

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INTERNATIONAL BUSINESS MACHINES CORPORATION

Petitioner

v.

DIGITAL DOORS, INC.

Patent Owner

Case IPR2023-00967

U.S. Patent No. 7,313,825

Claim 81

**DECLARATION OF EREZ ZADOK, PH.D.
ON BEHALF OF PETITIONER**

TABLE OF CONTENTS

	<u>Page</u>
I. Qualifications.....	1
II. Background.....	13
III. Relevant Law	15
A. Claim Construction.....	15
B. Obviousness.....	16
C. Ordinary Skill in the Art.....	18
IV. Summary of Opinions.....	19
V. Technology Overview	19
A. General Computer Operations.....	19
B. Data Storage Devices and Systems	21
C. Networked and Distributed Storage Systems.....	22
D. File and Data Security, Security Levels	25
E. Location Identification	31
VI. Overview Of The '825 Patent.....	32
A. Prosecution History of the '825 Patent	40
VII. Overview Of The Prior Art.....	44
A. Bossemeyer (U.S. Patent No. 7,010,701, "EX1005").....	44
B. Glick (U.S. Patent No. 6,985,588, "EX1006")	52

C.	Carmichael (U.S. Patent No. 7,913,919, “EX1007”).....	58
VIII.	Level of Ordinary Skill in the Art	61
IX.	Claim Construction.....	62
X.	Specific Grounds for Challenge	62
A.	Ground I: Bossemeyer In View Of Glick Renders Obvious Claim 81	62
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:	62
i.	A method of securing data having one or more security sensitive words, characters, data objects or icons	63
ii.	in a computer system with a plurality of security controlled memories as respective extract stores with security access controls thereat, ...	69
iii.	said security sensitive words, characters, data objects or icons extracted from said data to obtain extracted data and remainder data	74
iv.	which extracted data is stored in respective extract stores corresponding to a respective security level of said extract stores, ...	81

v.	said computer system having at least one portable computing device locatable with current location data, comprising:.....	86
a.	Smart Card Locatable With Current Location Data	87
b.	Smart Card Terminal Locatable With Current Location Data	92
2.	[81a] determining when said portable computing device is within a predetermined region based upon said current location data;	97
3.	[81b] permitting full or partial reconstruction of said data via said extracted data from said extract stores and remainder data.....	100
4.	[81c] only in the presence of a predetermined security clearance access control corresponding to said respective security level and	106
5.	[81d] only when said portable computing device is not beyond said predetermined region.....	110
6.	A POSITA Would Have Been Motivated To Combine Bossemeyer with Glick (Ground 1)	114
B.	Ground II: Bossemeyer In View Of Glick and Carmichael Renders Obvious Claim 81	131
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: 131
- i. A method of securing data having one or more security sensitive words, characters, data objects or icons 132
 - ii. in a computer system with a plurality of security controlled memories as respective extract stores with security access controls thereat, ...132
 - iii. said security sensitive words, characters, data objects or icons extracted from said data to obtain extracted data and remainder data 132
 - iv. which extracted data is stored in respective extract stores corresponding to a respective security level of said extract stores, ...133
 - v. said computer system having at least one portable computing device locatable with current location data, comprising:.....133
 - a. Smart Card Locatable With Current Location Data 133
 - b. Smart Card Terminal Locatable With Current Location Data 135
2. [81a] determining when said portable computing device is within a predetermined region based upon said current location data; 135
3. [81b] permitting full or partial reconstruction of said data via said extracted data from said extract stores and remainder data.....135

4.	[81c] only in the presence of a predetermined security clearance access control corresponding to said respective security level and	136
5.	[81d] only when said portable computing device is not beyond said predetermined region.....	136
6.	A POSITA Would Have Been Motivated To Combine Bossemeyer with Glick and Carmichael.....	136
XI.	Conclusion	147
XII.	Availability for Cross-Examination	147
XIII.	Right to Supplement	148
XIV.	Jurat.....	148

I, Erez Zadok, declare as follows:

1. My name is Erez Zadok.
2. I have been retained as an expert witness in the field of storage, file systems, and data security protocols on behalf of Petitioner International Business Machines Corporation (“IBM”) to provide expert opinions on the validity of U.S. Patent No. 7,313,825 (the “’825 Patent”).

I. Qualifications

3. In formulating my opinions, I have relied on my knowledge, training, and experience in the relevant field, which I will summarize briefly. A more detailed summary of my background, education, experience, and publications is set forth in my curriculum vitae (CV), which is submitted as EX1004.

4. I have personal knowledge of the facts and opinions set forth in this declaration and believe them to be true. If called upon to do so, I would testify competently thereto. I have been warned that willful false statements and the like are punishable by fine or imprisonment, or both. I have had no contact with any of the named inventors of the ’825 Patent.

5. My consulting company, Zadoks Consulting, LLC, is being compensated for my time at my current standard consulting rate. I am also being reimbursed for expenses that I may incur during the course of this work. My

compensation is not contingent upon the results of my study and analysis, the substance of my opinions, or the outcome of any proceeding involving the Challenged Claim(s). I have no financial interest in the outcome of this matter or in any litigation involving the '825 patent.

6. I am a Professor in the Computer Science Department at Stony Brook University (part of the State University of New York (“SUNY”) system). I direct the File-systems and Storage Lab (FSL) at Stony Brook’s Computer Science Department. My research interests include file systems and storage systems, operating systems, information technology and system administration, security and information assurance, networking, energy efficiency, performance and benchmarking, virtualization, cloud systems, compilers, applied machine learning, and software engineering.

7. I studied at a professional high school in Israel, focusing on electrical engineering (“EE”), and graduated in 1982. I spent one more year at the high school’s college division, receiving a special Certified Technician’s degree in EE. I then went on to serve in the Israeli Defense Forces for three years (1983-1986). I received my Bachelor of Science degree in computer science (“CS”) in 1991, my Master’s degree in CS in 1994, and my PhD in CS in 2001—all from Columbia University in New York.

8. When I began my undergraduate studies at Columbia University, I also started working as a student assistant in the various campus-wide computer labs, eventually becoming an assistant to the head labs manager, who was managing all public computer labs on campus. During that time, I also became more involved with research within the CS Department at Columbia University, conducting research on operating systems, file and storage systems, distributed and networked systems, security, and other topics. I also assisted the CS department's computer administrators in managing the department's computers, which included storage, IT, networking, and cyber-security related duties.

9. In 1991, I joined Columbia University's CS department as a full-time systems administrator, studying towards my MS degree part-time. My MS thesis topic is related to file system reliability, fault tolerance, replication, and failover in mobile networked storage systems using file virtualization. My main duties as a systems administrator involved installing, configuring, and managing many networked servers, proxies, and desktops running several operating systems, as well as network devices setup; this included many hardware upgrades, device upgrades, and BIOS firmware/chipset updates/upgrades. My duties also included ensuring reliable, secure, authenticated access to networked systems/storage and licensed software, as well as software updates, security and bug fixes. Examples of servers

and their protocols included email (SMTP), file transfer (FTP), domain names (DNS), network file systems (NFS), network news systems (NNTP), and Web (HTTP).

10. In 1994, I left my systems administrator position to pursue my doctoral studies at Columbia University. My PhD thesis topic was on versatile file system development using stackable (virtualized) file systems, with examples in the fields of security and encryption, efficiency, reliability, and failover. I continued to work part-time as a systems administrator at the CS department, and eventually I was asked to serve as manager to the entire information technology (“IT”) staff. From 1991 to 2001, I was also a member of the faculty-level Facilities Committee that oversaw all IT operations at the CS department.

11. As part of my PhD studies at Columbia, I collaborated on projects to develop advanced AI-like techniques to detect previously unknown viruses (a.k.a. “zero-day malware”), using data mining and rule-based detection. This work led to several highly cited papers (over 1,400 citations for one of the papers alone), and two patents. I also became a Teaching Assistant (TA) for a first-ever Computer Security course given at Columbia University’s CS department with Dr. Matt Blaze as instructor.

12. From 1990 to 1998, I consulted for SOS Corporation and HydraWEB Technologies, as a systems administrator and programmer, managing data storage use and backup/restore duties, as well as information assurance and cyber-security (*e.g.*, malware protection, software licensing). From 1994 to 2000, I led projects at HydraWEB Technologies, and then became the Director of Software Development—overseeing the development of several products and appliances such as stateful firewalls and HTTP load-balancers, utilizing network-virtualization and high-availability techniques. From 2009 to 2019, I have consulted for Packet General Networks, a startup specializing in secure, virtualized, network storage and applications’ data security in the cloud.

13. In 2001, I joined the faculty of Stony Brook University, a position I have held since that time. In 2002, I joined the Operations Committee, which oversees the IT operations of the CS department at Stony Brook University. From 2006 to 2010, I was the Director of IT Operations of the CS department; my day-to-day duties included setting policies regarding computing, hiring and training new staff, assisting any staff with topics of my specialty, defining requirements for new software/hardware, and purchasing. From 2010 to 2015, I had served as the Co-Chair to the Operations Committee. From 2016 to 2019, I oversaw the IT Operations as the Chair of the Operations Committee. A significant component of these duties

included defining and helping implement policies for data management, so as to ensure the security of users and their data, and data reliability and availability, while minimizing the inconvenience and performance impact to users. I personally helped setup and maintain an initial virtual-host infrastructure in the department. Since late 2019, I've been a member of the department's Executive Committee that also oversees all IT operations.

14. In 2017, I became the department's Graduate Academic Adviser, advising all Master students (over 400 annually on average) and many other graduate students on an assortment of academic matters.

15. Since 2001, I personally configured and managed my own research lab's network. This includes setting up and configuring multiple storage systems (*e.g.*, NFS, CIFS/SMB, NAS), virtual and physical environments, applications such as database and mail servers, user access control (*e.g.*, NIS, LDAP), backups and restores, snapshot policies, and more. I've personally installed, configured, changed, replaced parts, and upgraded components in numerous devices including mobile devices, laptops, desktops, and servers, both physical and virtual.

16. Since 1995, I have taught courses on operating systems, storage and file systems, advanced systems programming in Unix/C, systems administration, data structures, data/software security, and more. My courses often use storage, file

systems, distributed systems, and system/network security as key teaching principles and practical examples for assignments and projects. I have taught these concepts and techniques to my students, both to my direct advisees as well as in my courses. For example, in my graduate Operating Systems course, I often cover Linux's kernel mechanisms to protect users, applications, and data files, virtual file systems, as well as distributed storage systems (*e.g.*, NFS). And in the System Administration undergraduate course, I covered many topics such as networking, storage, backups, and configuring complex applications such as mail, web, and database servers.

17. My research often investigates computer systems from many angles: security, efficiency, energy use, scalability, reliability, portability, survivability, usability, ease-of-use, versatility, flexibility, and more. My research gives special attention to balancing five often-conflicting aspects of computer systems: performance, reliability, energy use, security, and ease-of-use.

18. Since joining Stony Brook University in 2001, my group in the File-systems and Storage Lab (FSL) has developed many file systems and operating system extensions; examples include a highly-secure cryptographic file system, a portable copy-on-write (COW) versioning file system, a tracing file system useful to detect intrusions, a replaying file system useful for forensics, a snapshotting and sandboxing file system, a namespace unification file system (that uses stackable,

virtualized, file-based COW), an anti-virus file system, an integrity-checking file system, a load balancing and replication/mirroring file system, network file system extensions for security and performance, distributed secure cloud-based storage systems, transactional key-value stores and file systems, OS-level embedded databases, a compiler to convert user-level C code to in-kernel efficient yet safe code, GCC plugins, stackable file system templates, and a Web-based backup system. Many of these projects used one form of virtualization or another (storage, network, host, etc.). I continue to maintain and release newer versions of some of these file systems and software.

19. I have published over 120 refereed publications (in ACM, IEEE, USENIX, and more). To date, my publications have been cited more than 11,000 times (as per Google Scholar as of April 17, 2023). My papers cover a wide range of related technologies such as file systems, storage systems, transactional systems, security, clouds and virtualization, performance benchmarking and optimization, energy efficiency, system administration, and more. I also published a book titled “Linux NFS and Automounter Administration” (Sybex, 2001), covering systems administration topics related to network storage and data security.

20. Some of my research has led to public software releases that have been used worldwide. I have publicly maintained the Amd Berkeley Automounter in a

package called “am-utils” since 1992; this software helps administrators manage the multitude of file system mounts on dozens of different Unix systems, especially helping to automate access to multiple NFS/NAS storage volumes. Since 1997, I have maintained and released several stackable (virtualized) file system software projects for Linux, FreeBSD, and/or Solaris, in a package called FiST. One of my stackable file system encryption projects, called Cryptfs, became the basis for IBM’s public release of eCryptfs, now part of Linux. Packet General Networks, for whom I have provided consulting services between 2009 and 2019, licensed another encryption file system called Ncryptfs. Another popular file system released in 2003, called Unionfs, offers virtual namespace unification, transparent shadow copying (a.k.a. copy-on-write or COW), file system snapshotting (*e.g.*, useful for forensics and disaster recovery), and the ability to save disk space by sharing a read-only copy of data among several computers, among other features.

21. My research and teaching make extensive use of data security features. For example, each time I taught the graduate operating system course, the first homework assignment includes the creation of a new system call that performs new or added functionality, often for encrypting a file or verifying its integrity; many of my other assignments cover topics of user/process access control, anti-virus filtering,

and more. Since 2001, over 1,000 graduate students were exposed to these simple principles directly through my teaching and research at Stony Brook University.

22. Moreover, in an undergraduate course titled “Advanced Systems Programming in Unix/C,” I cover many topics of system security and vulnerabilities, such as the structure of UNIX processes, and memory segments such as the heap and stack. This course covers details of several hundred Linux system calls. Often, the first assignment for this course is to develop a tool to encrypt/decrypt files using advanced ciphers, use digital signatures to certify the cipher keys used, and reliably recover files in case of failures. Since 2001, several hundred undergraduate students were exposed to these principles directly through my teaching and research at Stony Brook University.

23. In another undergraduate course, System Administration, I taught network configuration, security, and storage configuration and reliability. In a special topics course on Storage Systems, I covered many topics such as data deduplication, RAID, transactional storage, storage hardware including modern Flash based ones, virtual storage, backup/restore, snapshots and continuous data protection (CDP), NAS and SAN, and NFS.

24. Overall, in addition to the aforementioned experience, my technical experience relevant to the challenged patent(s) at the time of the alleged invention(s)

included the following: setting and managing up computer hosts (Unix, Windows, MacOS) with local storage and file systems; setting up and managing networked file systems (NFS, SMB/CIFS); setting up and managing secure backup/restore systems with separate data and meta-data storage repositories (Legato Networker), and restoring data from such backup systems; configuring and managing network domain name systems (DNS) to assign and identify hosts and their IP addresses; configuring and managing network firewalls, and setting up filtering rules by IP addresses; configuring filtering rules for Web and Email systems based on location (region, country of origin); configuring and using access controls to many hosts with multiple levels of security, from regular users vs. administrators (aka “root” or “superuser”), to POSIX permissions (*e.g.*, user, group, and other), to fine-grained access-control lists (ACLs) for one or more users and groups thereof, with disjunctive and conjunctive capabilities; investigating, researching, and developing secure and encrypted file system (including my own PhD dissertation).

25. My research has been supported by many federal and state grants as well as industry awards, including an NSF CAREER award, two IBM Faculty awards, two NetApp Faculty awards, a Western Digital award, a Facebook award, several Dell-EMC awards, and several equipment gifts. I received the 2008 SUNY Chancellor’s Excellence in Teaching award, and the 2022 SUNY Chancellor’s

Award for Excellence in Scholarship and Creative Activities (both awards can be given only once in a lifetime). In 2021 I was named an ACM Distinguished Member for “Outstanding Scientific Contributions to Computing.”

26. My service record to the community includes serving as the co-chair for the USENIX Annual Technical Conference in 2020 (ATC’20); serving as the co-chair for USENIX File and Storage Technologies (FAST’15) in 2015 and serving on the FAST Conference Steering Committee since 2015; serving on the ACM HotStorage Steering Committee in 2021; and serving as the co-chair in 2012 and on the Steering Committee of the ACM SYSTOR conference. I have served as an Associate Editor to the ACM Transactions on Storage (TOS) journal from 2009 to 2022; in late 2022, I was named the Editor-in-Chief for ACM’s TOS journal.

27. I am a named inventor on four patents, two titled “Systems and Methods for Detection of New Malicious Executables” (U.S. Patent No. 7,487,544, issued February 3, 2009; and U.S. Patent No. 7,979,907, issued July 12, 2011); and two more titled “Multi-Tier Caching,” (U.S. Patent No. 9,355,109, issued May 31, 2016; and U.S. Patent 9,959,279, issued May 1, 2018).

28. I have been disclosed as a testifying expert in 15 cases (including *inter partes* review (IPR) proceedings) in the past four years. I have been deposed 12 times and testified in trial twice.

II. Background

29. I have reviewed all of the exhibits cited in this declaration, including the following:

Exhibit No.	DESCRIPTION
1001	U.S. Patent No. 7,313,825 (“825 patent”)
1002	Prosecution History of U.S. Patent No. 7,313,825
1004	<i>My Curriculum Vitae</i>
1005	U.S. Patent No. 7,010,701 to Bossemeyer et al. (“Bossemeyer”)
1006	U.S. Patent No. 6,985,588 to Glick et al. (“Glick”)
1007	U.S. Patent No. 7,588,180 to Carmichael et al. (“Carmichael”)
1008	U.S. Publication No. 2004/0148290 to Merenda et al. (“Merenda”)
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)
1023	Microsoft Computer Dictionary, Fourth Edition, Copyright 1999, Excerpts
1024	Beck et al., Linux Kernel Internals, 2nd Ed., Copyright 1998, pp. 148-187

Exhibit No.	DESCRIPTION
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”)

30. I understand that the ’825 Patent has a filing date of March 19, 2003, claiming priority to applications 60/400,062, 60/400,112, 60/400,406, and 60/400,407, all dated August 2, 2002. EX1002 (’825 Prosecution History), 1, 3; EX1013 (Provisional Application No. 60/400,062); EX1014 (Provisional Application No. 60/400,112); EX1015 (Provisional Application No. 60/400,406); EX1016 (Provisional Application No. 60/400,407). The ’825 Patent also claims priority to a series of continuation-in-part patents (EX1009-EX1014); EX1001 (the ’825 Patent), 1:4-22. None of these patents disclose all the limitations of challenged claim 81, and therefore I have been informed and I understand that the ’825 Patent is not entitled to an earlier priority date based on any of these patents. Therefore, I assume that the earliest possible priority date of the ’825 Patent is August 2, 2002. I understand that all prior art references used in this declaration predate the earliest possible priority date of the ’825 Patent of August 2, 2002. Thus, I have considered

certain issues from the perspective of a person of ordinary skill in the art as described below as of August 2, 2002.

III. Relevant Law

31. I am not an attorney. For the purposes of this declaration, I have been informed about certain aspects of the law that are relevant to my opinions. My understanding of the law is as follows:

A. Claim Construction

32. I have been informed that claim construction is a matter of law and that the final claim construction will ultimately be determined by the Board. For the purposes of my analysis in this proceeding and with respect to the prior art, I have been informed that IPRs are currently reviewed under “the *Phillips* standard.”

33. I have been informed that under the *Phillips* standard, claim terms are given their plain and ordinary meaning as understood by a person of ordinary skill in the art at the time of the invention in light of the claim language and the patent specification.

34. I have been informed that embodiments described in the specification are generally encompassed by the claims.

35. I have been informed that the patentee can serve as their own lexicographer. As such, if a claim term is provided with a specific definition in the

specification, then I should interpret that claim term in light of the particular definition provided by the patentee.

B. Obviousness

36. I have been informed and understand that a patent claim can be considered to have been obvious to a person of ordinary skill in the art at the time the application was filed. This means that, even if all of the requirements of a claim are not found in a single prior art reference, the claim is not patentable if the differences between the subject matter in the prior art and the subject matter in the claim would have been obvious to a person of ordinary skill in the art at the time the application was filed.

37. I have been informed and understand that a determination of whether a claim would have been obvious should be based upon several factors, including, among others:

- the level of ordinary skill in the art at the time the application was filed;
- the scope and content of the prior art; and
- what differences, if any, existed between the claimed invention and the prior art.

38. I have been informed and understand that a claim can be unpatentable in light of a single prior art reference if it would have been obvious to modify that reference to come up with the claimed subject matter.

39. I have been informed and understand that the teachings of two or more references may be combined in the same way as disclosed in the claims, if such a combination would have been obvious to one having ordinary skill in the art.

40. In determining whether a combination based on either a single reference or multiple references would have been obvious, it is appropriate to consider, among other factors:

- whether the teachings of the prior art references disclose known concepts combined in familiar ways, which, when combined, would yield predictable results;
- whether a person of ordinary skill in the art would have implemented a predictable variation, and would have seen the benefit of doing so;
- whether the claimed elements represent one of a limited number of known design choices, and would have a reasonable expectation of success by those skilled in the art;
- whether a person of ordinary skill would have recognized a reason to combine known elements in the manner described in the claim;

- whether there is some teaching or suggestion in the prior art to make the modification or combination of elements claimed in the patent; and
- whether the claim applies a known technique that had been used to improve a similar device or method in a similar way.

