

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 IPR2023-00969

U.S. Patent No. 7,349,987

Claims 1, 6, 9, 10, 11, 15, 16, 21, 22, 23, and 27

DECLARATION OF EREZ ZADOK, PH.D.

ON BEHALF OF PETITIONER

TABLE OF CONTENTS

	<u>Page</u>
I. Qualifications.....	1
II. Background.....	12
III. Relevant Law	14
A. Claim Construction.....	14
B. Obviousness.....	15
C. Ordinary Skill in the Art.....	17
IV. Summary of Opinions.....	18
V. Technology Overview	18
A. General Computer Operations.....	19
B. Data Storage Devices and Systems	20
C. Networked and Distributed Storage Systems.....	22
D. File and Data Security, Security Levels.....	24
VI. Overview Of The '987 Patent.....	30
A. Prosecution History of the '987 Patent	34
VII. Overview Of The Prior Art.....	38
A. Bossemeyer (U.S. Patent No. 7,010,701, "EX1005 (Bossemeyer)").....	38
B. Merenda (U.S. Publication No. 2004/0148290, "EX1006 (Merenda)").....	46
C. Chaganti (U.S. Patent No. 6,845,448, "EX1007 (Chaganti)")	51

D.	Kohane (U.S. Publication No. 2004/0199765, “EX1008 (Kohane)”).....	56
VIII.	Level of Ordinary Skill in the Art	62
IX.	Claim Construction.....	62
X.	Specific Grounds For Challenge.....	63
A.	Ground 1: Claims 1, 6, 9, 10-11, 15-16, 21-23, And 27 Are Obvious Over Bossemeyer.....	63
1.	Independent Claims 1, 10, 16, and 22.....	63
i.	Claim 1, 10, 16, and 22 Preambles	63
a.	[1pre-i] A method of securing data having one or more security sensitive words, characters or icons in a computer system.....	63
b.	[10pre-i] A method of securing data with a parsing algorithm via a computer system	69
c.	[16pre-i] A computer readable storage medium encoded with programming instructions for securing data having one or more security sensitive words, characters or icons in a computer system.....	79
d.	[22pre-i] A computer readable storage medium encoded with programming instructions for securing data with a parsing algorithm via a computer system.....	81
e.	[1/16pre-ii] with a plurality of physically distinguishable memories respectively designated as a remainder store and a plurality of physically distinct extract stores corresponding to a plurality of security levels for respective subsets of said security sensitive words, characters or icons comprising:	82

	[10/22pre-ii] having physically distinguishable memories designated as a remainder store and a plurality of physically distinct extract stores corresponding to a plurality of security levels for respective subsets of said security sensitive words, characters or icons comprising:.....	82
ii.	[1/16a] extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data therefrom;	91
	[10/22a] parsing said data to obtain extracted data for respective associated security levels and remainder data therefrom;	91
iii.	[1/16b] storing said extracted data and said remainder data in said respective extract stores corresponding to an associated security level and said remainder store, respectively; and, ...	93
	[10/22b] storing said extracted data and said remainder data in said extract stores and said remainder store, respectively; and	93
iv.	[1/10/16/22c] permitting full or partial reconstruction of said data via said extracted data from respective extract stores and remainder data	98
v.	[1/10/16/22d] only in the presence of a predetermined security clearance corresponding to said associated security level for said respective extract stores.	104
2.	Dependent Claims 6 and 21	109
i.	[6pre] A method as claimed in claim 1 including	109
	[21pre] A storage medium with programming instructions as claimed in claim 16 including	109

ii.	[6/21a] establishing a plurality of security levels each with a respective security clearance.....	109
iii.	[6/21b] each said subset of said security sensitive words, characters or icons being correlated with said plurality of security levels and	114
iv.	[6/21c] the step of permitting reconstruction including the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.....	114
3.	Dependent Claim 9.....	120
i.	[9pre] A method as claimed in claim 1 including	120
ii.	[9a] assessing a charge for extracting, storing or permitting reconstruction.....	120
4.	Dependent Claims 11 and 23	124
i.	[11pre] A method as claimed in claim 10	124
	[23pre] A storage medium with programming instructions as claimed in claim 22	124
ii.	[11/23a] wherein the step of parsing parses the data granularly.	124
5.	Dependent Claims 15 and 27	125
i.	[15pre] A method as claimed in claim 10 including	125
	[27pre] A storage medium as claimed in claim 22 including	125
ii.	[15/27a] a further data security step of one from the group of storing said data without encryption, storing said data with encryption and destroying said data; said further data security step being	

