

Case IPR2023-00967
U.S. Patent No. 7,313,825

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INTERNATIONAL BUSINESS MACHINES CORPORATION
Petitioner

v.

DIGITAL DOORS, INC.
Patent Owner

IPR2023-00967
U.S. Patent No. 7,313,825

**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 '825 Patent.....	3
A. Overview Of The '825 Patent	3
B. Prosecution History Of The '825 Patent	7
C. Priority Date Of The '825 Patent	10
IV. Level Of Ordinary Skill In The Art.....	11
V. Claim Construction.....	11
VI. Relief Requested And The Reasons For The Requested Relief.....	11
A. Challenged Claim and Statutory Grounds for Challenge.....	11
1. Bossemeyer	12
2. Glick.....	19
3. Carmichael	23
B. Grounds 1-2: Claim 81 Is Obvious Over Bossemeyer With Glick (Ground 1) Or Bossemeyer With Glick And Carmichael (Ground 2)	26
1. [81pre] A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective extract stores with security access controls thereat, said security sensitive words, characters, data objects or icons extracted from said data to obtain extracted data and remainder data which extracted data is stored in respective extract stores corresponding to a respective security level of said	

	extract stores, said computer system having at least one portable computing device locatable with current location data, comprising:	26
2.	[81a] determining when said portable computing device is within a predetermined region based upon said current location data;	51
3.	[81b] permitting full or partial reconstruction of said data via said extracted data from said extract stores and remainder data.....	53
4.	[81c] only in the presence of a predetermined security clearance access control corresponding to said respective security level and	57
5.	[81d] only when said portable computing device is not beyond said predetermined region.....	60
6.	Reasons To Combine Bossemeyer With Glick (And Carmichael For Ground 2)	63
VII.	Discretionary Denial Would Be Inappropriate.....	74
A.	Discretionary Denial Under The <i>Fintiv</i> Factors Is Not Appropriate.....	74
1.	No evidence regarding a stay	74
2.	Parallel proceeding trial date	75
3.	Investment in the parallel proceeding.....	76
4.	Overlapping issues with the parallel proceeding	76
5.	Identity of parties	77
6.	Other circumstances.....	77
B.	Discretionary Denial Under 35 U.S.C. § 325(D) Is Not Appropriate.....	78
VIII.	Conclusion	78

IX.	Mandatory Notices.....	80
A.	Real Party-in-Interest	80
B.	Related Matters.....	80
C.	Lead and Back-up Counsel and Service Information	80

TABLE OF AUTHORITIES

<u>Cases</u>	<u>Pages(s)</u>
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020)	73, 75
<i>Dish Network L.L.C. v. Broadband iTV, Inc.</i> , IPR2020-01359, Paper 15 (Feb. 12, 2021)	73
<i>Intel Corp. v. PACT XPP Schweiz AG</i> , 61 F.4th 1373 (Fed. Cir. 2023)	64, 69
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007)	passim
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013 (Fed. Cir. 2017)	10
<i>PEAG LLC v. Varta Microbattery GmbH</i> , IPR2020-01214, Paper 8 (Jan. 6, 2021)	75
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	10
<i>Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC</i> , IPR2019-01393, Paper 24 (PTAB June 16, 2020)	73, 75
 <u>Statutes</u>	
35 U.S.C. § 311	1
35 U.S.C. § 314	73
35 U.S.C. § 325(D)	76
35 U.S.C. §102(e)	11, 18, 22
35 U.S.C. §103	11
35 U.S.C. §314(a)	1, 11

Rules

37 C.F.R. § 42.100	1
37 C.F.R. § 42.100(b)	10
37 C.F.R. § 42.104(a).....	2

EXHIBIT LIST

Exhibit No.	DESCRIPTION
1001	U.S. Patent No. 7,313,825 to Redlich et al.
1002	Prosecution History of U.S. 7,313,825
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. Patent No. 6,985,588 to Glick et al.
1007	U.S. Patent No. 7,913,919 to Carmichael et al.
1008	U.S. Publication No. 2004/0148290 to Merenda 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. Provisional Application No. 60/400,062
1014	U.S. Provisional Application No. 60/400,112
1015	U.S. Provisional Application No. 60/400,406
1016	U.S. Provisional Application No. 60/400,407
1017	U.S. Patent No. 7,322,047 (Continuation-in-part Application No. 10/277,196)
1018	U.S. Patent No. 7,349,987 (Continuation-in-part Application No. 10/155,192)
1019	U.S. Patent No. 7,191,252 (Continuation-in-part Application No. 10/155,525)
1020	U.S. Patent No. 7,140,044 (Continuation-in-part Application No. 10/008,209)
1021	U.S. Patent No. 7,146,644 (Continuation-in-part Application No. 10/008,218)
1022	U.S. Patent No. 7,103,915 (Continuation-in-part Application No. 09/916,397)

Exhibit No.	DESCRIPTION
1023	Microsoft Computer Dictionary, Fourth Edition, Copyright 1999, Excerpts
1024	Beck et al., Linux Kernel Internals, 2nd Ed., Copyright 1998, pp. 148-187
1025	DOD Standard, Department of Defense Trusted Computer System Evaluation Criteria, December 26, 1985 (“Orange Book”)
1026	Director of Central Intelligence Directive No. 1/16, Security of Compartmented Computer Operations (“CIA”)
1027	U.S. Patent No. 5,960,080 to Fahlman et al. (“Fahlman”)
1028	U.S. Patent No. 6,370,629 to Hastings et al. (“Hastings”)
1029	U.S. Patent No. 6,253,203 to O’Flaherty et al. (“O’Flaherty”)
1030	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 claim 81 (the “Challenged Claim”) of U.S. Patent No. 7,313,825 (“’825 Patent,” EX1001).

The Challenged Claim recites a method of securing data by separating and securing sensitive portions of the data and then controlling access to the sensitive data based on a security clearance and a portable device location. Digital Doors Inc. (“Digital Doors” or “Patent Owner”) obtained the Challenged Claim by arguing during prosecution that the prior art considered by the Examiner did not teach or suggest security-controlled memories with corresponding security access control and storing security sensitive data in respective security-controlled memories corresponding to a respective security level. In response to Patent Owner’s arguments, the Examiner noted that the prior art teaches separating data based on security levels and storing the data and allowing full or partial reconstruction of data based on a respective security clearance. However, the Examiner concluded that the considered prior art failed to teach storing only the security sensitive data for each security level at security-controlled memory for each security level and storing the remainder data at a separate memory location.

But what got the Challenged Claim allowed was an application of a well-known technology to a known problem. This Petition demonstrates that separating and securing sensitive data was known (EX1005, “Bossemeyer”), portable devices to access data were also known (EX1006, “Glick” and EX1007, “Carmichael”), controlling access to security sensitive data based on a corresponding security level was known (Bossemeyer), and controlling access based on location was known (Glick and Carmichael), and it would have been obvious to combine the prior art teachings.

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

II. Grounds For Standing

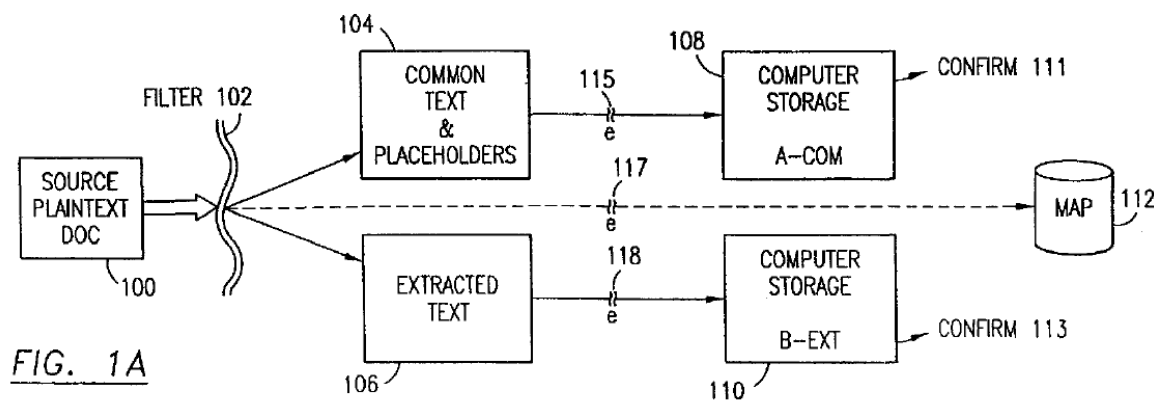
Petitioner certifies that the '825 Patent is eligible for IPR and that Petitioner is not barred or estopped from requesting IPR challenging the patent claims. 37 C.F.R. § 42.104(a).

III. Summary Of The '825 Patent

A. Overview Of The '825 Patent

The '825 Patent relates to “a process, program and system which operates to secure files and data objects in portable computing devices.” EX1001, 1:23-26.

Figure 1A, reproduced below, illustrates the disclosed data security system:



EX1001, Figure 1A. As shown, source document 100 which contains data is passed through filter 102. EX1001, 19:32-24. “Filter 102... separates out common text or remainder data 104 from uncommon text, words, characters, icons, or data objects.” EX1001, 19:45-48. The common data objects are then placed into remainder document or common data file 104, and the uncommon words (or security sensitive words) are placed into a separate extracted text or extracted data file 106. EX1001, 19:55-61. The remainder data and extracted data are then stored separately, with the remainder data stored in common storage memory 108, and the extracted data file

106 stored in a different memory computer storage 110. EX1001, 20:50-64. See EX1003, ¶¶51-55, 83-89.

As shown in Figure 14 below, the system can be portable, such as portable computing device 810.

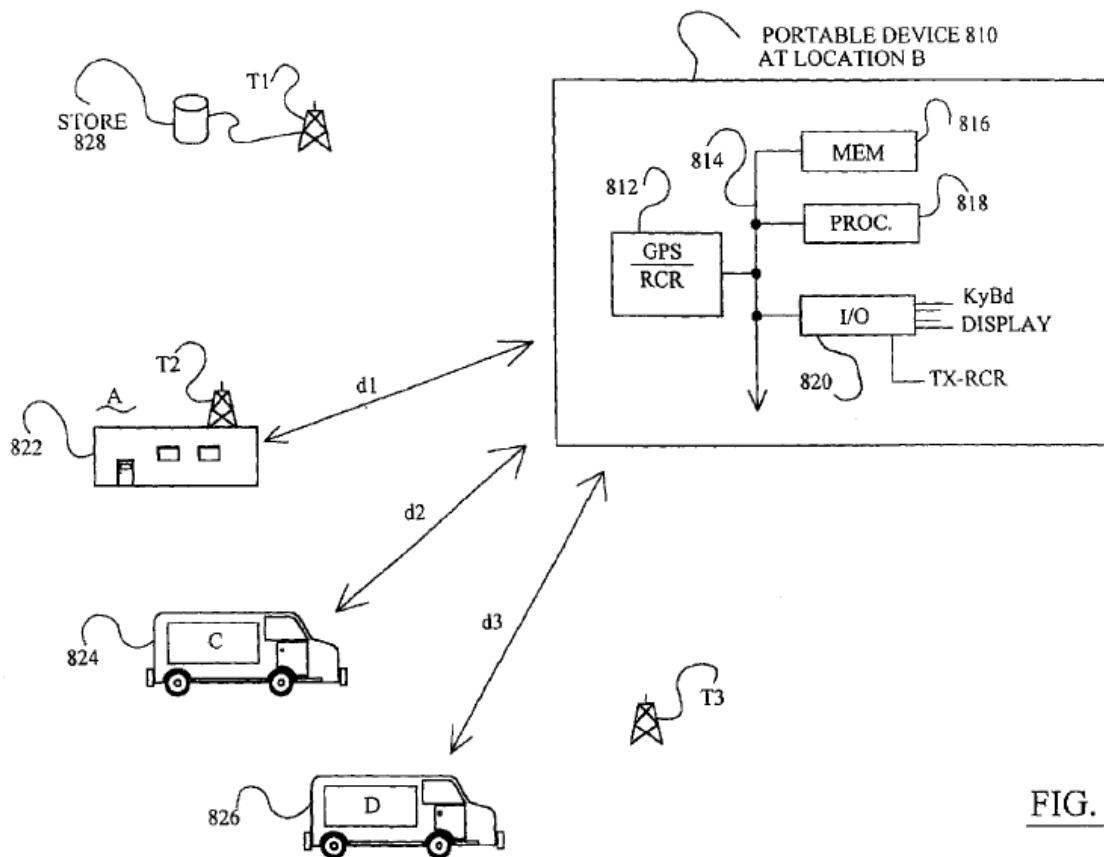


FIG. 14

EX1001, Figure 14. The system “can be applied to portable computing devices to secure files and data objects in such devices.” EX1001, 58:41-42. The portable computing device 810 includes a GPS system (or a receiver system) 812. EX1001, 59:29-34. See EX1003, ¶¶47-50, 90.

The device “provide[s] a security system for data based upon the location of the portable device, typically detected by a global position signal generator (GPS) or based upon triangulation data from several broadcast points.” EX1001, 58:42-48. The location serves as an “automated trigger []which activates the security program... when the portable computing device is beyond a predetermined region.” EX1001, 58:62-67. *See* EX1003, ¶¶91-92.

A flow chart for the portable security system program utilized in connection with portable computing device 810 is illustrated in Figure 15.

