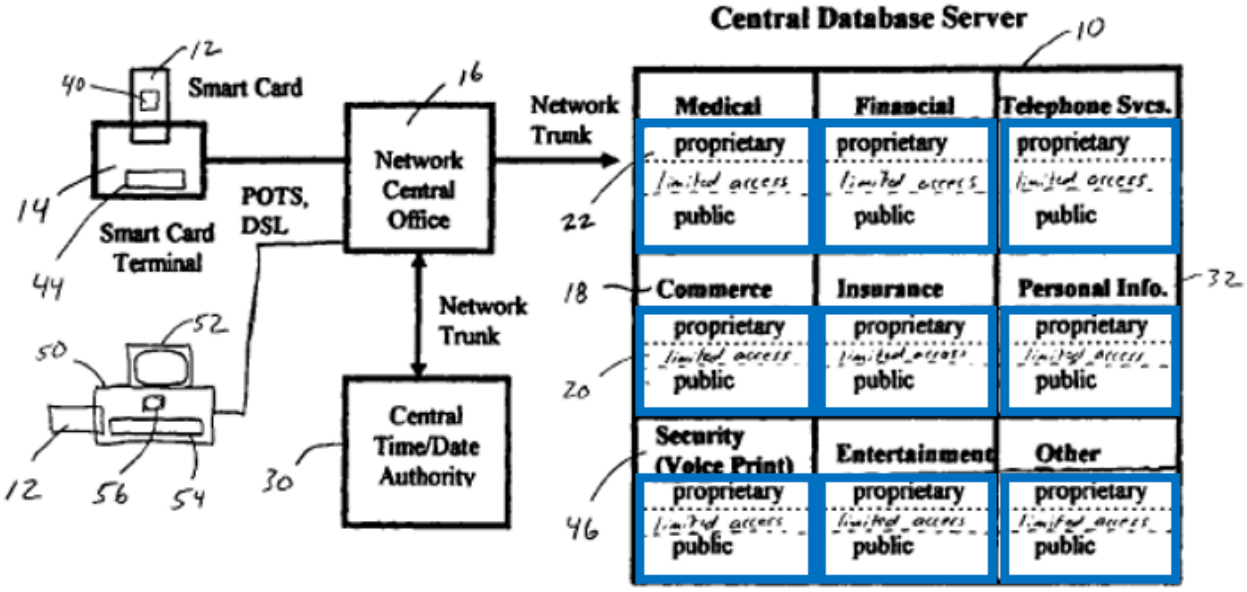


Figure 1

EX1005, Figure 1.

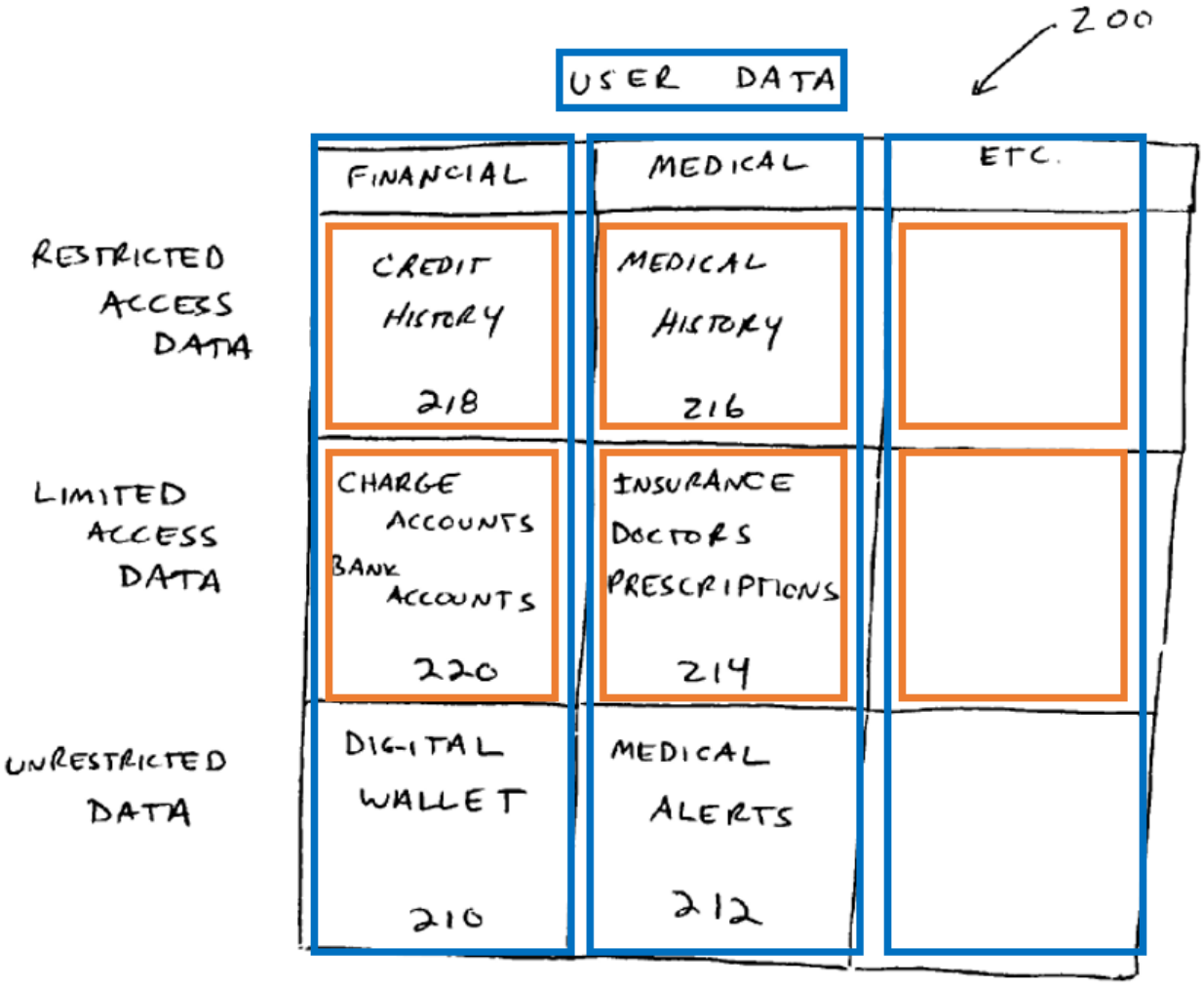


FIG. 3

EX1005, Figure 3. EX1003, ¶272.

Bossemeyer teaches controlling the access of sensitive information, *e.g.*, by allowing unrestricted or ***limited access*** or ***restricting access*** to the sensitive information. Accordingly, Bossemeyer's memory partitions have respective ***security levels***. EX1003, ¶274.

Second, in Bossemeyer, each ***security level*** has a ***respective clearance*** *e.g.*, ***user identification/authentication code*** or ***authorization/access code*** associated with a particular ***security level***. Specifically, Bossemeyer teaches that "***[d]ifferent user identification codes***, or data pointers, provided by smart cards 12 ***allow access to partitions in the database***." EX1005, 2:38-40; 3:63-4:6. Bossemeyer teaches that data with a ***limited access security level*** is "available to ***persons or selected groups with a user authentication code***" (EX1005, 2:44-45), while data with a ***proprietary information security level*** is "accessible only by the ***owner of the information or a group with privileges*** to that directory information." *Id.,* 2:45-47; 4:50-58. For example, a merchant with a corresponding merchant code can access information available to the particular merchant:

> The network server 10, 110 validates the user identification by decrypting the ***authorization code***. This information is then cross-referenced with the ***merchant code*** to identify ***the information available to the merchant***. The merchant can then view the information stored within the server 10, 110, upload/download information, and perform transactions which are recorded at the server 10, 110.

EX1005, 4:59-65; Figure 2. EX1003, ¶¶275-277.

In another example, Bossemeyer explains that a pharmacist will have ***clearance*** to access data with ***limited access security level***, *e.g.*, a user's ***insurance***

and prescription information 214, but will not have ***clearance*** to access data with ***proprietary information security level***, *e.g.*, a user's ***medical history 216***.