	independent of said parsing, storing and permitting reconstruction.	125
B.	Ground 2: Claims 1, 6, 9, 10-11, 15-16, 21-23, And 27 Are Obvious Over Bossemeyer With Merenda	131
1.	Independent Claims 1, 10, 16, and 22.....	131
i.	Claim 1, 10, 16, and 22 Preambles	131
a.	[1pre-i] A method of securing data having one or more security sensitive words, characters or icons in a computer system.....	131
b.	[10pre-i] A method of securing data with a parsing algorithm via a computer system	133
c.	[16pre-i] A computer readable storage medium encoded with programming instructions for securing data having one or more security sensitive words, characters or icons in a computer system	137
d.	[22pre-i] A computer readable storage medium encoded with programming instructions for securing data with a parsing algorithm via a computer system.....	138
e.	[1/16pre-ii] with a plurality of physically distinguishable memories respectively designated as a remainder store and a plurality of physically distinct extract stores corresponding to a plurality of security levels for respective subsets of said security sensitive words, characters or icons comprising:.....	138
	[10/22pre-ii] having physically distinguishable memories designated as a remainder store and a plurality of physically distinct extract stores corresponding to a plurality of security levels for	

	respective subsets of said security sensitive words, characters or icons comprising:.....	138
ii.	[1/16a] extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data therefrom;	141
	[10/22a] parsing said data to obtain extracted data for respective associated security levels and remainder data therefrom;	141
iii.	[1/16b] storing said extracted data and said remainder data in said respective extract stores corresponding to an associated security level and said remainder store, respectively; and, ...	143
	[10/22b] storing said extracted data and said remainder data in said extract stores and said remainder store, respectively; and	143
iv.	[1/10/16/22c] permitting full or partial reconstruction of said data via said extracted data from respective extract stores and remainder data	145
v.	[1/10/16/22d] only in the presence of a predetermined security clearance corresponding to said associated security level for said respective extract stores.	151
2.	Reasons To Combine Bossemeyer With Merenda	153
3.	Dependent Claims 6 and 21	174
i.	[6pre] A method as claimed in claim 1 including	174
	[21pre] A storage medium with programming instructions as claimed in claim 16 including	174
ii.	[6/21a] establishing a plurality of security levels each with a respective security clearance.....	174

iii.	[6/21b] each said subset of said security sensitive words, characters or icons being correlated with said plurality of security levels and	181
iv.	[6/21c] the step of permitting reconstruction including the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.....	181
4.	Dependent Claim 9.....	182
i.	[9pre] A method as claimed in claim 1 including	182
ii.	[9a] assessing a charge for extracting, storing or permitting reconstruction.....	182
5.	Dependent Claims 11 and 23	182
i.	[11pre] A method as claimed in claim 10	182
	[23pre] A storage medium with programming instructions as claimed in claim 22	182
ii.	[11/23a] wherein the step of parsing parses the data granularly.	183
6.	Dependent Claims 15 and 27	185
i.	[15pre] A method as claimed in claim 10 including	185
	[27pre] A storage medium as claimed in claim 22 including	185
ii.	[15/27a] a further data security step of one from the group of storing said data without encryption, storing said data with encryption and destroying said data; said further data security step being independent of said parsing, storing and permitting reconstruction.	185
C.	Ground 3: Claim 9 Is Obvious Over Bossemeyer With Chaganti	191