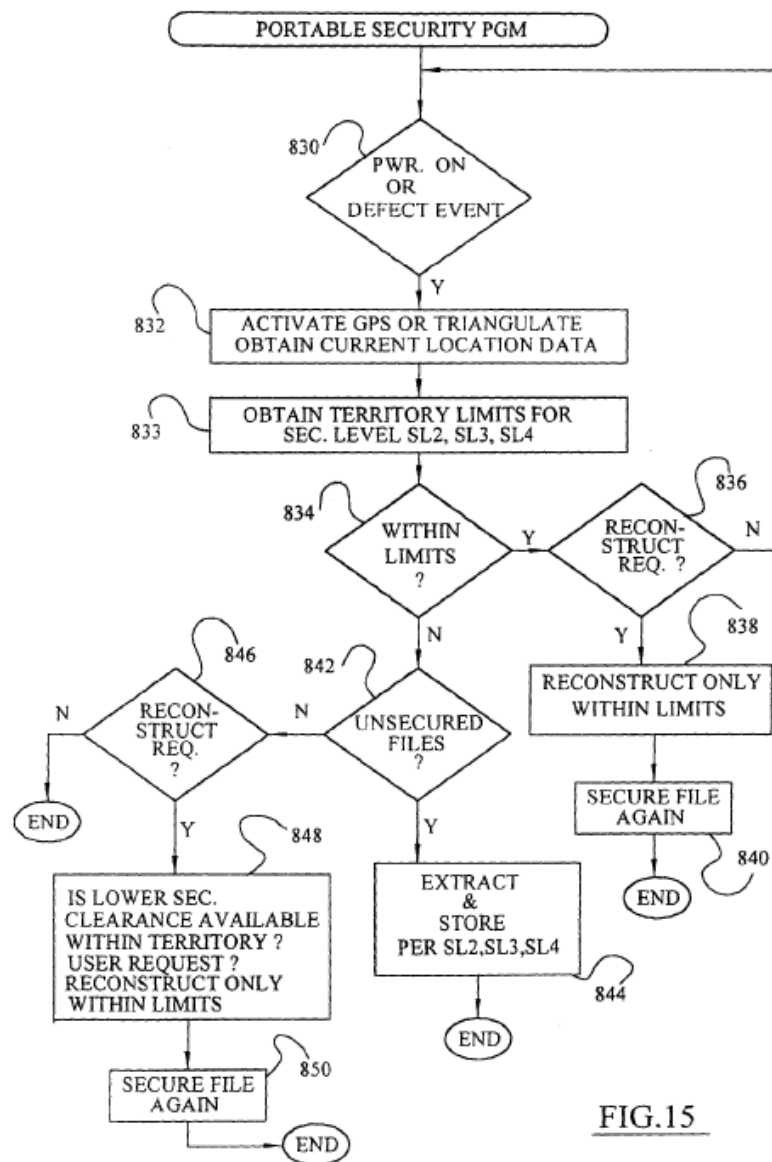


FIG.15

EX1001, Figure 15. The “automated trigger” is indicated by decision step 834, which “determines whether location B of portable computing device 810 is within or without the predetermined territory limits or predetermined region.” EX1001, 60:64-66. If within the region, the system determines if the user has initiated a reconstruction request. EX1001, 60:66-61:1. If a reconstruction request has been

initiated, at step 838 the system “reconstruct[s] only [if device 810 is] within limits.”

Id., Figure 15. EX1003, ¶¶93-94.

B. Prosecution History Of The '825 Patent

The '825 Patent was filed on March 19, 2003. EX1001, 1. The Examiner rejected claims—including claim 84 that ultimately issued as claim 81—as being obvious from U.S. Patent Nos. 5,960,080 (“Fahlman”), 6,370,629 (“Hastings”) and 6,253,203 (“O’Flaherty”). EX1002, 266. The Examiner explained Fahlman discloses the method of securing data in then-pending claim 84 but does not use a portable computing device. EX1002, 266-67. The Examiner noted Hastings teaches a portable computing device, determining when the device is beyond a certain location, and providing data when the device is not beyond the location. EX1002, 267. The Examiner also found that O’Flaherty teaches a remainder store and extract store in separate locations. EX1002, 267. The Examiner argued that the combination of the prior art features was obvious “to allow different information to be allowed in different locations (see Hastings [1:39-57]) and to prevent the ability to ascertain the identity of a customer (see O’Flaherty [14:26-57]).” EX1002, 267. EX1003, ¶¶95-97.

In response, Applicant amended claim 84 as shown below to recite, among others, “a plurality of security controlled memories as... extract stores with security

access controls” and that the “extracted data is stored in respective extract stores corresponding to a respective security level of said extract stores.”

84. (currently amended) A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective ~~designated as a remainder store and an extract store~~ extract stores with security access controls thereat, said security sensitive words, characters, data objects or icons extracted from said data to obtain extracted data and remainder data which extracted data is stored in respective extract stores corresponding to a respective security level of said extract stores , ~~said extract store and said remainder store, respectively~~, said computer system having at least one portable computing device locatable with ~~substantially~~ current location data, comprising:

determining when said portable computing device is within a predetermined region based upon said current location data;

permitting full or partial reconstruction of said data via said extracted data from said extract stores and remainder data only in the presence of a predetermined security clearance access control corresponding to said respective security level and only when said portable computing device is not beyond said predetermined region.

EX1002, 309. EX1003, ¶98.

In view of the amendments, Applicant argued that “none of the references [cited by the Examiner] show, teach or suggest ‘a plurality of security controlled memories as respective extract stores with security access control thereat, ... [and] storing said extracted data in respective extract stores corresponding to a respective security level of said extract stores...’” EX1002, 331. Applicant also alleged that

“[t]he claimed concept of multiple extract stores, with multiple security access controls, triggered to store critical data in respective secure access control extract stores is unique and patentable” because Fahlman “does not show, teach or suggest multiple extractions of security sensitive content to respective security level extract stores (multiple extract stores and respective security levels), and the requirement that the user apply a password or other security measure (‘security clearance access control’) before full or partial reconstruction of the data” nor does it show “multiple security level storage and retrieval.” EX1002, 331-32. Applicant also distinguished Hastings, arguing that it “does not show multiple levels of extraction to enable ‘storing said extracted data in respective extract stores corresponding to a respective security level of said extract stores.’” EX1002, 334. EX1003, ¶¶99-100.

The Examiner issued the Notice of Allowance on August 9, 2007. EX1002, 491. The Examiner stated that “[t]he prior art teaches filtering data based on security levels and storing the data and allowing full or partial reconstruction of data based on a respective security clearance. The prior art fails to teach storing only the extracted data for each security level at an extract store for each security level and storing the remainder data at a separate remainder store.” EX1002, 497. *See* EX1003, ¶¶47-82. EX1003, ¶¶101-102.

But as this Petition illustrates, storing sensitive data in extract stores based on the data security level, storing non-sensitive data in a separate store, and allowing

full or partial reconstruction based on a respective security clearance was known in the art. EX1003, ¶¶47-82. For example, Bossemeyer—a prior art reference that was not considered by the Examiner—discloses storing data in 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, ¶¶104-116.

C. Priority Date Of The '825 Patent

The earliest claimed priority date of the Challenged Claim is August 2, 2002, which is the filing date of four provisional applications which the '825 Patent claims priority to. Petitioner does not concede that the Challenged Claim is entitled to a priority date of August 2, 2002. However, because the prior art references discussed in this Petition qualify as prior art under either the filing date of the '825 Patent (March 19, 2003) or the August 2, 2002, date, Petitioner does not challenge the priority date of the Challenged Claim in this Petition but reserves the right to do so in other proceedings. EX1003, ¶¶30, 96.

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 August 2, 2002. Less professional experience can be substituted by additional education, and vice versa. EX1003, ¶¶131-32.

V. Claim Construction

Claim terms in IPR are construed according to their “ordinary and customary meaning” to those of skill in the art. 37 C.F.R. § 42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (*en banc*). Petitioner submits that, for the purposes of this proceeding and the grounds presented herein, no claim term requires express construction. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). EX1003, ¶¶133-134.

VI. Relief Requested And The Reasons For The Requested Relief

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

A. Challenged Claim and Statutory Grounds for Challenge

Petitioner requests cancellation of claim 81 of the ’825 Patent under 35 U.S.C. §103. This Petition, supported by the Declaration of Dr. Erez Zadok (EX1003),

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

Grounds	Claims	Basis
#1	81	Bossemeyer In View Of Glick
#2	81	Bossemeyer In View Of Glick And Carmichael

1. Bossemeyer

US Patent No. 7,010,701 (EX1005, “Bossemeyer”), filed on October 19, 1999, and issued on March 7, 2006, is prior art under at least 35 U.S.C. §102(e). EX1003, ¶104.

Bossemeyer describes “a network arrangement to provide access to an architecture that supports a variety of advanced smart card applications.” EX1005, 1:8-11. Smart cards are electronic devices that “can hold much more information [than data cards] and often include some ‘intelligence’ such as a microprocessor or the like.” EX1005, 1:34-38, 3:28-31 (“Smart card 12... contains circuitry 40 which includes a microprocessor and memory including random access memory (RAM) and read only memory (ROM).”). EX1003, ¶105.

Bossemeyer “describes a network arrangement which is readily accessible from different types of smart card terminals supporting various smart card applications. The network connections are facilitated by the present telephone

network or an interconnected network of computers such as the Internet.” EX1005, 1:44-49. Bossemeyer’s network arrangement also includes “a centralized server architecture [where] data related to an individual can be accessed by an individual smart card, predefined groups of smart card users, or the general public.” Ex1005, 1:49-52. EX1003, ¶106.

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

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

EX1005, 2:6-12.

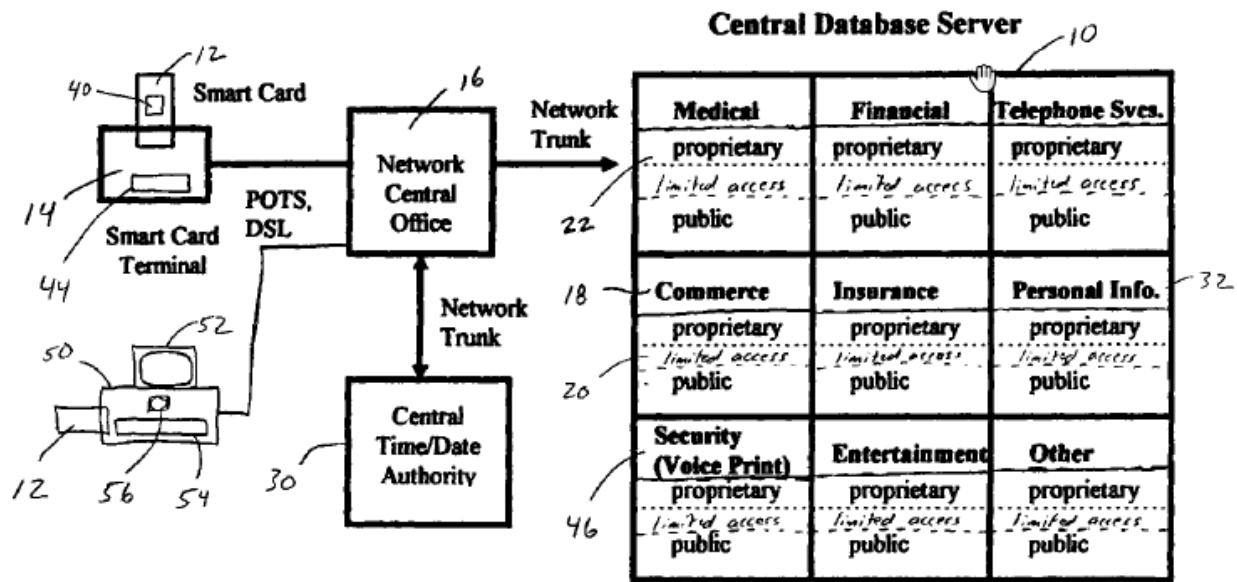


Figure 1

EX1005, Figure 1. EX1003, ¶107.

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 information, insurance information, medical information) in databases monitored by appropriate institutions. EX1005, 3:5-16 (“[I]n the merchant transaction discussed above, the purchaser’s credit files are more likely to be stored in a database monitored by the credit reporting companies such as TransUnion or Equifax, as opposed to the central database server 10.... In the same way, insurance information would ultimately reside with the insurer, medical records

with the health provider, financial records with the bank or broker, and so on.”).
EX1003, ¶¶108-109.

Bossemeyer’s system also includes “advance smart card terminals 50,” and “[a] smart card 12 coupled with such a terminal 50 having an established connection through the network central office 16 to the central database server 10 has the power of a typical networked computer.” EX1005, 4:11-15. EX1003, ¶110.

Bossemeyer further discloses controlling access to private or proprietary information. EX1005, 2:28-36 (“***Private or proprietary information*** is partitioned such that ***the owner of the information has control over how the information is transferred and used***. Thus, for example, medical information 22 provided to a health professional may be considered private and only available by way of special authorization from the owner of the information. In this way, ***the owner of the information contained within the central database server has control over how the information is transferred and used***.”). EX1003, ¶111.

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

Once the user’s authorization has been verified, data pointers on the smart card 12 provide access to the relevant partitioned memory portions of the central database server 10. Routing circuitry controlled by the microprocessor within the central database server 10 routes the

data pointer to appropriate memory locations or database of the information keeper relating to the application at issue such as medical, financial, etc. ***Data from these various locations is supplied back to the smart card terminal 14***, and if appropriate, the data stored on the smart card 12 is updated.

EX1005, 3:63-4:6.

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

EX1005, 4:50-58.

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

EX1005, 4:59-65; Figure 2. EX1003, ¶112.

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

The central database server 10 is a centralized partitioned database server which *partitions information* both *in terms of* the smart card application as well as *the accessibility of the information*. The information is stored by category (medical, financial, etc.) as well as *level of security (unrestricted, or public limited access, restricted)*. Thus, for example, in a retail purchase application 18, a merchant may require access to a user's credit information to determine whether to accept the user's credit for a particular dollar amount. This information may be partitioned in the limited access region 20 of commercial transaction applications 18.

EX1005, 2:17-27. EX1003, ¶113.

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

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

EX1005, 5:8-15.

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. EX1003, ¶114.

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 which may be necessary in the event of a medical emergency, but probably not be allowed to access any other user information.” EX1005, 5:16-19. “In contrast, a loan officer at a bank or automotive

dealership would be allowed to access to the user's credit history 218 as well as the user's financial account balances 220." EX1005, 5:20-22. EX1003, ¶¶114-116.

2. Glick

US Patent No. 6,985,588 (EX1006, "Glick") filed on October 30, 2000, and issued on January 10, 2006, is prior art under at least 35 U.S.C. §102(e). EX1003, ¶117.

Glick discloses a method for controlling access to information within a specific geographic area. Glick's method utilizes a location identity attribute that defines an area (location value and proximity value), such that the information can be accessed only within the area:

A method and apparatus for *controlling access to digital information* utilizes a location identity attribute that defines a specific geographic location. The location identity attribute is associated with the digital information such that *the digital information can be accessed only at the specific geographic location. The location identity attribute further includes a location value and a proximity value.* The location value corresponds to a location of an intended recipient appliance of the digital information, and may be further defined in terms of latitude, longitude and altitude dimensions.

EX1006, Abstract, 3:37-38 ("The proximity value corresponds to a zone that encompasses the location."), 3:44-46 ("[A]ccess to the digital information is allowed

only at the specific geographic location defined by the location identity attribute.”), 3:27-37, 3:43-60. EX1003, ¶¶118-119.

