

Case IPR2023-00969
U.S. Patent No. 7,349,987

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INTERNATIONAL BUSINESS MACHINES CORPORATION
Petitioner

v.

DIGITAL DOORS, INC.
Patent Owner

IPR2023-00969
U.S. Patent No. 7,349,987
PETITION FOR *INTER PARTES* REVIEW
UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104

Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

	<u>Page</u>
I. Introduction.....	1
II. Grounds For Standing.....	2
III. Summary Of The '987 Patent.....	3
A. Overview	3
B. Prosecution History	4
C. Priority Date	8
IV. Level Of Ordinary Skill In The Art.....	8
V. Claim Construction.....	9
VI. Relief Requested And The Reasons For The Requested Relief,.....	9
A. Challenged Claims And Statutory Grounds For Challenge.....	9
1. Bossemeyer	10
2. Merenda	15
3. Chaganti	15
4. Kohane	16
B. Grounds 1-2: Claims 1, 6, 9, 10-11, 15-16, 21-23, And 27 Are Obvious Over Bossemeyer (Ground 1) Or Bossemeyer With Merenda (Ground 2).....	18
1. Independent Claims 1, 10, 16 and 22.....	18
2. Dependent Claims 6 and 21	58
3. Dependent Claim 9.....	64
4. Dependent Claims 11 and 23	65

5.	Dependent Claims 15 and 27	67
C.	Grounds 3-4: Claim 9 Is Obvious Over Bossemeyer With Chaganti (Ground 3) Or Bossemeyer With Merenda And Chaganti (Ground 4).....	70
1.	Dependent Claim 9.....	70
D.	Grounds 5-6: Claims 15 And 27 Are Obvious Over Bossemeyer With Kohane Or Bossemeyer With Merenda and Kohane	73
1.	Dependent Claims 15 and 27	73
VII.	Discretionary Denial Would Be Inappropriate.....	77
A.	Discretionary Denial Under The <i>Fintiv</i> Factors Is Not Appropriate.....	77
1.	No evidence regarding a stay	77
2.	Parallel proceeding trial date	78
3.	Investment in the parallel proceeding.....	79
4.	Overlapping issues with the parallel proceeding	79
5.	Identity of parties	80
6.	Other circumstances.....	80
B.	Discretionary Denial Under 35 U.S.C. § 325(d) Is Not Appropriate.....	81
VIII.	Conclusion	81
IX.	Mandatory Notices.....	82
A.	Real Party-in-Interest	82
B.	Related Matters.....	82
C.	Lead and Back-up Counsel and Service Information	82

TABLE OF AUTHORITIES

Pages(s)

Cases

<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020)	77, 79
<i>Dish Network L.L.C. v. Broadband iTV, Inc.</i> , IPR2020-01359, Paper 15 (Feb. 12, 2021)	77
<i>In re Preda</i> , 401 F.2d 825 (C.C.P.A. 1968)	70, 74
<i>Intel Corp. v. PACT XPP Schweiz AG</i> , 61 F.4th 1373 (Fed. Cir. 2023)	54, 55
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007)	52, 55, 56
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013 (Fed. Cir. 2017)	9
<i>PEAG LLC v. Varta Microbattery GmbH</i> , IPR2020-01214, Paper 8 (PTAB Jan. 6, 2021)	79
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	9
<i>Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC</i> , IPR2019-01393, Paper 24 (PTAB June 16, 2020)	77, 80

Statutes

35 U.S.C. § 102(e)	10, 15
35 U.S.C. § 103	9
35 U.S.C. § 311	1

35 U.S.C. § 314.....	77
35 U.S.C. § 314(a)	1, 9
35 U.S.C. § 325(d)	81

Rules

37 C.F.R. § 42.100	1
37 C.F.R. § 42.100(b)	9
37 C.F.R. § 42.104(a).....	2

EXHIBIT LIST

Exhibit No.	DESCRIPTION
1001	U.S. Patent No. 7,349,987 to Redlich et al.
1002	Prosecution History of U.S. 7,349,987
1003	Declaration of Dr. Erez Zadok
1004	<i>Curriculum Vitae</i> 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	U.S. Patent No. 6,845,448 to Chaganti et al.
1008	U.S. Publication No. 2004/0199765 to Kohane et al.
1009	Amended Docket Control Order, <i>DigitalDoors, Inc. v. Int'l Bus. Machs. Corp.</i> , Civil Action No. 2:22-cv-00457-JRG-RSP (E.D. Tex. Apr. 5, 2023).
1010	Scheduling Order, <i>DigitalDoors, Inc. v. Int'l Bus. Machs. Corp.</i> , Civil Action No. 2:22-cv-00457-JRG-RSP (E.D. Tex. Feb. 7, 2023).
1011	Federal Case Management Statistics for the Eastern District of Texas, as of March 2023
1012	Plaintiff DigitalDoors, Inc.'s Disclosure of Asserted Claims and Initial Infringement Contentions, <i>DigitalDoors, Inc. v. Int'l Bus. Machs. Corp.</i> , Civil Action No. 2:22-cv-00457-JRG-RSP (E.D. Tex. Feb. 28, 2023).
1013	U.S. Patent No. 7,191,252 (Continuation-in-part Application No. 10/155,525)
1014	U.S. Patent No. 7,140,044 (Continuation-in-part Application No. 10/008,209)
1015	U.S. Patent No. 7,146,644 (Continuation-in-part Application No. 10/008,218)
1016	U.S. Patent No. 7,103,915 (Continuation-in-part Application No. 09/916,397)
1017	U.S. Provisional Application No. 60/247,242
1018	U.S. Provisional Application No. 60/247,232
1019	U.S. Patent No. 5,960,080 to Fahlman et al.
1020	U.S. Patent No. 6,602,298 to Kirshenbaum
1021	U.S. Publication No. 2001/0011250 to Paltenghe et al.
1022	US. Patent No. 6,473,741 to Baker
1023	US. Patent No. 5,982,897 to Clark

Exhibit No.	DESCRIPTION
1024	OceanStore: An Architecture for Global-Scale Persistent Storage (Nov. 12-15, 2000)
1025	US. Patent No. 5,933,834 to Aichelen
1026	Wylie et al., Survivable Information Storage Systems (Aug. 2000)
1027	US. Patent No. 5,956,400 to Chaum et al.
1028	Microsoft Computer Dictionary, Fourth Edition, Copyright 1999, Excerpts
1029	Beck et al., Linux Kernel Internals, 2nd Ed., Copyright 1998, pp. 148-187
1030	DOD Standard, Department of Defense Trusted Computer System Evaluation Criteria, December 26, 1985 (“Orange Book”)
1031	Director of Central Intelligence Directive No. 1/16, Security of Compartmented Computer Operations (“CIA”)
1032	Cheswick et al., Firewalls and Internet Security, Copyright 1994, p. 163
1033	Director’s June 21, 2022 Memorandum on Discretionary Denials

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 1, 6, 9-11, 15-16, 21-23, and 27 (“Challenged Claims”) of U.S. Patent No. 7,349,987 (“’987 Patent,” EX1001).

The Challenged Claims cover securing data by separating sensitive portions of the data and controlling access to the sensitive data based on a security clearance. Digital Doors Inc. (“Digital Doors” or “Patent Owner”) obtained the Challenged Claims after arguing that the amended claims cover “various levels of secret data...stored in ‘respective extract stores’ which are physically distinguishable and physically distinct” and that the prior art did not include “multi-level secured data storage, extraction for each security level, and full or partial reconstruction using multiple extract stores.” EX1002, 378-79, 390-91.

But the features that Patent Owner highlighted were neither new nor inventive. This Petition demonstrates that separating sensitive data at various security levels and storing the separated data at physically distinct locations was known. *See e.g.*, EX1005, (“Bossemeyer”), 5:8-9 (“[I]nformation is stored in three levels of security: unrestricted, limited access, and restricted.”), 3:5-18 (“[I]n the merchant transaction..., the purchaser’s credit files are...stored in a database monitored by the credit reporting companies....[I]nsurance information would

ultimately reside with the insurer, medical records with the health provider, financial records with the bank or broker, and so on.”).

Controlling access to sensitive data based on a corresponding security level was also known. 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....”); EX1006 (“Merenda”), ¶29 (“[A]ccess to the data elements in the private data set may be made on an element-by-element basis[—]the merchant may be provided with access to certain select pieces of private data..., such as the contact information (name, address, phone number, e-mail) but not to other sensitive data such as revenue, credit card etc.”)), and it would have been obvious to combine the prior art teachings.

The Petition, supported by Dr. Erez Zadok’s declaration, demonstrates that the combination of 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.

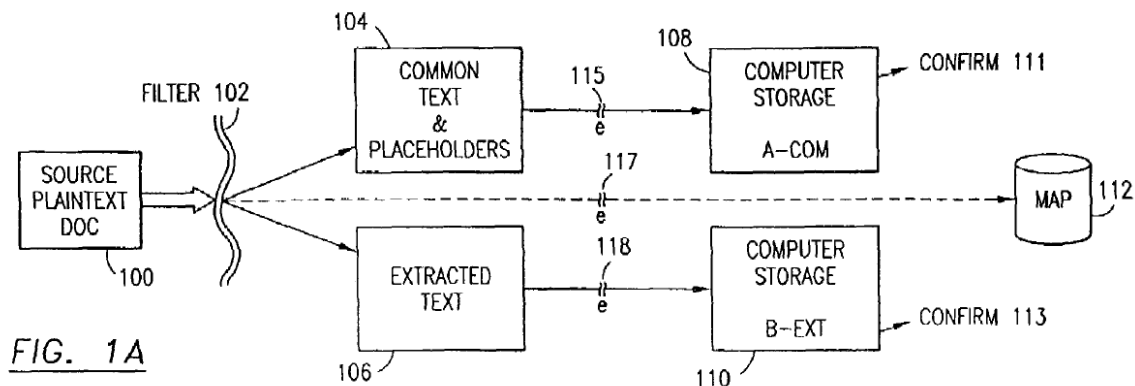
II. Grounds For Standing

Petitioner certifies that the ’987 Patent is eligible for IPR and that Petitioner is not barred or estopped from requesting IPR. 37 C.F.R. § 42.104(a).

III. Summary Of The '987 Patent

A. Overview

The '987 Patent relates to “parsing (typically through a filter), extracting and dispersion of the parsed or segregated data with the controlled reconstruction of data utilizing security protocols...” EX1001, 1:14-20. Figure 1A illustrates the disclosed data security system:



EX1001, Figure 1A. The system “splits, cuts and segments (that is, parses)” a source document. EX1001, 39:1-15, Figure 10. For example, as shown, source document 100...is passed through filter 102. EX1001, 18:2-4. “Filter 102... separates out common text or remainder data 104 from uncommon text, words, characters, icons or data objects.” EX1001, 18:15-17. 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 data file 106. EX1001, 18:25-31. The remainder and extracted data are 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, 19:14-15, 19:21-23. The source document “may be preserved with or without encryption, or destroyed as a further data security step.” EX1001, 42:6-8, 9:17-33.

The '987 Patent explains that the data security system may generate revenue by charging users at the data input or reconstruction stage, and that such features were well-known. EX1001, 45:34-46:34, Figure 13. EX1003, ¶¶79-84.

B. Prosecution History¹

The '987 Patent was filed on May 23, 2002. EX1001, 1. The Examiner initially rejected the claims over U.S. Patent Nos. 5,960,080 (“Fahlman”), 6,602,298 (“Kirshenbaum”), and other references. EX1002, 234-42; EX1019; EX1020. Applicant amended the claims to recite, among other things, “a plurality of memories respectively designated as a remainder store and...a plurality of extract stores corresponding to a *plurality of security levels* for respective subsets of said security sensitive words, characters or icons,” and “storing said extracted data and said remainder data in said respective extract stores corresponding to an associated security level and said remainder store, respectively.” EX1002, 251.

¹ Emphasis in this subsection is in the text of the prosecution history except for bold emphasis.

The Examiner maintained the rejections. EX1002, 277-90. The Examiner noted that Fahlman “shows a *method of securing data having one or more security sensitive words, characters or icons in a computer system with memories designated as a remainder store and an extract store*” and Kirshenbaum “shows that there are multiple stores and the stores may[]be on different locations,” and “[i]t would have been obvious to include the multi-level security feature in Kirshenbaum, because it increases the granularity of security control.” EX1002, 280-82.

In response, Applicant further amended the claims, for example as shown in claim 1 below, to recite “a plurality of physically distinguishable memories respectively designated as a remainder store and a plurality of physically distinct extract stores...,” and “permitting full or partial reconstruction of said data...”

1. (currently amended) A method of securing data having one or more security sensitive words, characters or icons in a computer system with a plurality of physically distinguishable memories respectively designated as a remainder store and a plurality of physically distinct extract stores corresponding to a plurality of security levels for respective subsets of said security sensitive words, characters or icons (~~FIG. 6, store 1, 2 or 3; FIG. 7, step 422~~) comprising:

extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data therefrom;

storing said extracted data and said remainder data in said respective extract stores corresponding to an associated security level and said remainder store, respectively; and,

permitting full or partial reconstruction of said data via said extracted data from respective extract stores and remainder data only in the presence of a predetermined security clearance corresponding to said associated security level for said respective extract stores.

EX1002, 371.

Applicant argued that the amended claims cover “various levels of secret data are stored in ‘respective extract stores’ which are physically distinguishable and physically distinct and this is essentially the same as *multiple levels of security with multiple levels of secure storage.*” EX1002, 378. Applicant contended “Kirshenbaum...and/or Fahlman...” did not include “multiple extractions of security sensitive words related to each of a plurality of security levels, and separate storage of those security sensitive words in different, physically distinct secured locations for each security level (‘respective extract stores’), and the requirement

that the user input a password ('security clearance') for each security level to reconstruct the data from 'respective extract stores.'" EX1002, 378-79.