41. I understand that one of ordinary skill in the art has ordinary creativity and is not an automaton.

42. I understand that in considering obviousness, it is important not to determine obviousness using the benefit of hindsight derived from the patent being considered.

C. Ordinary Skill in the Art

43. I understand that, in the context of an invalidity analysis, a person having ordinary skill in the art (“POSITA”) is a hypothetical person who looks to prior art at the time of the invention.

44. I further understand that the factors that may be considered in determining the level of ordinary skill in the art include: (1) the problems encountered in the art; (2) the prior art solutions to the problems encountered in the art; (3) the rapidity of innovation; (4) the sophistication of the technology; and (5) the education level of active workers in the field. I understand that these factors

need not all be taken into account for the analysis and that one or more of these factors may control.

IV. Summary of Opinions

45. It is my opinion that claim 81 of the '825 Patent is rendered obvious by the prior art identified below:

Ground	References	Invalid Claim
I	Bossemeyer, Glick	81
II	Bossemeyer, Glick, Carmichael	81

V. Technology Overview

46. In this section, I provide a brief overview of the background art as understood by a person of ordinary skill in the art as of August 2, 2002.

A. General Computer Operations

47. Computers are hardware and software devices that execute instructions. The hardware often includes a central processing unit (CPU), typically called “processor,” volatile memory (*e.g.*, RAM (random-access memory), or DRAM (dynamic random-access memory)), non-volatile (persistent) storage (*e.g.*, a hard disk or flash drive), and input/output (I/O) devices (*e.g.*, network interface card, mouse, keyboard, display). RAM, hard disks, and flash drives are considered,

generally, “storage” or “memory” devices because they can store and hold bits of information (whether persistently or not). Computers can have multiple storage devices. Processors are coupled to main memory using a memory bus and to peripherals such as hard disks and network interface cards using one or more I/O busses.

48. Memory and storage devices have considerable differences in their speeds, capacities, and costs. Non-volatile storage devices such as hard disks have the largest capacity, are least expensive per gigabyte, and are slowest (typically operating at millisecond speeds). Volatile DRAM devices are smaller, more expensive, and faster than hard disks (typically operating at microsecond speeds). CPUs’ own memory caches and operations are the smallest, most expensive, and fastest (typically operating at nanosecond speeds). Overall, CPUs are about 1,000× faster than DRAM, which in turn is about 1,000× faster than hard disks.

49. Computer programs are often written in a high-level human-readable language (*e.g.*, C, C++, Java), then translated using a compiler or script processor to machine instructions understood by the CPU (*e.g.*, Intel or AMD processor). Machine instructions—generally called “software”—are stored in files on persistent media, loaded into DRAM, and then loaded into the CPU where they can be executed. All modern computers operate in this manner, regardless of their purpose:

a small laptop, a server in a data center, a mainframe computer, a personal workstation, a proxy device, a firewall, a router, an appliance, a virtual machine, a handheld or mobile device, smart card, etc.

50. Users (including administrators) can login to one or more computers (*e.g.*, desktop, laptop, server) and execute one or more applications (*e.g.*, word processing, web browsing, backup tool).

B. Data Storage Devices and Systems

51. As mentioned in Section V.A above, computers often include two types of storage or memory devices. The first type is volatile memory device, called Random Access Memory (“RAM”), that is often used to hold programs that are executing and their data. EX1023 (Microsoft Dictionary), p. 372 (“RAM”).

52. The second type is a non-volatile, or persistent storage device, such as a hard disk drive (“HDD”). HDDs are used to store programs and data persistently. EX1023 (Microsoft Dictionary), p. 212 (“hard disk”).

53. HDDs are electro-mechanical devices with moving parts. Computers can also have other types of non-volatile storage devices that have no moving parts, also called “solid-state devices,” such as flash memories. EX1023 (Microsoft Dictionary), p. 188 (“flash memory”).

54. Moreover, any single device (*e.g.*, a hard disk) can be logically broken down into several units called “partitions.” EX1023 (Microsoft Dictionary), p. 144 (“**disk partition** *n.* A logical compartment on a physical disk drive. A single disk might have two or more logical disk partitions, each of which would be referenced with a different disk drive name. Multiple partitions are divided into a primary (boot) partition and one or more extended partitions.”).

55. Above the storage media often lives a logical software layer called a “file system.” File systems provide a convenient abstraction to users and applications of files, folders or directories, and naming. EX1023 (Microsoft Dictionary), p. 185 (“**file system** *n.* In an operating system, the overall structure in which files are named, stored, and organized. A file system consists of files, directories, or folders, and the information needed to locate and access these items. The term can also refer to the portion of an operating system that translates requests for file operations from an application program into low-level, sector-oriented tasks that can be understood by the drivers controlling the disk drives. *See also* driver.”).

C. Networked and Distributed Storage Systems

56. File systems can appear as local volumes (*e.g.*, the C:\ drive in Windows), but they can also be networked, where the physical storage resides on a remote file server. EX1023 (Microsoft Dictionary), p. 309 (“**Network File System**

n. See NFS.”), p. 311 (“**NFS** *n.* Acronym for Network File System. A distributed file system developed by Sun Microsystems, Inc. that allows users of Windows NT and UNIX workstations to access remote files and directories on a network as if they were local.”).

57. Even storage media can be networked into a large cluster of devices, that can export virtual block devices to individual hosts, called a “storage area network” (SAN). EX1023 (Microsoft Dictionary), p. 424 (“storage area network”), p. 432 (“system area network”), p. 398 (“SCSI network”).

58. When the amount of data to access grew large enough, and especially if the data had to be concurrently accessed from multiple users/applications, storage researchers and companies leveraged the principles of distributed to improve the performance, resiliency, and fault-tolerance of the storage system.

59. A single computer’s performance is limited by the physical maximum speeds of its network, processor, memory, and I/O devices. A distributed system, however, improves overall performance by using multiple computers concurrently to process many requests, thus increasing the aggregate throughput manyfold.

60. A single computer also represents a single point of failure: if that one computer is down, off, or broken into, then the service it offers is unavailable. A distributed system, conversely, improves resiliency and security by ensuring that the

failure of any one (or even few) components do not affect the overall service provided. This principle is called “fault tolerance.” EX1023 (Microsoft Dictionary), p. 179 (“**fault tolerance** *n.* The ability [] to respond to a catastrophic event or fault, such as a power outage or a hardware failure, in a way that ensures that no data is lost and any work in progress is not corrupted. [] In a fault-tolerant network, the system has the ability either to continue the system’s operation without loss of data or to shut the system down and restart it, recovering all processing that was in progress when the fault occurred.”).

61. NFS is but one example of a networked or distributed file system. Many complex software systems have been designed to operate in a distributed manner, where they are more resilient to failures and scale better than software running on a single node. EX1023 (Microsoft Dictionary), p. 147 (“**distributed system** *n.* A noncentralized network consisting of numerous computers that can communicate with one another and that appear to users as parts of a single, large, accessible ‘storehouse’ of shared hardware, software, and data. A distributed system is conceptually the opposite of a centralized, or monolithic, system in which clients connect to a single central computer, such as a mainframe.”), p. 146 (“**distributed file system** *n.* A file management system in which files may be located on multiple computers connected over a local or wide area network.”).

62. One example of a popular distributed system is that of databases, where different components are often distributed, stored, and managed separately. EX1023 (Microsoft Dictionary), p. 146 (“**distributed database** *n.* A database implemented on a network. The component partitions are distributed over various nodes (stations) of the network. Depending on the specific update and retrieval traffic, distributing the database can significantly enhance overall performance. *See also* partition (definition 2).”), p. 146 (“**distributed database management system** *n.* A database management system capable of managing a distributed database. *Acronym:* DDBMS. *See also* distributed database.”).

D. File and Data Security, Security Levels

63. All modern file and storage systems include measures of security to protect their data from unauthorized access. EX1023 (Microsoft Dictionary), p. 184 (“**file protection** *n.* A process or device by which the existence and integrity of a file are maintained. Methods of file protection range from allowing read-only access and assigning passwords to covering the write-protect notch on a disk and locking away floppy disks holding sensitive files.”).

64. The POSIX standard, first started in the late 1980s, codifies the access application program interfaces (APIs) that operating systems export to user applications. EX1023 (Microsoft Dictionary), p. 351 (“**POSIX** *n.* Acronym for

Portable Operating System Interface for UNIX. An IEEE standard that defines a set of operating-system services. Programs that adhere to the POSIX standard can be easily ported from one system to another. POSIX was based on UNIX system services, but it was created in a way that allows it to be implemented by other operating systems.”).

65. A simple data protection scheme defines whether users can only read files, only write files, or have both read and write access. EX1023 (Microsoft Dictionary), p. 13 (“**access permission** *n.* See permission.”), p. 388 (“**permission** *n.* In a networked or multiuser computer environment, the ability of a particular user to access a particular resource by means of his or her user account. Permissions are granted by the system administrator or other authorized person. Several levels of access can be given: read only, read and write (view and change), or read, write, and delete. *Also called* Access permission.”).

66. In the basic POSIX model, for example, a file has three sets of permissions (read, write, or execute) for three classes of users (owner, group member, and everyone else).

67. More sophisticated schemes generalize these simpler permission models to allow for lists of users, lists of groups, as well as logical operations on lists (*e.g.*, negation, conjunction, and disjunction). These are called “access control

lists,” or ACLs. EX1023 (Microsoft Dictionary), p. 12 (“**access control** *n.* The mechanisms for limiting access to certain items of information or to certain controls based on users’ identities and their membership in various predefined groups. Access control is typically used by system administrators for controlling user access to network resources, such as servers, directories, and files. *See also* access privileges, system administrator.”), p. 12 (“**access control list** *n.* A list associated with a file that contains information about which users or groups have permission to access or modify the file. *Acronym:* ACL.”).

68. ACLs existed in Unix systems since at least the 1990s (and I personally used them). EX1024 (“Beck”), p. 182 (“The inode table for a block group lists consecutive blocks, starting with the one specified, and consists of inodes 128 bytes in size (see Figure 6.7). In addition to the data already mentioned, these contain the time when the file was deleted (to use in restoring deleted files), entries for ACLs (Access Control Lists to enable access permissions to be differentiated more precisely) and information specific to the operating system used.”), p. 185 (“The development of the Ext2 file system is not yet complete. The list of planned expansions includes: [] ACLs []”).

69. Security has often been defined in terms of levels because it was more logical and convenient to use: each higher level progressively has greater security

control than the level just below, and hence subsumes the latter. The U.S. Department of Defense defined a standard in 1985, famously called the “Orange Book” (because the book’s cover was colored orange), which includes four general different levels of security (from A (most secure) to D (least secure)), each with one or more sub-levels of security. EX1023 (Microsoft Dictionary), p. 323 (Orange Book).

70. The Orange Book defines a “Security Level” as “The combination of a hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information.” and “sensitivity label” as “A piece of information that represents the security level of an object and that describes the sensitivity (e.g., classification) of the data in the object. Sensitivity labels are used by the TCB as the basis for mandatory access control decisions.” EX1025 (Orange Book), p. 111.

71. The Orange Book detailed how data of different security levels has to be stored in separate compartments or locations, for example level C1. EX1025 (Orange Book), p. 15 (“The Trusted Computing Base (TCB) of a class (C1) system nominally satisfies the discretionary security requirements by providing separation of users and data. It incorporates some form of credible controls capable of enforcing access limitations on an individual basis, i.e., [] allowing users to be able

to protect project or private information and to keep other users from accidentally reading or destroying their data. [].”

72. Even earlier than the Orange Book, in 1971 the CIA defined its policies for “Security of Compartmented Computer Operations” that data of different security levels preferably were stored and accessed by different computer systems. EX1026 (“CIA”), p. 2 (“**Policy 6.** Remotely accessed resource-sharing computer systems shall not be utilized for the concurrent processing and/or storage of two or more types of sensitive compartmented information [].”

73. A POSITA would have understood that separating information of different security levels into different compartments made it much easier to safeguard and control access to such information. This is no different than when people store some sensitive information (*e.g.*, bills) in a desk drawer at home, more sensitive information in a home safe (*e.g.*, passports), and the most sensitive information in a bank safe (*e.g.*, estate planning documents, home title/deed).

74. Similarly, the U.S. National Security Agency (NSA) defined its own standard called the “Red Book”, again defining multiple security levels. EX1023 (Microsoft Dictionary), p. 377 (“Red Book”).

75. A POSITA would have understood that these security levels can be applied to any piece of information, including paper and electronic documents and

data. The U.S. military has long had similar security levels, for example top-secret, secret, and confidential—each level being higher than the next and subsuming the access rights of those below (*e.g.*, a person with “secret” clearance could also access “confidential” documents but not those marked “top-secret”).

76. Even without having such standards, Unix administrators knew how to leverage much simpler POSIX permission models to effectively create security levels (something I did myself in the 1990s).

77. For example, one could create two Unix groups: (1) a group named “sales-managers” that includes the identities of all the sales managers in an organization and (2) a second group named “sales-people” the includes the same managers but also all the salespersons in the organization. In other words, the sales-people group includes everyone in the sales-managers group and more. A file whose access permissions are set to group sales-people will be accessible by all sales people as well as managers; but a file whose access permissions are set to group sales-managers will only be accessible to the sales managers, and hence regular salespersons will not have access to that file. In such a way, a two-level security hierarchy is created, with sales-managers being logically at a higher security level than sales-people. The same mechanism can be used to create an arbitrarily long set of security levels.

78. As discussed above, ACLs are more versatile than these simpler Unix permission models. Therefore, with ACLs, the construction of any number of data or file security levels becomes even easier.

E. Location Identification

79. Identifying the location of a user or electronic device has always been desired. For example, law enforcement agencies often try to identify the location of a suspect in order to prove or disprove their whereabouts; and credit-card companies want to know where a credit card had been used in relation to its owner, to reduce the chances of fraud.

80. On the Internet, each computer has a host name that uniquely identifies it. EX1023 (Microsoft Dictionary), p. 221 (“**host name** *n.* The name of a specific server on a specific network within the Internet, leftmost in the complete host specification. For example, www.microsoft.com indicates the server called ‘www’ within the network at Microsoft Corporation.”).

81. On the Internet, each computer also has an IP address that uniquely identifies it. EX1023 (Microsoft Dictionary), p. 248 (“IP address”). Each host name is part of a domain. EX1023 (Microsoft Dictionary), p. 150 (“domain”), p. 446 (“top-level domain”). These domains clearly identify the host location or geography. EX1023 (Microsoft Dictionary), p. 280 (“major geographic domain”).

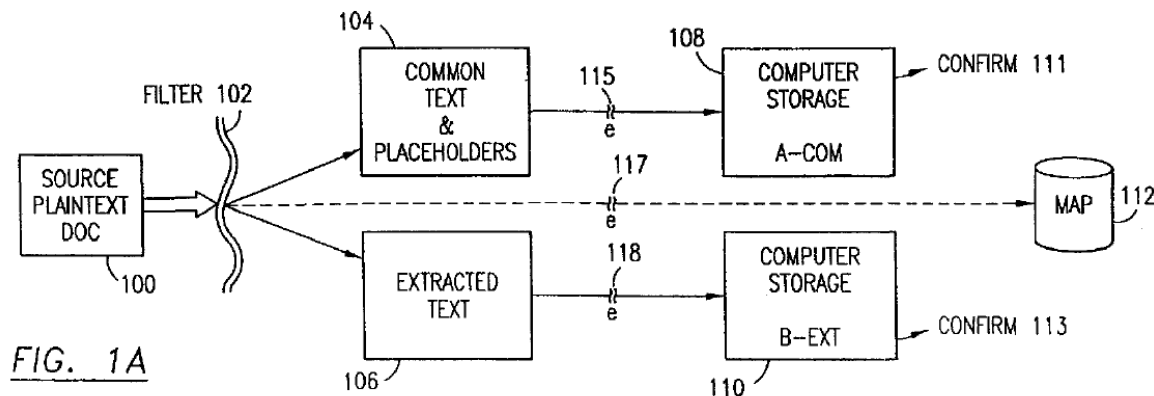
In the Internet, the Domain Name System is a world-wide distributed database that maps host names to IP addresses and vice versa. EX1023 (Microsoft Dictionary), p. 151 (“Domain Name System”), p. 148 (“DNS”). Numerous DNS Servers on the Internet manage this distributed database. EX1023 (Microsoft Dictionary), p. 148 (“DNS name server”), pp. 148-149 (“DNS server”).

82. In sum, a POSITA would have understood that simply having a computer’s IP address or host name is sufficient to identify its location. And once a location is known, simple access controls can be enforced to allow or deny access when one is inside or outside a specific geographic area. For example, a U.S. bank may allow its employees to access customer checking accounts from the corporate network and perhaps from approved satellite locations (*e.g.*, an employee working from home or while traveling), but not if the access is attempted from, say, a hostile foreign country.

VI. Overview Of The ’825 Patent

83. The ’825 Patent purports to create a new method that is used with a portable computing device to protect security sensitive words, icons, etc. by determining device location within or without (outside) a predetermined region and then extracting the security data from the file, text, or data object. EX1001 (the ’825 Patent), Abstract. According to the ’825 Patent, prior systems did not adequately

“limit the distribution and publication of security sensitive words, characters, or icons.” EX1001 (the '825 Patent), 1:45-46. Figure 1A, below, illustrates the disclosed security system:



EX1001 (the '825 Patent), Figure 1A.

84. As shown, a source document 100, which represents a data object that is “any item that can be represented in an electronic format at the electronic format can be manipulated by a computer” is sent to a filter 102 that “separates out common text or remainder data 104 from uncommon text, words, characters, icons, or data objects.” EX1001 (the '825 Patent), 19:42-48. “[R]emainder data’ is simply a short-hand representation of data that is not extracted or filtered by the system.” EX1001 (the '825 Patent), 20:55-57. Remainder data is data that can be “viewed, manipulated or further processed by the user inputting or initially processing the data.” EX1001 (the '825 Patent), 20:57-60. After the data is passed through the

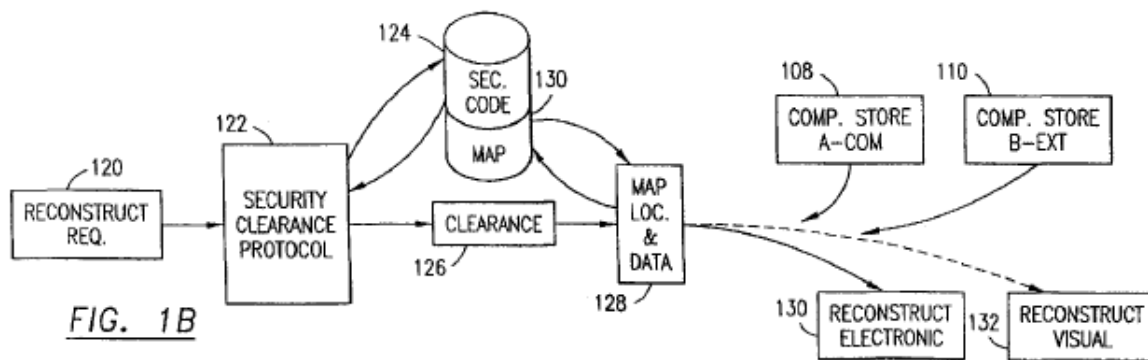
filter, the “security sensitive” objects are separated from remainder or common text 104 as extracted text 106. EX1001 (the ’825 Patent), 19:48-50.

85. After the data is separated, it is placed in storage. EX1001 (the ’825 Patent), 11:63-64. For storage, “the common text or the remainder data is stored in common storage memory 108.” EX1001 (the ’825 Patent), 20:50-51. “The extracted data file 106 is stored in a different memory computer storage 110,” but is preferably stored at a “different location than computer storage memory segment 110.” EX1001 (the ’825 Patent), 20:63-67-.

86. The security system is compatible with multiple security levels. EX1001 (the ’825 Patent), 39:54-62. “For security systems having multiple security levels, a plurality of filters would be created, each filter associated with a different security level.” EX1001 (the ’825 Patent), 21:62-65. Having multiple security levels “require[s]... a plurality of extracted documents 106... [where] each extracted document 106 would be stored in a respective, separate computer memory segment [] 110.” EX1001 (the ’825 Patent), 21:65-22:4. Having separate storage for extracted data of different security levels is “one of the many important features of the present invention.” EX1001 (the ’825 Patent), 22:5-7. The single remainder storage 108 would store all of the common or remainder text documents or data. EX1001 (the ’825 Patent), 21:67-22:2.

87. Once extracted, the categorized data objects are then “separated into one or more contiguous data streams” which are then “scattered to one or more storage memory memories.” EX1001 (the '825 Patent), 23:21-29.