Glick’s method first determines the location of an appliance (e.g., electronic device). EX1006, 3:46-48. Glick describes different ways of identifying location:

There are many ways to identify the location of the appliance, including: (1) resolving the appliance location from a street address for the appliance; (2) retrieving the appliance location from a file stored within the appliance; (3) recovering the appliance location from a GPS receiver embedded in the appliance; and (4) recovering the appliance location by triangulating RF signals received by the appliance.

EX1006, 3:48-55, 6:35-38 (“For the purposes of this invention, any coordinate system that uniquely identifies a place can be used for the location value 142 of the location identity attribute 140.”). EX1003, ¶¶120-121.

Glick explains that “[a]fter the appliance location is identified, it is compared to the specific geographic location defined by the location identity attribute. Access to the digital information is allowed only if the appliance location falls within the specific geographic location.” EX1006, 3:43-60, Abstract, 6:29-49, 7:4-21, 10:13-22, 11:28-38, Figure 2. EX1003, ¶122.

Figures 5 and 10 of Glick, annotated below, describe the steps for enforcing location identity and allowing information access within a predetermined region defined by a location value and a proximity value.

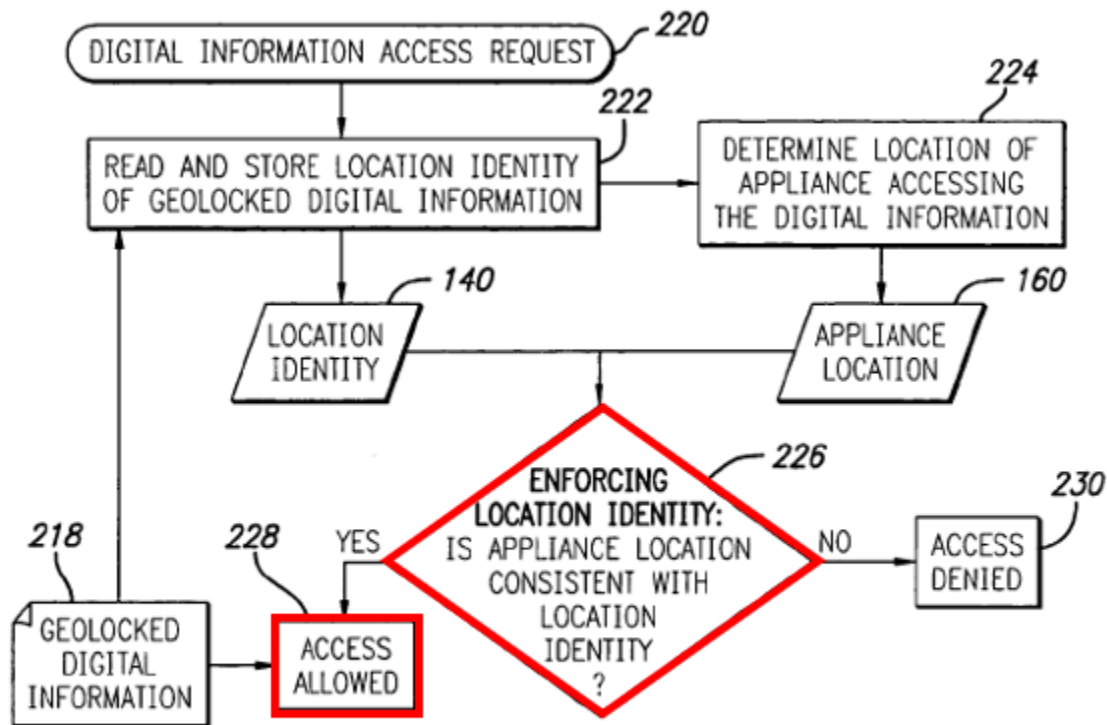


FIG. 5

EX1006, Figure 5; *id.*, 8:16-35 (“[T]he method starts at step 220 with a command to access the digital information. At step 224, the method determines the location of the appliance accessing the digital information...At step 226, the method determines whether the location of the appliance is consistent with the region defined by the location identity 140. If the appliance location 160 is consistent with the location identity 140, then access to the geolocked digital information 218 is allowed at step 228. Conversely, if the appliance location 160 is not consistent with the location identity 140, then access is denied at step 230.”). EX1003, ¶¶123-124.

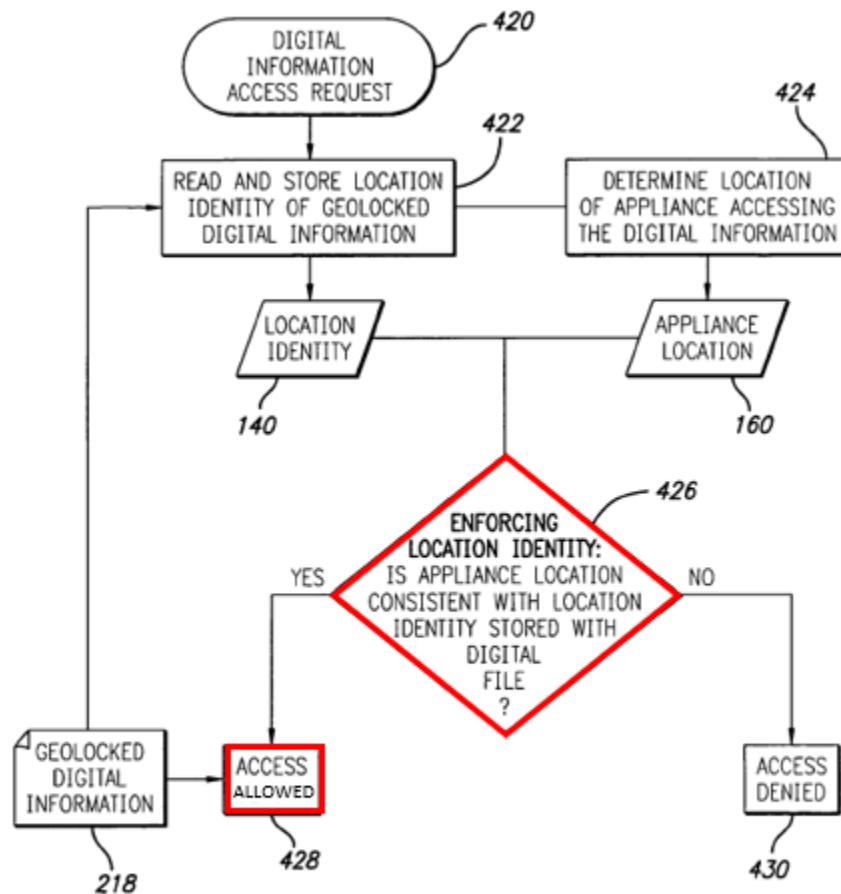


FIG. 10

EX1006, Figure 10 (modified)¹, 11:49-12:5. EX1003, ¶¶125-126.

¹ Block 428 in Figure 10 includes the text “ACCESS DENIED,” which is a typographical error. Modified Figure 10 in this Petition replaced “ACCESS DENIED” of block 428 with “ACCESS ALLOWED,” which is consistent with the description of Figure 10 in Glick. EX1006, 11:67-12:3 (“If the appliance location 160 is consistent with the location identity 140, then *the application or operating*

3. Carmichael

US Patent No. 7,913,919 (EX1007, “Carmichael”) filed on August 5, 2009, is a continuation of US Ser. No. 09/493,756, filed on January 28, 2000. Carmichael issued on March 29, 2011, and is prior art under at least 35 U.S.C. §102(e). EX1003, ¶127.

Carmichael discloses a smart card with a microprocessor, memory, and location tracking means for determining the location of the smart card. EX1007, Abstract (“A smart card capable of performing more than one function... [and] comprises *a microprocessor...* and *a location tracking means for determining a location of the smart card.*”), 4:65-5:2 (“In another innovative aspect, the present invention is directed to a system for locating the position of a smart card. The system can comprise a smart card having *a microprocessor* in electrical communication with *a memory means*, and *a location tracking means.*”). EX1003, ¶128.

Carmichael explains that “[t]he location of the smart card can be determined using *the location tracking means which can reside on the smart card*. In one embodiment the location tracking means transmits an identifiable signal, which is

system can access the geolocked digital information 218 at step 428.”). In addition, the language at steps 426 and 428 of Figure 10 correspond to steps 226 and 228 of Figure 5, in which step 228 recites “ACCESS ALLOWED.” EX1003, ¶126.

detectable by a **global positioning system** satellite.” EX1007, 3:58-62, 5:2-11 (“The system can further comprise a satellite in duplex communication with the location tracking means.... The satellite can be a global positioning system satellite or any other communications satellite.... The location tracking means on the smart card can also be capable of receiving coordinate data from the satellite and transmitting the data to the memory.”). EX1003, ¶128.

Figure 2 of Carmichael, reproduced below, shows a smart card that houses a **GSM (Global System Mobile Communications) chip** for use with a Global Positioning System (GPS) satellite network to locate the smart card.

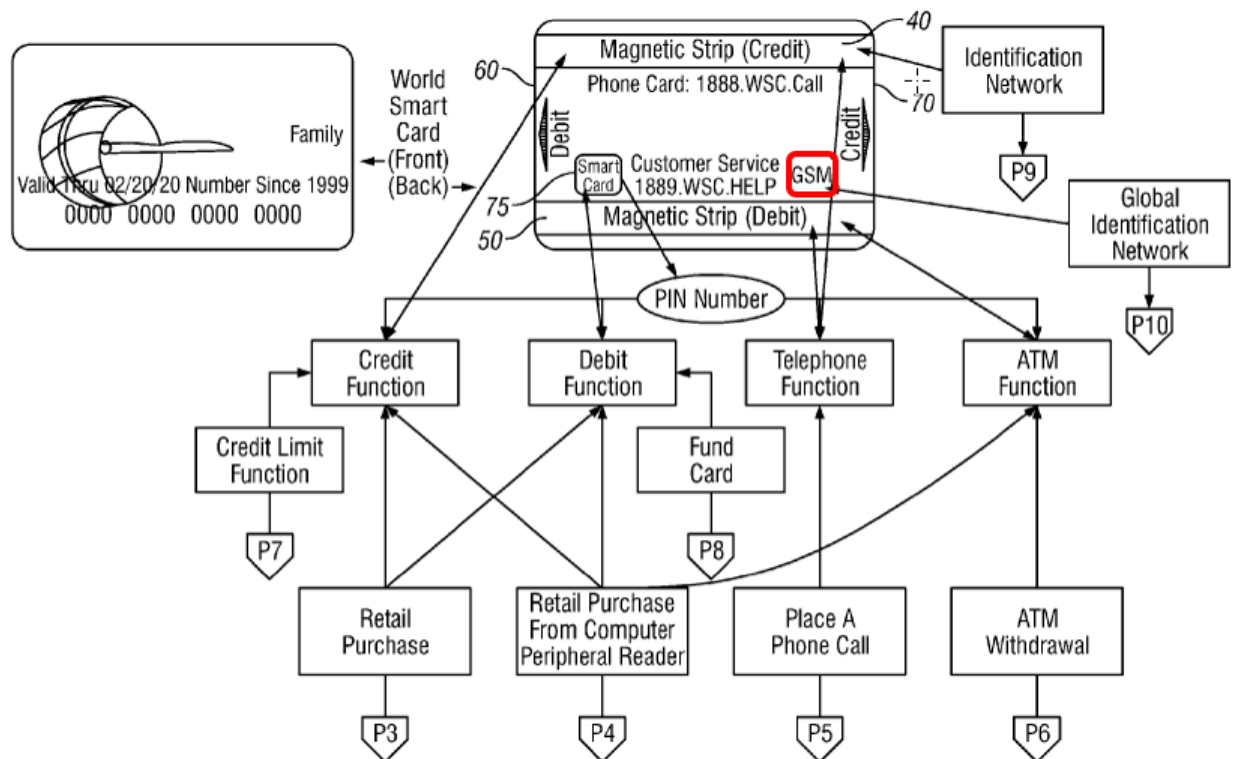


FIG. 2

EX1007, Figure 2, 2:35-38 (“The present invention ... couple[es] a **GSM chip** or signal transmitter to the smart card for use in connection with a Global Positioning System (GPS) satellite network or the like, to locate the smart card.”), 8:21-25 (“Also found on the smart card 1, as shown in FIG. 2, is a **GSM (Global System Mobile Communications) chip**. The GSM can either be activated by a police network terminal as described in FIG. 10, or through a signal transmitter that is contained on the **GSM chip** itself.”). EX1003, ¶129.

Carmichael also explains that the location of the smart card can be determined through the location of a smart card terminal. EX1007, 3:62:67 (“Alternatively, the location of the card can be determined by a central processing center which stores data relating to all of the functions of the smart card, and which can *identify the location of the card by identifying the location of the retail terminal or card reader to which the smart card is applied.*”), 8:34-37 (“Another type of location tracking function utilizes a device coupled to the card which transmits a unique signal which is detectable by a satellite, such as a global positioning system satellite.”), 9:16-25 (“*The location of the smart card 1 can also be determined* at the time the smart card 1 is used *by identifying the location of the retail terminal, automated teller machine, or peripheral card reader.* Thus, when a debit, telephone, ATM, or credit function is processed and the institution’s database is accessed, the institution will be capable of recognizing the location of the card based on the retail terminal,

automated teller machine, or peripheral card reader from which the request originates and setting the conversion of currency based on that information.”).

EX1003, ¶130.

B. Grounds 1-2: Claim 81 Is Obvious Over Bossemeyer With Glick (Ground 1) Or Bossemeyer With Glick And Carmichael (Ground 2)

1. [81pre] A method of securing data having one or more security sensitive words, characters, data objects or icons in a computer system with a plurality of security controlled memories as respective extract stores with security access controls thereat, said security sensitive words, characters, data objects or icons extracted from said data to obtain extracted data and remainder data which extracted data is stored in respective extract stores corresponding to a respective security level of said extract stores, said computer system having at least one portable computing device locatable with current location data, comprising:

To the extent the preamble is limiting, Bossemeyer in combination with Glick (and Carmichael for Ground 2) renders obvious the preamble, as explained below.

EX1003, ¶¶136-137, 271.

i. A method of securing data having one or more security sensitive words, characters, data objects or icons

Bossemeyer discloses and in combination with Glick renders obvious a “method of securing data having one or more security sensitive words, characters, data objects or icons.” Bossemeyer discloses partitioning sensitive data to control how the data is transferred and used. EX1005, 2:28-30 (“Private or proprietary information is partitioned such that *the owner of the information has control over*

*how the **information** is transferred and used.”*). 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).