> [I]nformation is stored in three levels of security: unrestricted, ***limited access***, and ***restricted***. In the pharmacy example, once the user's authentication code and merchant code have been verified by the system, the pharmacist may have ***access*** to the user's digital wallet 210, medical alerts 212, and ***insurance and prescription information 214***. Without further authorization, however, the pharmacy would not have access to the user's ***medical history 216***.

EX1005, 5:8-15.

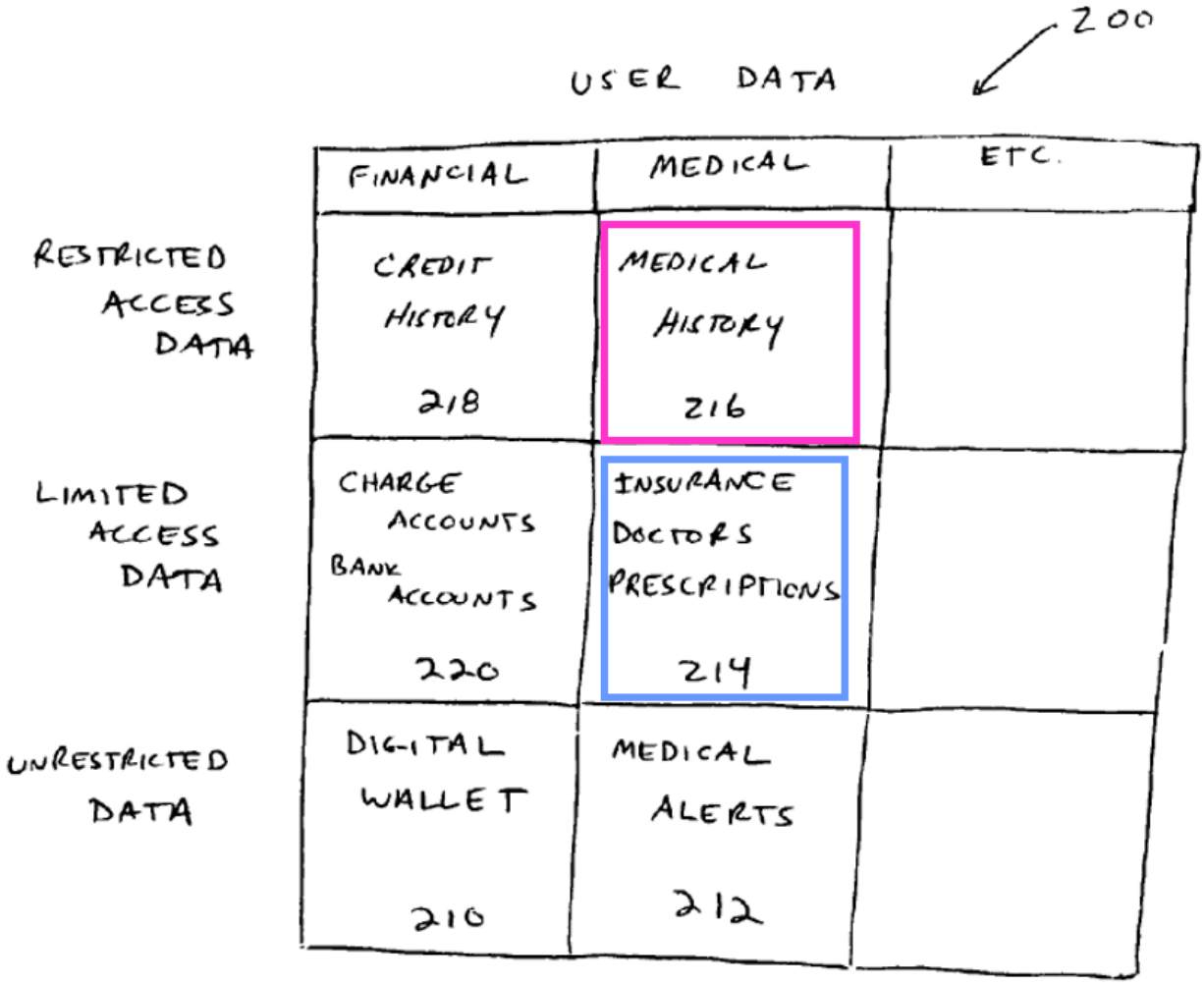


FIG. 3

EX1005, Figure 3. EX1003, ¶278.

For Ground 3, to the extent Patent Owner argues that Bossemeyer does not disclose this limitation, Merenda does for the reasons discussed in Section VI.B.1.vii. As discussed in Section VI.C.6, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable

expectation of success in combining Bossemeyer with Merenda. EX1003, ¶¶346-349.

2. [31/36/41a] extracting said security sensitive [content / words, characters or icons] from said [input] data to obtain extracted data for respective security levels [and remainder data therefrom];

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 3) this limitation. EX1003, ¶¶280, 291.

Bossemeyer discloses partitioning or separating (*e.g.*, extracting), ***data*** in terms of the ***data's level of security/accessibility***:

> The central database server 10 is a centralized partitioned database server which ***partitions information*** both ***in terms of*** the smart card application as well as ***the accessibility of the information***. The ***information*** is stored by category (medical, financial, etc.) as well as ***level of security (unrestricted, or public limited access, restricted)***… [A] merchant may require access to a user's credit information…This ***information*** may be partitioned in the limited access region 20 of commercial transaction applications 18."

EX1005, 2:17-27. EX1003, ¶281.

Specifically, Bossemeyer partitions or separates (*e.g.*, extracts), ***user data*** into subsets of ***extracted data***, *e.g.*, ***limited access information*** and/or ***proprietary information***, and ***remainder data***, *e.g.*, ***public information***:

> The ***information*** contained within the central database server…can be classified as ***public information*** available to all the world; ***limited***

> ***access information*** available to persons or selected groups with a user authentication code; or ***proprietary information*** accessible only by the owner of the information or a group with privileges to that directory information.

EX1005, 2:40-47. As discussed in Section VI.B.1.i.e, ***limited access information*** and/or ***proprietary information*** includes security sensitive content, such as, words, characters, data objects or icons. For example, Figure 1 of Bossemeyer shows ***medical information*** 22 stored in central database 10 as proprietary information.

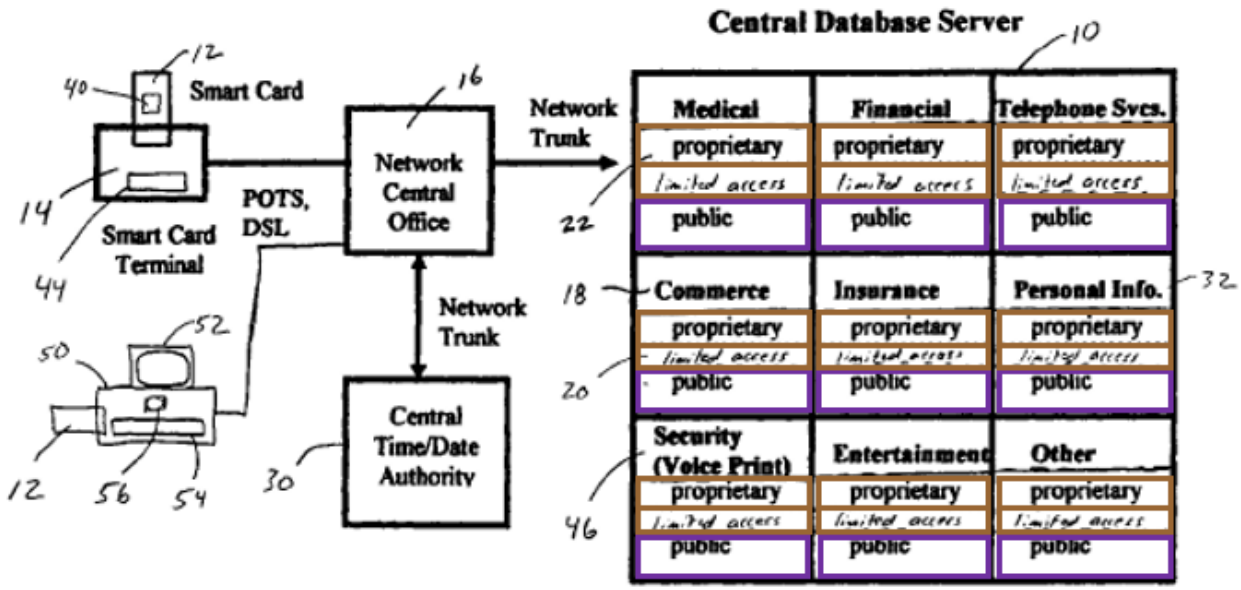


Figure 1

EX1005, Figure 1, 2:28-33 ("Private or proprietary information is partitioned such that the owner of the information has control over how the information is transferred and used. Thus, for example, ***medical information*** 22 provided to a health

professional may be considered private and only available by way of special authorization from the owner of the information."). EX1003, ¶¶282-283.