1.	Dependent Claim 9.....	191
i.	[9pre] A method as claimed in claim 1 including	191
ii.	[9a] assessing a charge for extracting, storing or permitting reconstruction.....	191
2.	Reasons To Combine Bossemeyer With Chaganti.....	197
D.	Ground 4: Claim 9 Is Obvious Over Bossemeyer With Merenda And Chaganti.....	203
1.	Dependent Claim 9.....	203
i.	[9pre] A method as claimed in claim 1 including	203
ii.	[9a] assessing a charge for extracting, storing or permitting reconstruction.....	204
E.	Ground 5: Claims 15 And 27 Are Obvious Over Bossemeyer With Kohane.....	204
1.	Dependent Claims 15 and 27	204
i.	[15pre] A method as claimed in claim 10 including	204
	[27pre] A storage medium as claimed in claim 22 including	204
ii.	[15/27a] a further data security step of one from the group of storing said data without encryption, storing said data with encryption and destroying said data; said further data security step being independent of said parsing, storing and permitting reconstruction.	205
2.	Reasons To Combine Bossemeyer With Kohane.....	209
F.	Ground 6: Claims 15 And 27 Are Obvious Over Bossemeyer With Merenda And Kohane	215
1.	Dependent Claims 15 and 27	215

i.	[15pre] A method as claimed in claim 10 including	215
	[27pre] A storage medium as claimed in claim 22 including	215
ii.	[15/27a] a further data security step of one from the group of storing said data without encryption, storing said data with encryption and destroying said data; said further data security step being independent of said parsing, storing and permitting reconstruction.	216
XI.	Conclusion	216
XII.	Availability for Cross-Examination	216
XIII.	Right to Supplement	217
XIV.	Jurat.....	217

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. 7,349,987 (the “’987 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 ’987 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 '987 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. 7,349,987 (“’987 Patent”)
1002	Prosecution History of U.S. Patent No. 7,349,987
1004	My <i>Curriculum Vitae</i>
1005	U.S. Patent No. 7,010,701 to Bossemeyer et al. (“Bossemeyer”)
1006	U.S. Publication No. 2004/0148290 to Merenda et al. (“Merenda”)
1007	U.S. Patent No. 6,845,448 to Chaganti et al. (“Chaganti”)
1008	U.S. Publication No. 2004/0199765 to Kohane et al. (“Kohane”)
1013	U.S. Patent No. 7,191,252 (Continuation-in-part Application No. 10/155,525)
1014	U.S. Patent No. 7,140,044 (Continuation-in-part Application No. 10/008,209)
1015	U.S. Patent No. 7,146,644 (Continuation-in-part Application No. 10/008,218)
1016	U.S. Patent No. 7,103,915 (Continuation-in-part Application No. 09/916,397)

Exhibit No.	DESCRIPTION
1017	U.S. Provisional Application No. 60/247,242
1018	U.S. Provisional Application No. 60/247,232
1019	U.S. Patent No. 5,960,080 to Fahlman et al. ("Fahlman")
1020	U.S. Patent No. 6,602,298 to Kirshenbaum ("Kirshenbaum")
1021	U.S. Publication No. 2001/0011250 to Paltenghe et al. ("Paltenghe")
1022	U.S. Patent No. 6,473,741 to Baker ("Baker")
1023	U.S. Patent No. 5,982,897 to Clark ("Clark")
1024	OceanStore: An Architecture for Global-Scale Persistent Storage (Nov. 12-15, 2000) ("OceanStore")
1025	U.S. Patent No. 5,933,834 to Aichelen ("Aichelen")
1026	Wylie et al., Survivable Information Storage Systems (Aug. 2000)
1027	U.S. Patent No. 5,956,400 to Chaum et al. ("Chaum")
1028	Microsoft Computer Dictionary, Fourth Edition, Copyright 1999, Excerpts
1029	Beck et al., Linux Kernel Internals, 2nd Ed., Copyright 1998, pp. 148-187
1030	DOD Standard, Department of Defense Trusted Computer System Evaluation Criteria, December 26, 1985 ("Orange Book")
1031	Director of Central Intelligence Directive No. 1/16, Security of Compartmented Computer Operations ("CIA")
1032	Cheswick et al., Firewalls and Internet Security, Copyright 1994, p. 163

30. I understand that the '987 Patent has a filing date of May 23, 2002, claiming priority to applications Nos. 60/247,242 and 60/247,232, both dated November 13, 2000. EX1001 (the '987 Patent), 1; EX1017 (Provisional Application No. 60/247,242); EX1018 (Provisional Application No. 60/247,232). Therefore, I assume that the earliest possible priority date of the '987 Patent is November 13,

2000. I understand that all prior art references used in this declaration predate the earliest possible priority date of the '987 Patent of November 13, 2000. Thus, I have considered certain issues from the perspective of a person of ordinary skill in the art as described below as of November 13, 2000.