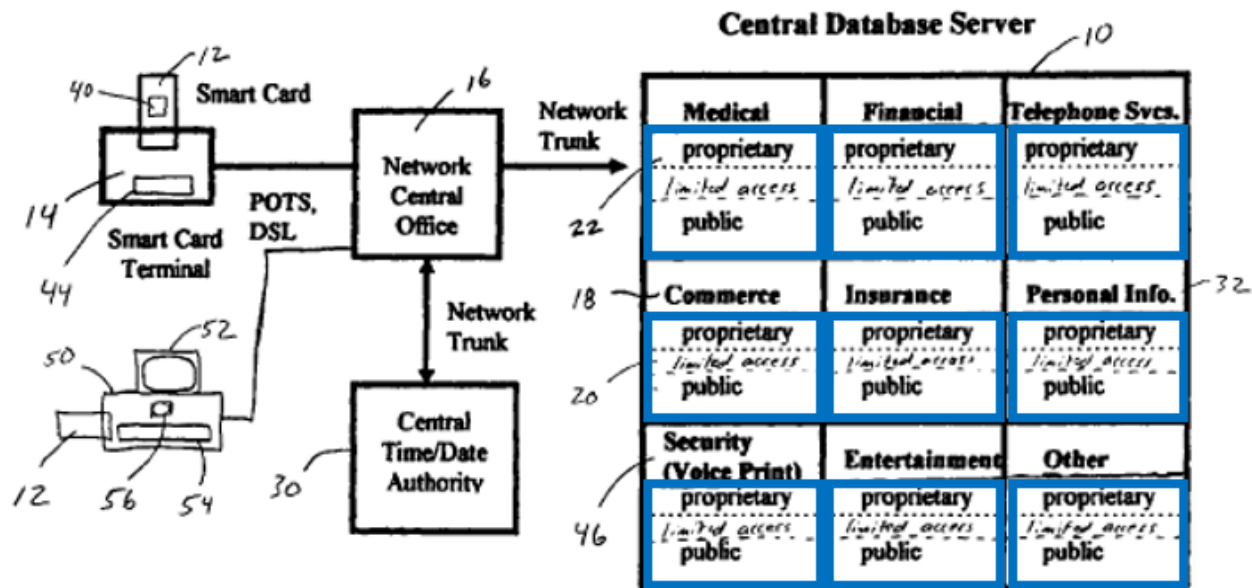


Figure 1

EX1005, Figure 1.

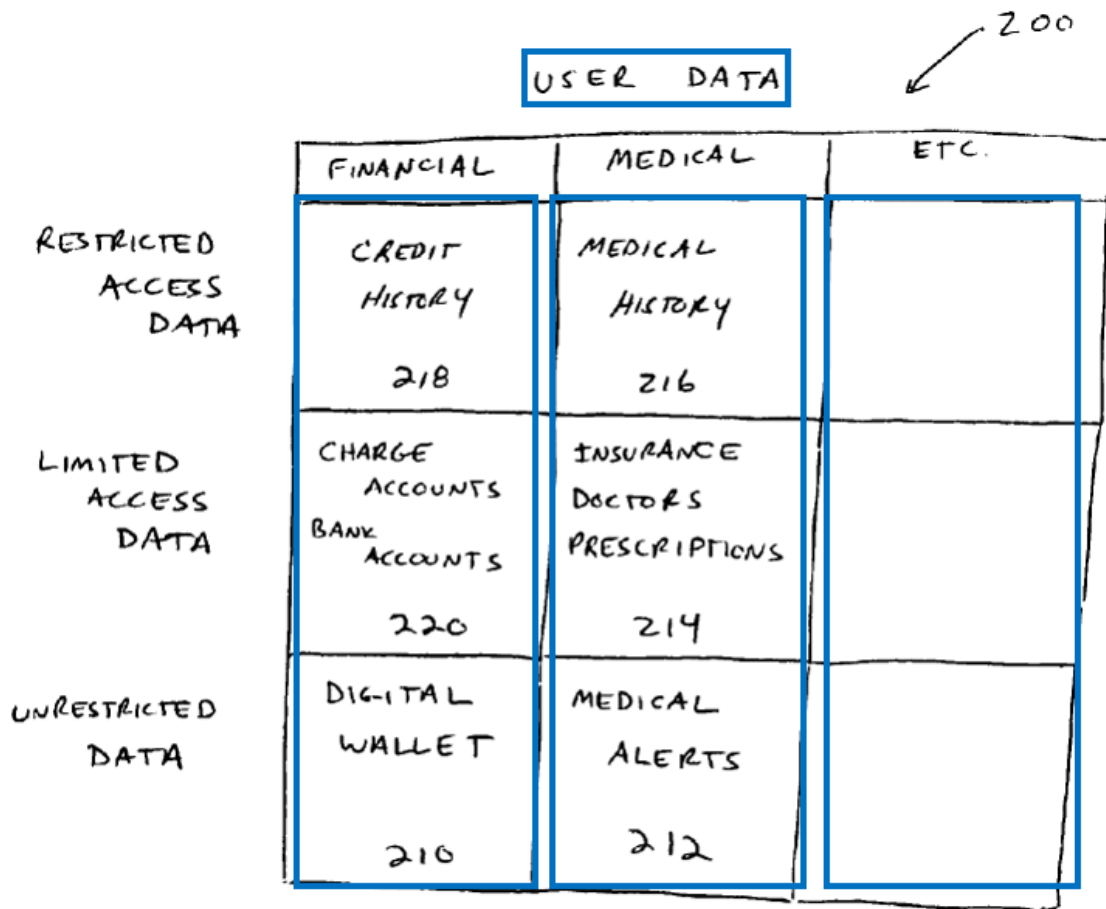


FIG. 3

EX1005, Figure 3. EX1003, ¶¶138-140.

A POSITA would have understood that Bossemeyer's "limited access information" and/or "proprietary information" would include security sensitive information, such as, words, characters, data objects 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. EX1003, ¶¶141-142.

In addition to the types of security sensitive information explicitly disclosed in Bossemeyer, a POSITA would have also found it obvious that Bossemeyer's method secures other types of security sensitive words, characters, data objects or icons. For example, Figure 3 of Bossemeyer includes additional columns for storing user data with a restricted- or limited-access security level (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, ¶143.

Further, Glick discloses securing data by preventing access to the data unless access is requested at a particular geographic location. EX1006, 3:44-46 (“[A]ccess to the digital information is allowed only at the specific geographic location defined by the location identity attribute.”). EX1003, ¶¶144-145.

As discussed below in Section VI.B.6, it would have been obvious to combine Glick with Bossemeyer to incorporate Glick's teaching of using location identity to control access to information stored in Bossemeyer's system and a POSITA would

have a reasonable expectation of success in combining Glick with Bossemeyer.
EX1003, ¶146.

Accordingly, Bossemeyer and Glick suggest a “method of securing data having one or more security sensitive words, characters, data objects or icons.”
EX1003, ¶¶147, 272.

- ii. **in a computer system with a plurality of security controlled memories as respective extract stores with security access controls thereat,**

Bossemeyer discloses “a computer system with a plurality of security controlled memories as respective extract stores with security access controls thereat.” EX1003, ¶¶148, 273.

First, Bossemeyer discloses an interconnected network of computers, i.e., a computer system. EX1005, 1:44-49 (“In this regard, the present invention describes a network arrangement which is readily accessible from different types of smart card terminals supporting various smart card applications. ***The network connections are facilitated by the present telephone network or an interconnected network of computers such as the Internet.***”), 4:11-15 (“A smart card 12 coupled with such a terminal 50 having an established connection through the network central office 16 to the central database server 10 has the power of ***a typical networked computer.***”), 4:19-22 (“It is contemplated that such smart card ‘docking stations’” could transform hotel room entertainment centers or airplane seat video screens into ***networked***

computers with the insertion of a user's smart card.”), 4:25-28 (“[T]he network arrangement of FIG. 2 is implemented over *an interconnected network of computers* such as the Internet 100 as well as or alternatively to the traditional telephone network 102.”). EX1003, ¶¶149-150.

Second, Bossemeyer's computer system includes a central database server with a *memory that is broken into different partitions*, i.e., *a plurality of security controlled memories*. EX1005, 2:6-9 (“The network arrangement makes use of a *central database server 10* that supports many different smart card applications, and supports many users within a given application.”), 2:13-16 (“The *central database server 10* includes *partitioned memory*, described in further detail below, as well as a microprocessor for processing data received from and transmitted to the smart card terminal 14.”). EX1003, ¶151.

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

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

may be partitioned in the limited access region 20 of commercial transaction applications 18.

EX1005, 2:17-27. EX1003, ¶152.

Therefore, Bossemeyer teaches controlling the access of sensitive information, e.g., by allowing unrestricted or limited access or restricting access to the sensitive information. Accordingly, Bossemeyer's memory partitions have security access controls. Figures 1 and 3 of Bossemeyer, reproduced below, illustrate the *memory partitions* with limited-access and restricted information.

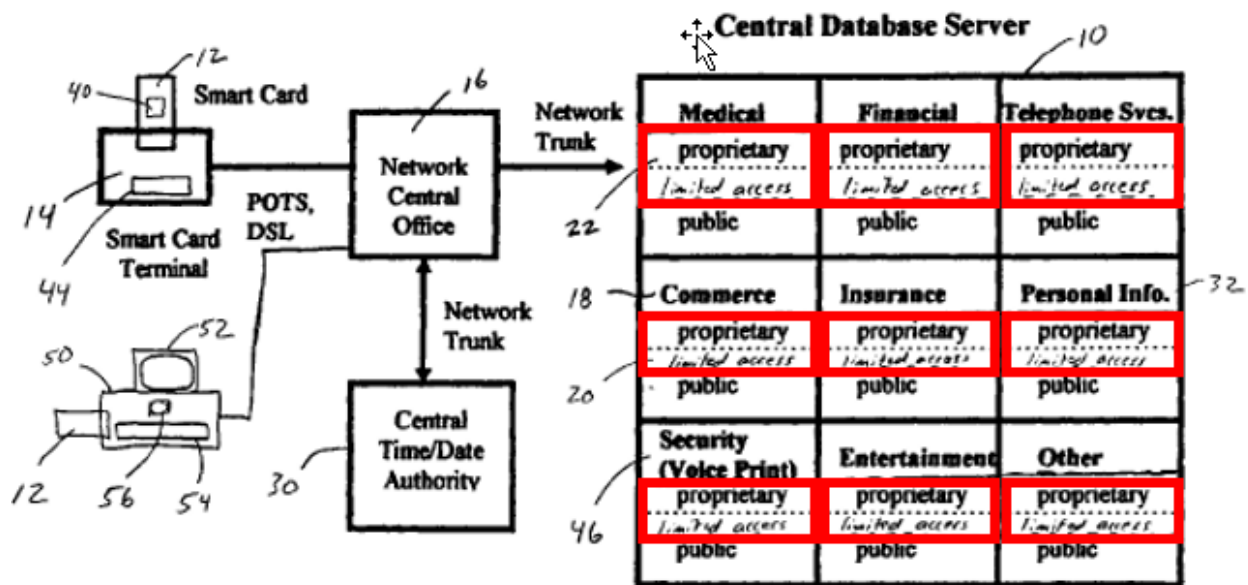


Figure 1

EX1005, Figure 1.

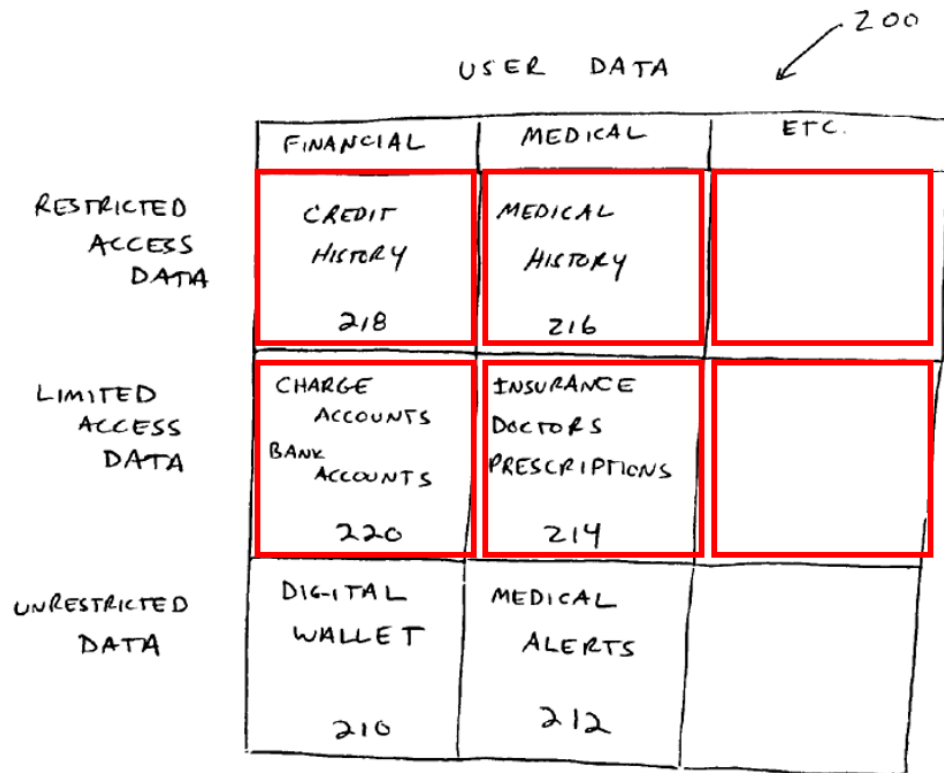


FIG. 3

EX1005, Figure 3. EX1003, ¶153.

To the extent Patent Owner argues that *plurality of security controlled memories* need to be separate physical memories and/or be implemented in separate locations, Bossemeyer also discloses that different servers at various locations can collectively make up the central database server, and that a server in a particular location (e.g., remote location) can store sensitive information:

Although the *central database server 10* is shown as a single server, *it is to be understood that multiple servers may comprise the central database server 10*. For example, in the merchant transaction discussed

above, the *purchaser's credit files* are more likely to be stored *in a database monitored by the credit reporting companies* such as TransUnion or Equifax, as opposed to the central database server 10.

EX1005, 3:3-9. EX1003, ¶154.

Bossemeyer's memories at various locations, e.g., databases at the credit reporting companies, that store sensitive information also satisfy the claimed *plurality of security controlled memories*. EX1003, ¶155.

The '825 Patent describes "extract stores" as memories that store sensitive information. EX1001, 10:6-13 ("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 memory partitions and/or remote memories that store sensitive information (limited-access and/or restricted information) are extract stores with security access controls. EX1003, ¶¶156-157.