Applicant also argued Fahlman did not include "a remainder store for non-secured data, multiple security levels, multiple extraction of security data, storage of extract data at multiple levels, nor presentment of corresponding security codes at each security level." EX1002, 381. Specifically, Applicant argued "Fahlman does not seem to store remainder or non-secure data in a separate remainder store location apart from secure data." EX1002, 382. Applicant distinguished the claims asserting that the references lacked "multi-level secured data storage, extraction for each security level, and full or partial reconstruction using multiple extract stores." EX1002, 390. The Examiner issued a Notice of Allowance. EX1002, 425, 428-30.

But as this Petition illustrates, separating and securing sensitive data at various security levels, storing the separated data at physically distinct locations, and allowing full/partial reconstruction based on a respective security clearance was known. For example, Bossemeyer—a prior art reference that was not considered by the Examiner—discloses storing data in physically distinct extract stores based on different security levels (e.g., unrestricted, public limited access, restricted (EX1005, 2:17-27)), storing non-sensitive data in a separate store (e.g., storing unrestricted data in stores 210, 212 (EX1005, Figure 3, 5:6-22)), and allowing full or partial reconstruction based on a respective security clearance (e.g., different user

identification codes allow access to partitions in the database (EX1005, 2:38-47, 3:63-4:6, 4:59-65)). EX1003, ¶¶85-93, 46-78.

C. Priority Date

The earliest claimed priority date is November 13, 2000, the filing date of two provisional applications which the '987 Patent claims priority to. *See* EX1017; EX1018. Petitioner does not concede that the Challenged Claims are entitled to that priority date. However, because the references discussed here qualify as prior art under the November 13, 2000, date, Petitioner does not challenge the priority date of the Challenged Claims here but reserves the right to do so in other proceedings.² EX1003, ¶30.

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, ¶131.

² Petitioner reserves the right to raise § 112 challenges in other proceedings.

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, no claim term requires express construction. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). EX1003, ¶134.

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

A. Challenged Claims And Statutory Grounds For Challenge

Petitioner requests the Board institute a trial for IPR and cancel the Challenged Claims under 35 U.S.C. §103. This Petition, supported by Dr. Erez Zadok’s Declaration (EX1003), demonstrates that there is a reasonable likelihood that Petitioner will prevail with respect to the Challenged Claims. 35 U.S.C. §314(a).

Grounds	Claims	Basis
#1	1, 6, 9, 10-11, 15-16, 21-23, and 27	(§103) Bossemeyer
#2	1, 6, 9, 10-11, 15-16, 21-23, and 27	(§103) Bossemeyer In View Of Merenda
#3	9	(§103) Bossemeyer In View Of Chaganti
#4	9	(§103) Bossemeyer In View Of Merenda and Chaganti
#5	15 and 27	(§103) Bossemeyer In View Of Kohane
#6	15 and 27	(§103) Bossemeyer In View Of Merenda and Kohane

1. Bossemeyer

US7,010,701 (EX1005), 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 which is readily accessible from different types of smart card terminals supporting various smart card applications.” EX1005, 1:44-49. Smart cards are devices that “can hold much more

information [than data cards] and often include some ‘intelligence’ such as a microprocessor....” EX1005, 1:34-38, 3:28-31. The network arrangement includes “a centralized server architecture [where] data...can be accessed by an individual smart card, predefined groups of... users, or the general public.” EX1005, 1:49-52.

Figure 1 shows an example:

The network arrangement makes use of a central database server 10 that supports many different smart card applications.... 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, 2:4-12.

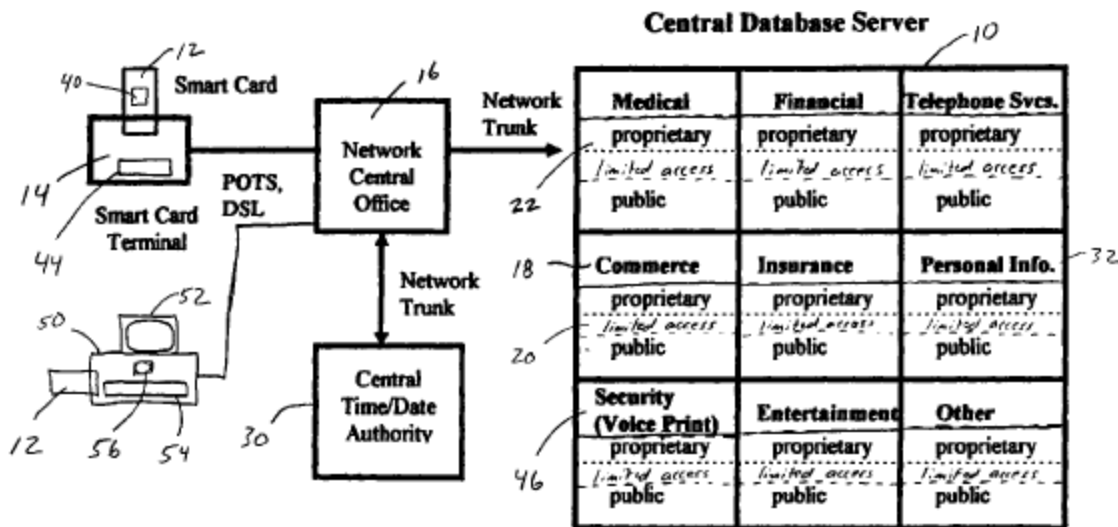


Figure 1

EX1005, Figure 1.

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 such as credit report companies, insurers, health providers, and banks. EX1005, 3:5-18.

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....*”).

Bossemeyer discloses accessing data from different locations of the system using a user identification/authentication 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...routes the data pointer to appropriate memory locations or database of the information keeper....Data from these various locations is supplied back to the smart card terminal 14....

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

“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.

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

200
↙

USER DATA

	FINANCIAL	MEDICAL	ETC.
RESTRICTED ACCESS DATA	CREDIT HISTORY 218	MEDICAL HISTORY 216	
LIMITED ACCESS DATA	CHARGE ACCOUNTS BANK ACCOUNTS 220	INSURANCE DOCTORS PRESCRIPTIONS 214	
UNRESTRICTED DATA	DIGITAL WALLET 210	MEDICAL ALERTS 212	

FIG. 3

EX1005, Figure 3.

Bossemeyer explains that different merchants may have access to information that has different levels of security. For example, “a grocer may have access to the user’s digital wallet 210 and medical alerts 212..., 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.” EX1005, 5:20-22.

Bossemeyer also discloses that its system is based on subscription services. EX1005, 5:23-31. EX1003, ¶¶94-107.

2. Merenda

US Publication 2004/0148290 (EX1006), filed on January, 14, 2004, is a divisional application of US Ser. 10/390,954, filed on Mar. 17, 2003, which is a divisional application of US Ser. 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).

Merenda describes a system “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.” EX1006, ¶2. Merenda describes that “data entered by a consumer into a Web form is separated into related records in a public and private data set.” *Id.*, ¶7. For example, a user of Merenda’s system requesting information, e.g., a merchant, can access only “certain select pieces of private data... but not to other sensitive data.” EX1006, ¶29. EX1003, ¶¶108-115.

3. Chaganti

US6,845,448 (EX1007, “Chaganti”), filed on January 7, 2000, and issued on January 18, 2005, is prior art under at least 35 U.S.C. §102(e).

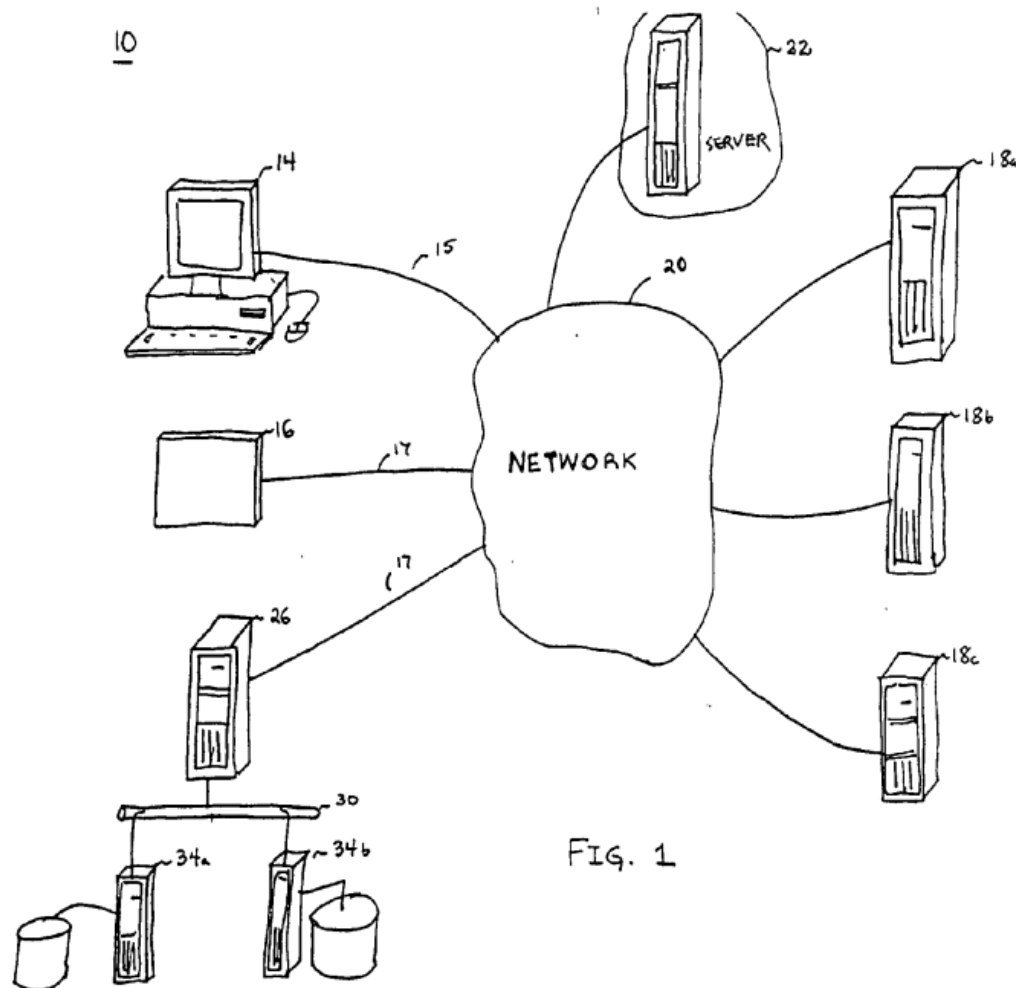
Chaganti describes systems for “storing personal information on a server computer and releasing such information to authorized requesters” by assessing charge fees for users and requesters. EX1007, Abstract, 2:21-43, 5:43-56 (“**[T]he**

fee is calculated based on a per transaction basis, or on a subscription basis, either from users that store information or from entities that request such information.”), 10:30-42, 12:42-67. EX1003, ¶¶116-123.

4. Kohane

US Publication 2004/0199765 (EX1008, “Kohane”), filed on December 22, 2003, is a continuation application of US Ser. 09/410,717, filed on October 1, 1999, and claims priority to provisional application 60/150,154, filed on August 20, 1999. Kohane published on October 7, 2004, and is prior art under at least 35 U.S.C. §102(e).

Kohane discloses a “record system 10 including client systems... ([i.e.,] agent systems) in communication with servers 18a, 18b, 18c (collectively, server 18) through a gateway server system 22 over a network 20.” EX1008, ¶23.



EX1008, Figure 1.

Kohane explains that “gateway server system 22 encrypts the record objects” and transmits to servers 18 and “the record objects traverse the network 20 in this encrypted form when subsequently downloaded by the gateway server system 22” from servers 18. EX1008, ¶58. The gateway server system 22 can also send record objects to the agent systems. EX1008, ¶60. Kohane describes that the record objects

in the agent systems 14, 16, 26 are deleted after being reviewed by those systems to enhance security. EX1008, ¶¶63. EX1003, ¶¶124-130.

B. Grounds 1-2: Claims 1, 6, 9, 10-11, 15-16, 21-23, And 27 Are Obvious Over Bossemeyer (Ground 1) Or Bossemeyer With Merenda (Ground 2)

1. Independent Claims 1, 10, 16 and 22

i. Claims 1, 10, 16, and 22 Preambles

To the extent the preamble is limiting, Bossemeyer alone (Ground 1) or with Merenda (Ground 2) teaches the preambles, as explained below. EX1003, ¶¶135, 264.

a. [1pre-i] A method of securing **data having one or more security sensitive words, characters or icons in a computer system**

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 2) this limitation. EX1003, ¶¶136, 265.

Bossemeyer discloses a method of securing **data**. Specifically, Bossemeyer discloses securing information (e.g., user data) by separating sensitive data to control how the data is transferred and used. 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.*”). Bossemeyer further discloses restricting access to sensitive data:

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 (reproduced below).