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 claims 1, 6, 9-11, 15-16, 21-23, and 27 of the '987 Patent are rendered obvious by the prior art identified below:

Ground	References	Invalid Claim(s)
1	Bossemeyer	1, 6, 9-11, 15-16, 21-23, and 27
2	Bossemeyer, Merenda	1, 6, 9-11, 15-16, 21-23, and 27
3	Bossemeyer, Chaganti	9
4	Bossemeyer, Merenda, Chaganti	9
5	Bossemeyer, Kohane	15 and 27
6	Bossemeyer, Merenda, Kohane	15 and 27

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 November 13, 2000.

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. EX1028 (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. EX1028 (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. EX1028 (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.” EX1028 (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. EX1028 (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. EX1028 (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). EX1028 (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 a few) components do not affect the overall service provided. This principle is called “fault tolerance.” EX1028 (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. EX1028 (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. EX1028 (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. EX1028 (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. EX1028 (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. EX1028 (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. EX1028 (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). EX1029 (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. EX1028 (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.” EX1030 (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. EX1030 (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. EX1031 (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. EX1021 (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”).

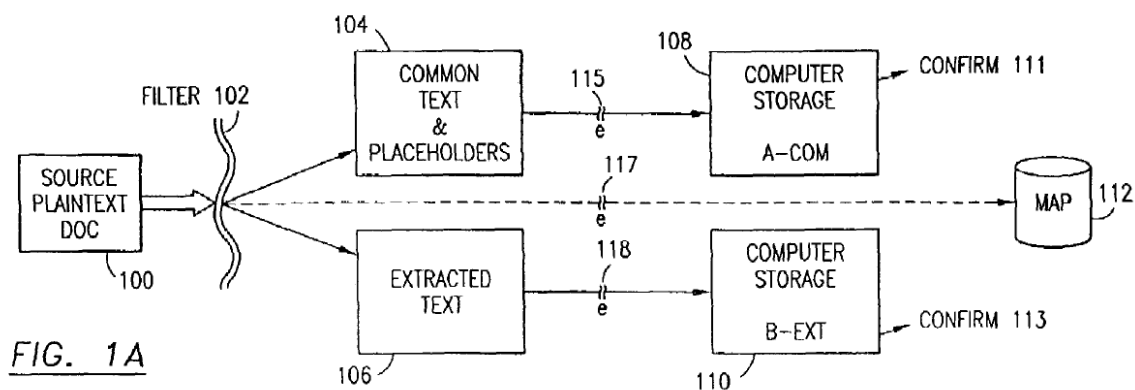
76. Even without having such standards, Unix administrators knew how to leverage much simpler POSIX permission models to effectively create security levels (something I did myself in the 1990s).

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.

VI. Overview Of The '987 Patent

79. The '987 Patent relates to “parsing (typically through a filter), extracting and dispersion of the parsed or segregated data with the controlled reconstruction of data utilizing security protocols to provide a system, method and programming instructions stored on computer readable medium for securing data.” EX1001 (the '987 Patent, 1:14-20). The '987 Patent purports to create a method and storage medium that is used to protect security sensitive words, icons, etc. by parsing data and extracting such security-sensitive information and then controlling access based on a security clearance. EX1001 (the '987 Patent), Abstract. According to the '987 Patent, prior systems did not adequately “limit the distribution and publication of security sensitive words, characters, or icons.” EX1001 (the '987 Patent), 1:33-35. Figure 1A, below, illustrates the disclosed security system:



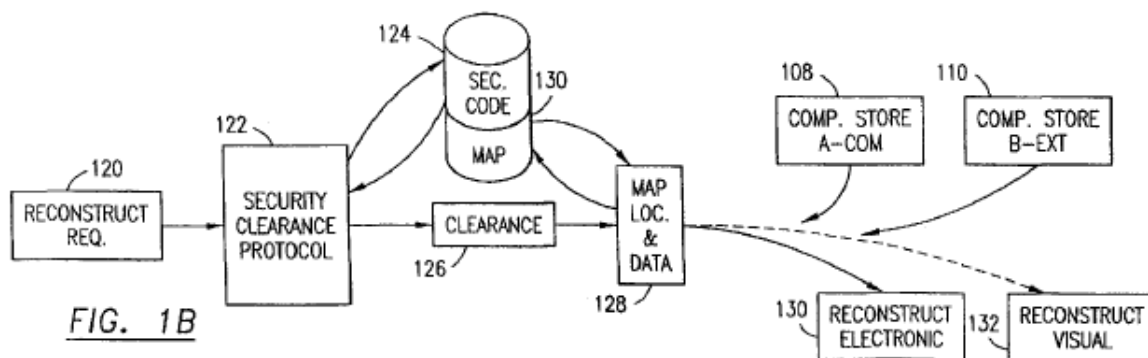
EX1001 (the '987 Patent), Figure 1A.

80. The '987 Patent discloses that the system “splits, cuts and segments (that is, parses)” a source document. EX1001 (the '987 Patent), 39:1-15, Figure 10. In the system shown in Figure 1A, a source document 100 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 '987 Patent), 18:15-17. The uncommon words (or security sensitive words) are placed into a separate extracted text or extracted data file 106, and the common data objects are placed into remainder document or common datafile 104. EX1001 (the '987 Patent), 18:25-31. The remainder and extracted data are stored separately, with the extracted data file 106 stored in a different memory computer storage 110, and the remainder data stored in common storage memory 108. EX1001 (the '987 Patent), 19:14-15, 19:21-23. The '987 Patent explains that the source document “may be preserved with or without encryption, or destroyed as a further data security step.” EX1001 (the '987 Patent), 42:6-8, 9:17-33 (“The original data may be maintained in its original state and stored as is customary, encrypted or destroyed.... Destruction of the original source is also an alternative embodiment.”).

81. The '987 Patent describes that its system is compatible with multiple security levels. EX1001 (the '987 Patent), 20:18-23 (“For security systems having multiple security levels, a plurality of filters would be created, each filter associated with a different security level.”). 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 ’987 Patent), 20:21-27. Having separate storage for extracted data of different security levels is “one of the many important features of the present invention.” EX1001 (the ’987 Patent), 20:28-30.

82. To enable secure storage of the data, the system reconstructs the data or data object that was previously in storage. EX1001 (the ’987 Patent), 8:7-9. Figure 1B, shown below, illustrates the major features of the reconstruction routine/system.



EX1001 (the ’987 Patent), Figure 1B.

83. 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 ’987 Patent), 20:59-64. 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 ’987 Patent), 20:65-21:3. 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 ’987 Patent), 21:3-4. “[M]ap 130 show[s] the location of [extracted and remainder] memory segments.” EX1001 (the ’987 Patent), 21:7-9. 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 ’987 Patent), 21:19-21.

84. The ’987 Patent also describes that the data security system can generate revenue through advertisement or charging users at the data input or reconstruction stage. EX1001 (the ’987 Patent), 45:34-46:34, Figure 13. The ’987 Patent also states that generating advertisement fees and charging fees for securing data were well known. EX1001 (the ’987 Patent), 45:46-49 (“It is well known that vendors selling goods and services over the Internet are willing to pay a certain percentage of their sales revenue to other entities referring customers to the vendor’s web sites.”), 46:11-17 (“[C]harge systems are known.”).

A. Prosecution History of the '987 Patent

85. I have reviewed the file history of the '987 Patent. EX1002 ('987 Prosecution History). I summarize the relevant information that I have reviewed pertaining to my opinion.