88. To enable secure storage of the data, the system reconstructs the data or data object that was previously in storage. EX1001 (the '825 Patent), 7:27-30. Figure 1B, shown below, illustrates the major features of the reconstruction routine/system.



EX1001 (the '825 Patent), Figure 1B.

89. Upon a user's reconstruction request, the system can execute a security clearance protocol routine 122 to determine whether the user has the proper security clearance. EX1001 (the '825 Patent), 24:50-54. Multiple users are allowed to use the system; in that case, “those multiple users have different security clearances” which in turn requires the security clearance protocol to “determine[] the level of security clearance and, hence, the full or partial reconstruction of the plaintext.”

EX1001 (the '825 Patent), 24:56-60. To ensure that clearance in step 126 is accurate, “the security code input by the user is checked against a security code database.”

EX1001 (the '825 Patent), 24:60-63. “[M]ap 130 show[s] the location of [extracted and remainder] memory segments.” EX1001 (the '825 Patent), 24:65-66. When the reconstruction phase occurs, “[f]unction 130 operates as a compiler to gather the extracted data and remainder data into a single plaintext document.” EX1001 (the '825 Patent), 25:9-11.

90. The system can be portable, such as portable computing device 810 shown in Figure 14.

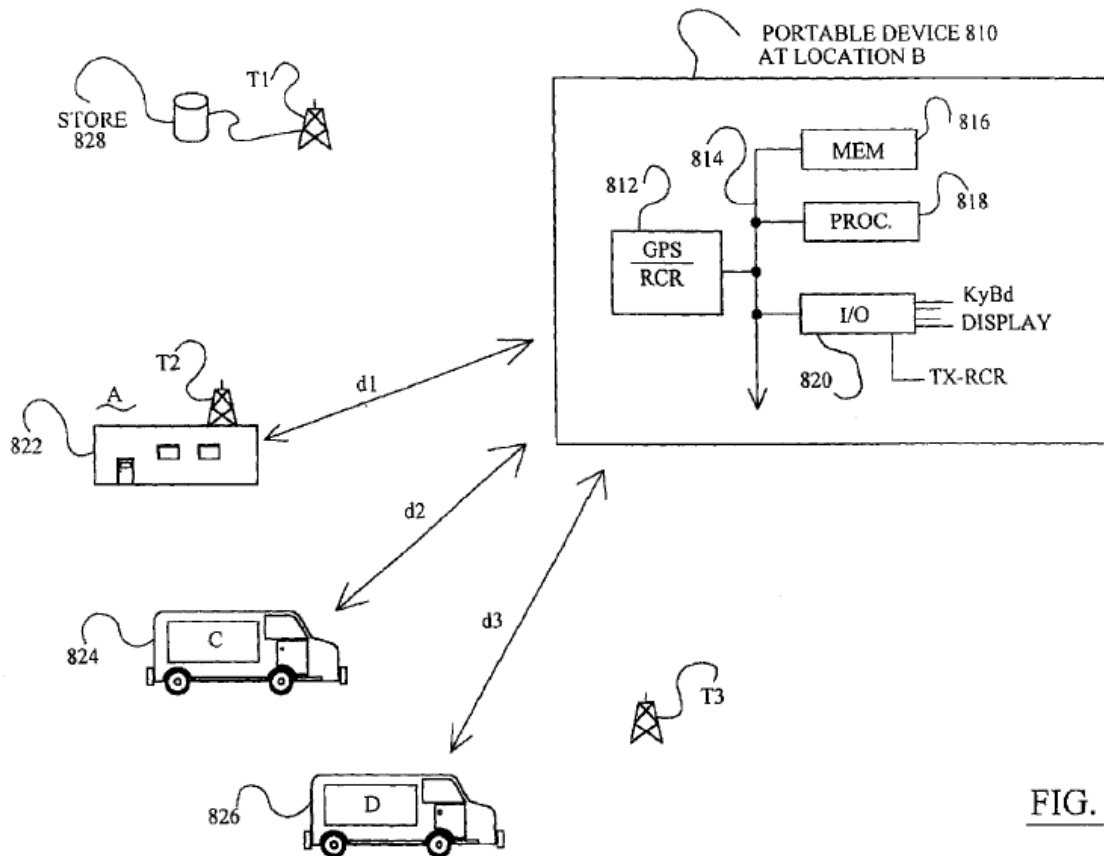


FIG. 14

EX1001 (the '825 Patent), Figure 14.

91. The invention “can be applied to portable computing devices to secure files and data objects in such devices.” EX1001 (the '825 Patent), 58:41-42. The device “permits reconstruction utilizing security protocols to provide 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 (the '825 Patent), 58:44-48.

92. The location in the system acts as an “automated trigger” or “location based access oriented security ... which activates the security program [] when the portable computing device is beyond a predetermined region.” EX1001 (the '825 Patent), 58:62-67. “The regions ... can consist of complex definitions of three dimensional areas of arbitrary shape and sizes, as long as those regions can be defined by algorithms.” EX1001 (the '825 Patent), 59:18-22. In addition, the system works both ways: “access can be denied if the portable device is within a certain region as compared with denying access when the device is beyond a predetermined region.” EX1001 (the '825 Patent), 59:24-28.

93. Figure 15, below, illustrates a basic flow chart for the portable security system program utilized in connection with portable computing device 810.

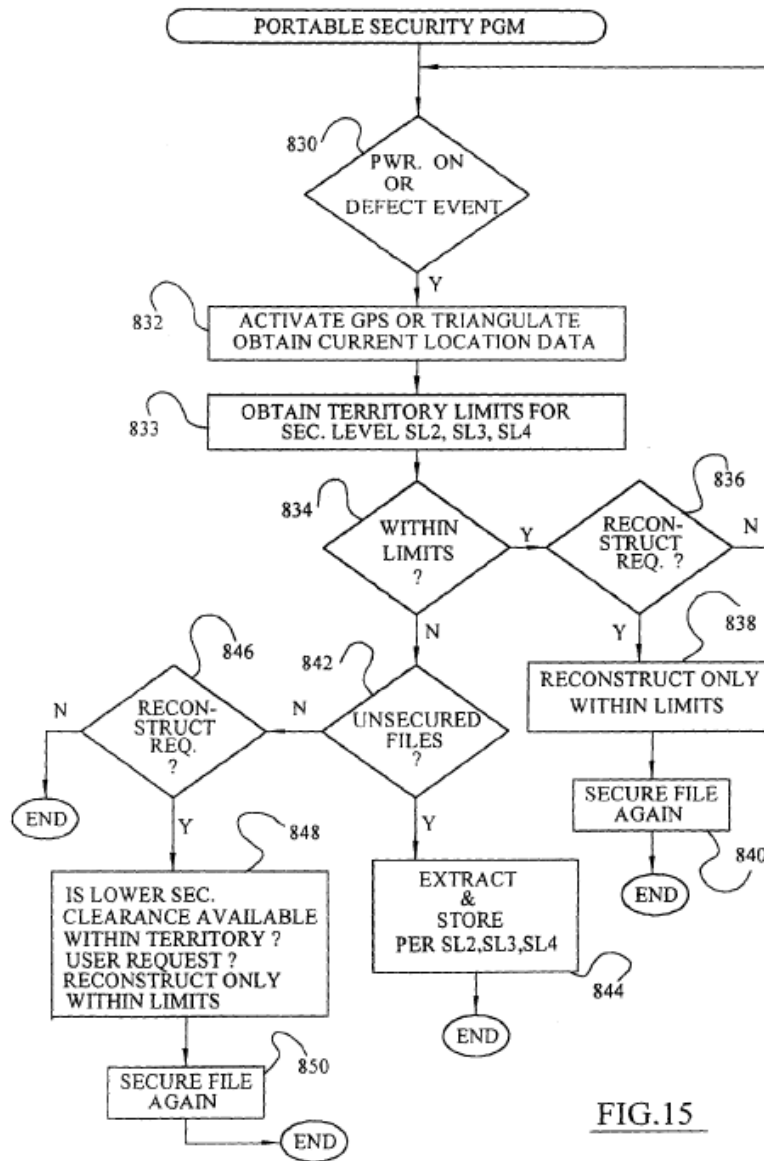


FIG.15

EX1001 (the '825 Patent), Figure 15.

94. 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 (the '825 Patent), 60:64-66. If within the region, the system determines if the user has

initiated a reconstruction request. EX1001 (the '825 Patent), 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.” EX1001 (the '825 Patent), Figure 15.

A. Prosecution History of the '825 Patent

95. I have reviewed the file history of the '825 patent. EX1002 ('825 Prosecution History). I summarize the relevant information that I have reviewed pertaining to my opinion.

96. The file history has what appears to be the application number of the application (*i.e.*, 10/390,807), the March 19, 2003, filing date, and the priority to provisional applications 60/400,062, 60/400,112, 60/400,406, and 60/400,407, all dated August 2, 2002. EX1002 ('825 Prosecution History), 1, 3. The application number and the filing date are consistent with the information shown on the cover of the '825 patent. EX1001 (the '825 Patent), Cover. The application was filed with 146 total claims, containing 8 independent claims. EX1002 ('825 Prosecution History), 2.

97. On January 23, 2007, the Examiner rejected claim 84 (which ultimately issued as claim 81) as being obvious over U.S. Patent Nos. 5,960,080 (EX1027, “Fahlman”), 6,370,629 (EX1028, “Hastings”) and 6,253,203 (EX1029, “O’Flaherty”). EX1002 ('825 Prosecution History), 266. The Examiner found that

Fahlman disclosed a method of securing data but did not have a portable computing device. EX1002 ('825 Prosecution History), 266-67. The Examiner further found that Hastings “teaches the use of a portable computing device; determining when the device is beyond a certain location; [and] providing data when the device is not beyond this location.” EX1002 ('825 Prosecution History), 267. The Examiner also found that O’Flaherty “teaches the remainder store and extract store are stored in separate locations.” EX1002 ('825 Prosecution History), 267. The Examiner argued that the combination of such features was obvious to a POSITA “to allow different information to be allowed in different locations (*see* EX1028 (Hastings), 1:39-57) and to prevent the ability to ascertain the identity of a customer (*see* EX1029 (O’Flaherty), 14:26-57).” EX1002 ('825 Prosecution History), 267.

98. The Applicant responded by amending claim 84 (as shown below) to remove “designated as a remainder store and an extract store” and to instead recite, among other things, “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 ('825 Prosecution History), 309.

99. The 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 ('825 Prosecution History), 331. The Applicant further argued that 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," thus making "[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." EX1002 ('825 Prosecution History), 331-32.

100. 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 ('825 Prosecution History), 334.

101. The Examiner mailed a Notice of Allowance on August 9, 2007. EX1002, 491.

102. The Examiner noted 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 (’825 Prosecution History), 497.

103. The ’825 Patent issued on December 25, 2007. EX1001 (the ’825 Patent), 1. As shown in this declaration, the cited prior art teaches these and the other features of the challenged claim.

VII. Overview Of The Prior Art

A. Bossemeyer (U.S. Patent No. 7,010,701, “EX1005”)

104. Bossemeyer is a U.S. Patent filed on October 19, 1999, and issued on March 7, 2006. I understand that Bossemeyer is prior art because it is a U.S. Patent that was filed prior to the earliest possible priority date of the ’825 Patent.

105. Bossemeyer is directed to “a network arrangement to provide access to an architecture that supports a variety of advanced smart card applications.” EX1005 (Bossemeyer), 1:9-11. Smart cards are electronic devices that “can hold much more information [than existing data cards],” where a “data card” includes “financial cards such as credit cards, debit cards, ATM cards, as well as non-financial data cards such as energy company cards, department store cards... driver’s licenses, building security cards, and personal identification cards.” EX1005 (Bossemeyer), 1:34-35, 1:17-22. Such smart cards “often include some ‘intelligence’ such as a microprocessor or the like.” EX1005 (Bossemeyer), 1:34-

37, 3:28-31 (“Smart card 12... contains circuitry 40 which includes a microprocessor and memory including random access memory (RAM) and read only memory (ROM).”).

106. Bossemeyer acknowledges that although “much prior work is focused on the design of smart cards, smart card readers, and applications for smart cards, there has been much less focus on the integration of a centralized server architecture or a network arrangement for multiple smart card applications.” EX1005 (Bossemeyer), 1:39-43. Bossemeyer discloses 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 (Bossemeyer), 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 (Bossemeyer), 1:49-52.

107. Figure 1 of Bossemeyer discloses an example of a network arrangement including a central database server.

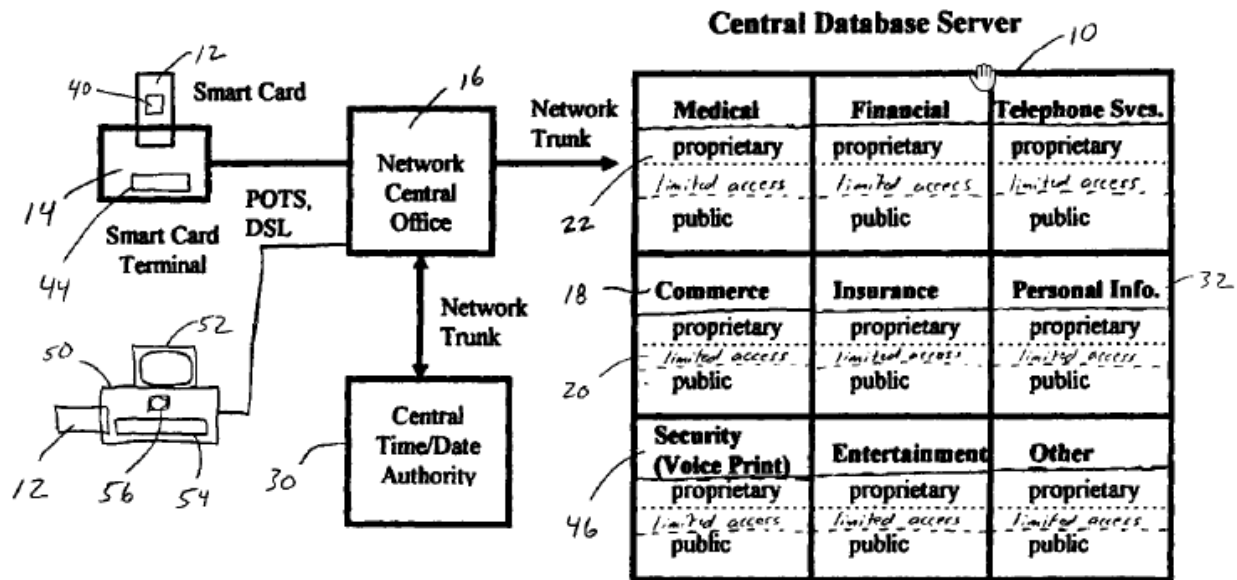


Figure 1

EX1005 (Bossemeyer), Figure 1.

108. Bossemeyer states that the “central database server 10 [] supports many different smart card applications, and supports many users within a given application.” EX1005 (Bossemeyer), 2:4-9. “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 (Bossemeyer), 2:9-12.

109. Bossemeyer discloses that the central database server can in fact comprise multiple servers. EX1005 (Bossemeyer), 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.”¹). Bossemeyer further discloses that the servers can store many types of information, sometimes controlled by different institutions. EX1005 (Bossemeyer), 3:5-16 (“For example... [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... [i]n 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.”).

110. Bossemeyer’s system further discloses “advance smart card terminals 50,” and that “[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 (Bossemeyer), 4:9-15.

111. Bossemeyer also discloses that “*Private or proprietary information is partitioned such that the owner of the information has control over how the information is transferred and used.*” EX1005 (Bossemeyer), 2:28-30. In other

¹ All emphases (italicized bold text and/or colored text) have been added, unless noted otherwise.

words, private or proprietary information is controlled by the owner of that information. 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.” EX1005 (Bossemeyer), 2:30-33. This is so that “*the owner of the information* contained within the central database server *has control over how the information is transferred and used.*” EX1005 (Bossemeyer), 2:34-36.

112. Bossemeyer discloses providing access to data from different partitions of the central database server using a user identification/authentication code or authorization/access code. See EX1005 (Bossemeyer), 3:63-4:6:

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.

See also, EX1005 (Bossemeyer), 4:50-58:

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.

See also, EX1005 (Bossemeyer), Figure 2, 4:59-65:

The network server 10, 110 validates the user identification by decrypting the authorization code. This information is then cross-referenced with the merchant code to identify the information available to the merchant. ***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.

113. In Bossemeyer, the information stored in the centralized database server is partitioned according to at least three distinct security levels: proprietary/restricted, limited access, or public/unrestricted. *See* EX1005 (Bossemeyer), 2:17-24:

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.

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

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 (Bossemeyer), Figure 3. Specifically, Figure 3 of Bossemeyer discloses examples of the type of information having three different levels of security. *See* EX1005 (Bossemeyer), 5:6-15:

[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.

115. A POSITA would have understood that while Bossemeyer discloses embodiments with three levels of security, nothing in Bossemeyer limits its system to only three levels. *See also* Section V.D above.

116. Bossemeyer further explains that different merchants may have different levels of security, and thus different access to information. One example Bossemeyer gives is that “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,” whereas “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 (Bossemeyer), 5:16-22.

B. Glick (U.S. Patent No. 6,985,588, “EX1006”)

117. U.S. Patent No. 6,985,588 (EX1006, “Glick”) was filed on October 30, 2000, and issued on January 10, 2006, and I understand is prior art under because it is a U.S. Patent that was filed prior to the earliest possible priority date of the ’825 Patent.

118. Glick discloses a method for controlling access to information using geographic location as a security measure. Glick’s method defines a known area, a “location identity attribute,” as a security measure that controls whether or not information can be accessed. *See* EX1006 (Glick), Abstract:

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.

See also EX1006 (Glick), 3:27-30 (“A method and apparatus for controlling access to digital information in accordance with the present invention utilizes a location identity attribute that defines a specific geographic location.”), 3:43-46 (“According

to a general embodiment of the invention, access to the digital information is allowed ***only at the specific geographic location*** defined by the location identity attribute.”).

119. The location identity attribute includes “a location value and a proximity value.” EX1006 (Glick), 3:32-34. The “proximity value corresponds to a zone that encompasses the location,” and the “location value corresponds to a location of an intended recipient appliance of the digital information, and may further be defined in terms of latitude, longitude and altitude dimensions.” EX1006 (Glick), 3:34-38.

120. Glick discloses that the first step of its method is to determine the location of an appliance (*e.g.*, electronic device). EX1006 (Glick), 3:46-68; *see also*, *id.*, 5:12-17 (“Appliance. Electronic devices, systems, networks and the like ...”). Glick discloses many different ways to identify location. *See* EX1006 (Glick), 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.***

However, “any coordinate system that uniquely identifies a place can be used for the location value 142 of the location identity attribute 140.” EX1006 (Glick), 6:35-38.

121. I note that the '825 Patent discloses identical methods to identify a location as disclosed in Glick. EX1001 (the '825 Patent), 58:60-63 (“The present invention can be linked with a location sensing circuit, such as a *global position sensor or system (GPS)* or other type of location sensing system, such as a system which utilizes *triangulated signals*.”).

122. Next, Glick discloses that the location of the appliance and the location attribute are compared. Only when the appliance is within the specific region will access to the digital information be allowed. EX1006 (Glick), 3:55-60 (“After 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.”).

123. Glick further discloses steps for enforcing location identity and allowing information access within a predetermine region defined by a location identity attribute (a proximity value and a location value), as illustrated in Figure 5:

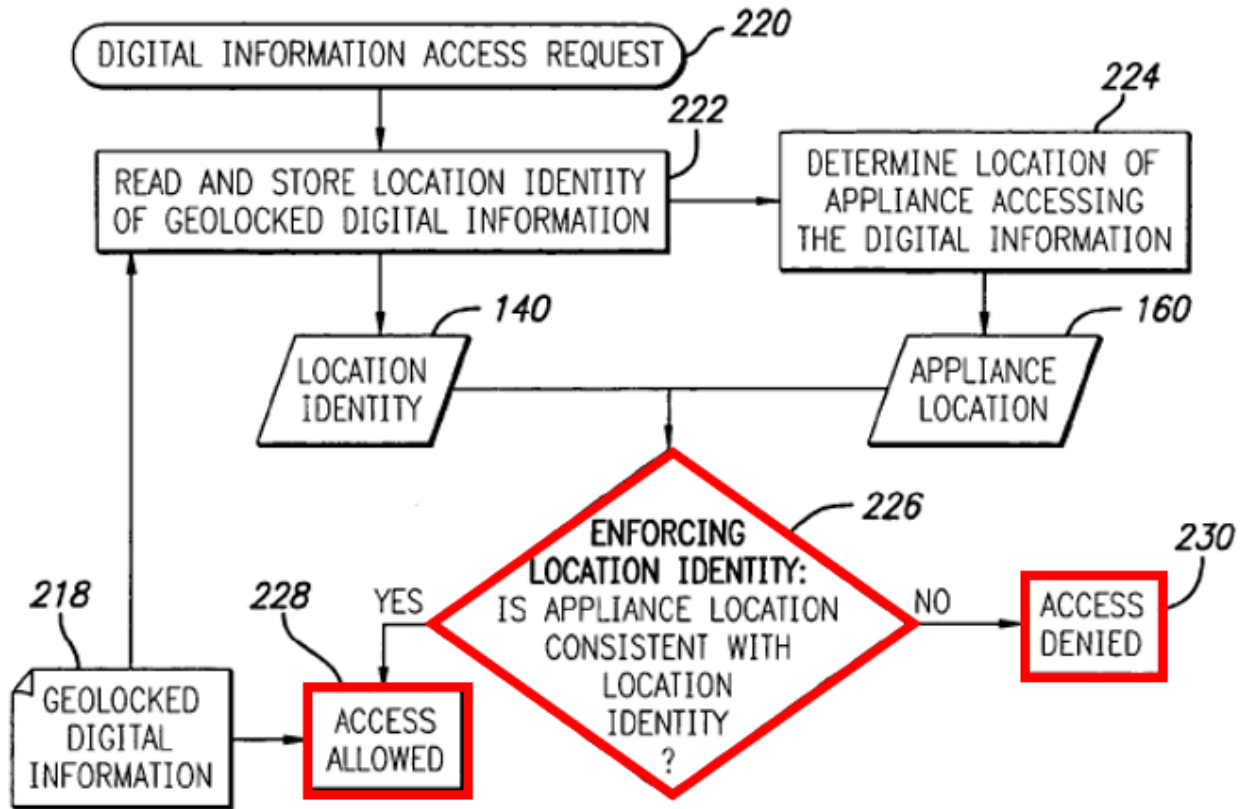


FIG. 5

EX1006 (Glick), Figure 5.²

124. In step 226, Glick discloses determining “whether the location of the appliance is consistent with the region defined by the location identity 140.”