Figure 3 of Bossemeyer provides another example of partitioning ***user data*** into ***extracted data*** and ***remainder data***.

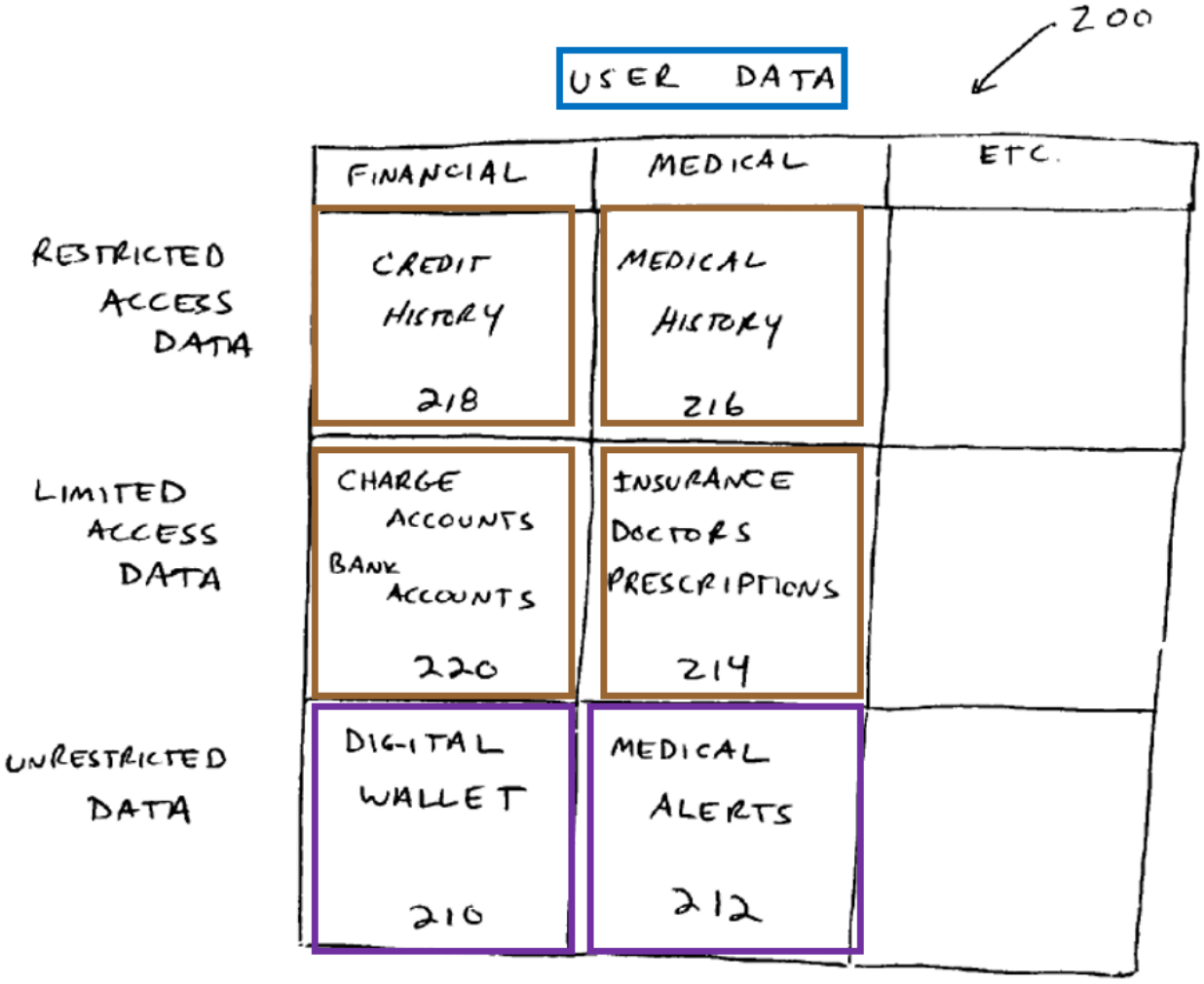


FIG. 3

EX1005, Figure 3, 5:9-22 ("In the pharmacy example, once the user's authentication code and merchant code have been verified by the system, the pharmacist may have

access to the ***user's digital wallet 210***, ***medical alerts 212***, and ***insurance and prescription information 214***. Without further authorization, however, the pharmacy would not have access to the user's ***medical history 216***."). EX1003, ¶¶284-287.

To the extent Patent Owner argues that Bossemeyer does not explicitly disclose "extracting data," a POSITA would have understood that when Bossemeyer's "central database server partitions [user] information…in terms of… the accessibility of the information" (EX1005, 2:17-20), Bossemeyer's method would filter and extract the secure sensitive information, (*e.g.*, restricted- and/or limited-data), from the received user data, (*e.g.*, from a user data file), to store the restricted- and/or limited-data in the appropriate security-level store, while storing the remaining information in the user data file as unrestricted data, (*e.g.*, public data). For example, a POSITA would have understood that Bossemeyer's method parses received information into private and non-private elements. *See e.g.,* EX1006, ¶7. ("[A] set of data may be parsed into private and non-private elements."). EX1003, ¶¶288-289.

For example, when Bossemeyer's central database server receives a ***user's medical data file***, as shown in Bossemeyer's Figure 3 below, Bossemeyer's method extracts the ***user's medical history information 216***, and ***insurance, doctors, prescriptions information 214***, and stores them into respective extract stores

corresponding to the appropriate ***respective security level***. For example, a POSITA would have understood that medical history information can include images of medical charts, insurance information can include icons of the user's insurance card, prescription information can include the names of the drugs prescribed to the user, etc.