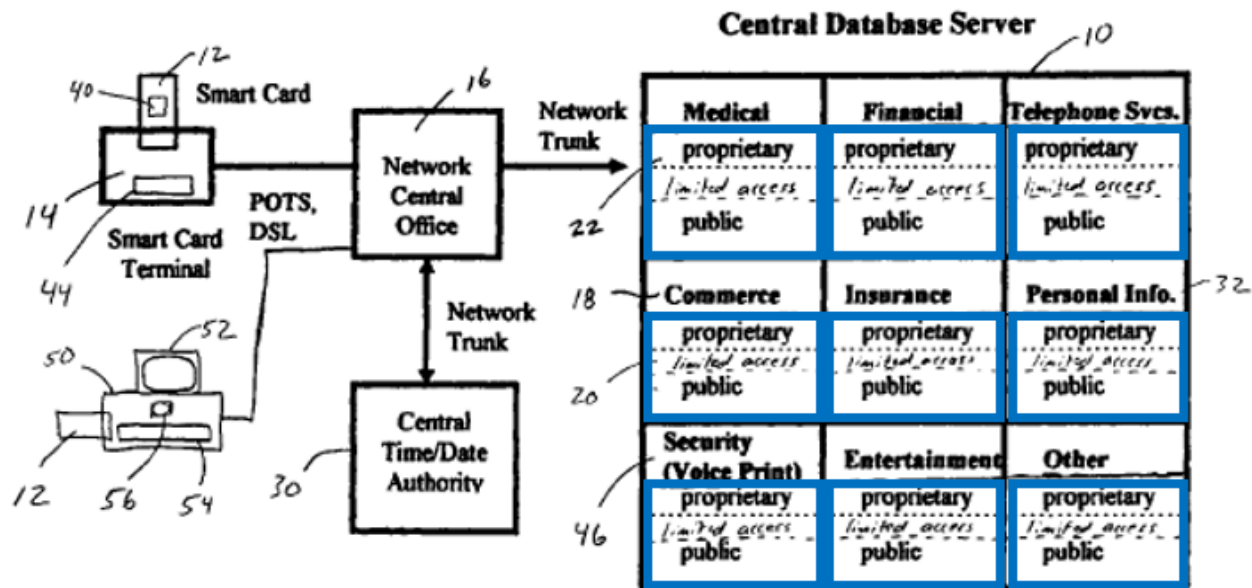


Figure 1

EX1005, Figure 1.

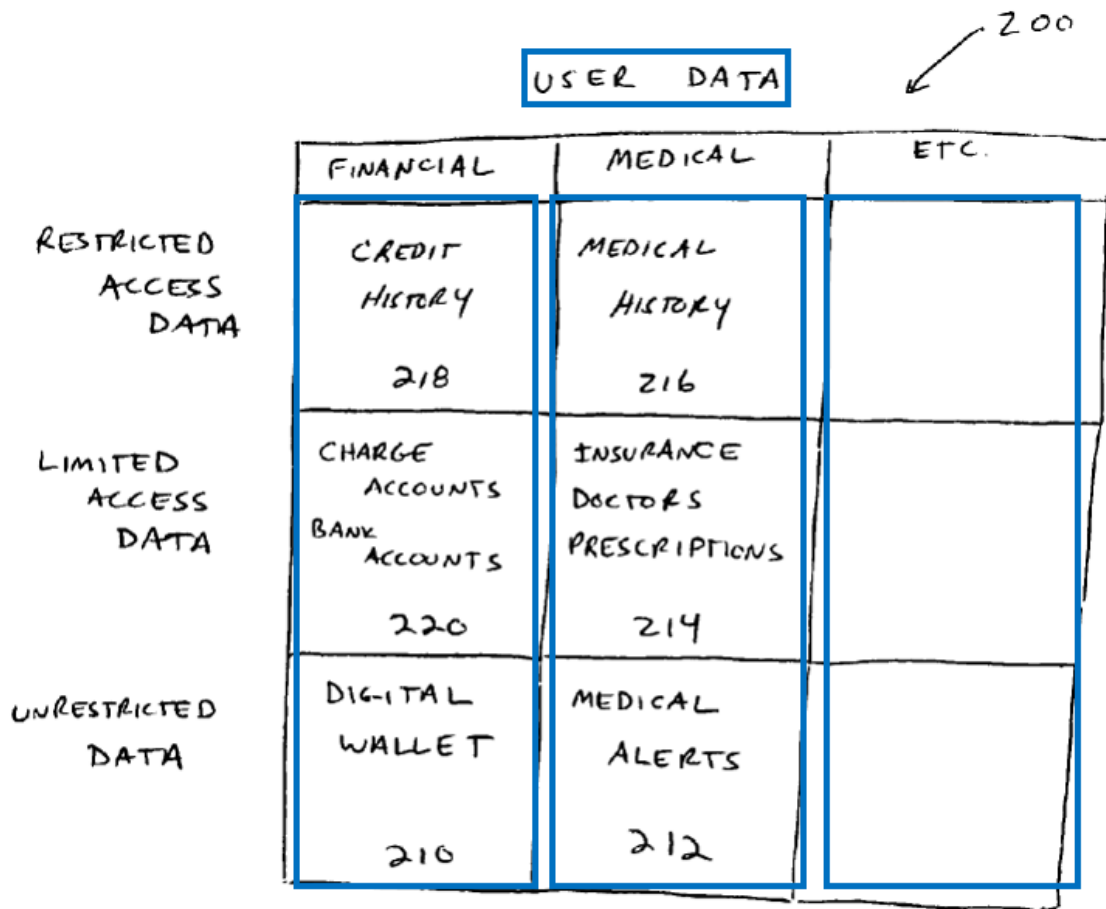


FIG. 3

EX1005, Figure 3. EX1003, ¶¶137-140.

A POSITA would have understood that Bossemeyer's "limited access information" and/or "proprietary information" would include security sensitive information, such as, words, characters, or icons, because Bossemeyer discloses restricting access to such information. Bossemeyer discloses different types of security sensitive information, 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 is highly sensitive information and 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.”); EX1006, ¶23 (“[F]or example, identifying input fields on a Web page... require[es] sensitive data input such as an address, credit card or social security number....”); EX1008, ¶5. EX1003, ¶¶141-143.

In addition to the types of information explicitly disclosed in Bossemeyer, it would have been obvious that Bossemeyer's method secures other types of security sensitive words, characters, or icons. For example, Figure 3 of Bossemeyer includes additional columns for storing user data with a restricted- or limited-access security level (e.g., financial data). Similarly, Figure 1 of Bossemeyer shows different types of data that include security sensitive information, e.g., stored as proprietary or limited access data. EX1003, ¶144.

Bossemeyer's method is performed in a computer system: Bossemeyer's network arrangement for securing data is implemented over an interconnected network of computers, i.e., a computer system having a plurality of computers. EX1005, 1:44-52 (“[A] network arrangement... 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 (“[S]uch 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... [and/]or... the traditional telephone network 102.”), Figures 1-3. The computer system has a plurality of memories for extract and remainder stores. EX1003, ¶145.

For Ground 2, to the extent Patent Owner argues that Bossemeyer does not teach this limitation, Merenda discloses it. EX1006, ¶23 (“ [A] set of *data* may be parsed into private and non-private elements. [T]his might entail...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....), ¶24 (“[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....”);
Figures 1, 2, 6. EX1003, ¶266.

Moreover, Merenda discloses separating the data into public and private data sets and allowing access to that data like Bossemeyer. EX1006, ¶25 (“As a result of the distribution of data elements..., it is desirable to establish a level of control over access to the public and private data stored therein.”). EX1003, ¶267.

As discussed in Section VI.B.1.vi, a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in combining them. EX1003, ¶¶313-344.

b. [10pre-i] A method of securing data with a parsing algorithm via a computer system

Bossemeyer discloses and/or renders obvious (or with Merenda for Ground 2) this limitation for the reasons in Section VI.B.1.i.a. EX1003, ¶¶147, 269.

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, ¶148.

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.a, *limited access information* and/or *proprietary information* includes security sensitive content, such as, words, characters, or icons. For example, Bossemeyer shows *medical information 22* stored as proprietary information:

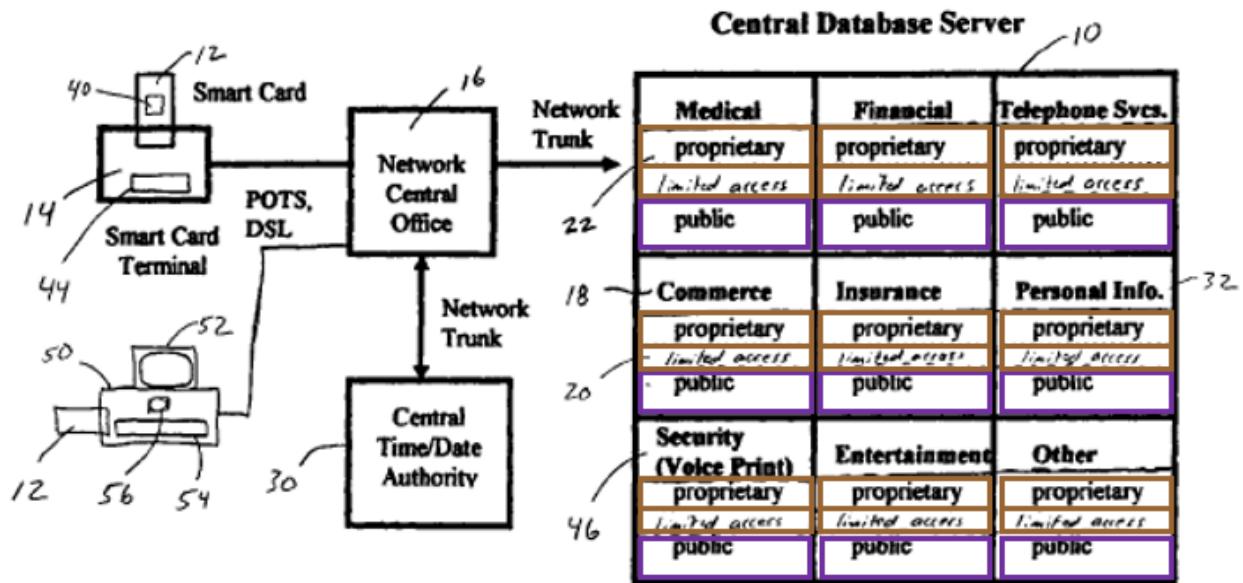


Figure 1

EX1005, Figure 1, 2:28-36 (“Private or proprietary information is partitioned such that the owner...has control over how the information is...used. *[M]edical 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, ¶¶149-151.

Figure 3 provides another example of partitioning or separating (e.g., extracting) *user data* into *extracted data* and *remainder data*:

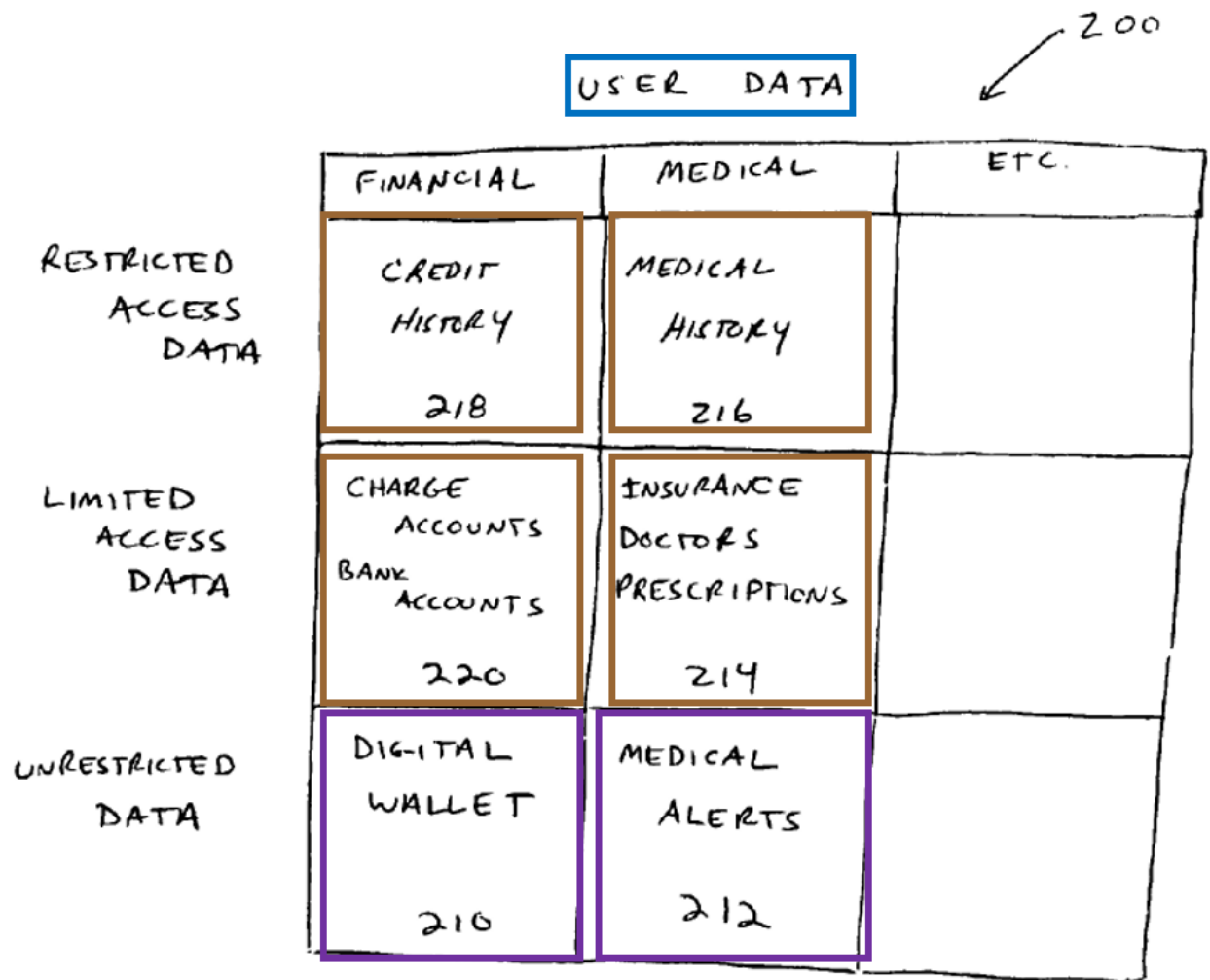


FIG. 3

EX1005, Figure 3, 5:6-9 (“[I]nformation is stored in three levels of security: unrestricted, limited access, and restricted.”), 5:9-15 (“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*.”). EX1003, ¶¶152-155.