Accordingly, Bossemeyer discloses this limitation. EX1003, ¶¶158, 273.

- iii. said security sensitive words, characters, data objects or icons extracted from said **data** to obtain **extracted data** and **remainder data**

Bossemeyer discloses and/or renders obvious this limitation. EX1003, ¶¶159, 171, 274.

Bossemeyer discloses partitioning a database server to partition or separate, e.g., extract, **user 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)*. Thus, for example, in a retail purchase application 18, a merchant may require access to a user's credit information to determine whether to accept the user's credit for a particular dollar amount. This *information may be partitioned in the limited access region 20 of commercial transaction applications 18.*"

EX1005, 2:17-27. EX1003, ¶160.

Specifically, in Bossemeyer, **user data** is partitioned, e.g., extracted, into **limited access information** and/or **proprietary information**, and **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, limited access information and/or proprietary information includes security sensitive information, such as, words, characters, data objects or icons. For example, Figure 1 of Bossemeyer shows *medical information* 22 stored in central database 10 as proprietary information.

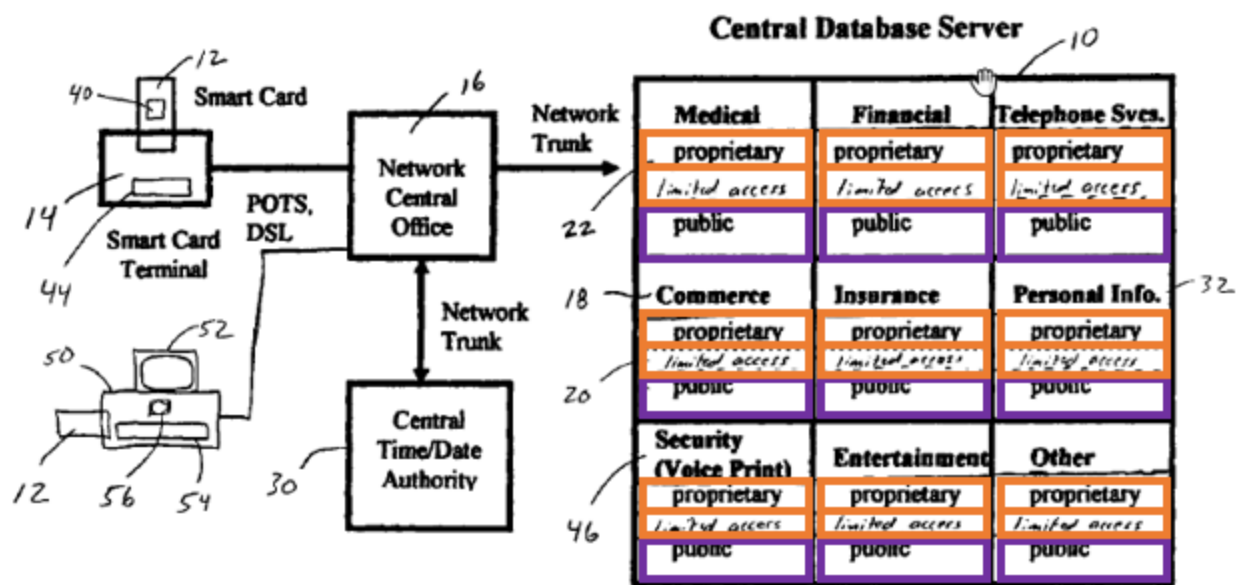


Figure 1

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

professional may be considered private and only available by way of special authorization from the owner of the information.”). EX1003, ¶¶161-163.

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

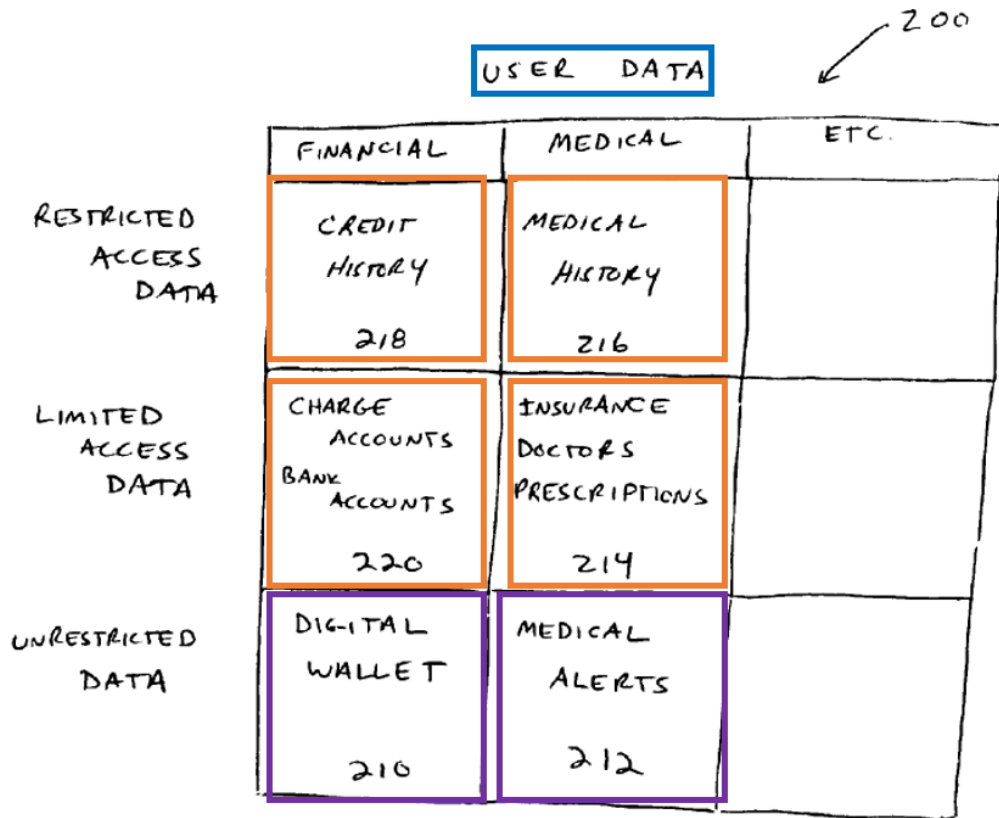


FIG. 3

EX1005, Figure 3, 5:9-15 (“In the pharmacy example, once the user’s authentication code and merchant code have been verified by the system, the pharmacist may have access to the *user’s digital wallet 210*, *medical alerts 212*, and *insurance and prescription information 214*. Without further authorization, however, the

pharmacy would not have access to the user's *medical history 216*.”). EX1003, ¶¶164-166.

To the extent that Patent Owner argues that Bossemeyer does not explicitly disclose “extracted data,” a POSITA would have understood that when Bossemeyer’s “central database server... partitions [user] information... in terms of... the accessibility of the information” (EX1005, 2:17-20), Bossemeyer’s method would filter, separate, and thus extract the secure sensitive information, e.g., restricted- and/or limited-data, from the received user data, e.g., from a user data file, to store the restricted- and/or limited-data in the appropriate security-level store, while storing the remaining information in the user data file as unrestricted data, e.g., public data. For example, a POSITA would have understood that Bossemeyer’s method can parse the received information into private and non-private elements. *See e.g.*, U.S. Publication No. 2004/0148290 (EX1008), ¶23. (“[A] set of data may be parsed into private and non-private elements.”). EX1003, ¶¶167-168.

When Bossemeyer’s central database server receives a *user’s medical data file*, as shown in Bossemeyer’s Figure 3 below, Bossemeyer’s method extracts the *user’s medical history information 216*, and *insurance, doctors, prescriptions information 214*, and stores them into respective extract stores corresponding to the appropriate respective security level. For example, a POSITA would have understood that medical history information can include images of medical charts,

insurance information can include icons of the user's insurance card, prescription information can include the names of the drugs prescribed to the user, etc.

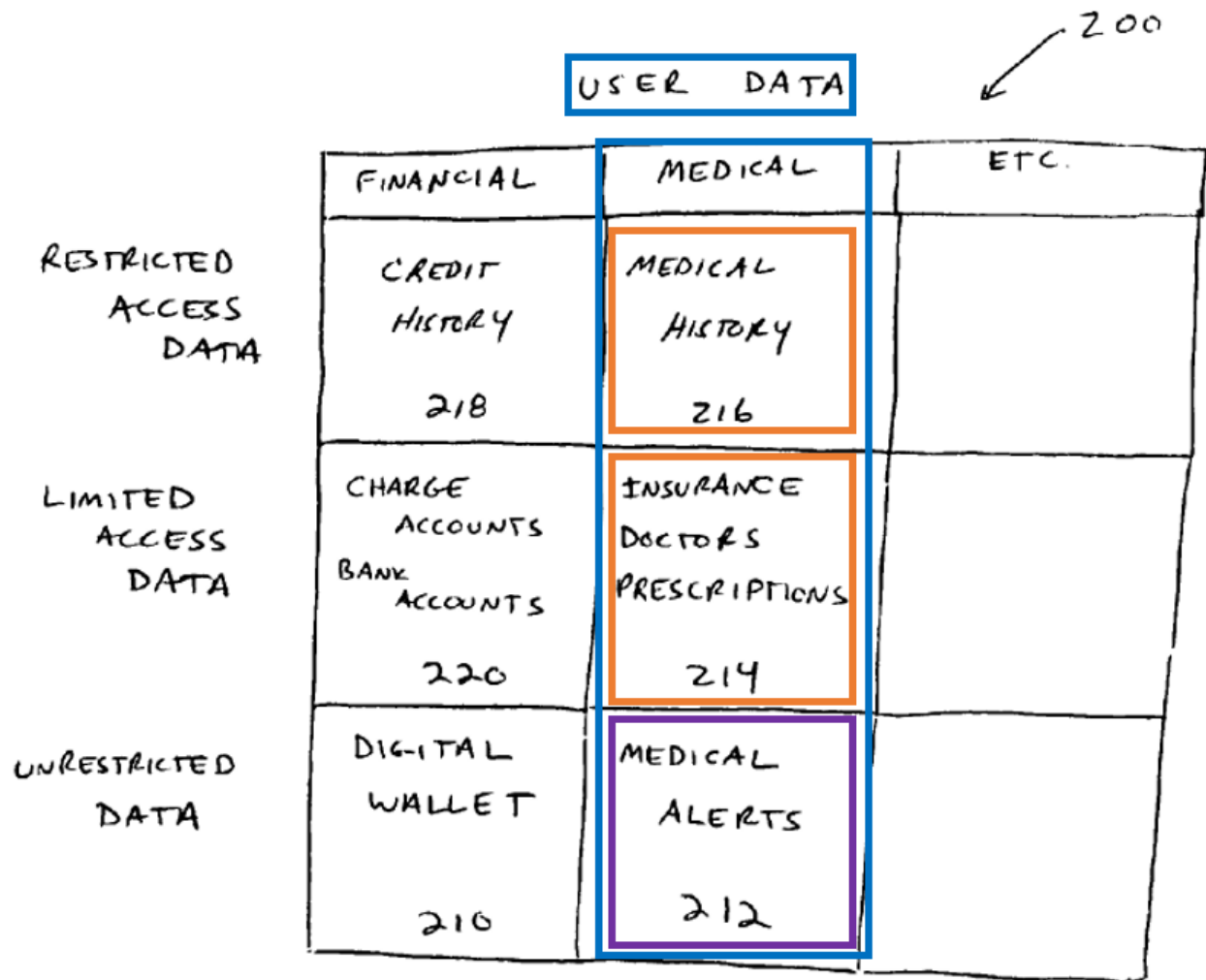


FIG. 3

EX1005, Figure 3. EX1003, ¶169-170.

- iv. which extracted data is stored in respective **extract stores** corresponding to a respective security level of said extract stores,

Bossemeyer discloses this limitation. EX1003, ¶¶172, 275.

As discussed in Sections VI.B.1.ii and VI.B.1.iii, Bossemeyer discloses storing sensitive data, i.e., extracted data, in either a “centralized partitioned database server” (EX1005, 2:17-18) or remote servers (*id.*, 3:3-18), as shown, for example, in Bossemeyer’s Figures 1 and 3.

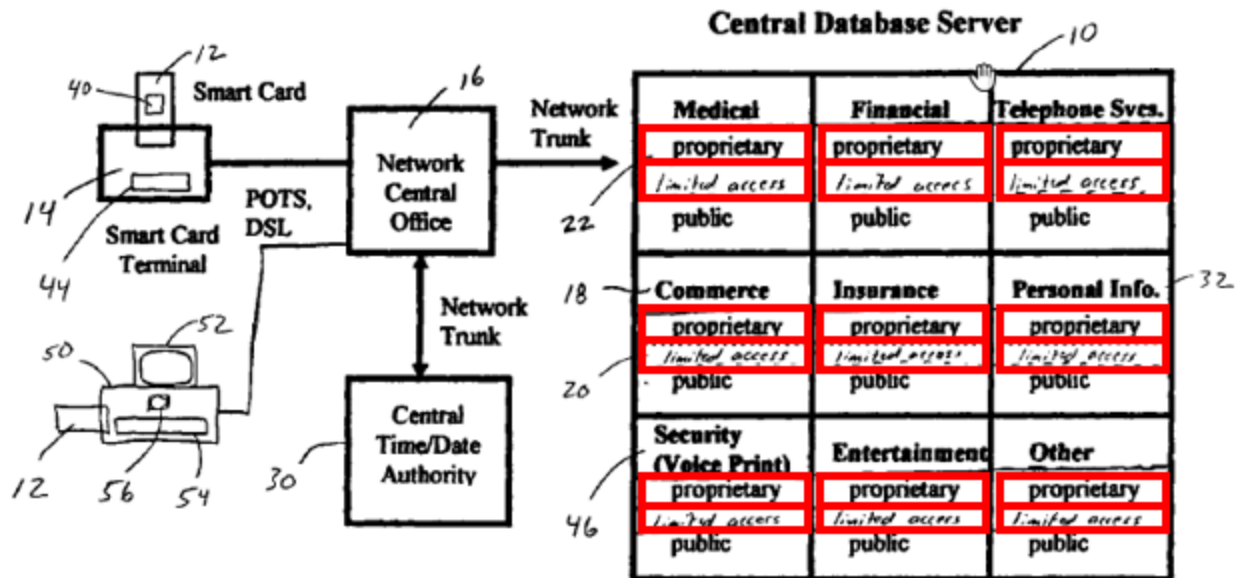


Figure 1

EX1005, Figure 1.