EX1006 (Glick), 8:27-29. “If the appliance location 160 is consistent with the

² All annotations in figures use colors and have been added, unless noted otherwise.

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.” EX1006 (Glick), 8:29:34.

125. Figure 10 of Glick also illustrates the steps for enforcing location identity and allowing information access within a predetermine region defined by a location identity attribute:

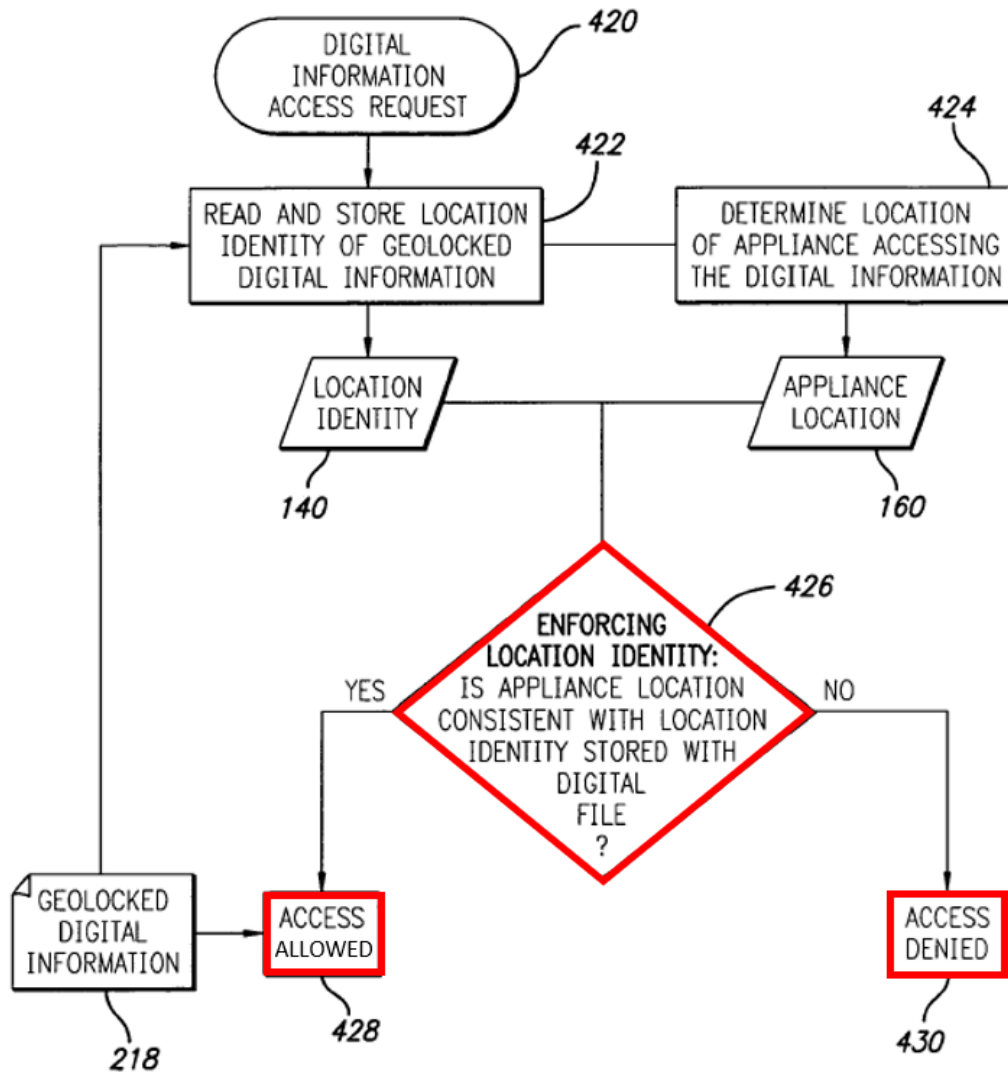


FIG. 10

EX1006 (Glick), Figure 10 (modified).

126. Figure 10 of Glick includes a typographical error. Glick states that “[i]f the appliance location 160 is consistent with the location identity 140, then the application or operating system can access the geolocked digital information 218 at

step 428.” EX1006 (Glick), 11:67-12:3. In addition, steps 426 and 428 in Figure 10 correspond to respective steps 226 and 228 of Figure 5. Step 228 in Figure 5 recites “ACCESS ALLOWED.” However, step 426 in Figure 10 states “ACCESS DENIED,” which does not correspond to the specification, the rest of the patent, or the logic of the figure as any POSITA would understand. Thus, the text of step 428 in Glick’s Figure 10 has been modified to instead state “ACCESS ALLOWED,” as consistent with the description of the illustration.

C. Carmichael (U.S. Patent No. 7,913,919, “EX1007”)

127. U.S. Patent No. 7,913,919 (EX1007, “Carmichael”) was filed on August 5, 2009, and issued on March 29, 2011. I understand that Carmichael is prior art because it is a U.S. Patent that has an effective priority date (January 28, 2000) that is prior to the earliest possible priority date of the ’825 Patent.

128. Carmichael discloses a smart card with multiple memories and a microprocessor, and a “location tracking means for determining a location of the smart card.” EX1007 (Carmichael), Abstract (“A smart card capable of performing more than one function, and said smart card comprising a first memory means comprising a first set of data to access a bank account, a second set of data to access a credit card account, a third set of data representing the identification of a holder of the smart card, and a fourth set of data to access telephone communication services.

The smart card further comprises *a microprocessor*, said microprocessor being in electrical communication with a second memory means, and *a location tracking means for determining a location of the smart card.*”).

129. Carmichael discloses that the location tracking means can reside on the smart card itself. EX1007 (Carmichael), 3:58-62 (“The 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 detectable by a global positioning system satellite.”). Carmichael discloses a smart card that contains a **GSM (Global System Mobile Communications) chip**³ for use with a GPS (Global Positioning System) satellite network to locate the smart card, as shown in Figure 2 below:

³ In this declaration I use colored text whose color matches figure annotations, claim language, or quotes across references, to aid in understanding my mapping of the evidence to the claims.

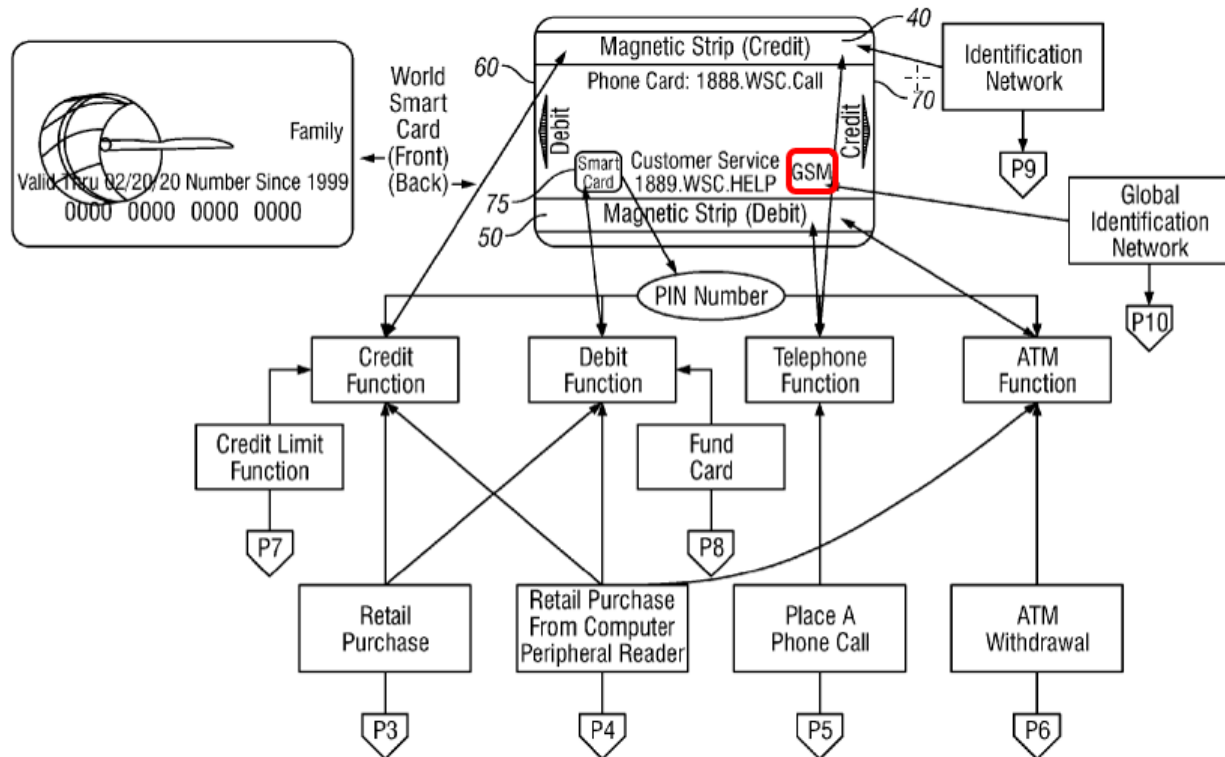


FIG. 2

EX1007 (Carmichael), 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.”).

130. Carmichael further discloses that the location of a smart card terminal can be used to determine the location of the smart card itself. EX1007 (Carmichael),

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.”).

VIII. Level of Ordinary Skill in the Art

131. In my opinion, a person of ordinary skill in the art (“POSITA”) in the field of the ’825 patent as of its earliest possible priority date of August 2, 2002, 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 storage systems and data security. In my opinion, additional education could make up for less practical experience, and vice versa.

132. I met these requirements for POSITA at the time of earliest possible priority date of the '825 patent.

IX. Claim Construction

133. I have reviewed the claims, specification, and file history of the '825 patent.

134. I have not construed any terms in my analysis, and I have afforded the claim terms their ordinary and customary meaning.

X. Specific Grounds for Challenge

135. The sections below demonstrate in detail how claim 81 of the '825 patent is not patentable over the prior art.

A. Ground I: Bossemeyer In View Of Glick Renders Obvious Claim 81

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:

136. I understand that the preamble may not be limiting. Nevertheless, Bossemeyer in combination with Glick renders obvious the preamble, as explained in the sections below.

137. A POSITA would have been motivated to combine the teachings of Bossemeyer with Glick, as I discuss in Section X.A.6 (below). That discussion applies equally here as well.

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

138. Bossemeyer discloses this limitation. Also, Bossemeyer alone and/or combined with Glick renders obvious this limitation.

139. Bossemeyer discloses partitioning certain information (data) and then storing said information by level of security. EX1005 (Bossemeyer), 2:17:22, 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.*”). A POSITA would understand that here, “information” is data. EX1023 (Microsoft Dictionary), p. 233 (“**information** *n.* The meaning of data as it is intended to be interpreted by people. Data consists of facts, which become information when they are seen in context and convey meaning to people. Computers process data without any understanding of what the data represents.”).

140. Bossemeyer also discloses restricting access to certain (sensitive) data.

See EX1005 (Bossemeyer), 2:40-50:

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.

Figures 1 and 3 also illustrate Bossemeyer's **data** access restrictions:

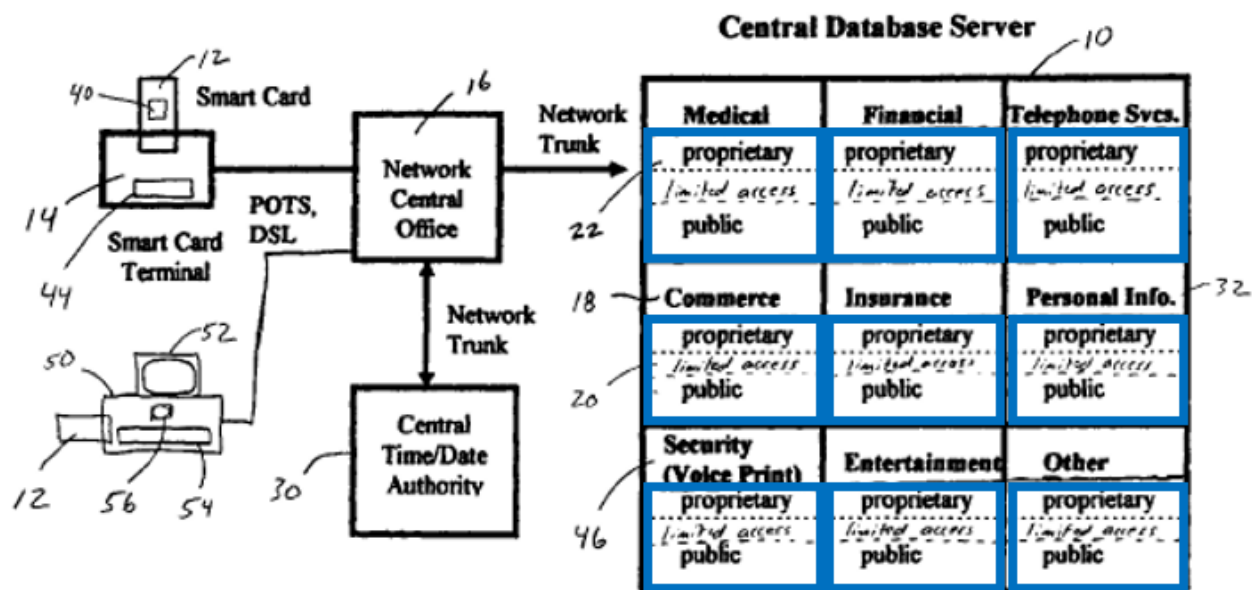


Figure 1

EX1005 (Bossemeyer), Figure 1.

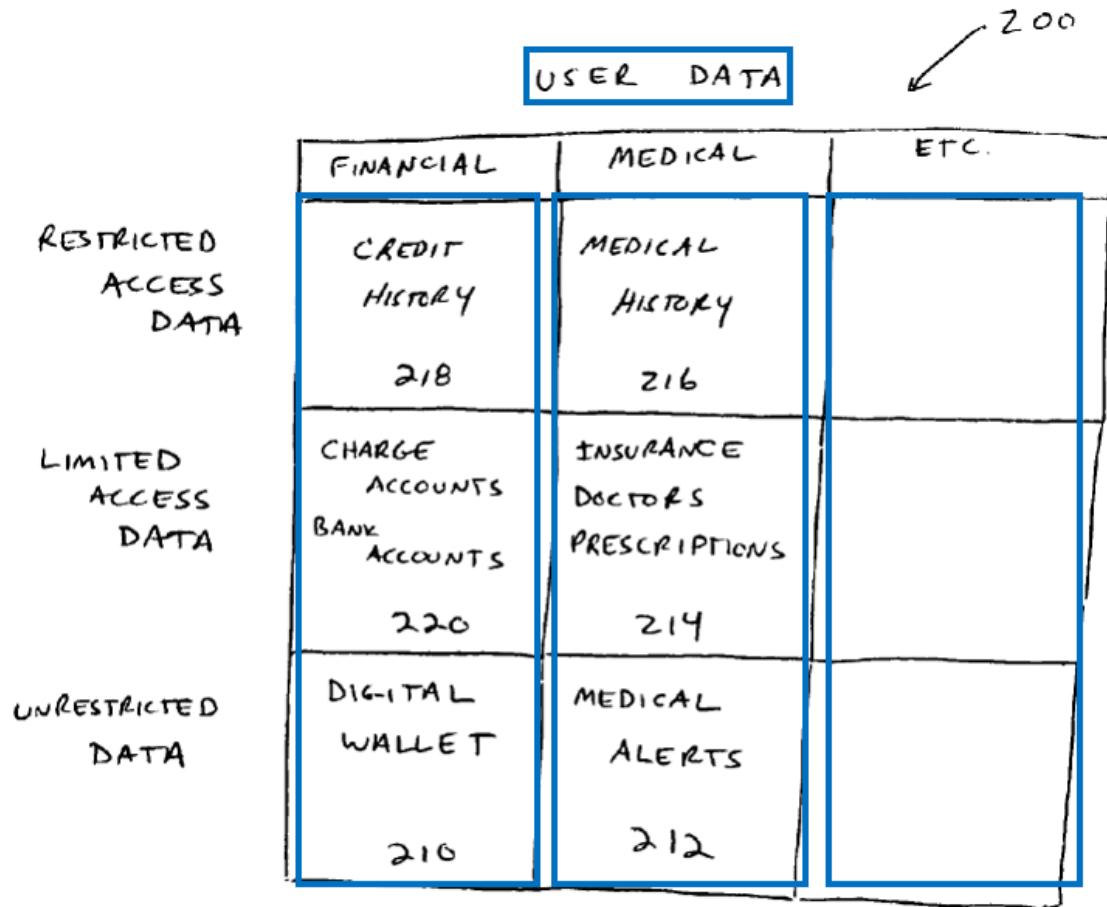


FIG. 3

EX1005 (Bossemeyer), Figure 3.

141. A POSITA would have understood Bossemeyer's "limited access information" and/or "proprietary information" to include security sensitive information, such as words, characters, and other data objects, because Bossemeyer discloses conditionally accessing such information. Bossemeyer discloses several types of security sensitive information, such as a user's medical history 216,

prescription information 214, credit history 218, and bank accounts 220, shown in Figure 3. The '825 Patent discusses the privacy of credit history, medical history, business trade secrets, and financial data (EX1001 (the '825 Patent), 1:46-49).

142. A POSITA would have understood that the medical history, prescription information, etc. described in Bossemeyer is highly sensitive information, as it includes images of medical charts, the names of drugs prescribed, information protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), etc., and thus would be “security sensitive words, characters, data objects or icons” under the meaning of this limitation. A POSITA would have understood that owners of such information (*e.g.*, patients) would not want such information made uncontrollably public, but rather control who should have access to such information and when (*e.g.*, medical professionals, family members). It was well known that sensitive information can include words, characters, or icons. See, *e.g.*, EX1005 (Bossemeyer), 3:25-27 (“[P]ersonal information 32 such as digitized photograph... can be included as part of a photo identification such as a driver’s license.”).

143. While Bossemeyer alone discloses this limitation, it also renders obvious this limitation. A POSITA would have found it obvious that Bossemeyer discloses other types of security sensitive words, characters, data objects or icons,

compared to those that were explicitly disclosed. Figure 1 of Bossemeyer shows other types of data that include security sensitive information that is stored as proprietary or limited access data, and Figure 3 of Bossemeyer includes additional columns for storing user data with a restricted or limited-access security level (*e.g.*, financial data, and column labeled “*etc.*”). A POSITA would have understood that, similar to medical information, owners of financial information would not want their credit history or credit card and banking information made uncontrollably public and would want to control it: if released, such information could be embarrassing, affect one’s ability to secure credit (*e.g.*, loans), and in the worst case could be used by hackers to empty one’s bank accounts.

144. While Bossemeyer alone discloses this limitation, combined with Glick it also renders obvious this limitation. Additionally, Glick discloses securing data by preventing access to the data (or only allowing data to be accessed) unless access is requested at a particular geographic location. EX1006 (Glick), 3:44-46 (“[A]ccess to the digital information is allowed only at the specific geographic location defined by the **location identity attribute**.”).

145. Continuing the aforementioned example risks of releasing financial information, a POSITA would have understood that further restricting access to such information based on location affords greater protection to users and institutions.