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 teaches separating sensitive information from user data. When Bossemeyer’s central database server receives a **user’s medical data file** (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. A POSITA would have understood that medical history information can include words and 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.

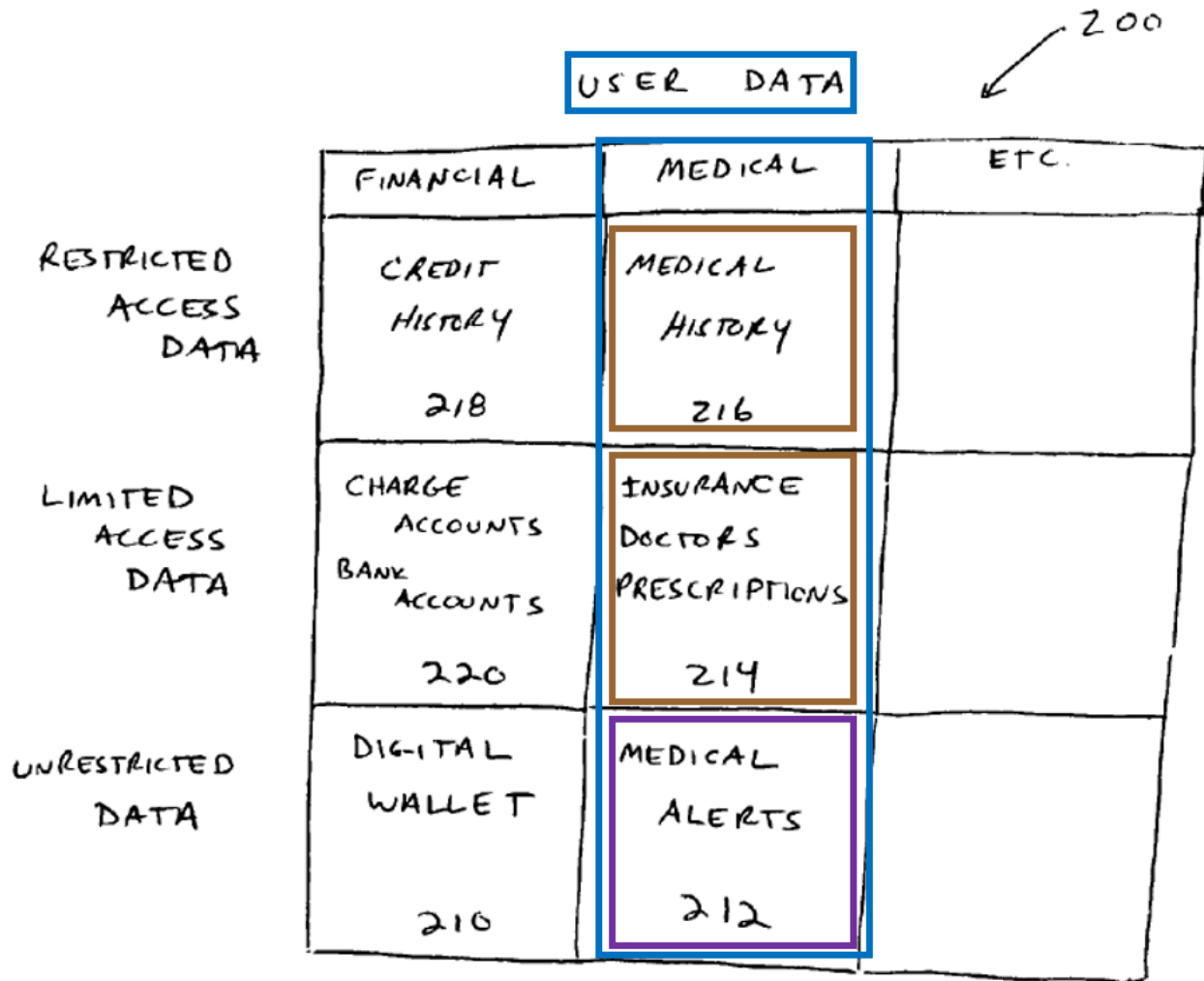


FIG. 3

EX1005, Figure 3. EX1003, ¶¶156-158.

Moreover, a POSITA would have understood that Bossemeyer's disclosure of separating user data utilized a parsing algorithm, because Bossemeyer's method would filter and split the sensitive information, (e.g., restricted- and/or limited-data), from the received user data, (e.g., from a user data file), and 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 (restricted, limited access data) and non-private (unrestricted data) elements. *See e.g.*, EX1005, 2:17-22, 3:3-18, Figures 1, 3; EX1006, ¶23 (“[A] set of data may be parsed into private and non-private elements.”). Indeed, the '987 Patent describes such a process in Bossemeyer as “parsing,” *see, e.g.*, EX1001, 19:11-13 (“The parsing occurs with the filtering of the plain text source document 100 and the subsequent storage of extracted data apart from remainder data.”), 39:8-10 (“[T]he parsing algorithm... splits, cuts and segments (that is, parses)....”), and algorithms for splitting was well known in the art, *see, e.g.*, EX1006, ¶7, EX1026, 64 (“Secret-sharing schemes can be thought of as a combination of splitting and replication techniques.”); EX1027, 3:33-47 (“Each new patient medical record entered by a physician into his terminal is split into two fragments: a fragment containing only medical information, and a fragment containing only patient identifying information.”). EX1003, ¶¶159-163.

For Ground 2, to the extent Patent Owner argues that Bossemeyer does not teach using a “parsing algorithm” to secure data, Merenda teaches it. Merenda specifically discloses 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*. 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, ¶31, Figures 1, 2, 3; Figure 8.

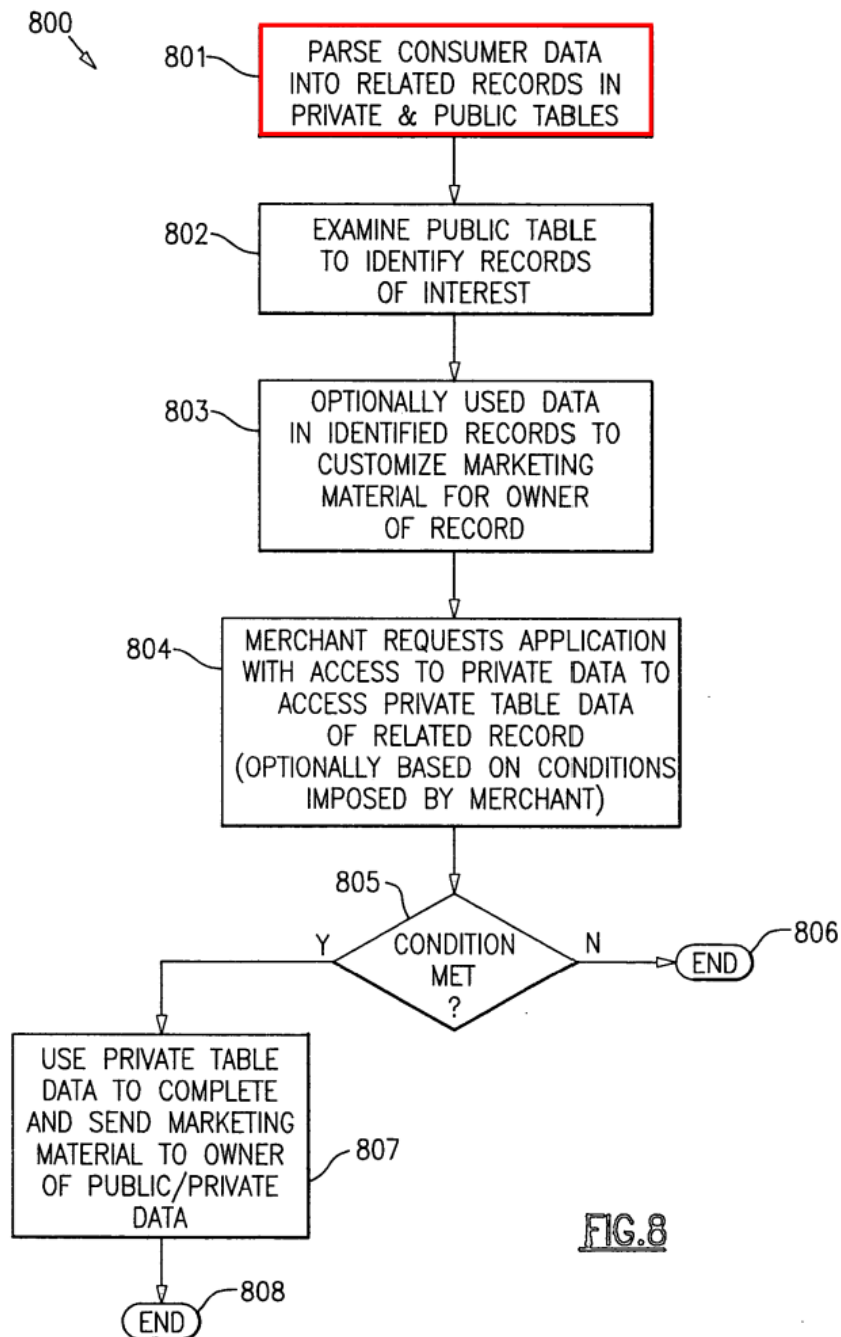


FIG.8

EX1006, Figure 8, ¶47. EX1003, ¶¶270-271.

As such, Merenda teaches parsing data into *public data* (e.g., *remainder data*) and *private data* (e.g., *extracted data*) and storing that data as respective public data

sets (e.g., *remainder store*) and private data sets (e.g., extract stores) , which results from utilizing a parsing algorithm. EX1006, ¶¶23-24, ¶31 (“Turning to FIG. 3[,]a web form may generate a number of data sets 301 a-d....Any of these data sets may be designated as including private data, and the remaining data sets include public data.”), Figures 1, 2, 3, ¶15 (“FIG. 1 illustrates a set of data elements parsed into private and public data sets.”), ¶47. It would have been obvious to combine Merenda’s teaching on parsing with Bossemeyer and meet this limitation. See Section VI.B.1.vi. EX1003, ¶272.

c. [16pre-i] A computer readable storage medium encoded with programming instructions for securing data having one or more security sensitive words, characters or icons in a computer system

Bossemeyer renders obvious alone (or with Merenda for Ground 2) this limitation for the reasons in Section VI.B.1.i.a. As discussed, Bossemeyer discloses a method for “securing data having one or more security sensitive words, characters or icons” in a computer system. 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 computer readable storage medium. For example, Bossemeyer’s method is computerized because Bossemeyer’s arrangement for securing data is implemented over an interconnected network of computers, i.e., a computer system for performing

Bossemeyer's method. Section VI.B.1.i.a. Bossemeyer's computer system would execute programming instructions, which would require storage in a storage medium. *See, e.g.*, EX1005, 2:13-16 ("The central database server 10 includes partitioned memory... as well as a microprocessor for processing data...."), 3:16-18, 3:28-38 ("Smart card 12...contains circuitry 40 which includes a microprocessor and memory including random access memory (RAM) and read only memory (ROM)."), 3:39-43, 3:56-66. To implement its computerized method, Bossemeyer's system would read the programming instructions from the storage medium and execute them, for example, in an execution unit. EX1003, ¶¶165-167.

For Ground 2, Merenda discloses "at least one *program storage device readable by a machine*....embodying at least one *program of instructions* executable by the machine...." EX1006, ¶50, ¶49. A POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in combining them. *See* Section VI.B.1.vi. EX1003, ¶¶275-276.

d. [22pre-i] A computer readable storage medium encoded with programming instructions for securing data with a parsing algorithm via a computer system

Bossemeyer renders obvious alone (or with Merenda for Ground 2) this limitation for the reasons in Sections VI.B.1.i.a, VI.B.1.i.b, and VI.B.1.i.c. EX1003, ¶¶169, 278.

e. [1/16pre-ii] with a plurality of physically distinguishable memories respectively designated as a remainder store and a plurality of physically distinct extract stores corresponding to a plurality of security levels for respective subsets of said security sensitive words, characters or icons comprising:

[10/22pre-ii] having physically distinguishable memories designated as a remainder store and a plurality of physically distinct extract stores corresponding to a plurality of security levels for respective subsets of said security sensitive words, characters or icons comprising:³

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 2) this limitation for the reasons in Sections VI.B.1.i.a and VI.B.1.i.b. EX1003, ¶¶170, 279.

Moreover, Bossemeyer describes a plurality of physically distinguishable memories for storing various sensitive information (in distinct extract stores) and public information (in a remainder store). Specifically, Bossemeyer discloses a plurality of physically distinct memories for storing a respective subset of sensitive information by application “category (medical, financial, etc.), as well as level of security (unrestricted, or public limited access, restricted).” *See, e.g.*, EX1005, 2:17-22. EX1003, ¶¶171-172.

³ Petitioner reserves the right to challenge the claims for, among others, lack of antecedent basis in other proceedings.