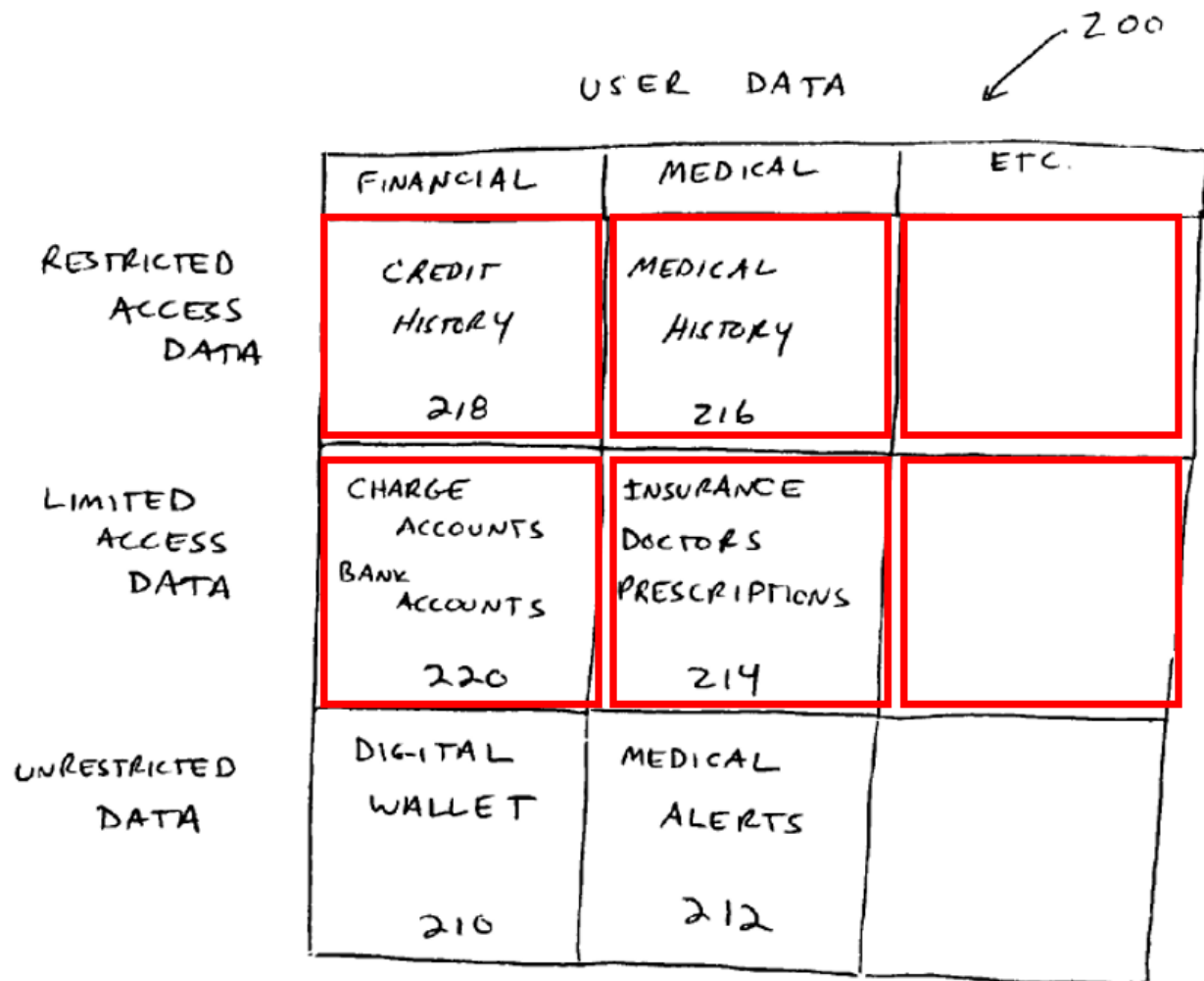


FIG. 3

EX1005, Figure 3. EX1003, ¶173.

Bossemeyer also discloses that sensitive data, e.g., limited access data or restricted access data, are stored in respective extract stores corresponding to a respective security level of said extract stores. Figures 1 and 3 show Bossemeyer's central database server partitioned into regions (**proprietary/restricted access**

region, limited access region, unrestricted/public access region) of corresponding security/access levels:

The central database server 10 is a centralized partitioned database server which *partitions information* both *in terms* of the smart card application as well as *the accessibility of the information*. The information is stored by category (medical, financial, etc.) as well as *level of security (unrestricted, or public limited access, restricted)*. Thus, for example, in a retail purchase application 18, a merchant may require access to a user's credit information to determine whether to accept the user's credit for a particular dollar amount. This information may be partitioned *in the limited access region 20* of commercial transaction applications 18.

EX1005, 2:17-27. EX1003, ¶¶174-175.

Furthermore, in connection with a merchant transaction example, Bossemeyer also discloses that a "purchaser's credit files are more likely to be stored in *a database monitored by the credit reporting companies such as TransUnion or Equifax*, as opposed to the central database server 10." EX1005, 3:6-9, 3:14-16 ("[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"). EX1003, ¶176.

Bossemeyer discloses multiple extract stores, each with its own security information residing with its respective data owner:

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 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. The network smart card server acts as a secured gatekeeper to such information and the smart card acts as the enabling key.”).

EX1005, 3:3-18, EX1003, ¶¶177-178.

Accordingly, Bossemeyer discloses that extracted data, e.g., insurance information or medical records, are stored in extract stores, e.g., insurer database/store or health provider database/store, respectively, corresponding to respective security level of the insurer database/store or health provider database/store. EX1003, ¶179.

Accordingly, Bossemeyer discloses this limitation. EX1003, ¶179.

- v. **said computer system having at least one portable computing device locatable with current location data, comprising:**

Bossemeyer in view of Glick (and Carmichael for Ground 2) renders obvious this limitation. As explained below, “portable computing device locatable with

current location data” is rendered obvious in two ways: (1) by Bossemeyer’s **smart card 12**; and (2) by Bossemeyer’s **smart card terminal 14** and/or **advance smart card terminal 50**. EX1003, ¶¶180-181, 276.

a. Smart Card Locatable With Current Location Data

As discussed in Section VI.A.1, Bossemeyer discloses that “[s]mart card 12 is formed of plastic or other suitable material and contains circuitry 40 which includes a *microprocessor and memory* including random access memory (RAM) and read only memory (ROM).)” EX1005, 3:28-31. A POSITA would have understood this smart card to be a “computer system” as claimed. Smart card 12 is also portable. EX1005, 1:31-34 (“*allowing consumers to carry just one card* for several types of transactions including those identified above. Such cards have been referred to as ‘smart’ cards.”). Accordingly, Bossemeyer’s **smart card 12** is a **portable computing device**. EX1003, ¶182.

A POSITA would have understood that the ’825 patent describes a “portable device” to include many form factors and sizes (from desktops to pagers), as long as it has a memory, processor, and “GPS or locator,” which would include a smart card. EX1001, 58:52-59 (“the term ‘portable computing device’ means a laptop computer, a PC with a movable feature, such as a PC mounted in a car, plane, truck or trailer, PDAs or personal data assistants, mobile or cellular phones configured with a

memory, a processor and some type of GPS or locator system to determine where the phone or cellular unit is located within a territory and digital pagers having similar electronic systems”). EX1003, ¶¶183-184.

Glick discloses a portable electronic device (appliance) that is locatable with current location data. EX1006, 3:46-48 (“As a first part of this enforcement process, the location of an appliance through which access to the digital information is sought is identified.”). Glick provides different examples for identifying the current location of the appliance:

There are many ways to identify the location of the appliance, including: (1) resolving the appliance location from a street address for the appliance; (2) retrieving the appliance location from a file stored within the appliance; (3) recovering the appliance location from a GPS receiver embedded in the appliance; and (4) recovering the appliance location by triangulating RF signals received by the appliance.

EX1006, 3:48-55, 6:35-38 (“For the purposes of this invention, any coordinate system that uniquely identifies a place can be used for the location value 142 of the **location identity attribute 140**.”). EX1003, ¶¶185-188.

Bossemeyer’s smart card 12 is an “appliance” as the term is used in Glick. For example, Glick defines “appliance” as:

Electronic devices, systems, networks, and the like with the minimum capacity to acquire digital information, transmit the information, and acquire location information. These electronic devices will often

include a processing capability to execute program instructions and a memory capacity for short term and long term data storage.

EX1006, 5:12-17. Glick also discloses that “[t]he method would be performed by a system or *device having a data processing capability and memory sufficient to enable receipt of digital information* communicated or distributed by another party, such as a personal computer, server, router, personal digital assistant (PDA), workstation, network, laptop, and the like.” EX1006, 8:7-14. Bossemeyer’s **smart card** is a *portable* electronic device with processing capability and memory capacity (“[s]mart card 12... contains circuitry 40 which includes a microprocessor and memory...” (EX1005, 3:28-30)), which can receive and transmit information (“[e]ach smart card 12 used with the system provides data pointers to the relevant partitions of the central database server 10. This reduces the amount of information which must be *stored or transferred to each smart card 12...*” (*id.*, 2:58-61)). EX1003, ¶¶189-191.

To the extent that Patent Owner argues that Bossemeyer does not explicitly disclose that smart card 12 is locatable with **current location data**, a POSITA would have also understood that smart cards, like the one disclosed in Bossemeyer, can also acquire location information. EX1007, 3:32-34 (“The smart card also may have a location tracking means for determining a location of the smart card.”), 3:58-59 (“The location of the smart card can be determined using the location tracking means

which can reside on the smart card.”). Accordingly, a POSITA would have found it obvious to use Bossemeyer’s smart card as a portable computing device locatable with current location data that performs Glick’s methods. As discussed below in Section VI.B.6, it would have been obvious to combine Glick with Bossemeyer to incorporate Glick’s teaching of using location identity to control access to information stored in Bossemeyer’s system, and a POSITA would have a reasonable expectation of success in combining Glick with Bossemeyer. EX1003, ¶¶190-193.

To the extent Patent Owner argues that Bossemeyer does not render obvious a smart card that is locatable with **current location data**, it would have been obvious to combine Bossemeyer (and Glick) with Carmichael (for Ground 2) to incorporate Carmichael’s explicit teachings of a smart card with “location tracking means for determining **a location of the smart card**.” EX1007, 3:32-34. Carmichael discloses that “[t]he location of the smart card can be determined using the location tracking means which can reside on the smart card.” EX1007, 3:58-59. Carmichael explains that “the location tracking means transmits an identifiable signal, which is detectable by a global positioning system satellite.” EX1007, 3:60-62. Carmichael also explains that “[a]lternatively, **the location of the card** can be determined by a central processing center... which can identify the location of the card by identifying the location of the retail terminal or card reader to which the smart card is applied.” EX1007, 3:62-67. EX1003, ¶¶192, 277-279.

As discussed below in Section VI.B.6, it would have been obvious to combine Carmichael with Bossemeyer (and Glick) to incorporate Carmichael's teaching of using a smart card with "location tracking means for determining a location of the smart card," and a POSITA would have a reasonable expectation of success in combining Glick and Carmichael with Bossemeyer. EX1003, ¶¶193, 280.

Accordingly, Bossemeyer in view of Glick (and Carmichael for Ground 2) renders obvious this limitation. EX1003, ¶¶194, 281.

b. Smart Card Terminal Locatable With Current Location Data

Alternatively, Bossemeyer's **smart card terminal 14** and/or **advance smart card terminal 50** render obvious this limitation in view of Glick (and Carmichael for Ground 2). EX1003, ¶¶195, 282.

As discussed in Section VI.A.1, Bossemeyer "describes a network arrangement which is readily accessible from different types of smart card terminals [**smart card terminal 14** and/or **advance smart card terminal 50**] supporting various smart card applications." EX1005, 1:44-47. EX1003, ¶196.

It would have been obvious to implement **smart card terminal 14** and/or **advance smart card terminal 50** as a computer, e.g., a laptop computer, with a peripheral smart card reader. EX1005, 4:9-11 ("[A]dvance smart card terminals 50 which include a display unit 52, a keyboard 54, and a pointing device such as a track

ball 56 or mouse.”), 1:39-40 (“[M]uch prior work is focused on the design of smart cards, *smart card readers*...”); EX1007, 4:1-4 (“[T]he central processing center can be accessed by the smart card by coupling the microprocessor located on the smart card to *a reader coupled to a computer* linked to the central processing center.”), 7:4-5 (“A computer peripheral smart card reader...”), 7:15-16 (“When the card is placed in the peripheral reader...”), 8:50-52 (“All of this information can be downloaded through a computer peripheral reader to a *computer* and viewed on a computer screen or printed out.”), 6:62-67 (“The debit function of the smart card 1 is activated by a card reader that is capable of communicating with the smart chip 75 through the card reader interface on the chip. *A card reader* capable of interfacing with the chip 75 can be located anywhere, including retail stores, or *linked to a computer at home or at work*.”), 5:54-56 (“FIG. 5 is a flow chart describing a method and system of using the smart card of the present invention in connection with a computer peripheral reader.”), Figure 5. EX1003, ¶¶197-200.

Specifically, a POSITA would have found it obvious to implement a smart card terminal as a laptop computer with a peripheral smart card reader, for example, to allow users of Bossemeyer’s system to carry the smart card terminal and interact with multiple smart card holders. For example, a hospital doctor or medical personnel can conveniently use a laptop computer with a peripheral smart card reader to read smart cards of different patients in different rooms/floors of a hospital.

Accordingly, Bossemeyer's **smart card terminal 14/50** is a portable computing device. EX1003, ¶201.

A POSITA would have also understood that smart card terminals, like the ones disclosed in Bossemeyer, are also locatable with current location data. EX1007, 9:16-25 (“The location of the smart card 1 can also be determined at the time the smart card 1 is used by *identifying the location of the retail terminal*, automated teller machine, or *peripheral card reader*. Thus, when a debit, telephone, ATM, or credit function is processed and the institution's database is accessed, the institution will be capable of recognizing *the location of the card based on the retail terminal*, automated teller machine, or *peripheral card reader* from which the request originates and setting the conversion of currency based on that information.”), 3:64-67 (“[W]hich can identify *the location of the card* by *identifying the location of the retail terminal or card reader* to which the smart card is applied.”). EX1003, ¶202.