For example, if a credit card holder is physically in New York, charges by a local gas station are likely valid; but if such charges show up all the way across the country, say in California, those charges are more likely fraudulent. Credit card companies have long understood these location-based shopping patterns and have themselves implemented methods for detecting and thwarting fraud, to protect their customers. A POSITA would therefore have understood the benefits of adding Glick's location-based restrictions to Bossemeyer's protection of (financial) information.

146. As discussed in Section X.A.6 (below), it would have been obvious to incorporate Glick's control of access to information via location identity with Bossemeyer's data system, and a POSITA would have had a reasonable expectation of success in combining Bossemeyer with Glick.

147. In sum, Bossemeyer discloses—and also Bossemeyer alone and/or Bossemeyer combined with Glick renders obvious—a method of securing (“partitioning”) **data** (“**information**”) having one or more security sensitive words, characters, data objects or icons (“limited access information” or “proprietary information”).

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

148. Bossemeyer discloses this limitation.

149. *First*, Bossemeyer discloses a network of computers, *i.e.*, a computer system. EX1005 (Bossemeyer), 1:47-49 (“***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.”).

150. Glick also discloses communication across multiple computers, *i.e.*, the claimed computer system. EX1006 (Glick), 12:51-56 (“[G]eolocked digital information can be ***communicated over a network*** including wide area networks such as the Internet, local networks such as intranets, dial-up access between a

personal and server *computers*, as an attachment to e-mail, or through a digital cell phone or other wireless device.”).

151. *Second*, Bossemeyer’s computer system includes a central database server with a **partitioned memory**, *i.e.*, **a plurality of security-controlled memories**. EX1005 (Bossemeyer), 2:13-16 (“The *central database server 10* includes **partitioned memory**... as well as a microprocessor for processing data received from and transmitted to the smart card terminal 14.”), 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.”).

152. Bossemeyer’s partitioned memory has different levels of security, *i.e.*, is security-controlled. *See* EX1005 (Bossemeyer), 2:17-27:

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.

153. Thus, Bossemeyer teaches controlling the access of sensitive information by allowing different levels of access (e.g., **limited**, **unrestricted**) to the sensitive information, and thus Bossemeyer's memory partitions have security access controls. Figures 1 and 3 of Bossemeyer illustrate the **memory partitions with limited-access and restricted information**:

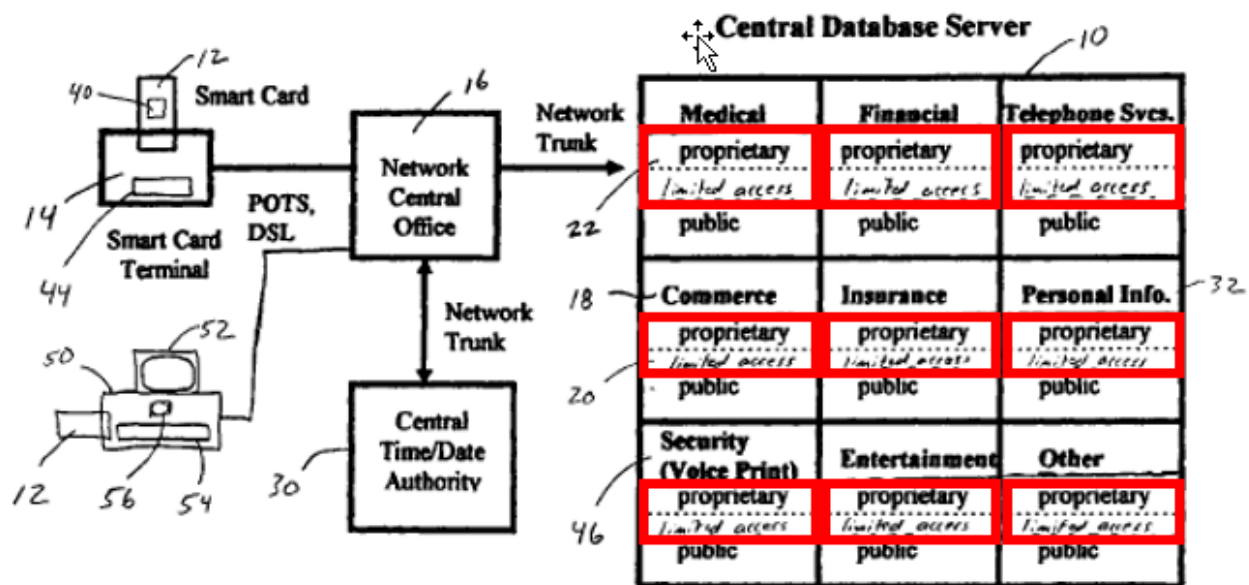


Figure 1

EX1005 (Bossemeyer), Figure 1.

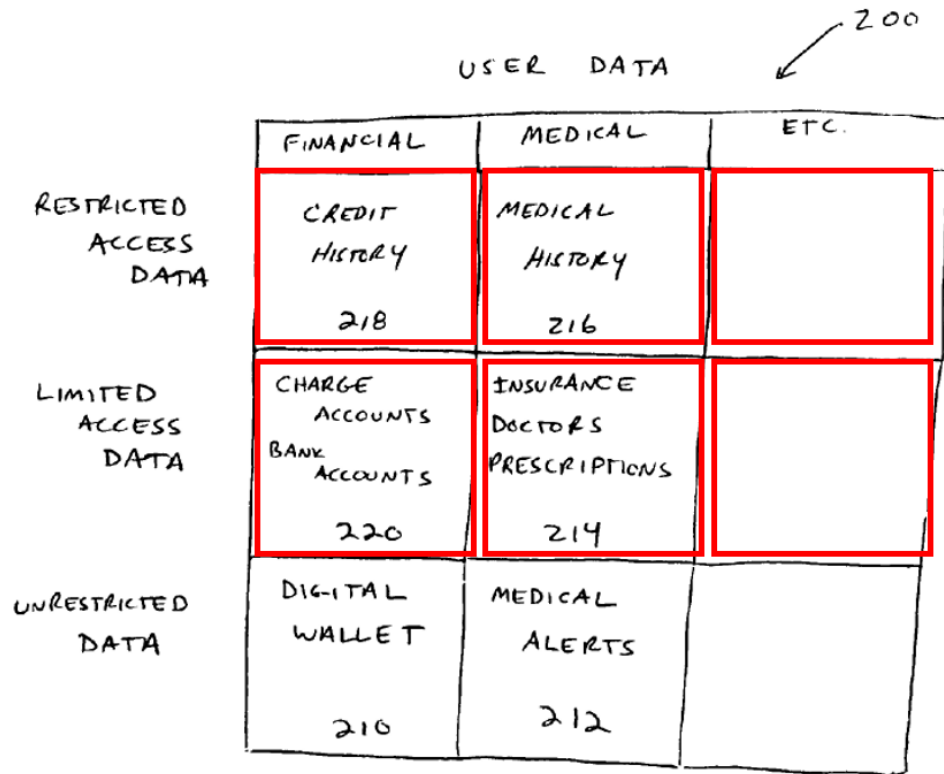


FIG. 3

EX1005 (Bossemeyer), Figure 3.

154. To the extent that Patent Owner argues that **a plurality of security controlled memories** need to be separate physical memories and/or be implemented in separate locations, Bossemeyer discloses that different servers at various locations can collectively make up the central database server, and that a server in a particular location can store sensitive information. See EX1005 (Bossemeyer), 3:3-19:

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.

155. Bossemeyer's memories at multiple locations (*e.g.*, TransUnion or Equifax) are different databases (in this example, maintained by different entities), and thus satisfy the claimed **plurality of security controlled memories**. I note that, while this example shows different security-controlled memories (databases) managed by different entities (TransUnion and Equifax), the '825 Patent does not require each such memory to be managed by a different entity.

156. The '825 Patent describes "**extract stores**" as the location where the extracted data is stored, where the extracted data comprises "*security sensitive words, characters or icons.*" EX1001 (the '825 Patent), 10:10-13 ("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.*"). Thus, 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. Accordingly, Bossemeyer discloses this limitation.

157. A POSITA would have understood that even a single computer has at least two memories: one volatile (DRAM) and another non-volatile (*e.g.*, hard disk).

Moreover, computers could also easily have multiple hard disks. Lastly, even a single hard disk could be partitioned into multiple partitions, each of which is a (storage) memory that can hold any information, including secure data. See also Section V.B above.

158. In sum, Bossemeyer discloses a computer system (“network arrangement”) with a plurality of security controlled memories as respective **extract stores** (“**partitions in the database**”) with security access controls thereat (“level of security (unrestricted, or **public limited access, restricted**)”).

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

159. Bossemeyer discloses and/or renders obvious this limitation.

160. Bossemeyer discloses partitioning a database server to partition or separate (e.g., extract) **user data** based on the data’s level of security. See EX1005 (Bossemeyer), 2:17-27:

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*.

161. Specifically, Bossemeyer discloses partitioning (e.g., extracting) **user data (information)** in the central database server into **limited access information and/or proprietary information**, and **public information**. See EX1005 (Bossemeyer), 2:40-47:

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.

162. A POSITA would have understood that Bossemeyer's "classifying" the information into three different categories means that such data has to be evaluated for its level of security, before it is stored in a specific extract store. Limited access information and/or proprietary information includes security sensitive information, such as, words, characters, data objects, or icons, as I explained in Section X.A.1.i (above).

163. Bossemeyer discloses an example where medical information within the central database server is private. EX1005 (Bossemeyer), 2:30-36 ("[F]or

example, medical information 22 provided to a health professional may be considered private and only available by way of special authorization of 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.”). Bossemeyer Figure 1 discloses that **medical information 22** is stored in central database 10 as proprietary information.

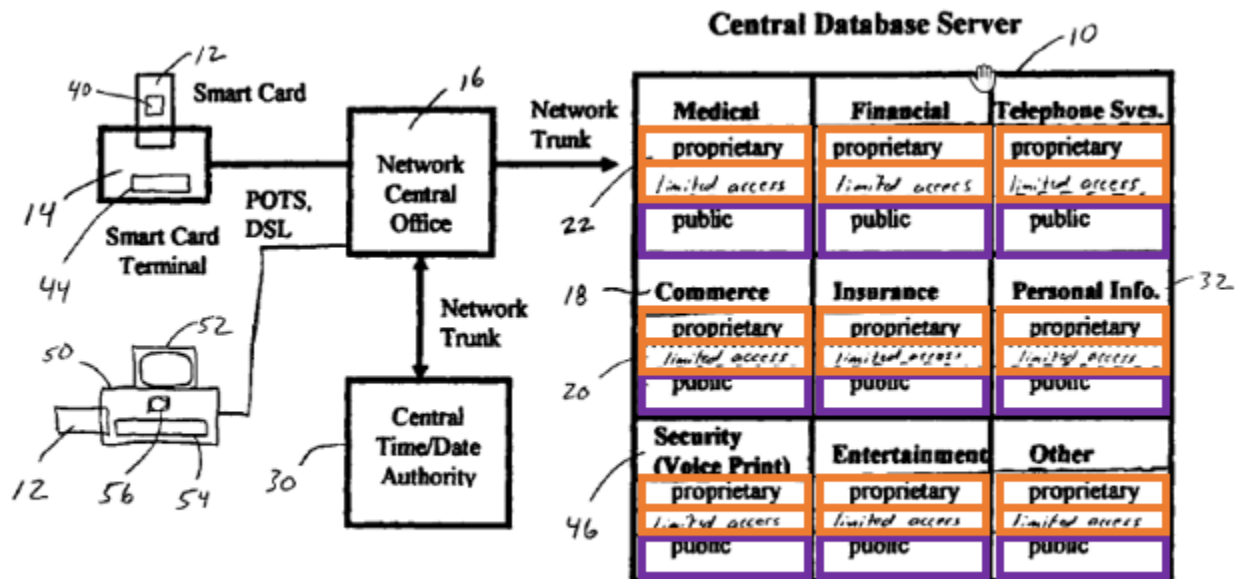


Figure 1

EX1005 (Bossemeyer), 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.”).

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

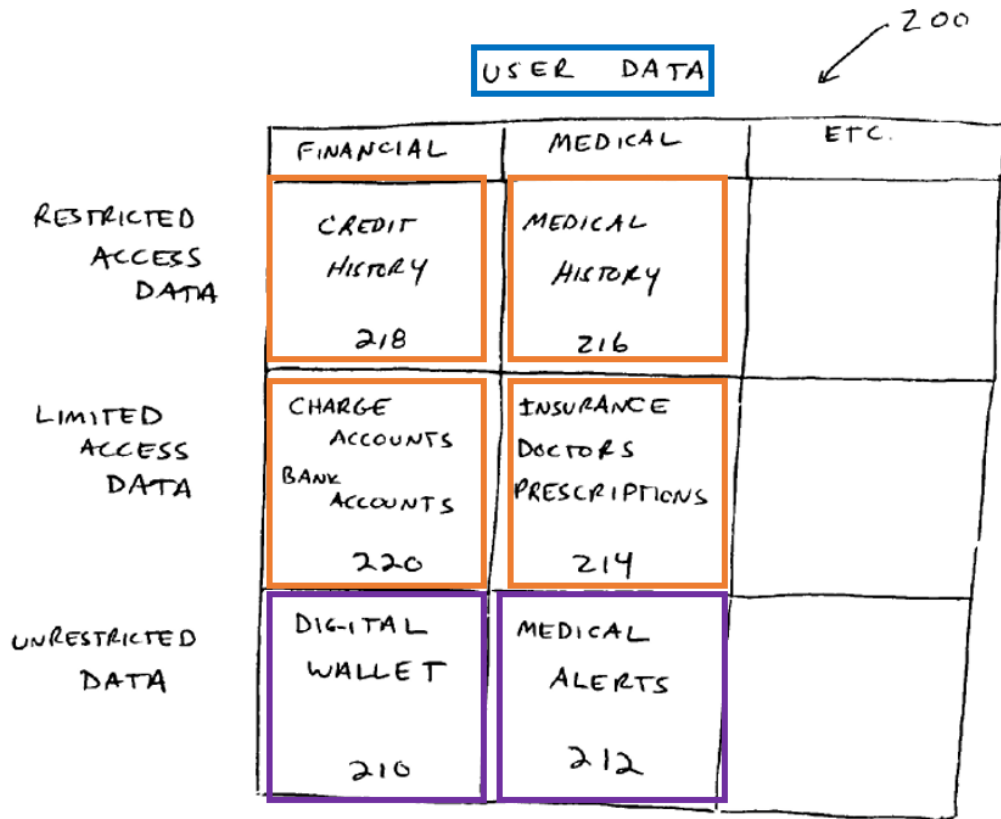


FIG. 3

EX1005 (Bossemeyer), 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**.”).

165. Bossemeyer discloses that the **restricted/limited access data** and **unrestricted data** after extraction are stored separately. EX1005 (Bossemeyer), 2:20-22 (“The information is *stored by... level of security* (unrestricted, or public limited access, restricted).”), 5:8-9 (“[I]nformation is stored in *three levels of security*: unrestricted, limited access, and restricted.”), Figure 3. Figure 3 demonstrates that the restricted/limited access data and the unrestricted data can be both partitioned from one another and yet reside in the same central database. EX1005 (Bossemeyer), 4:43-44 (“FIG. 3 shows a schematic diagram of the *partitioned* server database.”).

166. A POSITA would have understood that “stored by... level of security” and “stored in three levels of security” in Bossemeyer means that data belonging to one security level is logically stored in a different storage location than data of a different security level. Such different stores can be physical (*e.g.*, different hosts or hard disks) or logical (*e.g.*, different partitions of the same hard disk, stripes of a RAID array). See Section V.B above.

167. To the extent that Patent Owner argues that Bossemeyer does not explicitly disclose “extracted data,” a POSITA would have understood that Bossemeyer’s “limited access information” and “proprietary information” to mean “security sensitive” data under the meaning of the ’825 Patent, because such data

logically contains sensitive information that its owner would want to secure. Further, a POSITA would have understood that Bossemeyer's "public information" corresponds to "remainder data" under the meaning of the '825 Patent, because such data does not necessarily contain sensitive information that its owner would want to protect.

168. A POSITA would have understood that when Bossemeyer's "central database server... partitions information... in terms of... the accessibility of the information" (EX1005 (Bossemeyer), 2:17-20), that 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 and hence separate/break the received information into private and non-private elements. U.S. Publication No. 2004/0148290 ("Merenda," EX1008), ¶7 ("[A] set of data may be parsed into private and non-private elements."). *See also* EX1023 (Microsoft Dictionary), p. 333 ("**parse** *vb.* To break input into smaller chunks so that a program can act upon the information.>").

169. Bossemeyer further provides an example of extraction in Figure 3. When the central database server receives a **user's medical data file**, it extracts (partitions) the **user's medical history information 216** and **insurance/doctors/prescription information 214** and stores said information into respective extract stores (partitions) corresponding to the appropriate respective security level. *See e.g.*, EX1005 (Bossemeyer), 2:17-22; 5:6-15; 5:23-31.

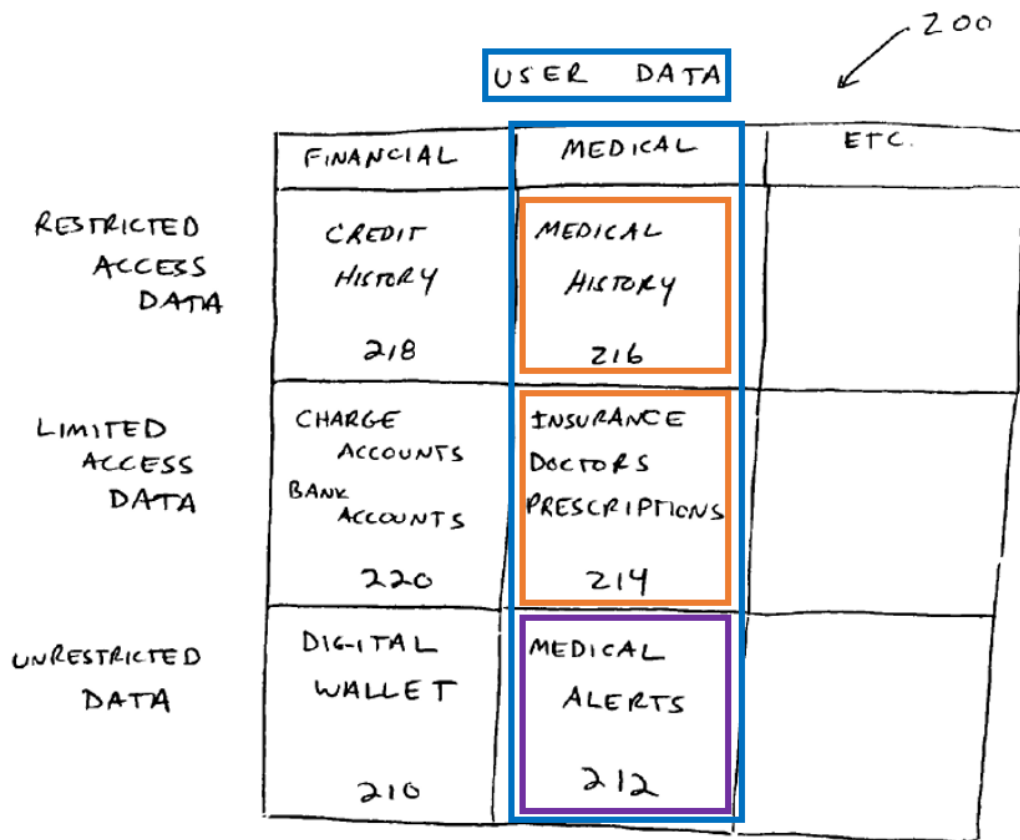


FIG. 3

EX1005 (Bossemeyer), Figure 3.

170. A POSITA would have understood that **medical history information** can include sensitive information such as 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.

171. In sum, Bossemeyer discloses and/or renders obvious that said security sensitive words, characters, data objects or icons ("information") [are/were] extracted ("partitioned") from said **data** to obtain **extracted data ("limited access information" or "proprietary information")** and **remainder data ("public information")**.

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

172. Bossemeyer discloses this limitation.

173. As discussed in Sections X.A.1.ii (above) and X.A.1.iii (above), Bossemeyer discloses storing sensitive data (extracted data) in either a "centralized partitioned database server" (EX1005 (Bossemeyer), 2:17-18) or remote servers (EX1005 (Bossemeyer), 3:3-18) as shown in Bossemeyer Figures 1 and 3.