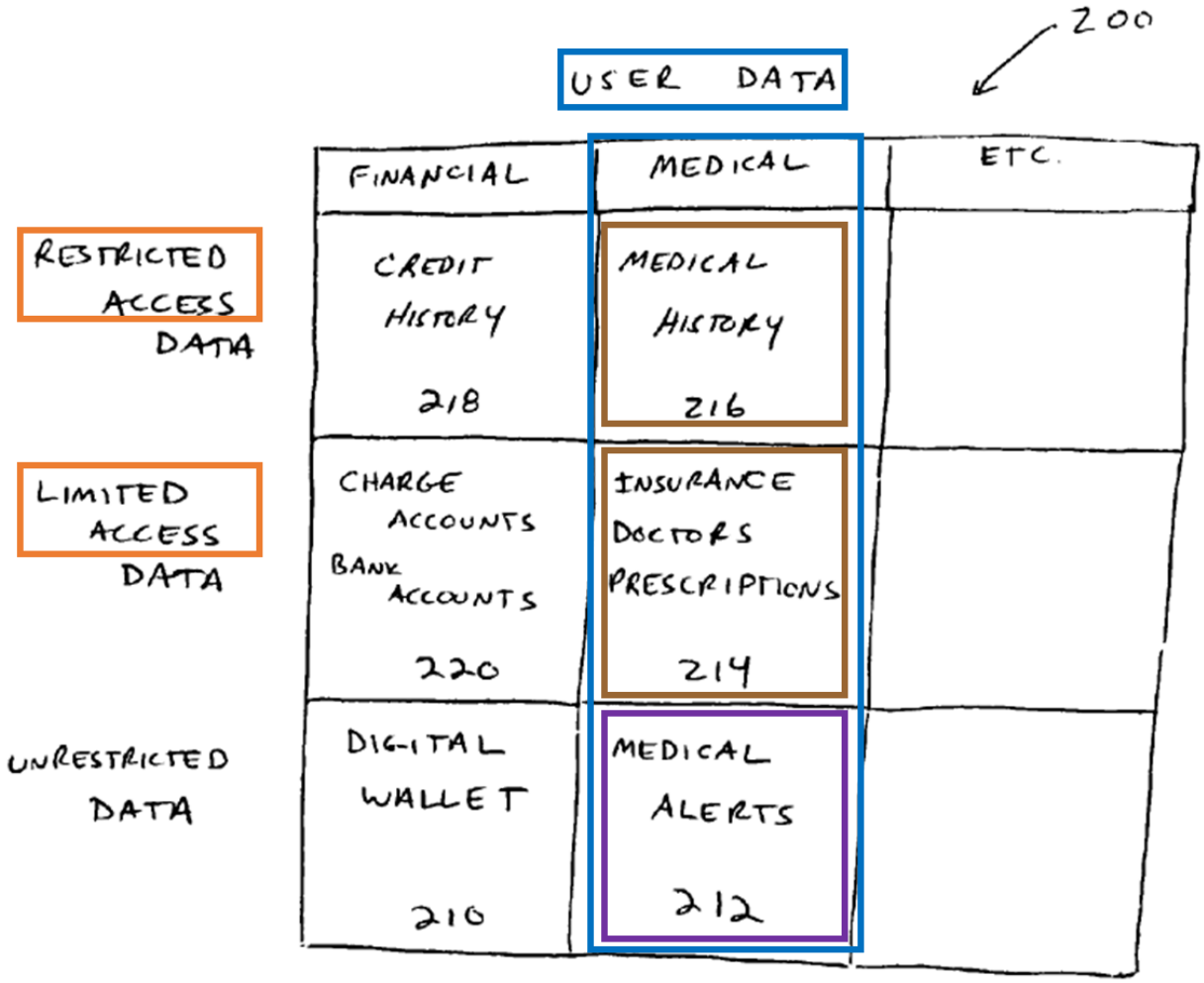


FIG. 3

EX1005, Figure 3. EX1003, ¶290.

For Ground 3, to the extent Patent Owner argues Bossemeyer does not disclose this limitation, Merenda discloses extracting, *e.g.*, parsing, security sensitive content, *e.g.*, ***private elements***, from ***user data*** to obtain subsets of ***extracted data***, e.g., ***address***, ***credit card*** or ***social security number*** and ***remainder data***, *e.g.*, ***non-private elements***. *See* Section VI.B.2. As discussed in Section VI.C.6, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in combining Bossemeyer with Merenda. EX1003, ¶¶350-353.

3. [31/36/41b] facilitating the storage of said extracted data in respective ones of said extract stores; and

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 3) this limitation. EX1003, ¶¶292, 297.

Bossemeyer discloses extracting security sensitive content from user data to obtain ***restricted access*** data (***credit history 218*** and ***medical history 216***) and ***limited access*** data (***charge/bank accounts 220*** and ***insurance, doctors, prescriptions 214***). As also discussed, Bossemeyer also discloses facilitating the storage of (storing) ***extracted data***, *e.g.*, ***restricted access data*** and ***limited access data*** in ***respective extract stores***. This is illustrated in Figure 3 below.

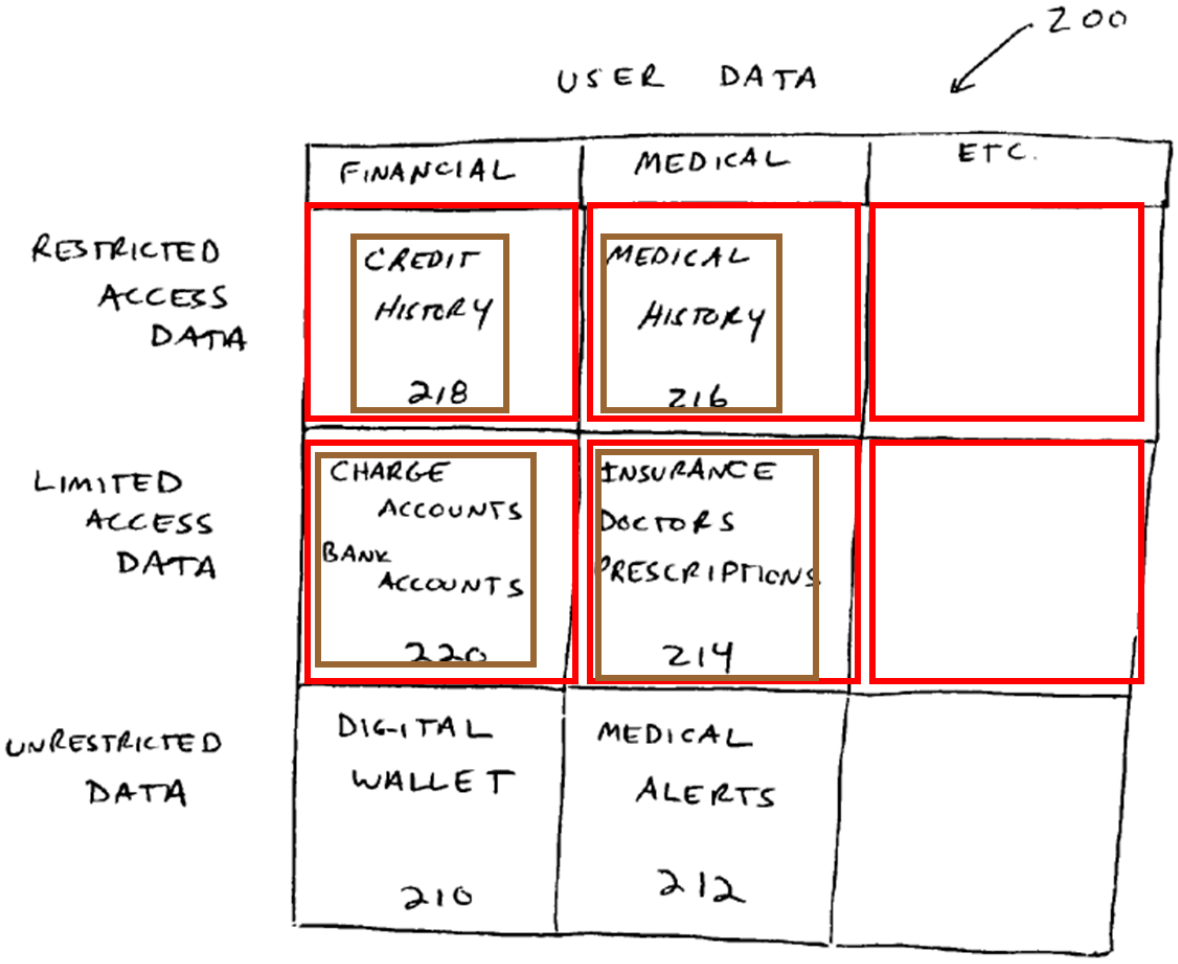


FIG. 3

EX1005, Figure 3; Figure 1. EX1003, ¶¶293-296. *see also* Section VI.C.1.v.

For Ground 3, to the extent Patent Owner argues that Bossemeyer does not disclose this limitation, Merenda does for the reasons discussed in Section VI.B.3. As discussed in Section VI.C.6, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in combining Bossemeyer with Merenda. EX1003, ¶¶354-357.

4. [31/36/41c] forwarding [any / said] remainder [input] data to a target[ed] destination in said distributed computer system

Bossemeyer discloses and/or renders obvious (or with Merenda for Ground 3) this limitation. Bossemeyer discloses storing ***public data*** (*e.g.*, ***remainder data***) in respective ***public information storage*** (*e.g.*, ***target destination***). EX1005, 2:17-22 ("The central database server 10 is a centralized partitioned database server which partitions information both in terms of the smart card application as well as the accessibility of the information. The information is stored by … level of security (***unrestricted***, or public limited access, restricted)."), 2:40-47 ("The information contained within the central database server is associated with the user identification codes on the smart cards 12 such that it can be classified as ***public information*** available to all the world; limited access information … or proprietary information…."), Figures 1, 3.