Bossemeyer's **smart card terminal 14** and/or **advance smart card terminal 50** is also an “appliance” as the term is used in Glick (EX1006, 5:12-17). Bossemeyer's **smart card terminals 14/50** are electronic devices with processing capability and memory capacity that can acquire and transmit information, and a capacity to acquire location information. EX1005, 2:13-16 (“The central database server 10 includes partitioned memory, described in further detail below, as well as

a microprocessor for processing *data received from and transmitted to the smart card terminal 14.*”), 4:9-14 (“[A]dvance smart card terminals 50 which include a display unit 52, a keyboard 54, and a pointing device such as a track ball 56 or mouse. ... [A] terminal 50 having *an established connection* through the network central office 16 to the central database server 10...”). A POSITA would have understood that receiving and transmitting data and/or maintaining an established connection with a networked device requires a processing capability to execute the receive/transmit instructions and a memory capacity, for example, to store the received data. EX1003, ¶¶203-204.

Accordingly, Bossemeyer in view of Glick (and Carmichael for Ground 2) renders obvious a “computer system having at least one **portable computing device** locatable with current location data” in two ways: (1) by Bossemeyer’s **smart card 12**; and (2) by Bossemeyer’s **smart card terminal 14** and/or **advance smart card terminal 50**. EX1003, ¶¶205-206, 282.

2. [81a] determining when said portable computing device is **within a predetermined region** based upon said **current location data**;

Bossemeyer in view of Glick renders obvious this limitation. Glick discloses that the *location of an appliance* is identified and then is compared to a *specific geographic location defined by the location identity attribute* to determine “*if the appliance location falls within the specific geographic location*”:

The location identity attribute is enforced by allowing access to the digital information only at the specific geographic location. As a first part of this enforcement process, *the location of an appliance through which access to the digital information is sought is identified. The appliance location is then compared to the specific geographic location defined by the location identity attribute*, and access to the digital information is allowed only *if the appliance location falls within the specific geographic location*.

EX1006, Abstract, 3:34-60, 8:16-35. EX1003, ¶¶207-208, 210, 283.

Glick also discloses that “[t]he location identity attribute further includes *a location value and a proximity value*” and that “[t]he proximity value corresponds to a zone that encompasses the location.” EX1006, 3:32-38. In Glick, “the location and proximity values 142, 143 are used to generate an area parameter 190 that defines *a shape of the geographic region defined by the location and proximity values*.” EX1006, 10:15-18, 6:29-39 (“FIG. 2 depicts a location identity attribute 140 as comprising two items of information: *a location value 142, and a proximity value 143*. The location value 142 corresponds to the unique position of a particular place.... The proximity value 143 corresponds to the extent of a zone or area that encompasses the location.”), 10:13-22, 11:28-38. EX1003, ¶209.

3. [81b] permitting full or partial reconstruction of said data via said **extracted data** from said extract stores and **remainder data**

Bossemeyer discloses and/or renders obvious this limitation. Bossemeyer discloses partitioning user data and storing them in a central database server according to different levels of security and then reconstructing the partitioned data, e.g., allowing access to the partitioned data, using “user identification codes”:

Different user identification codes... allow access to partitions in the database. 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, 2:38-47. EX1003, ¶¶211-212, 221, 284.

Specifically, Bossemeyer discloses that partitioned data is retrieved from the different partitioned memory portions of the central database server 10, and is presented, e.g., at a terminal, based on a particular user’s authorization:

Once the user’s authorization has been verified, data pointers on the smart card 12 provide access to the relevant partitioned memory portions of the central database server 10. Routing circuitry controlled by the microprocessor within the central database server 10 routes the data pointer to appropriate memory locations or database of the information keeper relating to the application at issue such as medical,

financial, etc. *Data from these various locations is supplied back to the smart card terminal 14, and if appropriate, the data stored on the smart card 12 is updated.*

EX1005, 3:63-4:6.

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, ¶¶213-214.

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. The system of Bossemeyer 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 then would merge these pieces of information (*i.e.*, reconstruct the original information to appear as before it was split into different security categories). Specifically, as Bossemeyer discloses, when the “[d]ata from these various locations is supplied back to the smart card terminal 14,” (EX1005, 4:3-5) 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, ¶¶215-217.

As an example, Bossemeyer discloses permitting partial reconstruction of a user's medical data (e.g., data including the user's *medical alerts 212*, and *insurance and prescription information 214*) and full reconstruction of data (e.g., data further including the user's *medical history 216*) with appropriate authorization:

FIG. 3 provides one example of the type of information accessible within or through the server 200. As mentioned above, information is stored in three levels of security: unrestricted, limited access, and restricted. In the pharmacy example, once the user's authentication code and merchant code have been verified by the system, the pharmacist may have access to the user's digital wallet 210, *medical alerts 212*, and *insurance and prescription information 214*. Without further authorization, however, the pharmacy would not have access to the user's *medical history 216*.

EX1005, 5:6-15.

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. EX1003, ¶¶218-219.

Glick also discloses an appliance that reconstructs requested information. EX1006, 4:4-8 (“The appliance that receives the encrypted digital information can generate a decryption key to decrypt the digital information based on the received area parameter and the appliance location determined in accordance with any of the foregoing methods.”). EX1003, ¶220.

4. [81c] only in the presence of a **predetermined security clearance access control** corresponding to said respective security level and

Bossemeyer discloses and/or renders obvious this limitation. EX1003, ¶¶222, 227, 285.

First, Bossemeyer discloses permitting reconstruction of user data in the presence of a **predetermined security clearance access control**, e.g., **user identification/authentication code** or **authorization/access code** associated with a particular security level.

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

EX1005, 2:38-47; *see also, id.*, 3:63-4:6.

Preferably, the smart card provides a one-time encrypted **user authentication code based on the user's digital signature or certificate**. This code, in turn, is transmitted over the communication network 100, 102 along with the merchant identification code to the server 10, 110. Thus, the digital signature of the card does not change,

but an *authorization code* generated by an encryption scheme known to the server provides a unique *access code* each time the card is involved in a transaction with the network.

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

EX1005, 4:50-65. EX1003, ¶223.

Second, Bossemeyer's *user identification codes* correspond to respective security levels. For example, as discussed in Section VI.B.3, Bossemeyer discloses an example describing accessing a user's medical data by permitting partial 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*):

FIG. 3 provides one example of the type of information accessible within or through the server 200. As mentioned above, information is stored in three levels of security: unrestricted, limited access, and restricted. In the pharmacy example, once the *user's authentication code* and merchant code have been verified by the system, the pharmacist may have access to the user's digital wallet 210, *medical alerts 212*, and *insurance and prescription information 214*. Without *further authorization*, however, the pharmacy would not have access to the user's *medical history 216*.

EX1005, 5:6-15.

USER DATA ↙ 200

	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. EX1003, ¶224.

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, ¶¶225-226.

5. [81d] only when said portable computing device is not beyond said predetermined region.

Bossemeyer in view of Glick renders this limitation obvious. As discussed in Section VI.B.2, Glick discloses determining if the appliance location falls within a predetermined region, i.e., not beyond the predetermined region. Glick also discloses that information can be accessed only when the appliance is not beyond the predetermined region:

A method and apparatus for *controlling access to digital information* utilizes a location identity attribute that defines a specific geographic location. The location identity attribute is associated with the digital information such that *the digital information can be accessed only at the specific geographic location. The location identity attribute further includes a location value and a proximity value.*

EX1006, Abstract, (“The appliance location is then compared to the specific geographic location defined by the location identity attribute, and *access to the digital information is allowed only if the appliance location falls within the specific geographic location.*”), 6:15-17 (“If an appliance 112 is located within the

geographic region A, then *the digital information 130 will be accessible by the appliance.*”). EX1003, ¶¶228-230, 233, 286.

Figures 5 and 10 of Glick, reproduced below, describe the steps for enforcing location identity and allowing access methods for accessing information only within a predetermined region.

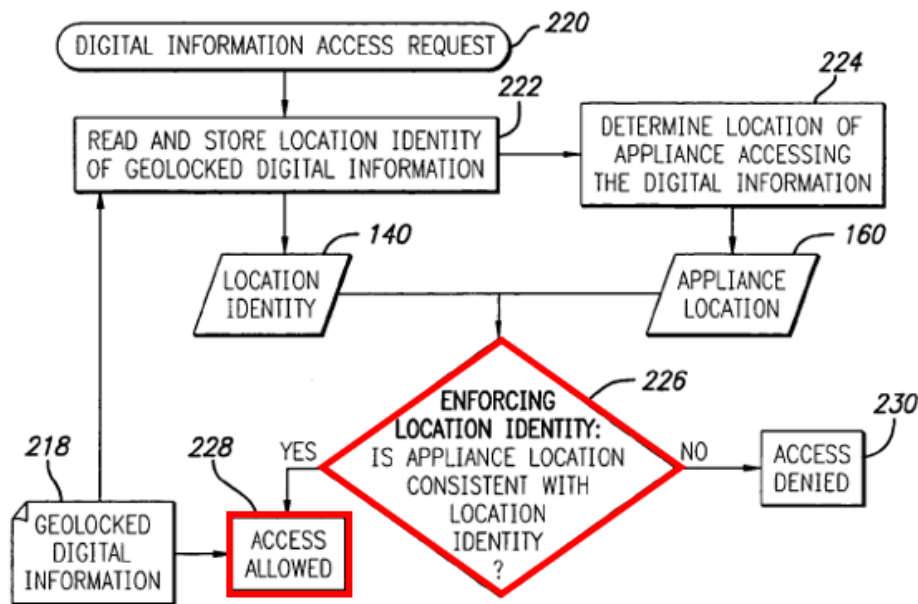


FIG. 5

EX1006, Figure 5.

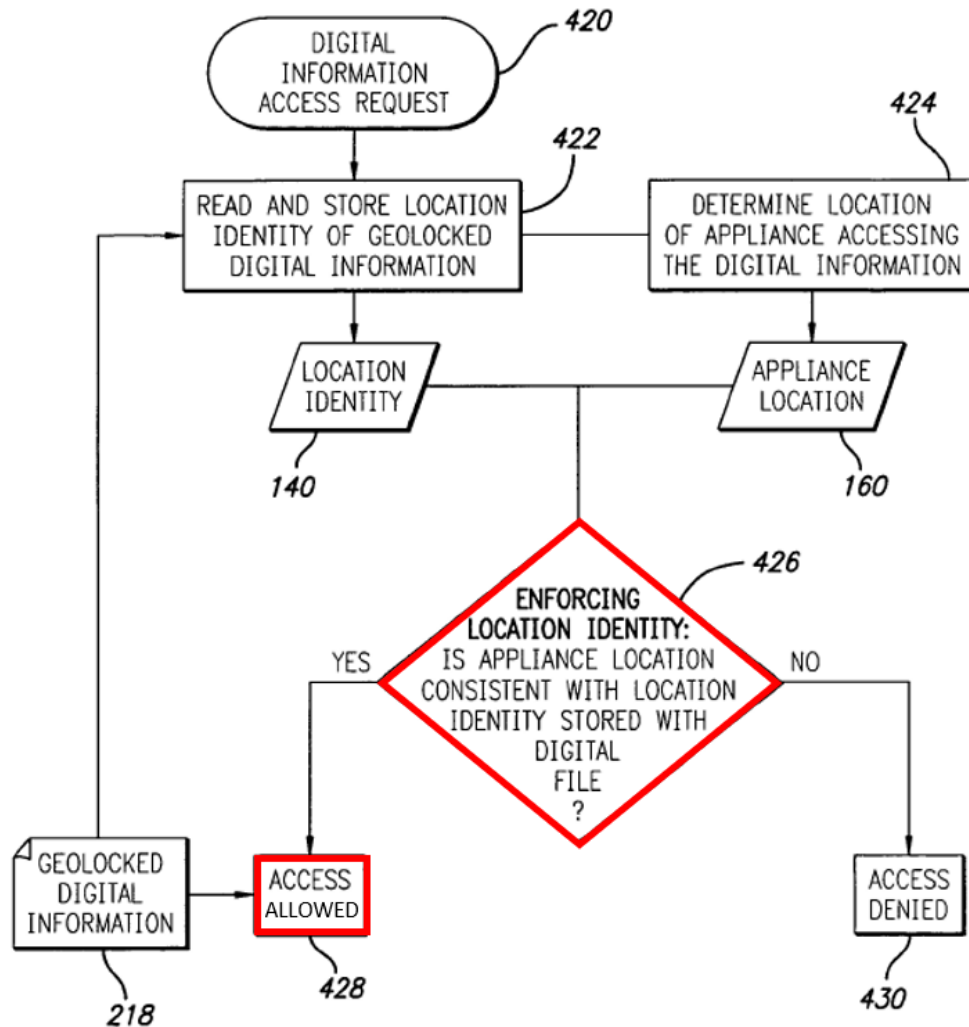


FIG. 10

EX1006, Figure 10, 8:22-34 (“At step 224, the method determines the location of the appliance accessing the digital information.... At step 226, the method determines whether the location of the appliance is consistent with the region defined by the location identity 140. *If the appliance location 160 is consistent with the location identity 140, then access to the geolocked digital information 218 is*

allowed at step 228. Conversely, if the appliance location 160 is not consistent with the location identity 140, then access is denied at step 230.”), 11:49-12:5. EX1003, ¶231.

Accordingly, a POSITA would have understood that Bossemeyer in view of Glick renders obvious reconstructing user’s data only when Bossemeyer’s portable computing device as modified by Glick is not beyond a predetermined region. EX1003, ¶¶232-233.

6. Reasons To Combine Bossemeyer With Glick (And Carmichael For Ground 2)

A POSITA would have been motivated to combine Bossemeyer and Glick to use location to control access to information, as taught by Glick, in Bossemeyer’s “network arrangement which is readily accessible from different types of smart card terminals supporting various smart card applications” (EX1005, 1:44-47), for several reasons. EX1003, ¶234.

First, the combination of Bossemeyer and Glick 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 Glick relate to the same field of providing different users access to information and address the same problem of controlling access to information. The Bossemeyer and Glick combination would merely involve using Glick’s location identity technique in

Bossemeyer's system according to the methods for determining the location disclosed in Glick. EX1005, 2:17-20 ("The central database server 10 is a centralized partitioned database server which partitions information both in terms of the smart card application as well as the accessibility of the information."), 1:49-52 ("With a centralized server architecture, data related to an individual can be accessed by an individual smart card, predefined groups of smart card users, or the general public."), 2:28-30 ("Private or proprietary information is partitioned such that the owner of the information has control over how the information is transferred and used."), 2:38-40 ("Different user identification codes, or data pointers, provided by smart cards 12 allow access to partitions in the database."); EX1006, Abstract ("A method and apparatus for controlling access to digital information utilizes a location identity attribute that defines a specific geographic location."), ("[T]he digital information can be accessed only at the specific geographic location."), 1:8-12 ("The present invention relates to the communication of digital information, and more particularly, to methods and systems for controlling interchange of digital information using a location integrity attribute associated with the digital information."), 3:48-55 ("There are many ways to identify the location of the appliance, including: (1) resolving the appliance location from a street address for the appliance; (2) retrieving the appliance location from a file stored within the appliance; (3) recovering the appliance location from a GPS receiver embedded in

the appliance; and (4) recovering the appliance location by triangulating RF signals received by the appliance.”); *see also*, EX1005, 2:40-55, 4:50-65, 5:6-31; EX1006, 3:17-23, 3:27-60. EX1003, ¶¶235-244.