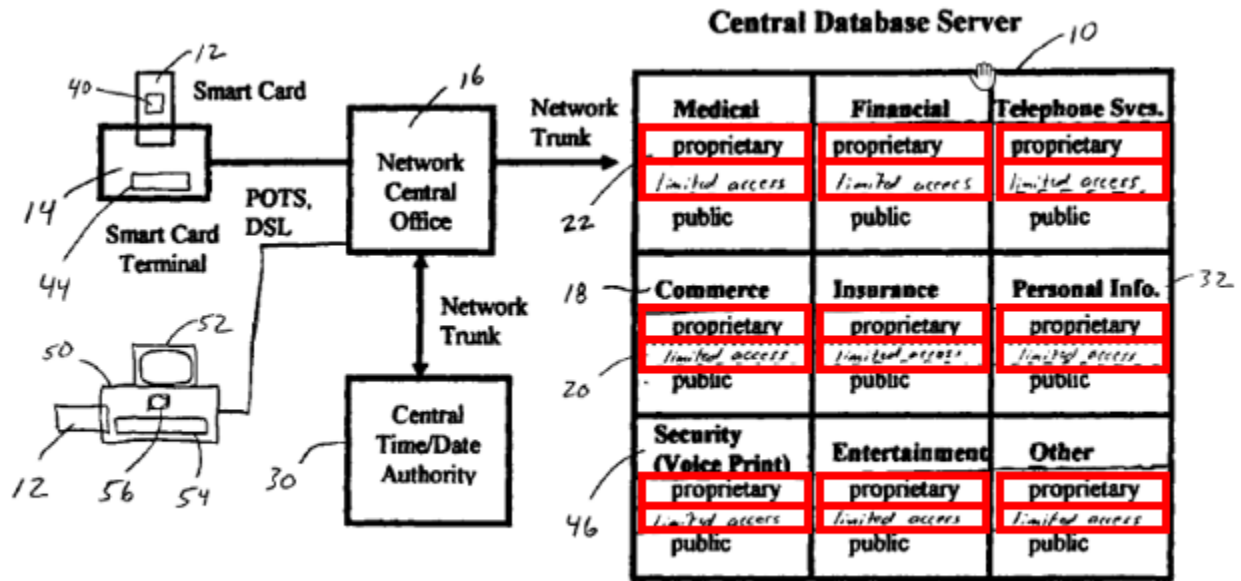


Figure 1

EX1005 (Bossemeyer), Figure 1.

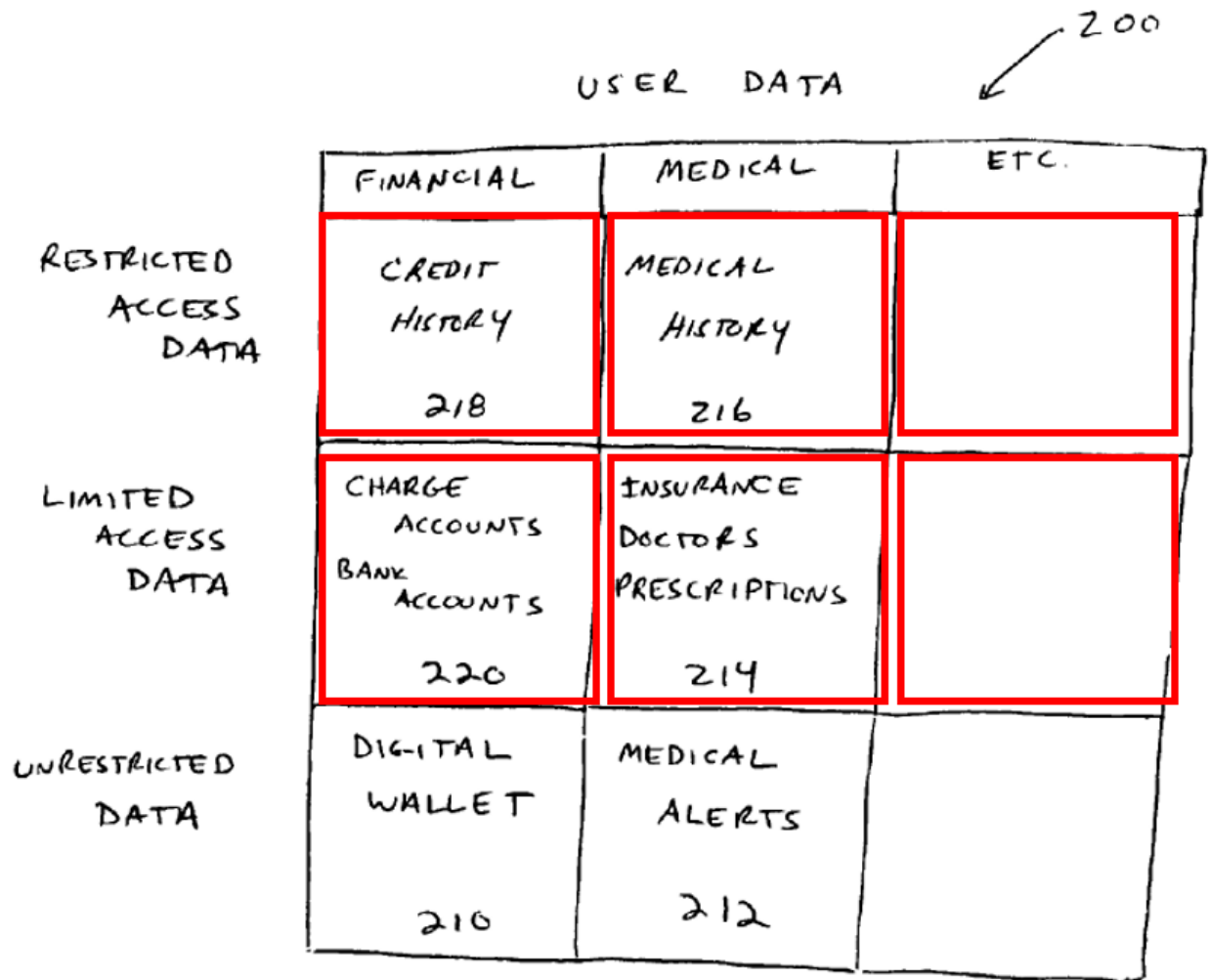


FIG. 3

EX1005 (Bossemeyer), Figure 3.

174. Bossemeyer further discloses that sensitive data (e.g., limited access data or restricted access data) is stored in respective **extract stores** corresponding to a respective security level of said extract stores, as shown in Bossemeyer's Figures 1 and 3 which illustrate a **proprietary/restricted access region**, a **limited access**

region, and an unrestricted/public access region of corresponding security/access levels. *See* EX1005 (Bossemeyer), 2:17-27:

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.

175. Bossemeyer discloses an example when, “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 (Bossemeyer), 2:22-27. A POSITA would have understood “limited access region 20,” as shown in Bossemeyer's Figure 1 above, to be a separate, distinct storage location for storing data designated for “limited access”—separately from information designated “proprietary” or “public,” because separating data of different security levels into separate compartments makes it easier to safeguard and control access to that data. *See* Section V.D above.

176. Bossemeyer further 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 (Bossemeyer), 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”). A POSITA would have understood that in this example, clearly, different credit-reporting companies, different banks, and different healthcare providers would want (and likely insist) on storing security data independently and on their own, because that would afford greater independence of operation and improved security (*e.g.*, if one entity’s computers are compromised by hackers, it won’t affect other entity’s data).

177. Bossemeyer discloses multiple extract stores, each with its own security information residing with its respective data owner. *See* EX1005 (Bossemeyer), 3:3-18:

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.

178. A POSITA would have understood the above disclosure to mean that each entity (*e.g.*, company, provider, bank) can have its own one or more databases to hold its own security data, because this would improve operational independence and security. Thus, Bossemeyer discloses that extracted data (*e.g.*, insurance information/medical records/prescription information) are stored in **extract stores** (*e.g.*, **insurer databases or a health provider database**) respectively, corresponding to respective security level of the insurer database or health provider database. Accordingly, Bossemeyer discloses this limitation.

179. In sum, Bossemeyer discloses that extracted data (“limited access information” or “proprietary information”) is stored in respective **extract stores** (“**public limited access**” or “**restricted**” partitions in the database servers) corresponding to a respective security level of said extract stores (“the information is stored by... level of security”).

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

180. Bossemeyer in view of Glick renders obvious this limitation.

181. As I explain in Sections X.A.1.v.a and X.A.1.v.b below, a “portable computing device locatable with **current location data**” is rendered obvious, dependent on the position of the location means, by either: (1) **Bossemeyer’s smart card 12**; or (2) Bossemeyer’s **smart card terminal 14** and/or **advance smart card terminal 50**.

a. Smart Card Locatable With **Current Location Data**

182. Bossemeyer discloses that the smart card is portable. EX1005 (Bossemeyer), 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.”). Bossemeyer also discloses that the smart card “contains circuitry 40 which includes a *microprocessor and memory* including random access memory (RAM) and read only memory (ROM).”). EX1005 (Bossemeyer), 3:28-31. Accordingly, Bossemeyer’s **smart card 12** is a portable computing device.

183. A POSITA would have understood that a “portable device” as disclosed in the ’825 Patent includes many shapes, capabilities, and sizes (*e.g.*, from full-size desktops to small pagers), as long as it has a memory, processor, and a “GPS or locator,” which would include a smart card. EX1001 (the ’825 Patent), 58:52-59 (“[T]he 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.*”).

184. A POSITA would have understood that smart cards would be a computing device in the '825 Patent's context because they have a processor and memory, and they can execute instructions. See Section V.A above.

185. Glick also discloses a portable computing device (which it calls an “appliance”) where the current location can be determined. EX1006 (Glick), 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 discloses determining the location of wireless devices. See EX1006 (Glick), 13:56-14:4:

In another exemplary application of the present invention, location identity is used to enhance confidentiality and security for wireless network connectivity. Wireless networking is coming of age with the advent of networking equipment and protocols such as the “Bluetooth” technology that allows wireless portable or workstations to connect to a network. “Bluetooth” is an open standard for short-range transmission of digital voice and data between mobile devices (e.g., laptops, PDAS, cellular telephones) and desktop devices that supports point-to-point and multipoint applications. Since every wireless

appliance communicating over the network will have *a unique location, location identity* can be utilized to establish a unique shared cryptographic key that can be used to maintain secure confidential communications for *wireless devices connecting over a public network*.

186. Glick discloses many ways in which the location of the device can be found. See EX1006 (Glick), 3:48-55:

(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.*

187. I note that the '825 Patent discloses identical methods to identify a location as disclosed in Glick. EX1001 (the '825 Patent) 58:60-63 ("The present invention can be linked with a location sensing circuit, such as a *global position sensor or system (GPS)* or other type of location sensing system, such as a system which utilizes *triangulated signals.*").

188. However, Glick is not limited to those examples. EX1006 (Glick), 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.**").

189. Glick discloses an “appliance,” which is a device at “a location of an intended recipient” “through which access to the digital information sought is identified.” EX1006 (Glick), 3:34-36 (“The location value corresponds to a location of an intended recipient appliance of the digital information”), 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.”), 5:12-17 (defining an “Appliance” as “[e]lectronic 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.”), 8:7-12 (“The 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.”).

190. A POSITA would have understood from Glick’s disclosures that its “appliance” is a general computing device. Glick’s appliances also take many shapes, capabilities, and sizes (*e.g.*, from full-size servers and workstations to small PDAs). Glick’s appliances have a processor and memory, and they can execute

instructions. Moreover, Glick's appliances (computing devices) include multiple ways to identify a location (*e.g.*, GPS, triangulation). *See* EX1006 (Glick), 3:48-55.

191. Bossemeyer's **smart card 12** is an "appliance" as defined in Glick, because both have a processor and memory, and both can execute instructions. Bossemeyer's smart card is a *portable* electronic device with processing capability and memory capacity which can receive and transmit information. EX1005 (Bossemeyer), 3:28-30 ("**Smart card 12**... contains circuitry 40 which includes a microprocessor and memory..."), 2:58-61 ("Each 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*...").

192. 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 understood that smart cards (like the one disclosed in Bossemeyer) can also acquire location information via the card itself. EX1007 (Carmichael), 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.

193. As I discuss in Sections X.A.6 (below), 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.

194. In sum, the combination of Bossemeyer and Glick renders obvious that said computer system having at least one portable computing device (a card a consumer can "carry" or an "appliance") [and is] locatable with **current location data** ("**location identity attribute**").

b. Smart Card Terminal Locatable With **Current Location Data**

195. Alternatively, Bossemeyer's **smart card terminal 14** and/or **advance smart card terminal 50** renders obvious this limitation in view of Glick.

196. As discussed in Section VII.A (above), Bossemeyer "describes a network arrangement which is readily accessible from different types of smart card terminals [**smart card terminal 14** and/or **advanced smart card terminal 50**] supporting various smart card applications." EX1005 (Bossemeyer), 1:44-47, 3:43-47 ("**Smart card terminal 14** is connected by a data link such as the plain old

telephone system (POTS) or a digital subscriber line (DSL) to the network central office 16 of the Public Switched Telephone Network.”), 3:49-51 (“[A] plurality of... **terminals 14** access the central database server 10 through the network central office 16.”).

197. Bossemeyer discloses that such terminals could be used as “‘docking stations’ [that] could transform hotel room entertainment centers or airplane seat video screens into networked computers with the insertion of a user’s smart card.” EX1005 (Bossemeyer), 4:19-22.

198. A POSITA would have found it obvious to implement **smart card terminal 14** and/or **advance smart card terminal 50** as a computer, or more specifically, a portable laptop computer, with a peripheral smart card reader. EX1005 (Bossemeyer), 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*...”).

199. A POSITA would have understood that smart cards and their readers were commonplace and could be easily integrated with computers at the time of the alleged invention. See EX1023 (Microsoft Dictionary), p. 412 (“**smart card** *n.* 1. In computers and electronics, a circuit board with built-in logic or firmware that

gives it some kind of independent decision-making ability.”). See also EX1005 (Bossemeyer), 1:35-38 (“Smart cards, however, differ from data cards in that they can hold much more information and often include some ‘intelligence’ such as a microprocessor or the like.”).

200. See also, EX1007 (Carmichael), 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.

201. A POSITA would have been motivated to combine a smart card terminal with a portable laptop computer and a peripheral card reader, for example,

to permit Bossemeyer's system to utilize a smart card terminal and interact with multiple smart card users. This would have the benefits of both portability and convenience. For example, medical information could be accessed by multiple doctors or medical personnel conveniently using the same laptop computer after they have inserted their respective smart cards into the terminal, or even the same person can access information using many different laptop computers, each equipped with a peripheral smart card reader. Accordingly, Bossemeyer's **smart card terminal 14** and/or **advance smart card terminal 50** are a portable computing device.

202. Additionally, a POSITA would have understood that smart card terminals (like the ones disclosed in Bossemeyer) are also locatable with current location data. EX1007 (Carmichael), 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.”).

203. The **smart card terminal 14** and/or **advance smart card terminal 50** as disclosed in Bossemeyer are an “appliance” as used in Glick. EX1006 (Glick), 5:12-17. Such **terminals 14** and **50** are electronic devices with processing and memory for the transmission and location of information. EX1005 (Bossemeyer), 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...”). See *also* Section X.A.1.v.a above.

204. A POSITA would have understood that receiving/transmitting data and/or maintaining a connection with a device connected to the network requires a processing capability to execute the receive/transmit instructions and a memory capacity, for example, to store the received data.

205. Thus, Bossemeyer in view of Glick 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**.

206. In sum, the combination of Bossemeyer and Glick renders obvious that said computer system having at least one portable computing device (a card a consumer can “carry” or an “appliance”) [and is] locatable with **current location data** (“**location identity attribute**” via a “terminal”).

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

207. Bossemeyer in view of Glick renders obvious this limitation. See Section X.A.6 below describing reasons why a POSITA would be motivated to combine Bossemeyer and Glick.

208. Glick discloses that the location of a device (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**.” See EX1006 (Glick), Abstract:

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.*

See EX1006 (Glick), 3:34-60:

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. The proximity value corresponds to a *zone that encompasses the location*.

According to a general embodiment of the invention, access to the digital information is allowed *only at the specific geographic location defined by the location identity attribute*. As a first part of this enforcement process, the location of an appliance through which access to the digital information is sought is identified. 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. *After 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*.

See EX1006 (Glick), 8:16-35:

Particularly, the method starts at step 220 with a command to access the digital information. At step 222, the geolocked digital information 218 is accessed to read and store the associated location identity attribute 140. It should be appreciated that only the location identity portion of the geolocked information is accessed, and not the digital information itself. The location identity 140 of the geolocked information is stored for further use in the method. At step 224, the method determines the location of the appliance accessing the digital information. As will be described below, there are numerous possible ways to determine the appliance location 160. The appliance location 160 is stored for further use in the method. 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.

209. Glick discloses that “[t]he location identity attribute further includes a *location value* and a *proximity value*” where “[t]he *proximity value corresponds to a zone that encompasses the location*” and “[t]he *location value 142* corresponds to the unique position of a particular place,” *i.e.*, “the location of an intended recipient appliance of the digital information.” EX1006 (Glick), 3:32-38, 6:29-39. The *location and proximity values* are then “used to generate an *area parameter*

190 that *defines a shape of the geographic region defined by the location and proximity values.*” EX1006 (Glick), 10:15-18; *see also id.*, 11:28-38:

At step 402, a location value 142 for the digital information is retrieved and stored for later use. At step 404, a proximity value 143 of the location identity attribute of the appliance is retrieved and stored for later use. As described above, various methods for generating the location and proximity values 142, 143 may be utilized. At step 406, the retrieved *location and proximity values 142, 143* are used to generate the location identity attribute 140. Then, at step 408, the digital information 416 is integrated with the location identity attribute 140 to provide geolocked digital information 418.

210. In sum, Bossemeyer in view of Glick renders obvious determining when said portable computing device is **within a predetermined region** (“**specific geographic location**” or “**a zone that encompasses the location**”) based upon said **current location data** (“**the location of an appliance**”).

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

211. Bossemeyer discloses and/or renders obvious this limitation.

212. As an initial matter, a POSITA would have understood that a system such as Bossemeyer separates (extracts) data into “remainder” and one or more “extract” stores. It would make little sense to separate such data and not enable any

form of accessing such separated/extracted data later on, with appropriate credentials. Therefore, a POSITA would have understood that Bossemeyer discloses and enables the logical merging (reconstruction) of said previously extracted data. Even the strictest of known security controls (*e.g.*, military grade) have to allow authorized users to access compartmentalized data. *See* Section V.D above.

213. Bossemeyer discloses partitioning information and storing said information (data) in a central database server according to different levels of security and then reconstructing the partitioned data, *e.g.*, allowing a user access to the partitioned data, using “user identification codes” or “data pointers.” EX1005 (Bossemeyer), 2:38-47 (“***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.”).

214. Specifically, Bossemeyer discloses that, based on a user’s authorization, partitioned data is retrieved from the different partitioned memory portions of the central database server 10, and is presented (*e.g.*, at a terminal). EX1005 (Bossemeyer), 3:63-4:6 (“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.*”), 4:59-65 (“The network server 10, 110 validates the user identification by decrypting the authorization code. This information is then cross-referenced with the merchant code to identify the information available to the merchant. 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.”).

215. A POSITA would have understood that for, say, a merchant or bank, to be able to process a financial transaction, it would have been obvious to partially or fully reconstruct the information, or else the transaction would fail. The system of Bossemeyer retrieves **remainder data** (e.g., **public information** such as a customer’s name), retrieve extracted data (e.g., **proprietary** or **limited access information** such as credit card numbers and account PIN/numbers), and then logically merges these pieces of information (i.e., reconstruct the original

information to appear as before it was split into different security categories). In other words, when the “data from these various locations is supplied back to the smart card terminal 14,” a POSITA would understand that said data is merged/reconstructed in that terminal, for example, to save the information in a local storage such that the terminal can retrieve it during the financial transaction, and therefore, to effectuate the action desired (*e.g.*, financial transaction).

216. Although Bossemeyer does not explicitly state that the information, once reaching the terminal, is merged/reconstructed, a POSITA would have understood that such logical merging would have been obvious to take place for the (secure) transaction to succeed: otherwise, why retrieve disparate information from different stores, send it to a single terminal location, only to not use it in unison, resulting in a failed transaction.

217. I note that this limitation only requires “permitting” the reconstruction to take place. In my opinion, Bossemeyer not just discloses such permitting, but also the actual reconstruction/merging of the information/data.

218. Bossemeyer discloses an example where Bossemeyer’s method permits at least a partial reconstruction of a user’s medical data (*e.g.*, **medical alerts 212** and **insurance and prescription information 214**) and/or full reconstruction of data

(e.g., **medical history 216**) with the correct level of authorization. See EX1005 (Bossemeyer), 5:6-15:

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**.