For example, Bossemeyer discloses storing various types of sensitive information (e.g., limited-access and/or restricted information for medical, financial, commerce, insurance, personal information (Figure 1); restricted data such as credit history 218, medical history 216, limited-access data for bank accounts, insurance (Figure 3)) at separate memory locations (distinct **extract stores**) based on their respective categories. EX1005, Figures 1, 3. Bossemeyer further discloses storing various types of public information (e.g., public data for medical, financial, commerce, insurance, personal info (Figure 1); unrestricted data such as digital wallet 210, medical alerts 212 (Figure 3)) at memory locations (**remainder store**) separate from the **extract stores**. EX1005, Figures 1, 3:

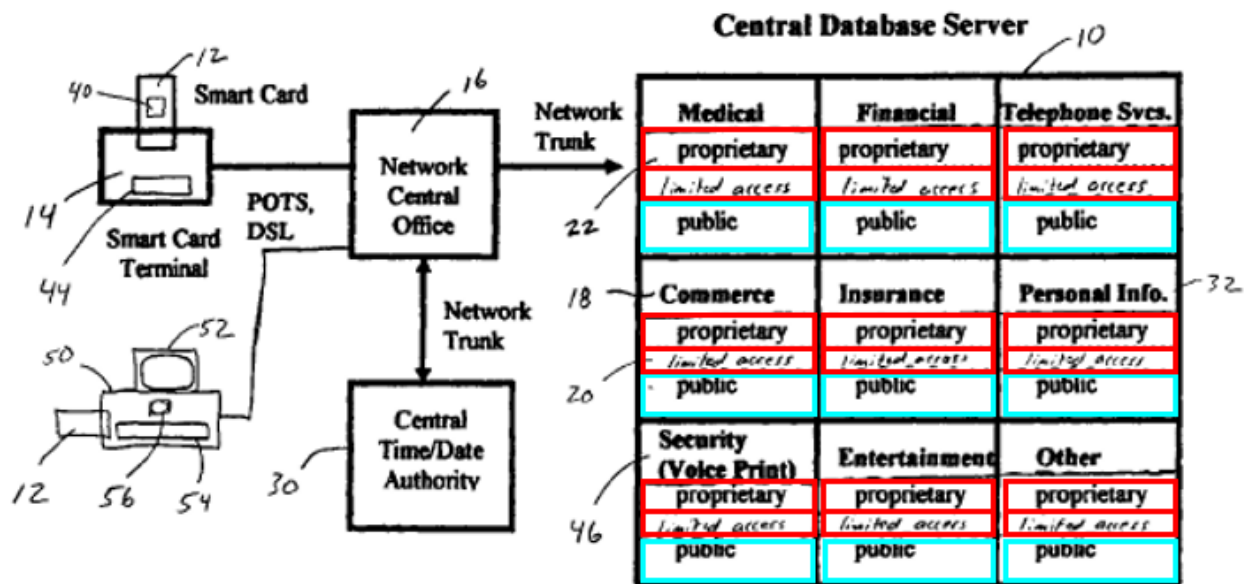


Figure 1

EX1005, Figure 1.

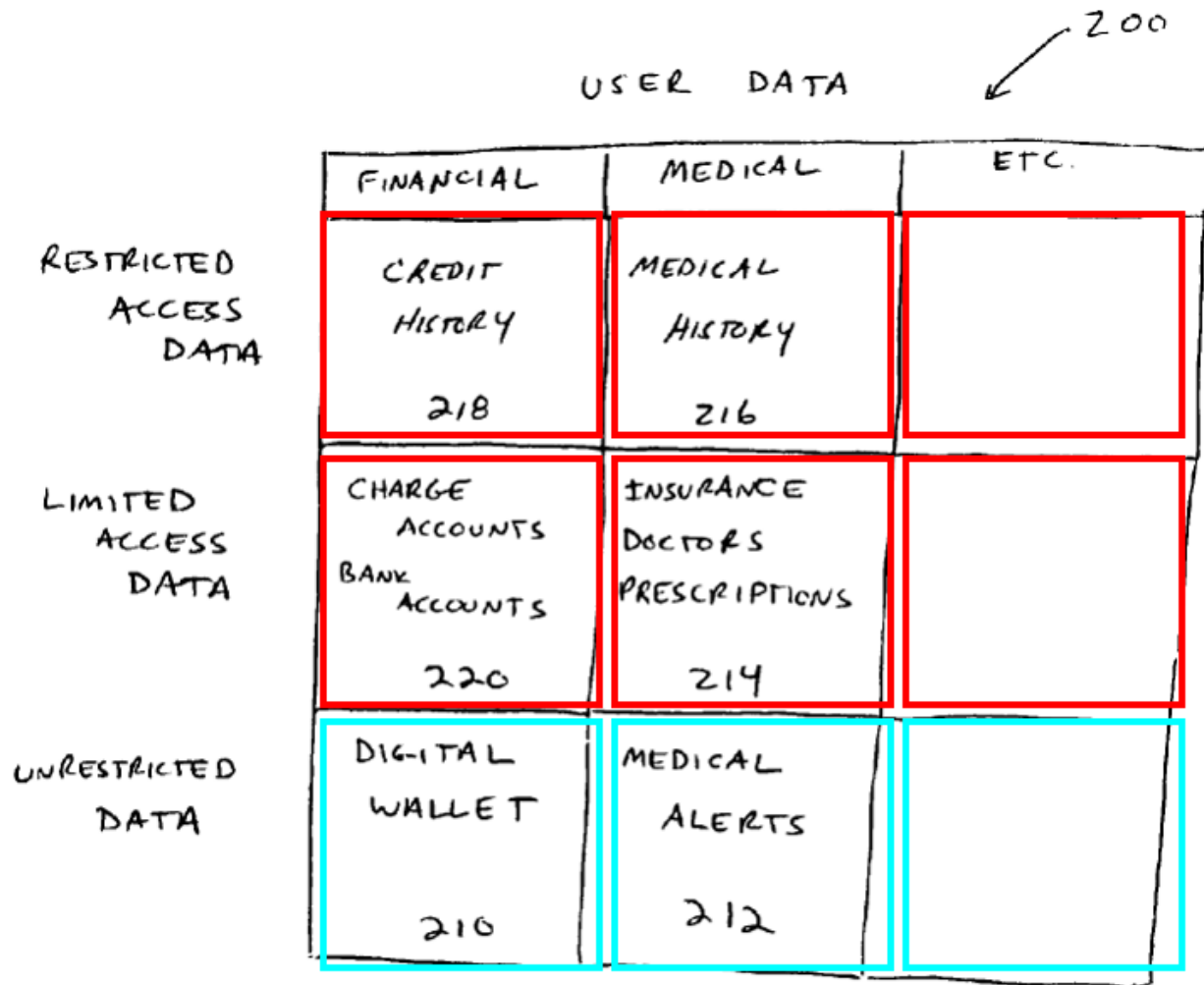


FIG. 3

EX1005, Figure 3. EX1003, ¶¶173-175.

The '987 Patent describes “extract stores” as memories that store sensitive information. EX1001, 9:37-44 (“The e-mail data has one or more *security sensitive words, characters or icons* and the method or computer program works in a distributed computer system with *a remote memory designated as an extract store*. The method extracts *the security sensitive words, characters or icons* from said e-

mail data to obtain extracted data and remainder data therefrom. *The extracted data is stored in the extract store.*”). Accordingly, Bossemeyer’s memories that store sensitive information (limited-access and/or restricted information) are extract stores. EX1003, ¶176.

Bossemeyer’s computer system has a plurality of *physically distinct exact stores* because Bossemeyer discloses that distinct servers at physically different locations 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. In such cases, the central database server 10 acts as a network smart card server which facilitates data transfer between the database containing the desired information and the merchant or person requesting the information. 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.

EX1005, 3:3-18. A POSITA would have understood that the public information (e.g., unrestricted data such as digital wallet and medical alerts in Figure 3) is stored in the central database server 10, physically separate from the extract stores, so as to

be accessible by various applications (e.g., credit card, bank applications). The requested information is retrieved from databases at different locations depending on the application at issue. EX1005, 3:66-4:6 (“Routing circuitry... 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.”). EX1003, ¶¶177-179.

Bossemeyer discloses that the distinct extract stores correspond to “a plurality of security levels for respective subsets of said security sensitive words, characters or icons.” Bossemeyer explains that its computer system stores different parts of the sensitive information based on the *levels of security/accessibility* (e.g., public limited access, restricted) at separate memory locations:

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, 2:17-27. Thus, a POSITA would have understood that respective sensitive information, which are subsets of the entire sensitive information, is stored with its data owner and that the subsets would have different security levels. For example, the health provider’s *extract store* would save “medical history” with “*restricted access*” and the insurer’s *extract store* would store “insurance” information with

“*limited access*.” See EX1005, Figure 3. The “medical history” and “insurance” information are subsets of the secured information having sensitive words, characters, or icons. EX1003, ¶¶180-183.

For Ground 2, to the extent Patent Owner argues that Bossemeyer does not disclose a plurality of security levels, Merenda discloses, or renders obvious, a plurality of security levels for private data sets. 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*).

*[A]ccess 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, ¶¶280-283.

Accordingly, Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 2) this limitation. EX1003, ¶¶184, 284.

ii. [1/16a] extracting said security sensitive words, characters or icons from said **data** to obtain **extracted data** and **remainder data** therefrom;

[10/22a] parsing said **data** to obtain **extracted data** for respective associated **security levels** and **remainder data** therefrom;

Bossemeyer discloses and/or renders obvious (or with Merenda for Ground 2) these limitations for the reasons in Section VI.B.1.i.b. EX1003, ¶¶185, 285.

Moreover, as discussed in Sections VI.B.1.i.b and VI.B.1.i.e, Bossemeyer separates (e.g., extracts) and parses, user data into subsets of **extracted data**, e.g., **limited access information** and/or **proprietary information**, and remainder data, e.g., public information. Various information of the **extracted data** is associated with respective **levels of security/accessibility** (e.g., **public limited access, restricted**). See, e.g., EX1005, 2:17-27 (“The information is stored by category (medical, financial, etc.) as well as **level of security (unrestricted, or public limited access, restricted)**.”). EX1003, ¶¶186-190.

For Ground 2, to the extent Patent Owner argues that Bossemeyer does not teach these limitations, Merenda discloses extracting by parsing security sensitive 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**.... [T]his might entail...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]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....”), ¶31 (“...Any of these data sets may be designated as including private data, and the *remaining data sets* include public data.”), Figures 1-3. EX1003, ¶¶286-289.

iii. [1/16b] storing said *extracted data* and said *remainder data* in said respective *extract stores* corresponding to an associated *security level* and said *remainder store*, respectively; and,

[10/22b] storing said *extracted data* and said *remainder data* in said *extract stores* and said *remainder store*, respectively; and

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 2) these limitations for the reasons in Section VI.B.1.i.e. EX1003, ¶¶191, 290.

Moreover, as discussed in Sections VI.B.1.i.b and VI.B.1.i.e, Bossemeyer teaches 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*) and *remainder data*. Bossemeyer also discloses storing *extracted data*, e.g., *restricted*

access data and *limited access data* in respective *extract stores* corresponding to their *security level* and the *remainder data* in the *remainder store*. Figure 3 illustrates this:

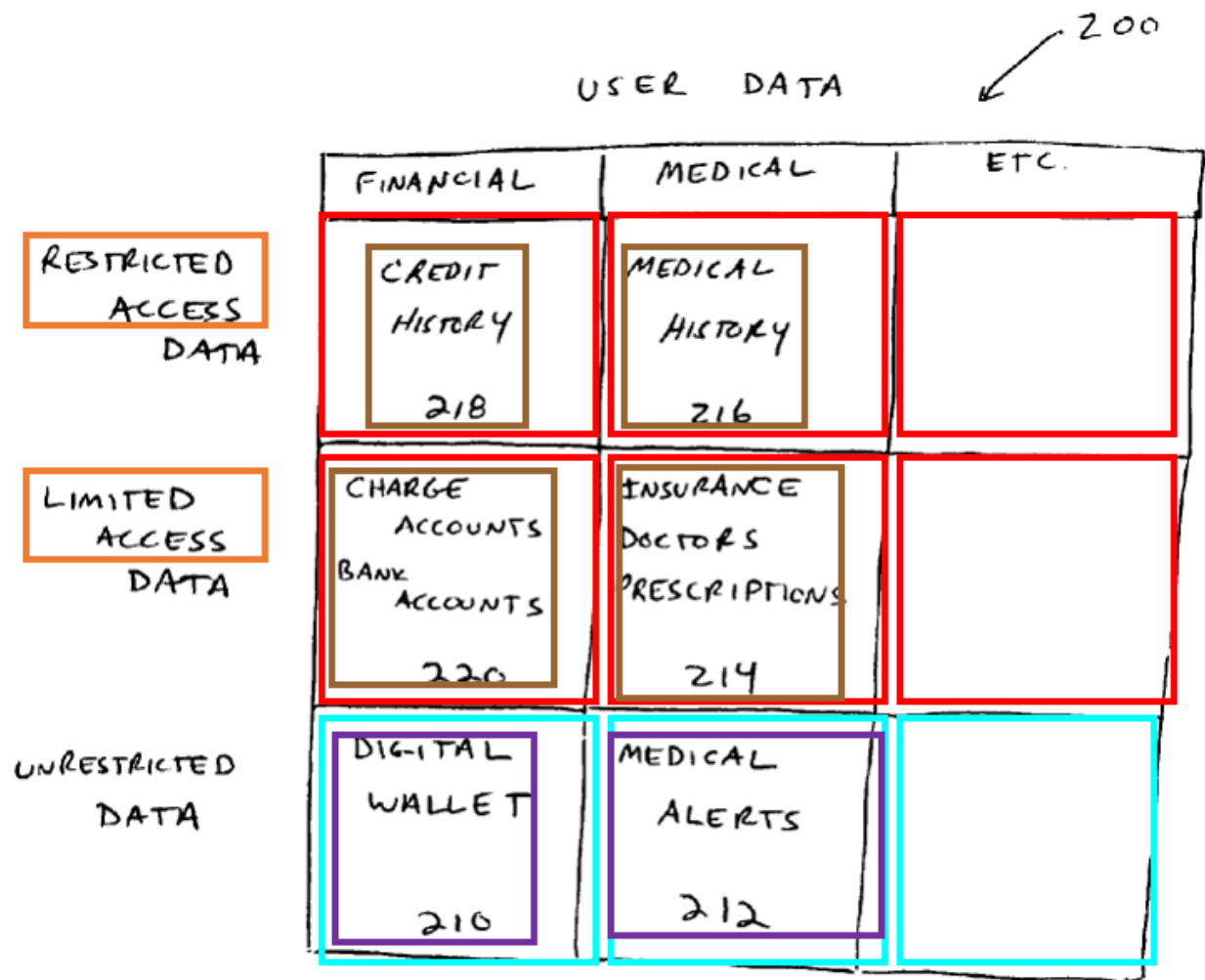


FIG. 3

EX1005, Figure 3; Figure 1. EX1003, ¶¶192-196.