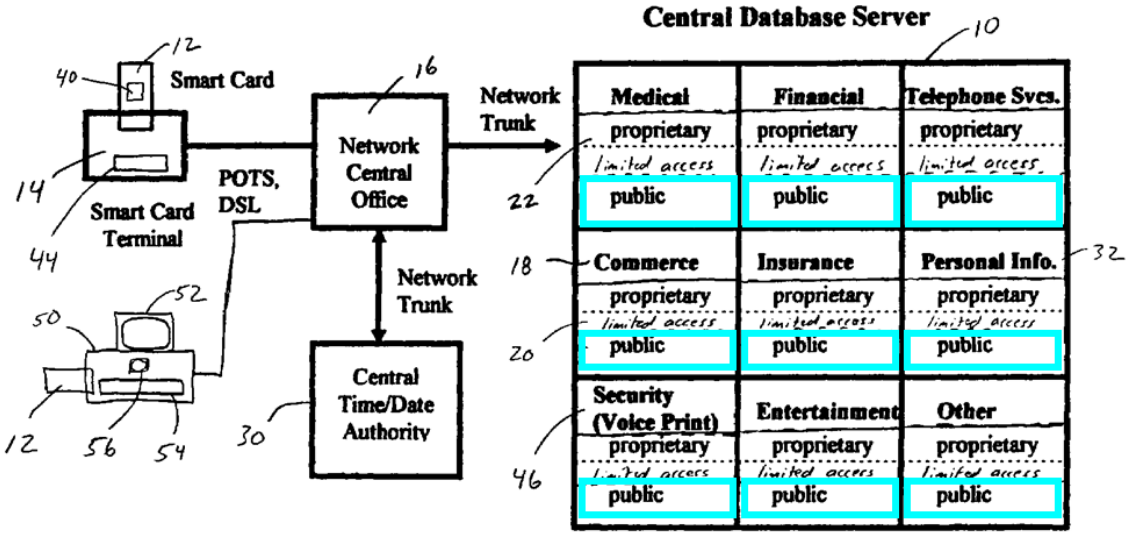


Figure 1

EX1005, Figure 1.

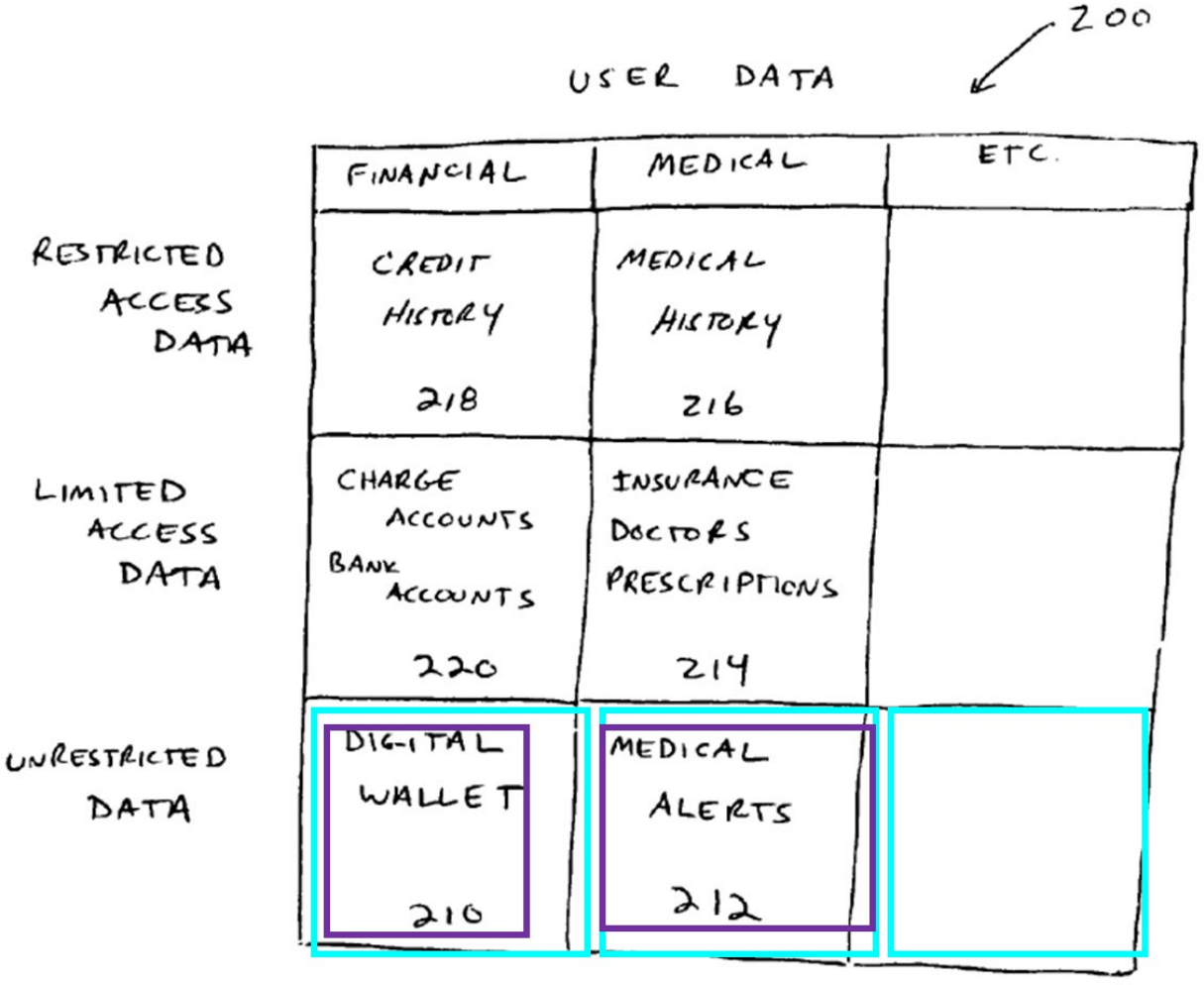


FIG. 3

EX1005, Figure 3. EX1003, ¶¶298-303.

For Ground 3, to the extent Patent Owner argues that Bossemeyer does not disclose this limitation, Merenda does for the reasons discussed in Section VI.B.4. As discussed in Section VI.C.6, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in combining Bossemeyer with Merenda. EX1003, ¶¶358-361.

5. [31/36/41d] and requiring [a respective] predetermined security clearance[s] [for / to] access [to / said corresponding] extract stores.

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 3) this limitation. As discussed in Sections VI.C.1.v and VI.C.1.vii, Bossemeyer discloses and/or renders obvious limited access and proprietary information and the ***extract stores*** storing them and allowing access to the limited access and proprietary information based on respective ***clearances***. EX1003, ¶¶304-305, 320.

Specifically, Bossemeyer discloses allowing access to the partitioned data, only in the presence of a ***predetermined security clearance***, *e.g.*, ***user identification/authentication code*** or ***authorization/access code*** associated with a particular security level:

> ***Different user identification codes***, or data pointers, provided by smart cards 12 ***allow access to partitions in the database***. The information contained within the central database server is associated with the ***user identification codes*** on the smart cards 12 such that it can be classified as public information available to all the world; ***limited access*** information available to ***persons or selected groups with a user authentication code***; or ***proprietary information*** accessible only by the ***owner of the information or a group with privileges to that directory information***.

EX1005, 2:38-47. EX1003, ¶¶306-308.

Specifically, Bossemeyer discloses that partitioned data is accessed from the ***extract stores*** of the central database server 10, and is presented, *e.g.*, at a terminal, based on a particular ***user's authorization***:

> Once the ***user's authorization*** has been verified, data pointers on the smart card 12 provide access to the relevant partitioned memory portions of the central database server 10. Routing circuitry controlled by the microprocessor within the central database server 10 routes the data pointer to appropriate memory locations or database of the information keeper relating to the application at issue such as medical, financial, etc. ***Data from these various locations is supplied back to the smart card terminal 14, and if appropriate, the data stored on the smart card 12 is updated***.

EX1005, 3:63-4:6.