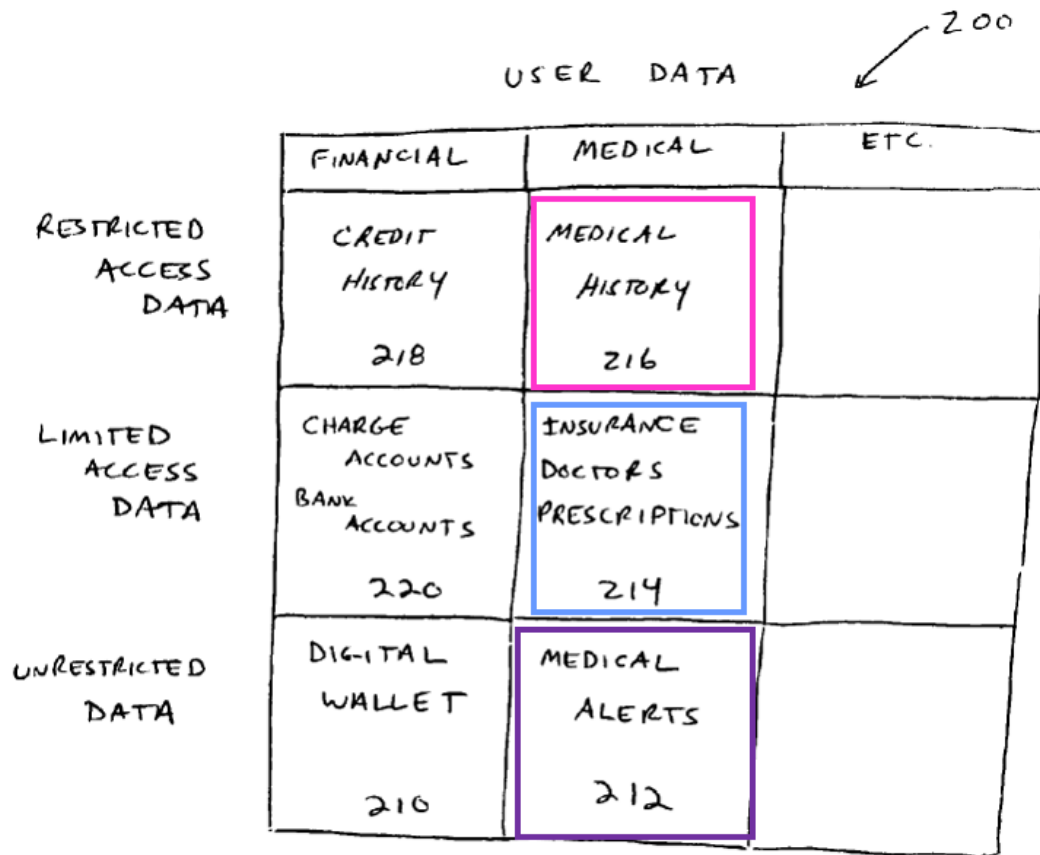


FIG. 3

EX1005 (Bossemeyer), Figure 3.

219. A POSITA would have understood from this example that for the pharmacist to be able to fill a prescription successfully, then the system of Bossemeyer has to first retrieve remainder data (e.g., public information such as a customer's medical alerts), retrieve extracted data (e.g., proprietary or limited access information such as medical history, insurance, or doctors' prescriptions), and then logically merge (reconstruct) these pieces of information.

220. Additionally, Glick discloses an appliance that reconstructs requested information in an analogous manner to Bossemeyer. EX1006 (Glick), 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.”); *see also* Section VII.B above.

221. In sum, Bossemeyer discloses permitting full or partial reconstruction.

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

222. Bossemeyer discloses and/or renders obvious this limitation.

223. *First*, Bossemeyer discloses permitting decryption of authentication codes, for the purpose of reconstruction of data, in the presence of a **predetermined security clearance access control**, *e.g.*, **user identification/authentication code** or **authorization/access code** or **data pointer** associated with a particular security level. A POSITA would have understood that these codes help protect the privacy of the data. *See* EX1005 (Bossemeyer), 2:38-47:

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*.

See EX1005 (Bossemeyer), 3:63-66:

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.

See EX1005 (Bossemeyer), 4:50-65:

Preferably, *the smart card provides a one-time encrypted user authentication code* based on the user's digital signature or certificate... 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.

224. *Second*, Bossemeyer's **user identification codes** correspond to respective security levels. For example, Bossemeyer discloses accessing a user's medical data based on the security level of the **user identification codes**. Specifically, Bossemeyer discloses accessing a user's certain medical data (*e.g.*, **medical alerts 212** and **insurance/prescription information 214**) using a user authentication code at the "unrestricted" and "limited access" security level, but requiring further authorization in the event access is required for other medical data (*e.g.*, **medical history 216**). *See* Section X.A.3 (above); *see also* EX1005 (Bossemeyer), 5:6-15:

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**.

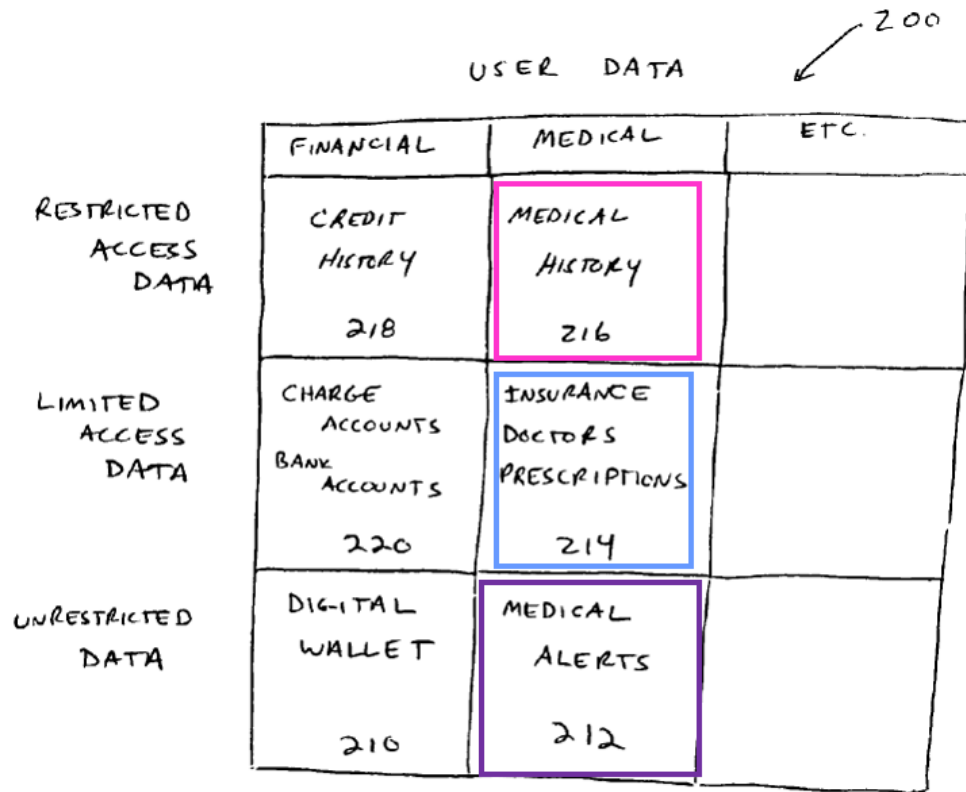


FIG. 3

EX1005 (Bossemeyer), Figure 3.

225. A POSITA would have understood that “**further authorization**” would require a *different* (or an additional) form of a user authentication code/data pointer (or an additional one) to authorize access to the “restricted access” data. EX1005 (Bossemeyer), 2:38-40 (“*Different* user identification codes, or data pointers, provided by smart cards 12 allow access to partitions in the database.”). A POSITA would have understood that different data that is deemed to have different security requirements and is separated accordingly, would have access controls or

codes corresponding to the different security levels, because different persons with different security clearances would need to only access data that corresponds to the persons security clearance, such that persons do not access data they are not unauthorized to. For that reason, data security systems often impose restrictions both for different users and also compartmentalize data at different security levels. *See* Section V.D above.

226. Note, however, that access controls need not be mutually exclusive: a “higher level” access control code could be used to grant access to lower levels of information as well, just as a military person with “top secret” clearance can also access “secret” or “confidential” information. *See* also Section V.D above.

227. In sum, Bossemeyer discloses and/or renders obvious only in the presence of **a predetermined security clearance access control** (“**user identification/authentication code**” or “**authorization/access code**” or “**further authorization**”) corresponding to said respective security level (“level of security (**unrestricted**, or **public limited access**, **restricted**)”).

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

228. Bossemeyer in combination with Glick renders obvious this limitation.

229. As discussed in Section VII.B (above), Glick discloses determining if the device (appliance) location is **within a predetermined geographic region**, *i.e.*, not beyond said predetermined region. *See* EX1006 (Glick), Abstract:

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 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*.

See also EX1006 (Glick), 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.”).

230. Glick discloses decrypting (reconstructing) the stored data based on the appliance’s location data (*i.e.*, when the **portable computing device** is not beyond a predetermined region). EX1006 (Glick), 4:8-13 (“If the appliance location is not within the proximate area of the location identity attribute, the appliance will be unable to generate a decryption key to decrypt the digital information. Thus,

allowing decryption of the digital information only at the specific geographic location enforces the location identity.”).

231. Glick discloses enforcing location identity and allowing access methods for accessing information only within a predetermined region, as illustrated in Figures 5 and 10 of Glick.

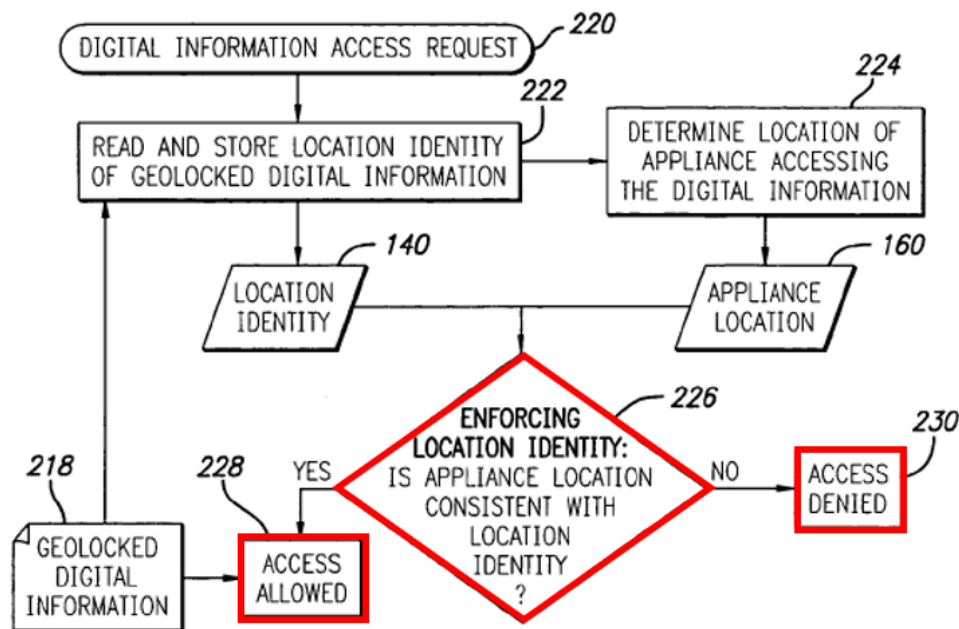


FIG. 5

EX1006 (Glick), Figure 5.

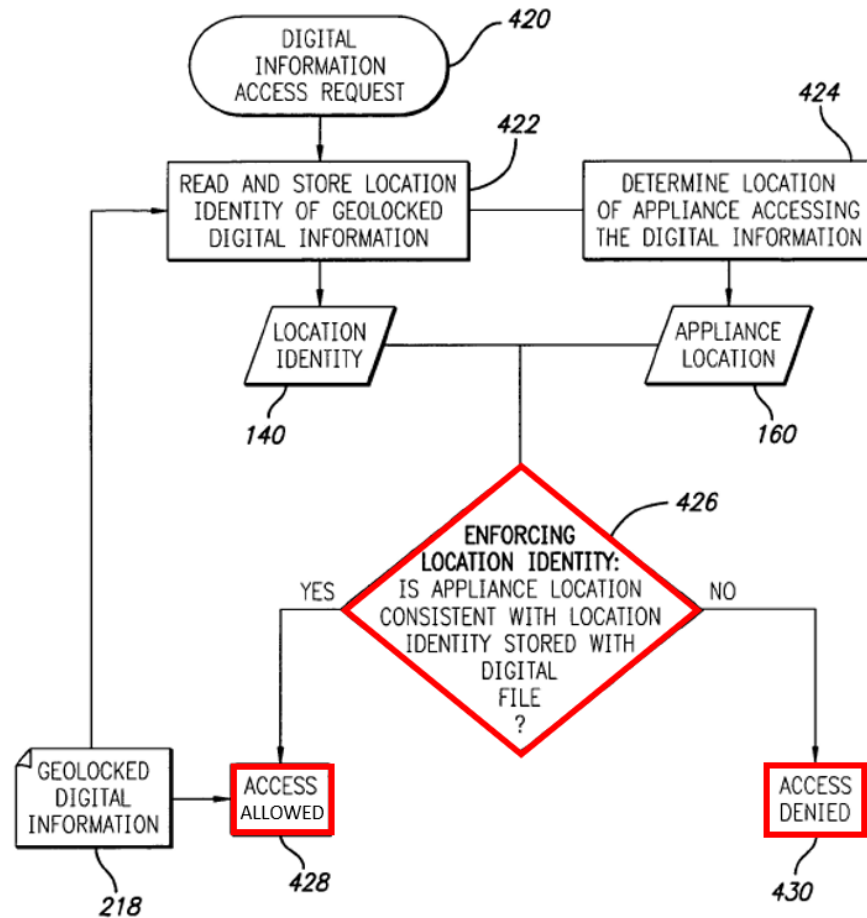


FIG. 10

EX1006 (Glick), Figure 10, 11:49-12:5, 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.”); *see also*, Section X.A.1.v above.

232. A POSITA would have understood that Bossemeyer in view of Glick renders obvious reconstructing a user’s data only when the **portable computing device** as disclosed in Bossemeyer and as modified by Glick is not beyond a predetermined region. Accordingly, this limitation is met.

233. In sum, Bossemeyer in view of Glick renders obvious only when said **portable computing device** is not beyond said predetermined region (“not within the proximate area of the location identity attribute”).

6. A POSITA Would Have Been Motivated To Combine Bossemeyer with Glick (Ground 1)

234. A POSITA would have been motivated to combine Bossemeyer with Glick to implement Glick’s location identity technique in Bossemeyer’s data security system. A POSITA would have been motivated to do so for at least five different reasons.

235. **First**, Bossemeyer provides a motivation to utilize location data as a security feature to control access to data because a POSITA would recognize that such a feature would increase security to Bossemeyer’s network. For example, banks can minimize fraud by limiting transactions to the geographical region of the card holder.

236. Bossemeyer and Glick both relate to the same field of managing and controlling information, or more specifically, providing different users access to different information.

237. Bossemeyer's network is shown in Figure 1, reproduced below.

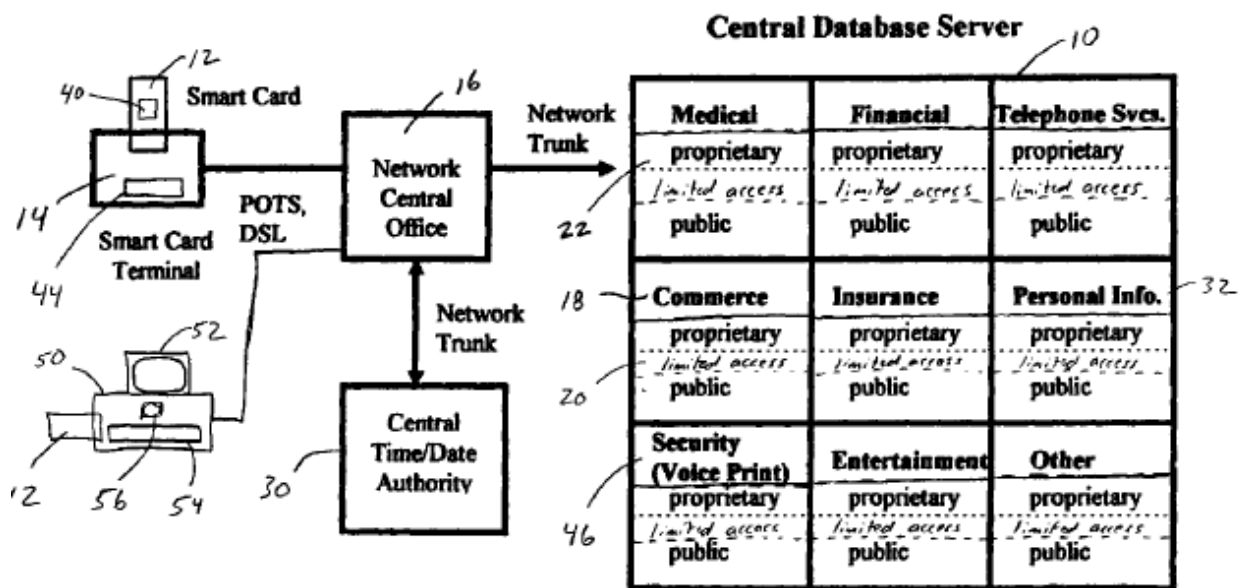


Figure 1

EX1005 (Bossemeyer), Figure 1.

238. As shown, Bossemeyer's system partitions data in a centralized database "both in terms of the smart card application *as well as the accessibility of the information.*" EX1005 (Bossemeyer), 2:17-20, 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.”).

239. Glick recognizes that “it would be desirable to provide an information interchange system and method that allows control over security and access to the information.” EX1006 (Glick), 3:19-22. Glick discloses a “*method and apparatus for controlling access to digital information.*” EX1006 (Glick), 3:27-28.

240. Thus, a POSITA would be motivated to combine the features of Bossemeyer with the features of Glick, because both disclose systems and methods for controlling secure access to information.

241. Bossemeyer’s method of controlling the accessibility of information serves as a security measure to “distinguish[] between public information and proprietary information stored in the partitioned memory locations.” EX1005 (Bossemeyer), Abstract.

242. Glick’s method also distinguishes between secure (“geolocked information”) and non-secure information (“digital information”). EX1006 (Glick), 5:20-23 (“Digital Information. Digital information is information that is represented in digital format. Examples of information that can be represented digitally include

text, data, software, music, video, graphics, etc.”), 5:36-39 (“Geolocked Information. Digital information that has been associated with a location identity attribute, and that can only be accessed within an area defined by the location identity attribute.”).

243. Thus, a POSITA would be motivated to combine the security features disclosed by Bossemeyer with the security features disclosed by Glick because both Bossemeyer and Glick contemplate controlling the access to *secure* information and differentiating such information from non-secure information. A POSITA would have known that when users consider security measures, they have to decide on how much security or what level of security to have. While each of Bossemeyer and Glick provide security measures, their combination yields better and stronger security. It is expected for users to consider how to increase security by adding more security measures. For example, a home owner can start with a lock and a key to lock their home, then add more locks and keys to increase the security, then add security cameras and alarms to increase security even further, following by adding a tall fence around the property, and so on.

244. Combining Bossemeyer and Glick would involve implementing known techniques according to the methods disclosed in Bossemeyer and Glick and such combination would yield predictable results.

245. **Second**, Glick identifies a known problem, *e.g.*, controlling access to information, and suggests using location identity to control access to that information to solve the problem.

246. Bossemeyer discloses controlling the “accessibility of the information” through security measures such as “data pointers” (EX1005 (Bossemeyer), 2:58-60), “user identification codes” (EX1005 (Bossemeyer), 2:37-40), or “user authentication codes” (EX1005 (Bossemeyer), 2:44-45). *See* EX1005 (Bossemeyer), 3:63-4:6:

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.

See also, EX1005 (Bossemeyer), 4:50-58:

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.

See also, EX1005 (Bossemeyer), Figure 2, 4:59-65:

The network server 10, 110 validates the user identification by decrypting the authorization code. This information is then cross-referenced with the merchant code to identify the information available to the merchant. ***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.

See also EX1005 (Bossemeyer), 2:13-27:

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.

247. Bossemeyer does not explicitly show that location data can serve as a security measure. But Bossemeyer's method is not restricted to this particular

embodiment. EX1005 (Bossemeyer), 5:32-37 (“While the invention has been described in connection with one or more embodiments, it will be understood that the invention is not limited to those embodiments. On the contrary, the invention covers all alternatives, modifications, and equivalents, as may be included within the spirit and scope of the appended claims.”).

248. Moreover, Bossemeyer discloses that its invention to operates over the Internet. EX1005 (Bossemeyer), 1:47-49 (“The network connections are facilitated by the present telephone network or an interconnected network of computers such as the Internet.”). A POSITA would recognize that on the Internet, computers have hostnames and associated network (IP) addresses, and those can easily serve to identify a location and hence be used to restrict access. For example, to control access from the entire country of China, one need only resolve the IP address to its hostname and find out that it ends in a “.cn” top-level domain extension; similarly, to control access to within the Stanford University campus (known to be located in Stanford, California), one can check to see if the hostname corresponding to the accessing IP addressed ends in “stanford.edu”. See also Section V.E above.

249. Glick discloses a data security system that uses a location identity attribute to control access to information within the system. *See* EX1006 (Glick), Abstract:

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.

See also EX1006 (Glick), 3:27-30 (“A method and apparatus for *controlling access to digital information* in accordance with the present invention utilizes a *location identity attribute* that defines a specific geographic location.”), 3:43-46 (“According to a general embodiment of the invention, access to the digital information is allowed only at the specific geographic location defined by the location identity attribute.”).