For Ground 2, to the extent Patent Owner argues that Bossemeyer does not teach these limitations, Merenda discloses parsing data into *public data* (e.g.,

remainder data) and *private data* (e.g., *extracted data*) and storing that data as respective public data sets (e.g., *remainder store*) and private data sets (e.g., extract stores), which are preferably databases. As explained in Sections VI.B.1.i.a, VI.B.1.i.b, and VI.B.1.ii., Merenda discloses separating the data elements at any desired level of granularity resulting in multiple private data sets. EX1006, ¶24. Additionally, Merenda discloses providing differing levels of access, including determining access level on an element-by-element basis. *Id.*, ¶29 (“[A]ccess to the data elements in the *private data set* may be made on an element-by-element basis[—]the merchant may be provided with access to certain select pieces of private data...such as the *contact information* (*name, address, phone number, e-mail*) but not to other sensitive data such as *revenue, credit card* etc.”), ¶31. EX1003, ¶¶291-295.

iv. [1/10/22/16c] permitting full or partial reconstruction of said *data* via said *extracted data* from respective *extract stores* and *remainder data*

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 2) these limitations. EX1003, ¶¶197, 296.

As discussed in Sections VI.B.1.i.e and VI.B.1.ii, Bossemeyer discloses extracting *user data* to obtain *extracted data* and *remainder data* and storing *extracted data* in respective *extract stores* according to different levels of security. Bossemeyer also discloses permitting the full or partial reconstruction of the user

data, e.g., allowing access to the data stored at different memory locations (e.g., servers), using “user identification codes” or “data pointers.” EX1005, 3:3-18, 2:38-47 (“Different user identification codes, or data pointers, ... allow access to partitions in the database. The information contained... can be classified as public information...[,] limited access information...or proprietary information...”). EX1003, ¶¶198-201.

Specifically, Bossemeyer discloses that extracted and remainder data are retrieved from different memory locations, and are presented, e.g., at a terminal, based on a particular user’s authorization:

Once the user’s authorization has been verified...Routing circuitry... 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.

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. EX1003, ¶¶202-203.

As Dr. Zadok explains, when a merchant or bank initiates a financial transaction, partial or full reconstruction of user information enables the processing of the financial transaction, otherwise the transaction would fail. Bossemeyer's system retrieves **remainder data** (e.g., **public information** such as a customer's name), retrieves extracted data (e.g., **proprietary** or **limited access information** such as credit card numbers and account PIN/numbers), and merges these pieces of information (i.e., reconstruct the original information to appear as before it was split into different security categories). As Bossemeyer discloses, when the "[d]ata from these various locations is supplied back to the smart card terminal 14," (EX1005, 4:3-6), a POSITA would understand that said data is merged/reconstructed in that terminal, for example, it would be stored locally during the financial transaction, so that the terminal can use the information to effectuate the financial transaction. EX1003, ¶¶204-206.

For example, Bossemeyer discloses permitting reconstruction of some of a user's medical data (e.g., data including the user's **medical alerts 212**, and **insurance and prescription information 214**) and of all of the user's data (e.g., data further including the user's **medical history 216**) with additional authorization:

[O]nce 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.

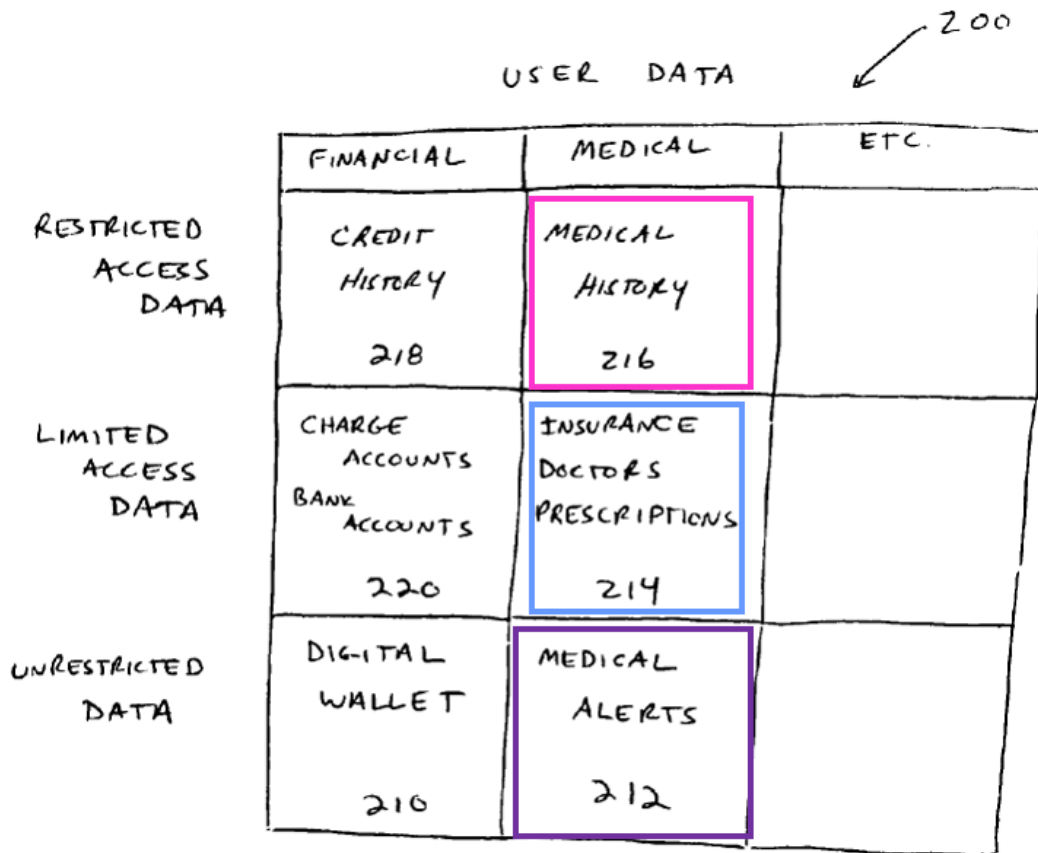


FIG. 3

EX1005, Figure 3. EX1003, ¶¶207-209.

For Ground 2, to the extent Patent Owner argues that Bossemeyer does not teach this limitation, Merenda discloses providing partial access to data (for example, access to public data or access to a subset of public and private data) and/or

complete access to the data. Merenda discloses providing access to public data (e.g., remainder data) without restriction. EX1006, ¶7. Merenda also discloses providing access to fully reconstructed data by combining the public and private data when the requester has a certain predetermined security clearance, for example, when the consumer has indicated that the requester, such as a merchant, can access private data. *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....*”). 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.*”), ¶30 (“[T]he combined information...may be provided to the merchant....”). Further, Merenda discloses accessing fully or partially reconstructed data based on any desired level of granularity. *Id.*, ¶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, ¶¶297-.

- v. [1/10/16/22d] only in the presence of a **predetermined security clearance** corresponding to said associated **security level** for said respective **extract stores**.

Bossemeyer discloses and/or renders obvious alone (or with Merenda for Ground 2) these limitations. EX1003, ¶¶210, 307.

First, Bossemeyer discloses permitting reconstruction of user 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... 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; 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**....[A]n **authorization code** generated by an encryption scheme known to the server provides a unique **access code** each time....

The network server 10, 110 validates the user identification by decrypting the *authorization code*....The merchant can then view the information stored....

EX1005, 4:50-65. EX1003, ¶¶211-213.

Second, Bossemeyer's *user identification codes* correspond to respective *security levels*, which as discussed in Sections VI.B.1.i.e, VI.B.1.ii, and VI.B.1.iii, correspond to respective *extract stores*. Bossemeyer discloses accessing a user's medical data by permitting partial reconstruction or full reconstruction 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 allow access to the 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 allow access to the user's medical data with “restricted access” security level (e.g., the user's *medical history 216*):

[I]nformation is stored in three levels of security: unrestricted, limited access, and restricted. [O]nce the *user's authentication code* and merchant code have been verified..., 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.

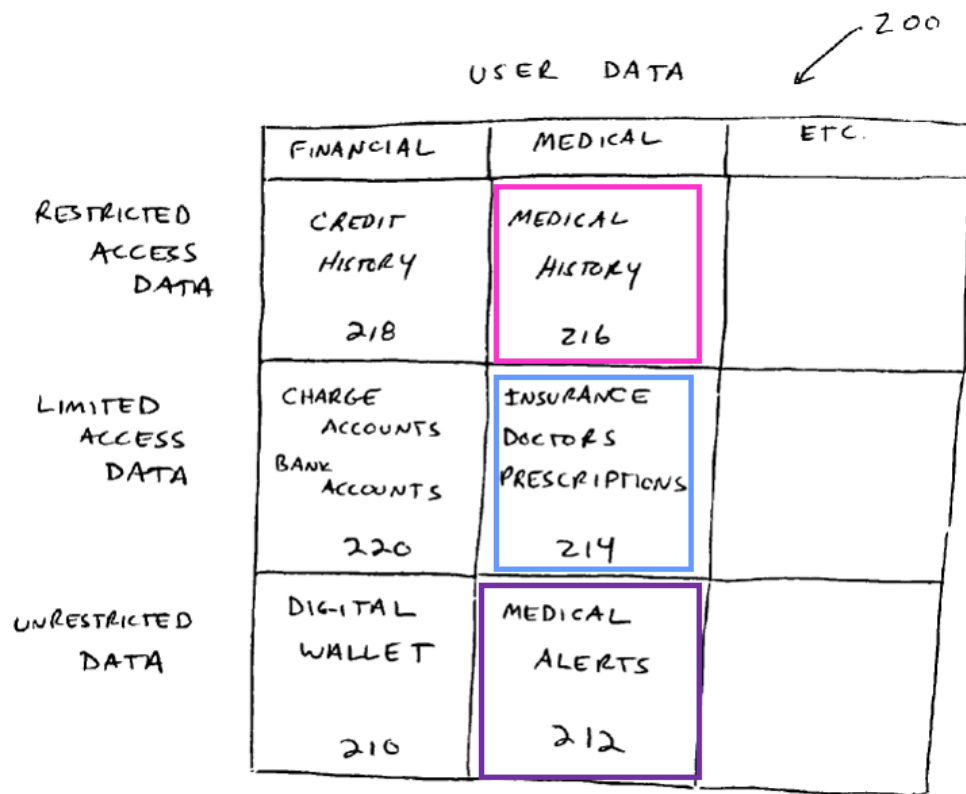


FIG. 3

EX1005, Figure 3. EX1003, ¶¶214-215.

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, ¶¶216-219.

For Ground 2, to the extent Patent owner argues that Bossemeyer does not teach this limitation, Merenda discloses providing partial access and/or complete access to the data only in the presence of predetermined security clearance for a respective security level. As discussed in Sections VI.B.1.i.a, VI.B.1.i.b, and VI.B.2.ii, Merenda discloses that private data sets can be assigned different security levels. For example, someone (e.g., merchant) requesting information can access *only certain portions of the private information*. After a merchant is “provided with access” (e.g., *a first predetermined security clearance*) to selected private data sets, the merchant can access those selected private data sets (e.g., private data sets having *a first security level*, such as name, address, phone number, e-mail). But without further authorization (e.g., *a second predetermined security clearance*), the merchant 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 214, such as the contact information...but not to other sensitive data....

EX1006, ¶29. EX1003, ¶¶308-309.

In Merenda, the predetermined clearance can be an indication by the owner of the information, e.g., a consumer. EX1006, ¶7 (“The private records would be

available only per the indication of the consumer to the merchant in the population.”), ¶10, ¶25; ¶¶8-9, 23-26, 29-30, 34-36. EX1003, ¶310.

The predetermined security clearance can be *a pass code* provided to a merchant. EX1006, ¶9 (“With *the pass code* the merchants are provided with the ability to view the particular consumers private data record in the private data set.”). EX1003, ¶¶311-312.

vi. Reasons To Combine Bossemeyer With Merenda⁴

A POSITA would have been motivated to combine Bossemeyer and Merenda to parse user data that includes private and non-private elements using a parsing algorithm, as taught by Merenda, to extract private elements and store them separately from non-private elements, and include Merenda’s techniques of user data entry. EX1003, ¶313.

As an initial matter, a POSITA would have understood that to “parse” means to segment or break up the data. EX1003, ¶314.

First, the combination 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

⁴ These reasons apply to the entirety of Grounds 2, 4, and 6.

controlling the access. The combination would merely involve using Merenda's data parsing technique (parsing algorithm) in Bossemeyer's system according to 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; 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... or in such a manner as to protect the privacy concerns of the consumer."), ¶26; *see also*, EX1005, 2:40-55, 4:50-65, 5:6-31; EX1006, ¶¶10-13, 23, 29, 34-35. EX1003, ¶¶315-320.