> Preferably, the smart card provides a one-time encrypted ***user authentication code based on the user's digital signature or certificate***. This code, in turn, is transmitted over the communication network 100, 102 along with the merchant identification code to the server 10, 110. Thus, the digital signature of the card does not change, but an ***authorization code*** generated by an encryption scheme known to the server provides a unique ***access code*** each time the card is involved in a transaction with the network.
>
> The network server 10, 110 ***validates the user identification*** by decrypting the ***authorization code***. This information is then cross-referenced with the merchant code ***to identify the information available to the merchant***. ***The merchant can then view the***

> ***information*** stored within the server 10, 110, upload/download information, and perform transactions which are recorded at the server 10, 110.

EX1005, 4:50-65. EX1003, ¶¶309-310.

Bossemeyer's ***user identification codes*** correspond to respective ***security levels***, which as discussed in Sections VI.B.1.i.c, VI.B.1.i.d, VI.B.1.iii, and VI.B.1.iv, correspond to respective ***extract stores***. For example, Bossemeyer discloses accessing a user's medical data by permitting partial reconstruction (*e.g.*, reconstruction of some) or full reconstruction (*e.g.*, reconstruction of all) of the user's medical data based on the ***security level*** of the ***user identification codes***. Specifically, Bossemeyer discloses using the ***user authentication code*** to access a user's medical data with "***unrestricted***" and "***limited access***" security level (*e.g.*, the user's ***medical alerts 212*** and ***insurance and prescription information 214***) but requiring ***further authorization*** to access the user's medical data with "restricted access" security level (*e.g.*, the user's ***medical history 216***):

> FIG. 3 provides one example of the type of information accessible within or through the server 200. As mentioned above, information is stored in three levels of security: unrestricted, limited access, and restricted. In the pharmacy example, once the ***user's authentication code*** and merchant code have been verified by the system, the pharmacist may have access to the user's digital wallet 210, ***medical alerts 212***, and ***insurance and prescription information 214***. Without

further authorization, however, the pharmacy would not have access to the user's ***medical history 216***.

EX1005, 5:6-15.

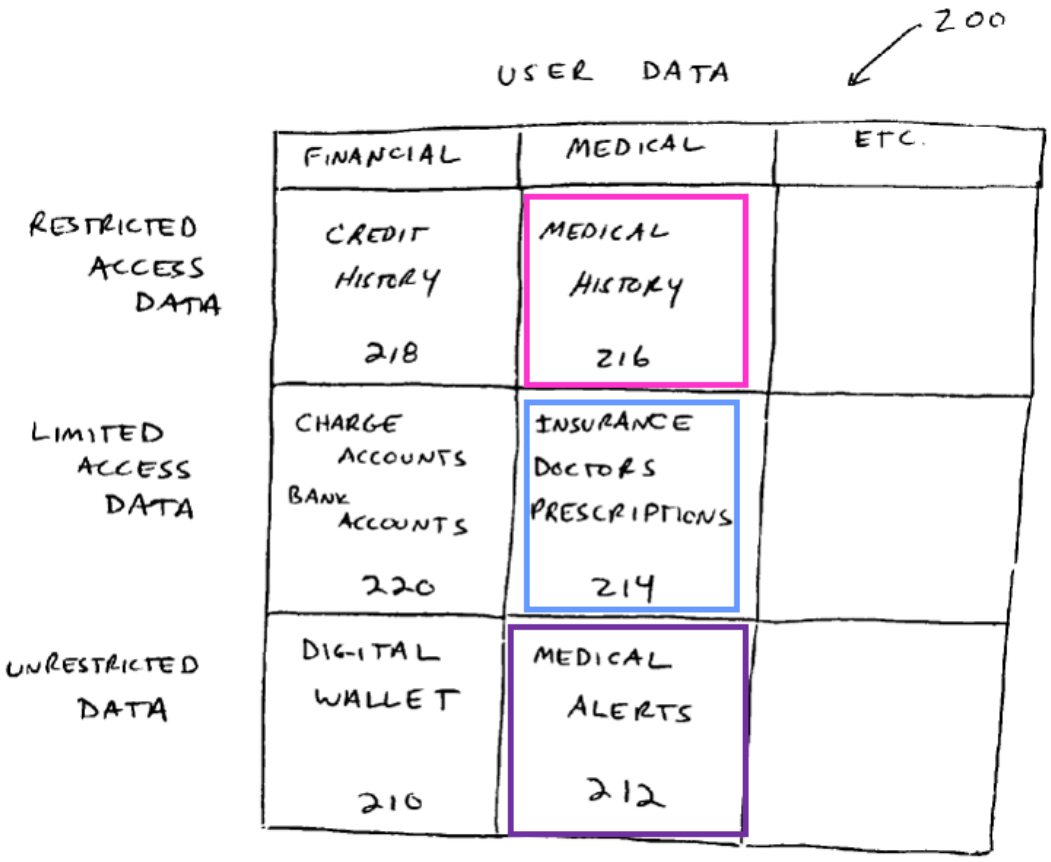


FIG. 3

EX1005, Figure 3. EX1003, ¶¶311-312, 314-319.

A POSITA would have understood that "***further authorization***" would be in the form of a different ***user authorization code*** that allows access to the "restricted access" data. EX1005, 2:38-40 ("***Different*** ***user identification codes***, or data

pointers, provided by smart cards 12 ***allow access to partitions in the database***."). EX1003, ¶¶313.

For Ground 3, to the extent Patent Owner argues that Bossemeyer does not disclose this limitation, Merenda does for the reasons discussed in Section VI.B.5. As discussed in Section VI.C.6, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in combining Bossemeyer with Merenda. For example, a POSITA would have been motivated to use Merenda's key identifier with Bossemeyer's partitioned databases. EX1003, ¶¶362-366.

6. Reasons to Combine Bossemeyer with Merenda

A POSITA would have been motivated to combine Bossemeyer and Merenda to parse user data that includes private and non-private elements, as taught by Merenda, in Bossemeyer's system to extract the private elements and subsequently store them separately from the non-private elements, for several reasons. EX1003, ¶367.

First, the combination of Bossemeyer and Merenda represents the use of known techniques according to known methods in the same way to yield predictable results. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). Bossemeyer and Merenda relate to the same field of providing different users access to information and address the same problem of controlling access to information. The Bossemeyer

and Merenda combination would merely involve using Merenda's data parsing technique in Bossemeyer's system according to the methods for separating private and non-private elements within user data. EX1005, 2:17-20 ("The central database server 10 is a centralized partitioned database server which partitions information both in terms of the smart card application as well as the accessibility of the information."), 1:49-52 ("With a centralized server architecture, data related to an individual can be accessed by an individual smart card, predefined groups of smart card users, or the general public."), 2:28-30 ("Private or proprietary information is partitioned such that the owner of the information has control over how the information is transferred and used."), 2:38-40 ("Different user identification codes, or data pointers, provided by smart cards 12 allow access to partitions in the database."); EX1006, ¶25 ("As a result of the distribution of data elements among various public and private data sets, it is desirable to establish a level of control over access to the public and private data stored therein… The present invention is directed toward providing the level of control 108 required in keeping the public and private data separate, and allowing access to the private data either at the explicit direction of the consumer 109 (the individual that is the subject of the public and private data) or in such a manner as to protect the privacy concerns of the consumer."), ¶26 ("The public data set does not impose any access restrictions to its viewing audience 206. Other items of information, [may be] designated as… private

data elements 207 and as such will be stored separately in a private data set 208 which imposes certain restrictions on access by the viewing audience 206."); *see also,* EX1005, 2:40-55, 4:50-65, 5:6-31; EX1006, ¶¶10-13, 23, 29, 34-35. EX1003, ¶¶368-372.

Second, a POSITA would have been motivated to combine Bossemeyer with Merenda, because Merenda identifies a known problem (e.g., controlling access to private information) and provides a solution to address the problem (e.g., parsing user data to extract the private elements and store private elements and non-private elements in separate memory stores). "Nothing more is required to show a motivation to combine under *KSR*…." *See Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373, 1381 (Fed. Cir. 2023) (holding that it was "enough for [Petitioner] to show that there was a known problem" in the art and that the referenced prior art helped address that issue). Merenda's use of parsing data to extract private elements and store the private elements separately from non-private elements, thereby controlling access to sensitive/proprietary information is a "universal motivation" known in the field of providing users with access to information and improves the technology, by ensuring that access to the sensitive/proprietary information is only limited to specific users (*e.g.*, merchants that have been granted access to the information). "'Universal' motivations known in a particular field to improve technology provide 'a motivation to combine prior art references even absent any

hint of suggestion in the references themselves.'" *Intel Corp.,* 61 F.4th at 1380. EX1003, ¶¶373-376.