250. A POSITA would have been motivated to modify Bossemeyer’s system to use Glick’s location identity attribute. The combination of Bossemeyer with Glick merely uses Glick’s location identify technique in Bossemeyer’s data system according to the methods for determining the location disclosed in Glick.

251. Glick discloses that “[a] method and apparatus for *controlling access to digital information* utilizes a *location identity attribute* that defines a specific geographic location,” that “can be accessed *only at the specific geographic*

location.” EX1006 (Glick), Abstract, 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 identity 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.”).

252. ***Third***, a POSITA would have been motivated to modify Bossemeyer’s system in view of Glick because Glick’s geographic security feature 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 user information.***

253. For example, banks require a PIN number for a customer to withdraw cash from an ATM, but that does not necessarily prevent a thief from draining one’s account if they steal an ATM card or its information and also have knowledge of or can guess a PIN number. Banks can minimize such fraud by limiting ATM transactions to the geographical region of the card holder (*i.e.*, it is suspicious to see

one ATM transaction in New York, followed minutes later by another from a bank in California—a legitimate customer could not have physically traveled coast-to-coast within minutes).

254. Specifically, a POSITA would have been motivated to add a location-based security feature (as opposed to any other additional security feature) because Bossemeyer relates to a “centralized server architecture.” EX1005 (Bossemeyer), 1:49-52.

255. Bossemeyer’s network arrangement improves upon the design of smart cards, smart card readers, and applications for smart cards by “focus[ing] on the integration of a centralized server architecture or a network arrangement for multiple smart card applications” that is “readily accessible from different types of smart card terminals supporting various smart card applications.” EX1005 (Bossemeyer), 1:39-47. Such a centralized server architecture allows “data related to an individual [to] be accessed by an individual smart card, predefined groups of smart card users, or the general public.” EX1005 (Bossemeyer), 1:49-52.

256. Glick teaches that “[t]he present invention satisfies the need for a way to *control the interchange of digital information that allows control over security and access to the information*, and which prevents unauthorized copying of copyright-protected content.” EX1006 (Glick), 5:4-8.

257. A POSITA would have been motivated to control Bossemeyer's centralized system not only with authorization codes to verify *who* is accessing the system (as disclosed by Bossemeyer), but also with authorization to verify *where* the system is being accessed from (as disclosed by Glick), and further to verify *whoever* is granted access is *where* they are supposed to be (Bossemeyer in combination with Glick).

258. As discussed in Section X.A.4 (above) Bossemeyer discloses accessing user data only in the presence of a predetermined security clearance access control. Combining Bossemeyer with 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 those who use Bossemeyer's system. For example, Glick's location-based control could be used to ensure that a user's medical information is only accessed within the hospital itself, thus adding *another layer of security* by preventing HIPAA violations or breaches of individuals' privacy who seek to access the information outside of the hospital's premises.

259. Bossemeyer discloses another example where a user's financial information is accessed in a merchant transaction so that the "merchant may... determine whether to accept the user's credit for a particular dollar amount." EX1005 (Bossemeyer), 2:22-26. The location-based control could be used to ensure

that a user's financial information is only accessed by retail locations, thus preventing access of individuals who are not involved in a legitimate transaction with the user.

260. **Fourth**, a POSITA would have been motivated to combine Bossemeyer with Glick, because the combination would merely involve using Glick's location identity to control access to information in Bossemeyer's network arrangement with a central database server storing user information, which was ready for improvement to yield predictable results.

261. For example, this would be a trivial change to a software application in a single if-then-else clause: instead of performing a logical check "if user has the right credentials, then allow access, else deny access," a programmer would merely add the location-based check to yield: "if user has the right credentials *and the access is requested from a permitted location*, then allow access, else deny access."

262. **Fifth**, Glick acknowledges that advances in computer, telecommunications and networking technology allow companies and individuals to access and share vast amounts of information. *See* EX1006 (Glick), 1:14-29:

Rapid advances in computer, telecommunications and networking technology have enabled an avalanche of new opportunities and applications that were impossible just a few years ago. These advances are exemplified by the explosive growth in popularity of the Internet.

As known in the art, the Internet is an interconnection of computer networks that enables computers of all kinds to communicate with each other and share information. Companies, individuals, government agencies, charitable organizations, and academic centers, of all sizes, regularly use the Internet to share information, deliver services, and exchange a wide range of content. The Internet functions as a distributed network of systems that is neither controlled nor managed by any one entity. Physical and logical pathways that facilitate the exchange of information connect these networks to each other.

263. However, Glick recognizes that the uncontrolled flow of information can come with a cost of security risks and access. *See* EX1006 (Glick), 1:30-37:

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.

264. Glick therefore concludes that “it would be desirable to provide an information interchange system and method that allows control over security and access to the information...” EX1006 (Glick), 3:19-22. Glick provides multiple examples of the benefits of using location identity to control access of information.

See EX1006 (Glick), 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.”).

265. Glick discloses that location identity can be used to prevent unauthorized use and copying of digital information/media. *See* EX1006 (Glick), 12:64-13:14:

In an exemplary application of the present invention, the *location identity attribute may be used to combat the problem of piracy and unauthorized use and copying of digital film*. A customer would rent or buy digital video media (e.g., DVD) in a manner analogous to that when renting or purchasing film at a commercial video rental store. The location identity attribute is utilized at the time of purchase of the digital video media. Specifically, the location identity attribute corresponding to the customer’s home address would be physically stored on a re-writable portion of the digital video media. The DVD player in the customer’s home will be coded to enforce the location identity attribute in order to limit the playback of the digital video media to the particular geographic region and time period. Even if the media is copied, lost or stolen, it can only be viewed within its playback region and time span, and thus serves as a robust solution to the problems associated with unauthorized use of digital media.

266. 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. *See* EX1006 (Glick), 13:35-55:

In another exemplary application of the invention, location identity is used to “narrowcast” information over public networks. Narrowcasting refers to the *transmission of information to a limited audience* (in contrast with broadcasting whereby information is transmitted to a large audience). Many types of information are useable only within a location context, e.g., local weather, traffic information, movie schedules, store information, etc. Applications that use such location-dependent information may be referred to as location-based applications. *Location identity provides a way to use a broadcast type protocol to send information over a network that is identified by the location for which it is pertinent, e.g., local area for weather, store location for sale and advertising information, etc.* Using the location of the client appliance, the client applications can utilize the location identity attached to the information to *screen information selectively based on their current location*. It can also provide a way to establish a unique location-based shared cryptographic key to maintain secure confidential communications for geographically limited narrowcast applications.

267. Glick further discloses that location identity can be used to enhance confidentiality and security for network connectivity. *See* EX1006 (Glick), 13:56-14:4:

In another exemplary application of the present invention, location identity is used to enhance confidentiality and security for wireless network connectivity... Since every wireless appliance communicating over the network will have a unique location, ***location identity can be utilized to establish a unique shared cryptographic key that can be used to maintain secure confidential communications for wireless devices connecting over a public network.***

268. A POSITA would have found that Bossemeyer and Glick were analogous to the '825 Patent. All three pertain to the same field of endeavor, *i.e.*, securing and controlling access to security-sensitive information. *Compare* EX1001 (the '825 Patent), 1:23-26 (“The present invention relates to a data security system and method and, more specifically, to a process, program and system which operates to secure files and data objects in portable computing devices.”) *with* EX1005 (Bossemeyer), 1:44-47 (“[T]he present invention describes a network arrangement which is readily accessible from different types of smart card terminals supporting various smart card applications.”), 3:16-18 (“The network smart card server acts as a secured gatekeeper to such information and the smart card acts as the enabling key.”) *and with* EX1006 (Glick), Abstract (“A method and apparatus for controlling access to digital information utilizes a location identity attribute that defines a specific geographic location.”).

269. 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 are still reasonably pertinent to the particular problem with which the '825 Patent's invention is involved, *i.e.*, securing digital information. *Compare* EX1001 (the '825 Patent), 6:55-58 ("It is an object of the present invention to provide a data security system, an information processing system and a method for securely storing data and rebuilding that data in the presence of an adequate security clearance.") *with* EX1005 (Bossemeyer), 2:17-22 ("The central database server 10 is a centralized partitioned database server which partitions information both in terms of the smart card application as well as the accessibility of the information. The information is stored by category (medical, financial, etc.) as well as level of security (unrestricted, or public limited access, restricted)."); *Compare also* EX1001 (the '825 Patent), 7:64-65 ("It is a further object of the present invention to secure files and data objects in portable computing devices."), *with* EX1006 (Glick), Abstract ("A method and apparatus for controlling access to digital information utilizes a location identity attribute that defines a specific geographic location.").

270. A POSITA would also have had a reasonable expectation of success in combining Bossemeyer with Glick. Indeed, as I discuss in Section X.A.1.v (above), 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 (Glick), 8:7-12 (“[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.”). Accordingly, implementing Glick’s teachings in Bossemeyer’s system would be well within the ability of a POSITA.

B. Ground II: Bossemeyer In View Of Glick and Carmichael Renders Obvious Claim 81

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:**

271. I understand that the preamble may not be limiting. Nevertheless, Bossemeyer in combination with Glick and Carmichael discloses the preamble for the reasons discussed below and in Section X.A.1 (above).

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

272. As I explained in Section X.A.1.i above, Bossemeyer discloses this limitation. Also, Bossemeyer alone and/or combined with Glick renders obvious this limitation. Bossemeyer in combination with Glick and Carmichael also renders obvious this limitation for the reasons discussed in Section X.A.1.i above.

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

273. As I explained in Section X.A.1.ii above, Bossemeyer discloses this limitation. Bossemeyer in combination with Glick and Carmichael also renders obvious this limitation for the reasons discussed in Section X.A.1.ii above.

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

274. As I explained in Section X.A.1.iii above, Bossemeyer discloses and/or renders obvious this limitation. Bossemeyer in combination with Glick and Carmichael also renders obvious this limitation for the reasons discussed in Section X.A.1.iii above.

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

275. As I explained in Section X.A.1.iv above, Bossemeyer discloses this limitation. Bossemeyer in combination with Glick and Carmichael also renders obvious this limitation for the reasons discussed in Section X.A.1.iv above.

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

276. As I explained in Section X.A.1.v above, Bossemeyer in view of Glick renders obvious this limitation. Bossemeyer in combination with Glick and Carmichael also renders obvious this limitation for the reasons discussed in Section X.A.1.v above and for the additional reasons discussed below.

- a. Smart Card Locatable With **Current Location Data****

277. As I discussed in Section X.A.1.v.a above, Bossemeyer in combination with Glick renders obvious a smart card locatable with **current location data**.

278. Carmichael explicitly discloses a smart card with “location tracking means for determining **a location of the smart card**.” EX1007 (Carmichael), 3:32-34. 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 to incorporate Carmichael’s

location tracking means. 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 (Carmichael), 3:58-59.

279. Carmichael explains that “the location tracking means transmits an identifiable signal, which is detectable by a global positioning system satellite. Alternatively, 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 (Carmichael), 3:60-67. Therefore, a POSITA would have understood that Bossemeyer’s central database server can identify the location of the card, in view of Carmichael’s teaching.

280. As I explain in Section X.B.6 below, it would have been obvious to combine Bossemeyer, Glick, and Carmichael to incorporate Carmichael’s teaching of using a smart card with location tracking means, and a POSITA would have had a reasonable expectation of success in combining Bossemeyer, Glick, and Carmichael. Accordingly, Bossemeyer in view of Glick and Carmichael renders obvious this limitation.

281. In sum, the combination of Bossemeyer, Glick, and Carmichael renders obvious a computer system having at least one portable computing device (a card a

consumer can “carry” or an “appliance”) [is] locatable with **current location data** (Glick’s “**location identity attribute**” and Carmichael’s “**location tracking means for determining a location of the smart card**”).

b. Smart Card Terminal Locatable With Current Location Data

282. As I explained in Section X.B.1.v.b above, Bossemeyer in combination with Glick renders obvious a smart card terminal with current location data. For the same reasons, Bossemeyer in combination with Glick and Carmichael also renders obvious a smart card terminal with current location data.

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

283. As I explained in Section X.A.2 above, Bossemeyer in combination with Glick and Carmichael renders obvious this limitation for the same reasons explained in Section X.A.2 above.

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

284. As I explained in Section X.A.3 above, Bossemeyer discloses this limitation. Bossemeyer in combination with Glick and Carmichael discloses this limitation for the same reasons explained in Section X.A.3 above.

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

285. As I explained in Section X.A.4 above, Bossemeyer discloses and/or renders obvious this limitation. Bossemeyer in combination with Glick and Carmichael discloses and/or renders obvious this limitation for the same reasons explained in Section X.A.4 above.

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

286. As I explained in Section X.A.5 above, Bossemeyer in combination with Glick discloses this limitation. Bossemeyer in combination with Glick and Carmichael discloses this limitation for the same reasons explained in Section X.A.5 above,.

6. A POSITA Would Have Been Motivated To Combine Bossemeyer with Glick and Carmichael

287. As discussed in Section X.A.6 above, a POSITA would have been motivated to combine Bossemeyer with Glick. A POSITA would have been further motivated to combine Bossemeyer with Glick and Carmichael, such as to implement Carmichael's teaching of a location tracking means in Bossemeyer's smart card "for determining a location of the smart card" (EX1007 (Carmichael), 3:32-34). A POSITA would have been motivated to do so for at least five reasons.

288. **First**, the combination of Bossemeyer and Glick with Carmichael represents the use of known techniques according to known methods in the same way to yield predictable results.

289. The Bossemeyer and Carmichael combination would merely involve including Carmichael's location tracking means, *e.g.*, a GSM chip, into Bossemeyer's smart card in the same way as taught by Carmichael. This is because both Bossemeyer and Carmichael disclose similar systems (*e.g.*, smart cards) and methods (*e.g.*, smart card applications). EX1005 (Bossemeyer), 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 (Carmichael), 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.”).

290. ***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 these problems (e.g., using a GSM chip) to determine the location of the smart card.

291. Carmichael’s tracking means could be used to locate Bossemeyer’s smart card, or when the user of Bossemeyer’s card needs to be located. *See* EX1007 (Carmichael), 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.***

See also EX1007 (Carmichael), 3:58-62:

The 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 detectable by a global positioning system satellite.

292. Carmichael's disclosed solution, using a GSM chip, can be used in multiple ways to determine the location of a smart card. *See* EX1007 (Carmichael), 8:21-33:

Also found on the smart card 1... 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. If used by way of a police tracking system, the card is coupled to a police terminal, which is capable of interfacing with the GSM chip. The police terminal is in duplex communication with a satellite, such as a global positioning system satellite. The satellite relays location information back to the institution. Thus, individuals holding the card can be identified with the identification function and located using the location tracking function of the GSM.

See also EX1007 (Carmichael), 8:34-42:

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. The global positioning system satellite is in duplex communication with the transmitter, which is in electrical communication with a memory associated with the microprocessor on the smart chip 75. The satellite

sends coordinate or location data to the transmitter, which relays the information to the microprocessor.

293. **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).

294. For example, Carmichael's technique enables map functionality on a smart card. *See* EX1007 (Carmichael), 8:42-56:

The program enables the microprocessor to process the coordinate data received from the satellite, to store said data in a non-volatile memory, and to ***generate a travel log based on said data***. The program also enables the microprocessor to ***generate a map of all of the global positions in which the smart card 1 has been located over a predetermined length of time***. This information can be used by the holder of the smart card 1 to review all of the places he or she has been during a predetermined period. All of this information can be downloaded through a computer peripheral reader to a computer and viewed on a computer screen or printed out. Alternatively, all of the location information can be relayed to the institution issuing the smart

card and can be stored by the institution for retrieval by computer or telephone access by the cardholder.

295. ***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.

296. For example, Bossemeyer's smart card was known and "covers all alternatives, modifications, and equivalents" (EX1005 (Bossemeyer), 5:32-37), which would have yielded predictable results (locating a smart card) with a known technique (a GSM chip in connection with a GPS network). *See* EX1007 (Carmichael), 3:58-67:

The 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 detectable by a global positioning system satellite. 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.

297. ***Fifth***, Carmichael provides express teachings, suggestions, and 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. *See* EX1007 (Carmichael), 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.***

See also EX1007 (Carmichael), 8:34-56:

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. The global positioning system satellite is in duplex communication with the transmitter, which is in electrical communication with a memory associated with the microprocessor on the smart chip 75. The satellite sends coordinate or location data to the transmitter, which relays the information to the microprocessor. The program enables the microprocessor to process the coordinate data received from the satellite, to store said data in a non-volatile memory, and to ***generate a travel log based on said data.*** The program also enables the

microprocessor to *generate a map of all of the global positions in which the smart card 1 has been located over a predetermined length of time*. This information can be used by the holder of the smart card 1 to review all of the places he or she has been during a predetermined period. All of this information can be downloaded through a computer peripheral reader to a computer and viewed on a computer screen or printed out. Alternatively, all of the location information can be relayed to the institution issuing the smart card and can be stored by the institution for retrieval by computer or telephone access by the cardholder.

298. 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. *See* EX1007 (Carmichael), 2:60-3:3:

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.

See also EX1007 (Carmichael), 3:4-19:

Other limitations of known smart cards and credit cards is that they are not capable of categorizing, automatically storing, and generating information for multiple accounts in real time as transactions occur. The present invention solves this problem by coupling an IC to the card, which can store data about various kinds of transactions as they occur, and that data can be recalled at a later time to generate charts, spread sheets, schedules, account statements, and account summaries. Moreover, the IC of the present invention has this capability for all of the functions of the smart card, including the credit, debit, telephone, ATM, GPS, and identification functions. This information can be extremely useful for immediately accessing account information as well as *movement history through the GPS system*. Thus, for example, the present invention allows a traveler to *generate a map or a travel log of where he/she has been for a predetermined length of time*.

299. As discussed above in Section X.A.6 above, a POSITA would have found that Bossemeyer and Glick were analogous to the '825 Patent. A POSITA would apply that same reasoning to Carmichael, because all four pertain to the same field of endeavor, *i.e.*, securing and controlling access to security-sensitive information. *Compare* EX1001 (the '825 Patent), 1:23-26 ("The present invention relates to a data security system and method and, more specifically, to a process, program and system which operates to secure files and data objects in portable computing devices.") *with* EX1007 (Carmichael), 3:35-45 ("The first memory

means can be a magnetic strip which can hold one or more of the following information: ... a bank account number, ... the holder's name, address, social security number, ... and any other identification number.”).

300. 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 are still reasonably pertinent to the particular problem with which the '825 Patent's invention is involved, *i.e.*, securing digital information, for the same reasons discussed in Section X.A.6 above. Additionally, Carmichael is also reasonably pertinent to the particular problem of securing digital information. *Compare* EX1001 (the '825 Patent), 6:55-58 (“It is an object of the present invention to provide a data security system, an information processing system and a method for securely storing data and rebuilding that data in the presence of an adequate security clearance.”) *with* EX1007 (Carmichael), 4:46-50 (“In another innovative aspect, the invention is directed to a method of gaining access through an access device upon payment of a value using a smart card comprising a microprocessor in electrical communication with a memory and a location tracking means.”).

301. Combining Carmichael's location tracking means with Bossemeyer's system would have been obvious to a POSITA at the time. Further, in addition to the reasons discussed in Section X.A.6 above, a POSITA would have been able to

combine Bossemeyer, Glick, and Carmichael with a reasonable expectation of success, because the combination would merely involve including Carmichael's location tracking means (*e.g.*, a GSM chip) into Bossemeyer's smart card in the same way as taught by Carmichael.

302. For example, Bossemeyer and Carmichael both relate to smart cards, a central server(s), and terminals that facilitate smart card applications. *Compare* EX1005 (Bossemeyer), 1:51-52 (“an individual smart card, predefined groups of smart card users”), 1:45-47 (“different types of smart card terminals supporting various smart card applications”), 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”), *with* EX1007 (Carmichael), 1:8 (“The present invention relates to smart cards”), 4:1-4 (“the 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”), 4:46-50 (“the invention is directed to a method of gaining access through an access device upon payment of a value using a smart card comprising a microprocessor in electrical communication with a memory and a location tracking means”).

303. Carmichael's “central processing center” and Bossemeyer's “central database server” both contain distinct memories for different functions. *Compare*

EX1005 (Bossemeyer), 5:51-52 (disclosing a “server that includes a plurality of application-specific partitioned memory locations”), *with* EX1007 (Carmichael), 3:63-64 (disclosing a “central processing center which stores data relating to all of the function 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.”).

XI. Conclusion

304. In my opinion, the challenged claim 81 of the '825 Patent is unpatentable.

XII. Availability for Cross-Examination

305. In signing this declaration, I recognize that the declaration will be filed as evidence in a case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross examination in the case and that cross examination will take place within the United States. If cross examination is required of me, I will appear for cross examination within the United States during the time allotted for cross examination.

XIII. Right to Supplement

306. I reserve the right to supplement my opinions in the future to respond to any arguments that the Patent Owner may raise and to take into account new information as it becomes available to me.

XIV. Jurat

307. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1101 of Title 18 of the United States Code.



May 30, 2023

Dr. Erez Zadok