Moreover, the combination would merely use Merenda's methods of entering data, e.g., using a Web form, in Bossemeyer's system where both teach populating

data by the user's actions. *Compare* EX1005, 5:23-31 *with* EX1006, ¶7 (“[D]ata entered by a consumer into a Web form is separated into related records in a public and private data set.”), ¶¶8, 26, 31–32, 34. EX1003, ¶¶321-322.

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*....” *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, ¶¶323-326.

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. EX1003, ¶327.

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. The combination would also permit users of Bossemeyer's system to enter data using Merenda's techniques (e.g., web form entry) and to indicate user preferences such as desires to be contacted by certain merchants. *See, e.g.*, EX1006, ¶¶31, ¶34. EX1003, ¶¶328-331.

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 and data entry) 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, ¶¶332-334.

Fifth, Merenda provides express motivations that would have led a POSITA to combine Merenda and Bossemeyer. 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....” EX1006, ¶3. Merenda recognizes that “[t]he overwhelming benefits attendant to this ubiquity, however, are counterbalanced...by the inevitable loss of privacy associated with accessing a global computer network.” *Id.* Merenda also discloses that “merchants seeking to leverage data about Internet user[]s to better focus their marketing efforts

must do so in a manner that respects the privacy interests of their intended customer.”

Id., ¶4. EX1003, ¶¶335-337.

Merenda provides examples of the benefits of its methods for respecting the privacy interests of the public. For 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:

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. 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... select merchant to whom they wish their private data to be provided.”). Merenda’s method also allows merchants to data mine or statistically process the customer’s private information. *Id.*, ¶¶12, 5. EX1003, ¶¶338-339.

A POSITA would have found that Bossemeyer and Merenda were analogous to or reasonably pertinent to the particular problem of the ’987 Patent. EX1003, ¶¶340-341.

A POSITA would also have had a reasonable expectation of success in combining Bossemeyer with Merenda. The combination would merely involve including known data entry methods (e.g., web form entry) and parsing user data 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. EX1006, ¶23. EX1003, ¶¶342-344.

2. Dependent Claims 6 and 21

i. [6pre] A method as claimed in claim 1 including

[21pre] A storage medium with programming instructions as claimed in claim 16 including

Bossemeyer alone (or with Merenda for Ground 2) renders obvious claims 1 and 16. *See* Section VI.B.1. EX1003, ¶¶220, 345.

ii. [6/21a] establishing a plurality of security levels each with a respective security clearance

Bossemeyer discloses this limitation. EX1003, ¶221.

As discussed in Section VI.B.1.ii, Bossemeyer discloses establishing a plurality of security levels. Bossemeyer further discloses that each *security level* has a *security 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* (or “*information*”) 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; 4:50-59. For example, a merchant with a corresponding code can access the allowed information. EX1005, 4:59-65 (“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...*”); Figure 2. EX1003, ¶¶222-225.

As another example, Bossemeyer describes 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*. [O]nce the user’s authentication code and merchant code have been verified...the pharmacist may have access to...*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.

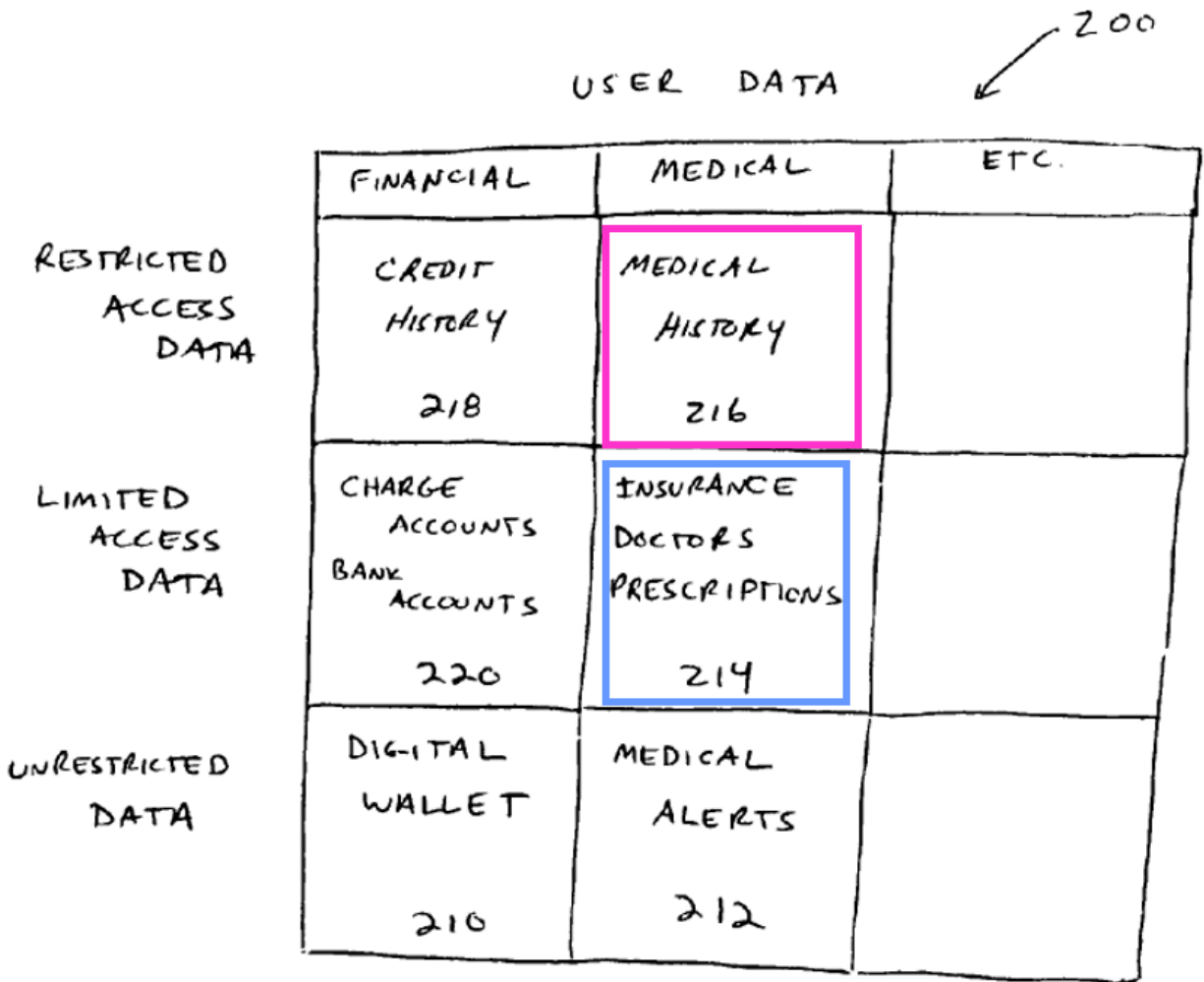


FIG. 3

EX1005, Figure 3. EX1003, ¶¶226-227.

For Ground 2, Merenda discloses a method for securing data by separating the data into public and private or sensitive data sets and allowing access to that data based on predetermined security clearances. EX1006, ¶25. Public data may be available without restriction, while private or sensitive data would only be available based on the predetermined level(s) indicated, for example, by the consumer (e.g.,

the individual who provides the data) or the level of control indicated for the data set:

...[A] public data set is available, without restriction, to the entire population of Internet users, or... to a select subset of merchants 107 who subscribe to a marketing service that accumulates such data.... The present invention is directed toward...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..... Other items of information, such as the name, location, phone, e-mail, revenue, number of employees, may...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, ¶¶346-354.

Merenda discloses, or renders obvious, a plurality of security levels for the private data sets. 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*).

*[A]ccess 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, ¶¶355-357.

- iii. **[6/21b] each said subset of said security sensitive words, characters or icons being correlated with said plurality of security levels and**

Bossemeyer discloses this limitation. EX1003, ¶¶228, 358.

As discussed in Sections VI.B.1.i.e and VI.B.1.ii, Bossemeyer discloses that each subset of the security sensitive words, characters or icons are stored in the plurality of physically distinct extract stores corresponding to the plurality of security levels. Thus, each subset is correlated with the plurality of security levels.

EX1003, ¶229.

- iv. **[6/21c] the step of permitting reconstruction including the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.**

Bossemeyer discloses this limitation. EX1003, ¶¶230, 359.

As discussed in Sections VI.B.1.v-VI.B.1.v, Bossemeyer discloses permitting a partial reconstruction of the user data in the presence of a predetermined security clearance levels. EX1003, ¶231.

Bossemeyer further discloses using its computer system to reconstruct the user data from transactions involving multiple partial reconstructions. For example, Bossemeyer describes reconstructing user data by a pharmacist's request to access "insurance and prescription information 214" (correlated with the "limited access" level) and a request by other merchants (e.g., automotive dealership, bank officer) to access the user's "credit history" (correlated with the "restricted access" level). EX1005, 3:6-22, 3:53-4:6, 5:6-22. A POSITA would have understood that Bossemeyer (and the Bossemeyer/Merenda) system allowed transactions with different requesters (e.g., pharmacists, commercial merchants, financial officers) and thus permitted a plurality of partial reconstructions. *Id.*, 3:6-22, 3:53-4:6, 5:6-22, 4:23-42 (merchants A and B can use Bossemeyer's system). EX1003, ¶¶232-235.

As another example, when a user visits a health provider (e.g., "dentist/doctor") and makes a credit card payment for medical services, that transaction would request medical history information and charge/credit or bank information that have different security levels (e.g., restricted access data such as medical history, limited access data such as charge/bank accounts). *See* EX1005,

Figure 3. Thus, a POSITA would understand that such a medical service transaction requires a plurality of reconstructions from information received from servers with different security levels. EX1003, ¶¶236-237.

Accordingly, a POSITA would understand that Bossemeyer discloses permitting “a plurality of partial reconstructions” of the user data “in the presence of respective ones of said plurality of security clearance levels.” EX1003, ¶238.

3. Dependent Claim 9

i. [9pre] A method as claimed in claim 1 including

Bossemeyer alone (or with Merenda for Ground 2) renders obvious claim 1. *See* Section VI.B.1. EX1003, ¶¶239, 360.

ii. [9a] assessing a charge for extracting, storing or permitting reconstruction.

Bossemeyer renders obvious this limitation. EX1003, ¶¶240, 361.

At the outset, the '987 Patent admits that assessing a charge to a merchant or user during the data securing stage or reconstruction stage was well known in the art. EX1001, 45:34-46:34, Figure 13. For example, the '987 Patent explains that “charge systems are known” for “security service” (EX1001, 46:11-16), and “[i]t is well known that vendors selling goods and services over the Internet are willing to pay a certain percentage of their sales revenue to other entities referring customers to the vendor’s web sites” (EX1001, 45:46-49). EX1003, ¶¶241-243.

Bossemeyer also teaches that data is stored by charging a subscription fee to merchants and users:

Data is stored in the server in several ways. Merchant profiles become populated *when a merchant subscribes* to the service.... Similarly, the user data becomes populated *when the user subscribes* as part of the smart card activation process. Additional data is created as the user and the merchants interact with the system.

EX1005, 5:23-31. Thus, a POSITA would have understood that Bossemeyer's computer system could assess a subscription charge to merchants and users for extracting, storing, or permitting reconstruction of the user data during their transactions, and charging a fee was a well-known technique. *See* EX1005, 5:23-31; EX1001, 45:34-46:34. Thus, a POSITA would have found it obvious to assess and charge a fee to meet this limitation. EX1003, ¶¶244-246.

4. Dependent Claims 11 and 23

i. [11pre] A method as claimed in claim 10

[23pre] A storage medium with programming instructions as claimed in claim 22

Bossemeyer alone (or with Merenda for Ground 2) renders obvious claims 10 and 22. *See* Section VI.B.1. EX1003, ¶¶247, 362.

ii. [11/23a] wherein the step of parsing parses the data granularly.

Bossemeyer alone (or with Merenda for Ground 2) renders obvious this limitation for the reasons in Sections VI.B.1.i.b and VI.B.1.ii. A POSITA would have understood that the data Bossemeyer parses is necessarily at *some* granularity (e.g., fine, coarse), because it is smaller than the whole of the original data prior to parsing. EX1003, ¶¶248-249, 363.

For Ground 2, Merenda discloses parsing the data elements at any desired level of granularity resulting in multiple private data sets. *See*, EX1006, ¶24 (“[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 and in the combination of individually public data sets 103, 104 into a combined private data set 105.”); ¶23 (“[T]he notion that such separation, at various levels of sophistication and granularity can, and does occur, is essential to the practice of the invention.”). EX1003, ¶¶364-365.

Additionally, Merenda discloses providing differing levels of access, including determining access level on an element-by-element basis. EX1006, ¶29 (“[A]ccess to the data elements in the *private data set* may be made on an element-by-element basis[—]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, ¶¶366-367.

5. Dependent Claims 15 and 27

- i. [15pre] A method as claimed in claim 10 including
[27pre] A storage medium as claimed in claim 22 including**

Bossemeyer alone (or with Merenda) renders obvious claims 10 and 22. *See* Section VI.B.1. EX1003, ¶¶250, 368.

- ii. [15/27a] a further data security step of one from the group of storing said data without encryption, storing said data with encryption and destroying said data; said further data security step being independent of said parsing, storing and permitting reconstruction.**

As an initial matter, the claimed “further data security step” does not impose a narrowing limitation on the claimed “data.” That is, the “data” will either exist (stored with or without encryption) or will not exist (get destroyed). In any case, Bossemeyer alone (or with Merenda) renders obvious this limitation. EX1003, ¶¶251-253.