Third, a POSITA would have been motivated to use Merenda's parsing technique to identify private elements within user data, because it would improve Bossemeyer's system for controlling access to sensitive/proprietary information. Bossemeyer's system would improve by using Merenda's technique because it would enable separation of private elements and non-private elements where "such separation [can occur] at ***various levels of sophistication and granularity***…" EX1006, ¶23. That is, the combination would merely be a use of a known technique (*e.g.*, parsing user data) to improve similar methods (*e.g.*, controlling access to information) in the same way (*e.g.*, by allowing access to information at the appropriate granularity level). *KSR*, 550 U.S. at 417. As discussed in Section VI.B.1.ii, Bossemeyer discloses extracting security sensitive content in terms of the data's level of security or accessibility. Adding Merenda's teachings of parsing user data to identify various private elements would be an improvement to the security and access control afforded to users of Bossemeyer's system, because it would allow the separation of the private elements "at various levels of sophistication and granularity…" (EX1006, ¶23) and therefore could allow a greater number of security levels to correspond to the different private elements. For example, implementing Merenda's technique in Bossemeyer's system could allow access to groups of users

(*e.g.*, merchants) that, otherwise, would not have access to portions of the user data. EX1003, ¶¶377-379.

Fourth, a POSITA would have been motivated to combine Bossemeyer with Merenda, because the combination would involve applying a known technique (e.g., using Merenda's parsing of user information) to a known device (e.g., Bossemeyer's network arrangement with a central database server storing user information), which was ready for improvement to yield predictable results. *KSR*, 550 U.S. at 401. EX1003, ¶¶380-382.

Fifth, Merenda provides express motivations that would have led a POSITA to combine Merenda's and Bossemeyer's teachings. Indeed, Merenda acknowledges that "[t]he incredible growth of the Internet has provided ready access to a wealth of information. The World Wide Web is an ever-expanding repository of information spanning any and all conceivable topics limited only by the imagination of the information content provider." EX1006, ¶3. However, Merenda recognizes that "[t]he overwhelming benefits attendant to this ubiquity, however, are counterbalanced to some extent by the inevitable loss of privacy associated with accessing a global computer network." *Id.* Merenda also discloses that "[a]s the Internet evolves into the dominant commercial medium, merchants seeking to leverage data about Internet user's [sic] to better focus their marketing efforts must

do so in a manner that respects the privacy interests of their intended customer." *Id.,* ¶4. EX1003, ¶¶383-385.

Merenda provides examples of the benefits of its methods for respecting the privacy interests of the public. In one example, Merenda teaches that user private information will be available to merchants only if the user indicates that a particular merchant can access their private information:

> In an embodiment of the invention, data entered by a consumer into a Web form is separated into related records in a public and private data set. The public records would be available without restriction for read access by a population of merchants. ***The private records would be available only per the indication of the consumer to the merchant in the population***.

EX1006, ¶7; ¶8 ("Upon entering the data the consumer may be prompted to indicate whether they wish to provide merchants with access to their private data."). In fact, Merenda's method allows consumers to allow access to private data only to selected merchants among the available merchants. EX1006, ¶8 ("The consumer may be offered and [sic] opportunity to choose among the population of merchant the select merchant to whom they wish their private data to be provided.") Merenda's disclosed method also allows merchants to data mine or statistically process the customer's private information. *Id.,* ¶12 ("In an exemplary embodiment the merchants … are provided with the ability to data mine or statistically process the

whole of the private data set while being restricted from reading any of the individual data records therein."), ¶5 ("[T]he system should provide access to the private database for performing data mining operations or other types of analysis which do not expose the individual records therein and accordingly raise no privacy concerns."). EX1003, ¶¶386-388.

A POSITA would have found that Merenda and Bossemeyer were analogous to the '268 Patent. All three pertain to the same field of endeavor, *i.e.*, securing security-sensitive information. *Compare* EX1001, 1:19-20 ("The present invention relates to a data security system and method.") *with and* EX1005, 1:8-11 ("This invention relates to smart card applications and, more particularly, to a network arrangement to provide access to an architecture that supports a variety of advanced smart card applications."), 1:44-47 ("[T]he present invention describes a network arrangement which is readily accessible from different types of smart card terminals supporting various smart card applications."), *and* EX1006, ¶2 ("The present invention in relates in general to the field of data processing, and in particular to a method, system and program product for allowing the viewer of a public data set to access related records in a private data set based upon a link which may be selectively provided to the viewer to authorize such access."). EX1003, ¶389.

To the extent that Patent Owner argues that the references are not in the same field of endeavor as the '268 Patent, Merenda and Bossemeyer are still reasonably

pertinent to the particular problem with which the '268 Patent's invention is involved, *i.e.*, securing digital information. *Compare* EX1001, 6:26-29 ("It is an object of the present invention to provide a data security system, an information processing system and a method for securely storing data and rebuilding that data in the presence of an adequate security clearance."), 6:65-67 ("It is an object of the present invention to parse, disperse and reconstruct the data or data object thereby enabling secure storage of the data."), 7:9-11 ("It is a further object of the present invention to secure e-mail data transmissions and web browser transmissions by extraction of security sensitive data."), *with* EX1005, 2:17-22 ("The central database server 10 is a centralized partitioned database server which partitions information both in terms of the smart card application as well as the accessibility of the information. The information is stored by category (medical, financial, etc.) as well as level of security (unrestricted, or public limited access, restricted)."), *and* EX1006, ¶23 ("Fundamental to the implementation of the present invention is the notion that a set of data may be parsed into private and non-private elements."), ¶37 ("The separation of data into public and private data sets creates a volume of public data which is generally usable by the viewing public 206. This data has value by itself for marketing purposes, as it can be used for data mining to spot trends, in IT purchasing etc."), ¶23 ("At the most simplistic level [parsing data into private and non-private elements] might entail, for example, identifying input fields on a Web

page as requiring sensitive data input… versus non-sensitive information."). EX1003, ¶390.

A POSITA would also have had a reasonable expectation of success in combining Merenda with Bossemeyer. Combining Merenda with Bossemeyer would merely involve including parsing user data according to Merenda's method in Bossemeyer's system and storing private elements within the user data according to their respective security level in Bossemeyer's various extract stores. In fact, Merenda provides different ways for doing so, all of which are within the reach of a POSITA:

> [A] set of data may be parsed into private and non-private elements. At the most simplistic level this might entail, for example, ***identifying input fields on a Web page*** as requiring sensitive data input such as an address, credit card or social security number, versus non-sensitive information such as the name of the item being purchased, the date, time etc. At a more sophisticated level this notion might entail ***the combination of otherwise non-sensitive data elements into a combined sensitive data construct***. For example, information such as the state and town in which a person resides may be itself be deemed not sensitive but when combined with the person's occupation and alma mater, it may become a simple task to narrow the field down to a single person, and as such the combination of that data may be deemed sensitive. For purposes of the present invention the mechanics by which the various data elements are parsed into sensitive and public

> data sets is not critical, however the notion that such separation, at various levels of sophistication and granularity can, and does occur, is essential to the practice of the invention.

EX1006, ¶23. EX1003, ¶¶391-393.

VII. Discretionary Denial Would Be Inappropriate

A. Discretionary Denial Under The *Fintiv* Factors Is Not Appropriate

The six factors considered for §314 denial strongly favor institution. *See Apple Inc. v. Fintiv, Inc*., IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential).

1. No evidence regarding a stay

No motion to stay has been filed, so this factor is neutral. *Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24, 7 (PTAB June 16, 2020) (informative); *see also Dish Network L.L.C. v. Broadband iTV, Inc.*, IPR2020-01359, Paper 15 (Feb. 12, 2021) ("It would be improper to speculate, at this stage, what the Texas court might do regarding a motion to stay…").