Second, a POSITA would have been motivated to combine Bossemeyer with Glick, because Glick identifies a known problem, e.g., controlling access to information, and provides a solution to address the problem, e.g., using location identity to control access to that information. “Nothing more is required to show a motivation to combine under *KSR*...” *See Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373, 1381 (Fed. Cir. 2023) (holding that it was “enough for [Petitioner] to show that there was a known problem” in the art and that the referenced prior art helped address that issue). Glick’s use of location identity to control 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 a specific location or region. “‘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, ¶¶245-251.

Third, a POSITA would have been motivated to use Glick’s location identity to control access to sensitive/proprietary information, because it would improve

Bossemeyer's system by using location identity to control access to information stored in Bossemeyer's central database server, thereby adding an extra level of security when accessing stored user information. That is, the combination would merely be a use of a known technique (e.g., using location identity) to improve similar methods (e.g., controlling access to information) in the same way (e.g., by allowing access to information only within a predetermined region). *KSR*, 550 U.S. at 417. As discussed in Sections VI.B.3 and VI.B.4, Bossemeyer discloses accessing user data only in the presence of a predetermined security clearance access control. Adding Glick's teachings of using location identity to control access to user data would be an improvement to the security and access control afforded to users of Bossemeyer's system. For example, without Glick's location-based access control, medical personnel that have a user's authentication code could have access to a user's sensitive medical data, for example, outside of the hospital premises, which could potentially compromise the security of the data, e.g., by allowing non-medical personnel to view the data. EX1003, ¶¶252-259.

Fourth, a POSITA would have been motivated to combine Bossemeyer with Glick, because the combination would involve applying a known technique (e.g., using Glick's location identity to control access to information) to a known device (e.g., Bossemeyer's network arrangement with a central database server storing user

information), which was ready for improvement to yield predictable results. *KSR*, 550 U.S. at 401. EX1003, ¶¶260-261.

Fifth, Glick provides express motivations that would have led a POSITA to combine Glick's and Bossemeyer's teachings. Indeed, Glick acknowledges that advances in computer, telecommunications and networking technology allow companies and individuals to access and share vast amounts of information. EX1006, 1:14-29. However, Glick recognizes that:

In spite of the tremendous value that this information access has brought to society, there are also enormous costs associated with the uncontrolled flow of information. ***One of the most important considerations for a communication system is the control over information security and access.*** In many cases, a sender of information wants to ensure that the intended recipient can only access the information, and that any other unintended recipients of the information are denied access.

Id., 1:30-34. Glick also discloses that "it would be desirable to provide an information interchange system and method that ***allows control over security and access to the information.***" *Id.*, 3:19-22. Glick provides numerous examples of the benefits of using location identity to control access of information. *Id.*, 12:42-44 ("There are numerous applications and data formats in which the location identity attribute can be used to control access to digital information."). Glick discloses that location identity can be used to prevent unauthorized use and copying of digital

information/media. *Id.*, 12:64-13:14. Glick also discloses that location identity can be used to transmit information to a limited audience within a particular geographic region, facilitating location-based applications. *Id.*, 13:35-55. Glick also discloses that location identity can be used to enhance confidentiality and security for network connectivity. *Id.*, 13:56-14:4. EX1003, ¶¶262-267.

A POSITA would also have had a reasonable expectation of success in combining Bossemeyer with Glick. Indeed, as discussed in Section VI.B.1.v, both Bossemeyer’s **smart card 12** and Bossemeyer’s **smart card terminals 14/50** are “appliances,” as the term is used in Glick, because they have data processing capabilities and memory sufficient to receive and transmit information. EX1006, 8:7-14. (“[Glick’s] method would be performed by a system or device having a data processing capability and memory sufficient to enable receipt of digital information communicated or distributed by another party, such as a personal computer, server, router, personal digital assistant (PDA), workstation, network, laptop, and the like.”). EX1003, ¶270.

As discussed in Section VI.B.1.v.1, to the extent Patent Owner argues that Bossemeyer does not render obvious a smart card that is locatable with current location data, a POSITA would have also been motivated to combine Bossemeyer (and/or Glick) with Carmichael to implement Carmichael’s teaching of a location

tracking means in Bossemeyer's smart card "for determining a location of the smart card" (EX1007, 3:32-34), for several reasons. EX1003, ¶287.

First, the combination of Bossemeyer (and/or Glick) with Carmichael represents the use of known techniques according to known methods in the same way to yield predictable results. *KSR*, 550 U.S. at 416. Bossemeyer and Carmichael relate to the same field of smart cards and applications that are facilitated by the use of smart cards. The Bossemeyer and Carmichael combination would merely involve including Carmichael's location tracking means, e.g., (GSM chip), into Bossemeyer's smart card in the same way as taught by Carmichael, because Bossemeyer and Carmichael disclose similar systems and methods. EX1005, Abstract ("A network for smart card applications using a smart card in combination with a smart card terminal."), 1:8-11 ("This invention relates to smart card applications and, more particularly, to a network arrangement to provide access to an architecture that supports a variety of advanced smart card applications."); EX1007, 1:8-14 ("The present invention relates to smart cards. In particular, the present invention relates to multi-application or multi-function smart cards and systems and methods for implementing multiple functions on a single smart card. More particularly the present invention relates to payment, banking, identification, location, and currency exchange systems using a smart card."), 4:6-12 ("The location tracking capabilities of the smart card are particularly useful for when the smart card

is lost or stolen, or when a person holding the smart card needs to be located. The location tracking capabilities also make it possible for the smart card holder to generate a travel log or a map of the locations in which he has traveled while carrying the card.”). EX1003, ¶¶288-289.

Second, a POSITA would have been motivated to combine Bossemeyer with Carmichael, because Carmichael identifies known problems (e.g., enabling location-based smart card applications, locating lost or stolen cards, automatically altering the currency of the stored value), and provides a solution to address the problem, e.g., using a GSM chip, to determine the location of the smart card. “Nothing more is required to show a motivation to combine under *KSR*...” *See Intel Corp.*, 61 F.4th at 1373. Carmichael’s use of location tracking means in a portable device, e.g., smart card, e.g., by using a GSM chip in the device, to enable locating the portable device is a “universal motivation” known in the field of geo-tracking and improves the technology, by enabling applications to utilize the location of the portable device to offer location-related services to the portable device user. “[U]niversal’ 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, ¶¶290-292.

Third, a POSITA would have been motivated to use Carmichael’s location tracking means in Bossemeyer’s smart card to determine the location of

Bossemeyer's smart card, because it would improve Bossemeyer's smart card system by enabling location-based smart card applications. That is, the combination would merely be a use of a known technique (e.g., using location tracking means) to improve similar methods (e.g., enabling new smart card applications) in the same way (e.g., by using the information stored in the smart card at different terminals). *KSR*, 550 U.S. at 417. Carmichael's use of location tracking means to enable location-based smart card applications is a "universal motivation" known in the field of smart cards and improves the technology, by enabling a new set of smart card applications that would not have been possible without the ability to determine the location of the smart card. EX1003, ¶¶293-294.

Fourth, a POSITA would have been motivated to combine Bossemeyer with Carmichael because the combination would involve applying a known technique (e.g., using Carmichael's location tracking means to locate a smart card) to a known device (e.g., Bossemeyer's smart card), which was ready for improvement to yield predictable results. *KSR*, 550 U.S. at 401. EX1003, ¶¶295-296.

Fifth, Carmichael provides express teachings, suggestions, or motivations that would have led a POSITA to combine Carmichael's and Bossemeyer's teachings. Indeed, Carmichael discloses that the location tracking capabilities of the smart card are useful to retrieve lost or stolen cards and/or generate travel maps:

The location tracking capabilities of the smart card are particularly useful for when the smart card is lost or stolen, or when a person holding the smart card needs to be located. The location tracking capabilities also make it possible for the smart card holder to generate a travel log or a map of the locations in which he has traveled while carrying the card.

EX1007, 4:6-12. EX1003, ¶297.

Carmichael also discloses that the location tracking capabilities of the smart card solve the problem of altering the currency of the stored monetary value in the card:

Another disadvantage of current credit and smart cards is that they are incapable of altering the currency of the stored value. The present invention solves this problem by providing a program associated with the smart chip, which can automatically communicate with a central source of currency exchange rate information for converting in real time the currency of the stored value and for generating and providing a current exchange schedule for currencies of any nation. Therefore, travelers can easily and conveniently use their smart cards in foreign countries and can even obtain currency exchange information by using their smart card.

EX1007, 2:60-3:3, 3:4-19. EX1003, ¶298.

A POSITA would have found that Bossemeyer and Glick (and Carmichael for Ground 2) were analogous to the '825 Patent. All three (or four) pertain to the same

field of endeavor, *i.e.*, securing security-sensitive information. *Compare* EX1001, 1:23-26 *with* EX1005, 1:8-11, 1:44-47 *and* EX1006, Abstract, *and also with* EX1007, 3:35-45. EX1003, ¶¶268, 299.

To the extent that Patent Owner argues that the references are not in the same field of endeavor as the '825 Patent, Bossemeyer and Glick (and Carmichael for Ground 2) are still reasonably pertinent to the particular problem with which the '825 Patent's invention is involved, *i.e.*, securing digital information. *Compare* EX1001, 6:55-58 *with* EX1005, 2:17-22; *compare also* EX1001, 7:64-65 *with* EX1006, Abstract, *and also with* EX1007, 4:46-50. EX1003, ¶¶269, 300.

A POSITA would also have had a reasonable expectation of success in combining Bossemeyer and Glick with Carmichael. Combining Bossemeyer (and/or Glick) with Carmichael would merely involve including Carmichael's location tracking means, *e.g.*, (GSM chip), into Bossemeyer's smart card in the same way as taught by Carmichael, because Bossemeyer and Carmichael disclose similar systems and methods. For example, Bossemeyer and Carmichael are both directed to smart cards, a central server(s), and terminals that facilitate smart card applications. *Compare* EX1005, 1:45-47, 3:3-5, *with* EX1007, 1:8, 4:1-6, 4:46-50. Carmichael's "central processing center" is a "central database server" as the term is used in Bossemeyer, where both contain distinct memories for different functions. *Compare* EX1005, 5:50-52 (disclosing a "server that includes a plurality of

application-specific partitioned memory locations”), *with* EX1007, 3:63-64 (disclosing a “central processing center which stores data relating to all of the functions of the smart card”), 4:59-64 (“Other steps of the method can include operatively coupling the smart card to the access device, reading at least of the four sets of data, performing a first authentication process on said at least one set of data, and permitting access if said step of performing a first authentication process meets a required condition.”). EX1003, ¶¶301-303.

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 Board’s Final Written Decision is expected in December 2024.² While trial is currently scheduled for August 19, 2024 (EX1010), the Board recognizes “that scheduled trial dates are unreliable and often change.” *See* Director’s June 21, 2022 Memorandum on Discretionary Denials (“Memo”), 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 this factor [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.” Memo, 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 the Eastern District of Texas between 19 months (March 2023) and 24.2 months (March 2022). EX1011, 1. Accordingly, the projected trial date for purposes of *Fintiv* is between June 2024 (which is unlikely since June 2024 is before the scheduled trial date of August 2024) and December 2024—approximately 24.2 months after November 28, 2022—and around the Board’s Final Written Decision,

² December 2024 is 18 months after June 2023, when Petitioner expects a notice of accorded filing date for this petition.

which is expected in December 2024. Because the projected trial date based on the two most recent statistics is either before or “around the same time or after” the Board’s expected final written decision, and because the median-time-to-trial statistics can fluctuate by months for consecutive periods, this factor is neutral.

3. Investment in the parallel proceeding

The co-pending litigation is in its very early stages, and the investment in it has been minimal. *See* EX1009, EX1010. The parties have not exchanged preliminary positions on claim construction and expert discovery has not begun. *See PEAG LLC v. Varta Microbattery GmbH*, IPR2020-01214, Paper 8, 17 (Jan. 6, 2021). Further, the Markman hearing is not scheduled until March of 2024. EX1009, 4.

Moreover, Patent Owner served their infringement contentions on February 28, 2023. *See* 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 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 Claim unpatentable as obvious. “[T]he PTAB will not deny institution of an IPR or PGR under *Fintiv* (i) when a petition presents compelling evidence of unpatentability.” Memo, 9. “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 ’825 Patent claims no more than the known concept of storing sensitive data in security-controlled memories. The evidence of unpatentability is compelling, and thus the PTAB should not deny institution under *Fintiv*.

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

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

Discretionary denial under § 325(d) is not warranted because the challenges presented in this petition are neither cumulative nor redundant to the prosecution of the '825 patent. The PTO has not previously considered Bossemeyer, Glick, or Carmichael in connection with the claims of the '825 Patent. Further, the combination is not redundant to any combination of references considered during prosecution. Additionally, Dr. Zadok is an expert in the relevant art, and his analysis of the prior art has not been presented to the PTO. EX1003, ¶¶45-304. 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 Claim is unpatentable.

Case IPR2023-00967
U.S. Patent No. 7,313,825

Dated: May 31, 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 '825 patent is or was involved in the following case:

Case Heading	Number	Court	Date
<i>DigitalDoors, Inc.³ 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

³ The '825 Patent cover page (EX1001, 1) and the USPTO assignment database (<https://assignment.uspto.gov/patent/index.html#/patent/search/resultAssignment?searchInput=7313825&id=13896-755>) identify “Digital Doors, Inc.” as the assignee of the '825 Patent.

Case IPR2023-00967
U.S. Patent No. 7,313,825

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

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 13,514. 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: May 31, 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. 7,313,825;
- Exhibit List;
- Exhibits 1001-1030;
- 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 May XXX, 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:

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

Case IPR2023-00967
U.S. Patent No. 7,313,825

Dated: May 31, 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