First, Bossemeyer discloses that, in some examples, the user data is “stored on the smart card.” EX1005, 3:52-4:6 (“Data from these various locations [(e.g., medical, financial institutes) is supplied back to the smart card terminal 14, and *if appropriate, the data stored on the smart card 12* is updated.”), 5:27-31 (“[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 the merchants interact with the system.”). In those examples, Bossemeyer’s smart card stores user data (as it could be later “updated”), for example, by the user’s entry of data upon activation, before sending the data to the network smart card server (central database server). EX1005, 4:3-6, 5:28-30. Moreover, Bossemeyer describes that the data stored in the smart card may or may not be encrypted because it optionally has an “encryption capability.” EX1005, 3:28-38. Accordingly, a POSITA would have understood that Bossemeyer’s smart card can store user data with or without encryption, and that such storing is independent of parsing, storing, and reconstruction using parsed data as the storing is unrelated to the separation of sensitive content at the central database server. Bossemeyer thus teaches this limitation. EX1003, ¶¶254-258.

Second, Bossemeyer, alternatively, discloses destroying user data in the smart card after the user data is sent to the network smart card server because its system could “reduce[] the amount of information which must be stored... to each smart card 12 and enable[] data to be shared across groups of cards” by using data pointers to access information in remote servers. EX1005, 2:58-63, 4:7-17, Abstract. Bossemeyer explains that such an approach supports “complex applications which may... require more resources than could be economically stored or transferred to the smart card 12” by deleting user data in the card and storing data elsewhere. EX1005, 2:63-3:2 (“...This allows greater capacity than could otherwise be

achieved by storing information on the cards alone.”). Thus, a POSITA would have understood that, in some examples, Bossemeyer deletes the smart card’s user data that is transferred to and stored in remote servers to avoid requiring a large storage capacity in the card, and the deletion is independent of parsing, storing, and reconstruction using parsed data because the storing is unrelated to the separation of sensitive content at the central database server. Bossemeyer thus teaches this limitation. EX1003, ¶¶259-263.

For Ground 2, Bossemeyer discloses that “the user data becomes populated when the user subscribes as part of the smart card activation process.” EX1005, 5:28-30. Merenda discloses that a user enters data through a website on the user’s computer device. EX1006, ¶7. Like Bossemeyer, Merenda discloses that the user data provided by the user is “separated” into parts. *Id.*, ¶7 (“[D]ata entered by a consumer into a Web form is *separated* into related records in a public and private data set.”), ¶¶23-24, 34, Figures 1, 4. EX1003, ¶¶369-375.

A POSITA would have found obvious to use Merenda’s method of entering user data through a website, when a user subscribes to Bossemeyer’s smart card services, because using a website and the Internet was a ubiquitous way of signing up to different services from different providers. A POSITA would have also reasonably inferred that the user data, including the entered data, is later destroyed because it ceased to exist and would have to be reconstructed by later

“aggregat[ing]” its separated elements (EX1006, ¶32), as well as to preserve the privacy of the user signing up for Bossemeyer’s smart card services, when, for example, the user signs up for those services from public computers. *See In re Preda*, 401 F.2d 825, 826 (C.C.P.A. 1968). For example, in the Bossemeyer/Merenda system, the user data being moved from the user’s computer device to the central database server would cease to exist in its original form, and thus a POSITA would have understood that the entered user data is destroyed. A POSITA would have understood that the destruction in the user’s computer is independent of parsing, storing, and reconstruction using parsed data that occurs elsewhere (e.g., the central database). EX1003, ¶¶376-381.

C. Grounds 3-4: Claim 9 Is Obvious Over Bossemeyer With Chaganti (Ground 3) Or Bossemeyer With Merenda And Chaganti (Ground 4)

1. Dependent Claim 9

i. [9pre] A method as claimed in claim 1 including

Bossemeyer alone (or with Merenda) renders obvious claim 1. *See* Section VI.B.1. EX1003, ¶¶382, 408.

ii. [9a] assessing a charge for extracting, storing or permitting reconstruction.

Bossemeyer/Chaganti (Ground 3) and Bossemeyer/Merenda/Chaganti (Ground 4) render obvious this limitation for the reasons in Section VI.B.3.i. EX1003, ¶¶383, 409-410.

Additionally, Chaganti discloses this limitation. Chaganti describes a computer system (e.g., Personal Information Repository Service Provider (PIRSP)) for storing personal information assigned with a plurality of security levels and providing the information upon a request. *See, e.g.,* EX1007, 2:22-43, 5:29-42. Chaganti also discloses that the operation of its system is based on “*fee[s]*” which “is calculated based on a per transaction basis, or on a subscription basis, either *from users that store information or from entities that request such information.*” EX1007, 5:43-56, 9:1-14 (“The user account management module 112 optionally allows the user 103 to select a *payment plan for the services* rendered by the PIRSP....”), 10:30-42 (“The server computer 100... enables [potential requesters] to establish a *payment/billing plan* for accessing information objects stored by the user 103.”), 12:42-67 (“[T]he requester 105 is *charged a fee* for receiving the information objects, on a per-object basis, or on a subscription basis....”). EX1003, ¶¶384-393.

It would have been obvious to modify Bossemeyer and/or the combined Bossemeyer/Merenda system to charge a fee for securing data (by extracting sensitive content), storing it, or reconstructing it, as taught by Chaganti. A POSITA would have been motivated to include assessing and charging a fee in the modified systems to generate revenue and improve the database of the computer system for securing data, including to share a portion of the revenue with the user. EX1007,

5:43-56 (“These payment methods (e.g., fee per transaction, subscription basis...)... generate... sources of revenue for the PIRSP via advertisements, referrals, introductions, chain marketing methods...”), 12:52-56 (“The PIRSP may provide an incentive to the user 103 by paying a portion of the fee to the user 103.”). Charging a subscription fee was well known and a routine system design choice. EX1005, 5:23-31 (“Merchant profiles become populated when a merchant *subscribes* to the service.... [T]he user data becomes populated when the user *subscribes* as part of the smart card activation process.”); EX1007, 12:52-54 (“[T]he requester 105 is charged a fee for receiving the information objects....”). Thus, a POSITA would have found it obvious to try and place an assessment and fee charging system in the computer system. EX1003, ¶¶394-398, 410.

A POSITA would have had a reasonable expectation of success to make the combination because it amounts to a simple combination of known techniques and components to build a system with a subscription on charge-by-transaction service. Indeed, charged-based systems were known. *See, e.g.*, EX1005, 5:23-31; EX1007, 5:43-56, 10:30-42, 12:42-67; EX1021, ¶48 (“Upon request by a third party merchant or service provider 27, a profile or aggregate of consumer information may be provided to the third party merchant or service provider by the information bank 23 *for a fee.*”), ¶¶61-63; EX1022, 8:64-67 (“By participating in the massive archival of all firm data at a central service bureau 20, a service bureau 20 can organize all these

data and coordinate dissemination of such data *for a rental fee or user fee.*”); EX1023, 6:59-63 (“When used in conjunction with the registration key this allows for *fee based* or commercial control of access to the high precision navigational data.”); EX1024, p.1 (“We envision a cooperative utility in which consumers *pay a monthly fee* in exchange for access to persistent storage.”). EX1003, ¶¶399-404.

A POSITA would have found that Chaganti was analogous to or reasonably pertinent to the particular problem of the ’987 Patent. EX1003, ¶¶405-406.

D. Grounds 5-6: Claims 15 And 27 Are Obvious Over Bossemeyer With Kohane Or Bossemeyer With Merenda and Kohane

1. Dependent Claims 15 and 27

- i. [15pre] A method as claimed in claim 10 including
[27pre] A storage medium as claimed in claim 22 including

Bossemeyer alone (or with Merenda) renders obvious claims 10 and 22. *See* Section VI.B.1. EX1003, ¶¶411, 433.

- ii. [15/27a] a further data security step of one from the group of storing said **data** without encryption, storing said **data** with encryption and destroying said **data**; said further data security step being independent of said parsing, storing and permitting reconstruction.

Bossemeyer/Kohane (Ground 5) and Bossemeyer/Merenda/Kohane (Ground 6) render obvious this limitation for the reasons in Section VI.B.5.ii. EX1003, ¶¶412, 434.

Additionally, Kohane teaches this limitation. *First*, Kohane discloses a networked computer system where gateway server system 22 receives “object records” (e.g., user data such as dental, medical, legal information) from various agent systems, encrypts the records, and sends them to servers 18 (e.g., remote storages). *See, e.g.*, EX1008, ¶¶24, 26, 32, 30, 37, 42. Specifically, Kohane explains that “gateway server system 22 encrypts the record objects” to secure transmission to the servers 18. EX1008, ¶58. Kohane further discloses that, “[o]n the gateway server system 22, *each record objects remains in encrypted form*” except when certain record objects are “decrypted” when an authorized agent accesses them. EX1008, ¶59. Because the gateway server system 22 maintains the record objects only in encrypted form, a POSITA would have reasonably inferred that the original unencrypted data would have been destroyed after encryption, specifically to ensure no one without an encryption/decryption key could access and review the data. *See In re Preda*, 401 F.2d 825, 826 (C.C.P.A. 1968). EX1003, ¶¶413-419.

It would have been obvious to modify Bossemeyer and the combined Bossemeyer/Merenda system to store the user data with encryption and then destroy the unencrypted version as taught by Kohane. A POSITA would have been motivated to encrypt the data and destroy its original version to secure and maintain confidentiality when transmitting the parsed data between Bossemeyer’s network smart card server and other remote databases (e.g., credit card companies, insurers,

health care providers). EX1008, ¶58 (“[S]uch record objects traverse the network 20 in encrypted form when the gateway server system 22 uploads the record objects to the server 18.... Consequently, the information in the record objects remain unintelligible to anyone who intercepts the transmission of the record objects between the gateway server system 22 and the server 18...”), ¶57 (“[T]he confidentiality of the information stored in the records is of utmost importance.”). Thus, a POSITA would have found it obvious to store the data with encryption and destroy the original version for confidentiality and prevent unauthorized access of the data. The storing and destruction are independent of parsing the user data step, and the storing of and reconstruction by using the parsed data steps. A POSITA would have had a reasonable expectation of success because it amounts to a simple combination of known techniques and components to encrypt information and remove unencrypted information to secure the system. EX1003, ¶¶422-423, 426.

Second, Kohane discloses that, in some examples, the agent systems (e.g., personal computer, smart card, measurement equipment) destroy its user data to secure information:

Data security can be enhanced at the agent systems 14, 16, 26 by not storing any record objects at the agent systems 14, 16, 26. Accordingly, after the agent completes reviewing the record object, ***the agent system 14, 16, 26 deletes the corresponding information*** from the respective

agent system, including all downloaded files and cached copies of the downloaded Web page.

EX1008, ¶63. EX1003, ¶¶420-421.

It would have been obvious to modify Bossemeyer's system and the combined Bossemeyer/Merenda system to delete the user data in devices (e.g., smart card, personal computers) connected to Bossemeyer's central database server once the devices finish utilizing the data, as taught by Kohane. A POSITA would have been motivated to delete the user data residing in those devices to reduce the required storage capacity and increase data security. EX1005, 2:58-3:2 ("This...facilitates more complex applications which may otherwise require more resources than could be economically stored or transferred to the smart card 12."), EX1008, ¶63 ("Data security can be enhanced at the agent systems...by... delet[ing] the corresponding information."). The deletion of the data is independent of parsing the user data step, and the storing of and reconstruction using the parsed data steps. EX1003, ¶¶424-425.

A POSITA would have had a reasonable expectation of success to make the combination because it amounts to a simple combination of known techniques and components for deleting information in computers, which was a routine practice, *see, e.g.*, EX1001, 24:1-2 ("Deletion systems are known to persons of ordinary skill in the art."); EX1025, 6:57-60 ("After the object is copied..., the original copy of

the object can be deleted which allows the space to be reclaimed....”), for example, deleting user data residing in devices where the data is stored in remote servers, EX1008, ¶¶41, 63. EX1003, ¶¶427-428.

A POSITA would have found that Kohane was analogous to or reasonably pertinent to the particular problem of the ’987 Patent. EX1003, ¶¶429-432.

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 at 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 Final Written Decision is expected in December 2024.⁵ Although trial is currently scheduled for August 19, 2024 (EX1010), the Board recognizes “that scheduled trial dates are unreliable and often change.” EX1033, 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.” EX1033, 9.

The co-pending district court case was filed in the Eastern District of Texas 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). EX1011, 1. Accordingly, the projected trial date for purposes of *Fintiv* is 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 in December 2024. Because the projected trial date based on the two most recent

⁵ December 2024 is 18 months after June 2023, when Petitioner expects a notice of accorded filing date.

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, and the investment in it has been minimal. *See* EX1009, 1010. 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 (PTAB Jan. 6, 2021). Further, the Markman hearing is not scheduled until March of 2024. EX1009, 4.

Moreover, Patent Owner served their infringement contentions on Petitioner and confirmed which claims were being asserted only on February 28, 2023. EX1012. Under *Fintiv*, Petitioner’s prompt filing “weigh[s] against exercising the authority to deny institution.” *Fintiv*, Paper 11 at 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 at 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 Claims 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.” Memo, 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.” Memo, 4. Here, the Petition plainly shows that the ’987 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 '987 patent prosecution. The PTO has not previously considered Bossemeyer or Merenda. 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, ¶¶94-435. 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 9, 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 '987 patent is or was involved in the following case:

Case Heading	Number	Court	Date
<i>DigitalDoors, Inc. v. International Business Machines Corporation</i>	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
Desmarais LLP
230 Park Ave
New York, NY 10023

Phone: (212) 351-3400
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

Case IPR2023-00969
U.S. Patent No. 7,349,987

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 13,993. 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 9, 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. 7,349,987;
- Exhibit List;
- Exhibits 1001-1033;
- 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 9, 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

Case IPR2023-00969
U.S. Patent No. 7,349,987

Dated: June 9, 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