2. Parallel proceeding trial date

This factor is neutral. The Board's Final Written Decision is expected in December 2024/January 2025.[1] Although trial is currently scheduled for August 19, 2024 (EX1008), the Board recognizes "that scheduled trial dates are unreliable and often change." *See* Director's Memorandum on Discretionary Denials ("EX1015"), 8. Accordingly, the Board now uses median time-to-trial statistics in the relevant venue to determine a projected trial date for *Fintiv* purposes: "The PTAB will weigh [factor 2] against exercising discretion to deny institution under *Fintiv* if the median time-to-trial is around the same time or after the projected statutory deadline for the PTAB's final written decision." EX1015, 9.

The co-pending district court case was filed in EDTX on November 28, 2022. The statistics for the two most recent periods show a median time-to-trial in EDTX between 19 months (March 2023) and 24.2 months (March 2022). EX1009, 1. Accordingly, the projected trial date for purposes of *Fintiv* is between June 2024 (which is unlikely since June 2024 is before the scheduled trial date of August 2024) and December 2024—approximately 24.2 months after November 28, 2022—and around the Board's Final Written Decision, which is expected late December

[1] December 2024/January 2025 is 18 months after June/July 2023, when Petitioner expects a notice of accorded filing date.

2024/January 2025. Because the projected trial date based on the two most recent statistics is either before or "around the same time or after" the Board's expected final written decision, and because the median-time-to-trial statistics can fluctuate by months for consecutive periods, this factor is neutral.

3. Investment in the parallel proceeding

The co-pending litigation is in its very early stages with minimal investment. *See* EX1007, EX1010. The parties have not exchanged preliminary positions on claim construction, and expert discovery has not begun. *See PEAG LLC v. Varta Microbattery GmbH*, IPR2020-01214, Paper 8, 17 (Jan. 6, 2021) Further, the Markman hearing is not scheduled until March of 2024. EX1007, 4.

Moreover, Patent Owner served their infringement contentions on Petitioner and confirmed which claims were being asserted only on February 28, 2023. EX1010. Under *Fintiv*, Petitioner's prompt filing "weigh[s] against exercising the authority to deny institution." *Fintiv*, Paper 11, 11 ("If the evidence shows that the petitioner filed the petition expeditiously, such as promptly after becoming aware of the claims being asserted, this fact has weighed against exercising the authority to deny institution under NHK"). This factor favors institution.

4. Overlapping issues with the parallel proceeding

Petitioner stipulates that if the IPR is instituted, Petitioner will not pursue the same grounds in the district court litigation. *Sand Revolution II LLC v. Continental*

Intermodal Group – Trucking LLC, IPR2019-01393, Paper 24, 7 (June 16, 2020) (informative).

5. Identity of parties

Petitioner is a defendant in the litigation. That is true of most Petitioners in IPR proceedings. Accordingly, this factor should not be a basis for denying institution.

6. Other circumstances

The prior art presented in this Petition renders the Challenged Claim unpatentable as obvious. "[T]he PTAB will not deny institution of an IPR or PGR under *Fintiv* (i) when a petition presents compelling evidence of unpatentability." EX1015, 2. "Compelling, meritorious challenges are those in which the evidence, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence." EX1015, 4. Here, the Petition plainly shows that the '268 Patent claims no more than the known concept of storing sensitive data in security-controlled memories. The evidence of unpatentability is compelling, and thus the PTAB should not deny institution under *Fintiv*.

As such, because the *Fintiv* factors are either neutral or weigh against discretionary denial, and institution should not be denied on discretionary factors.

B. Discretionary Denial Under 35 U.S.C. § 325(d) Is Not Appropriate

Discretionary denial under § 325(d) is not warranted because the challenges presented in this petition are neither cumulative nor redundant to the prosecution of the ’268 patent. The PTO has not previously considered Bossemeyer or Merenda in connection with the claims of the ’268 Patent. Further, the combination is not redundant to any combination of references considered during prosecution. Additionally, Dr. Zadok is an expert in the relevant art, and his analysis of the prior art has not been presented to the PTO. EX1003, ¶¶46-394, 115. In view of the new information presented in this Petition, the Board has ample discretion to institute an IPR on the grounds presented.

VIII. Conclusion

Accordingly, Petitioner has established a reasonable likelihood that the Challenged Claims are unpatentable.

Dated: June 26, 2023

Respectfully submitted,

/Theodoros Konstantakopoulos/
Theodoros Konstantakopoulos
(Reg. No. 74,155)
tkonstantakopoulos@desmaraisllp.com
DESMARAIS LLP
230 Park Ave
New York, NY 10169
212-808-1060 (telephone)
212-351-3401 (facsimile)

Counsel for Petitioner

IX. Mandatory Notices

A. Real Party-in-Interest

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner certifies that the real party-in-interest is International Business Machines Corporation.

B. Related Matters

Pursuant to 37 C.F.R. § 42.8(b)(2), to the best knowledge of the Petitioner, the '268 patent is or was involved in the following case:

Case Heading	Number	Court	Date
DigitalDoors, Inc.[2] *v. International Business Machines Corporation*	2:22-cv-457	EDTX	Nov. 29, 2022

C. Lead and Back-up Counsel and Service Information

Lead Counsel
Theodoros Konstantakopoulos
Desmarais LLP
230 Park Ave
New York, NY 10023

Phone: (212) 351-3400
tkonstantakopoulos@desmaraisllp.com
USPTO Reg. No. 74,155

Back-up Counsel
Brian D. Matty

Phone: (212) 351-3400

[2] The '268 Patent cover page (EX1001, 1) and the USPTO assignment database (https://assignment.uspto.gov/patent/index.html#/patent/search/resultAbstract?id=7958268&type=patNum) identify "Digital Doors, Inc." as the assignee of the '268 Patent.

Desmarais LLP
230 Park Ave
New York, NY 10023

bmatty@desmaraisllp.com
USPTO Reg. No. 70,358

Emily Weber
Desmarais LLP
101 California Street
San Francisco, CA 94111

Phone: (415) 573-1858
eweber@desmaraisllp.com
USPTO Reg. No. 79,973

Please address all correspondence to lead and back-up counsel. Petitioner consents to service in this proceeding by email at the addresses above and at IBMDigitalDoorsIPRService@desmaraisllp.com.

CERTIFICATION UNDER 37 C.F.R. § 42.24(d)

Pursuant to 37 C.F.R. § 42.24(d), Petitioner hereby certifies, in accordance with and in reliance on the word count provided by the word-processing system used to prepare this Petition, that the number of words in this paper is 13,962. Pursuant to 37 C.F.R. § 42.24(d), this word count excludes the table of contents, table of authorities, mandatory notices under § 42.8, certificate of service, certificate of word count, appendix of exhibits, and any claim listing.

Dated: June 26, 2023

Respectfully submitted,

/Theodoros Konstantakopoulos/

Theodoros Konstantakopoulos
(Reg. No. 74,155)
tkonstantakopoulos@desmaraisllp.com
DESMARAIS LLP
230 Park Ave
New York, NY 10169
212-808-1060 (telephone)
212-351-3401 (facsimile)

Counsel for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), the undersigned certifies that a complete copy of the foregoing materials:

- Petition for Inter Partes Review Under 35 U.S.C. § 312 and 37 C.F.R. § 42.104 of U.S. 7,322,268;
- Exhibit List;
- Exhibits 1001-1020;
- Word Count Certification Under 37 CFR § 42.24(d);
- Petitioner's Power of Attorney

was served on counsel of record for Patent Owner by filing this document through P-TACTS on June 26, 2023, and by sending this document via Federal Express Priority Overnight shipping, which is at least as fast and reliable as U.S. Priority Mail Express, to counsel of record for Patent Owner at the correspondence address indicated in Patent Center:

Robert Kain
The Concept Law Group, P.A.
6400 N. Andrews Ave
Suite 500
FT LAUDERDALE, FL 33309
UNITED STATES

Dated: June 26, 2023

Respectfully submitted,

/Theodoros Konstantakopoulos/
Theodoros Konstantakopoulos
(Reg. No. 74,155)
tkonstantakopoulos@desmaraisllp.com
DESMARAIS LLP
230 Park Ave
New York, NY 10169
212-808-1060 (telephone)
212-351-3401 (facsimile)

Counsel for Petitioner