86. The '987 Patent was filed as U.S. Ser. No. 10/155,192 on May 23, 2002. EX1002 ('987 Prosecution History), 1, 3.

87. On August 11, 2005, the Examiner rejected all claim 1-27: claims 1-2, 6-12, 16, 17, and 21-27 as being obvious over U.S. Patent Nos. 5,960,080 (EX1019 ("Fahlman")) and 6,602,298 (EX1020 ("Kirshenbaum")); claims 3-5 and 18-20 as being obvious over Fahlman, Kirshenbaum, and U.S. Publication No. 2002/0116644 ("Mastrianni"); claims 13 and 15 as being obvious over Fahlman, Kirshenbaum, and U.S. Patent No. 6,487,538 ("Gupta"); and claim 14 as being obvious over Fahlman, Kirshenbaum, Gupta, and U.S. Patent. No. 6,771,290 ("Hoyle"). EX1002 ('987 Prosecution History), 232-42.

88. Applicant amended the claims, for example as shown in claim 1 below:

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

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

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

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

EX1002 ('987 Prosecution History), 251; *see also id.*, 250-67.

89. On June 1, 2006, the Examiner issued an action maintaining rejections to all claims: claims 1-2, 6-12, 16, 17, and 21-27 as being obvious over Fahlman and Kirshenbaum); claims 3-5 and 18-20 as being obvious over Fahlman, Kirshenbaum, and U.S. Patent No. 6,073,165 ("Narasimhan"); claims 13 and 15 as being obvious over Fahlman, Kirshenbaum, and Gupta; and claim 14 as being obvious over Fahlman, Kirshenbaum, Gupta, and Hoyle. EX1002 ('987 Prosecution History), 277-90. Among other things, the Examiner stated that Fahlman "shows a *method of securing data having one or more security sensitive words, characters or icons in a*

computer system with memories designated as a remainder store and an extract store” and Kirshenbaum “shows that there are multiple stores and the stores maybe [sic] on different locations,” and “[i]t would have been obvious to include the multi-level security feature in Kirshenbaum, because it increases the granularity of security control.” EX1002 ('987 Prosecution History), 280-82.

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

1. (currently amended) A method of securing data having one or more security sensitive words, characters or icons in a computer system with a plurality of <u>physically distinguishable</u> memories respectively designated as a remainder store and a plurality of <u>physically distinct</u> extract stores corresponding to a plurality of security levels for respective subsets of said security sensitive words, characters or icons (~~FIG. 6, store 1, 2 or 3; FIG. 7, step 422~~) comprising: extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data therefrom; storing said extracted data and said remainder data in said respective extract stores corresponding to an associated security level and said remainder store, respectively; and, permitting <u>full or partial</u> reconstruction of said data via said extracted data from respective extract stores and remainder data only in the presence of a predetermined security clearance corresponding to said associated security level for said respective extract stores.

EX1002 ('987 Prosecution History), 297, 371; *see also id.*, 296-18, 369-92.

91. In particular, in a response dated October 17, 2006, Applicant argued that the amended claims cover “various levels of secret data are stored in ‘respective extract stores’ which are physically distinguishable and physically distinct and this is essentially the same as ***multiple levels of security with multiple levels of secure storage.***” EX1002 ('987 Prosecution History), 378. Applicant argued that “Kirshenbaum...and/or Fahlman... do not show, teach or suggest multiple extractions of security sensitive words related to each of a plurality of security levels, and separate storage of those security sensitive words in different, physically distinct secured locations for each security level (‘respective extract stores’), and the requirement that the user input a password (‘security clearance’) for each security level to reconstruct the data from ‘respective extract stores.’” EX1002 ('987 Prosecution History), 378-79.

92. Applicant further contended that Fahlman did not include “a remainder store for non-secured data, multiple security levels, multiple extraction of security data, storage of extract data at multiple levels, nor presentment of corresponding security codes at each security level.” EX1002 ('987 Prosecution History), 381. More specifically, Applicant argued “Fahlman does not seem to store remainder or non-secure data in a separate remainder store location apart from secure data.” EX1002 ('987 Prosecution History), 382. Applicant distinguished the claims,

arguing that the references lacked “multi-level secured data storage, extraction for each security level, and full or partial reconstruction using multiple extract stores.” EX1002 (’987 Prosecution History), 390. On November 15, 2007, the Examiner issued a Notice of Allowance. EX1002 (’987 Prosecution History), 425, 428-30.

93. The ’987 Patent issued on March 25, 2008. EX1001 (the ’987 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 (Bossemeyer)”)

94. 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 ’987 Patent.

95. 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).”).

96. 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.

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

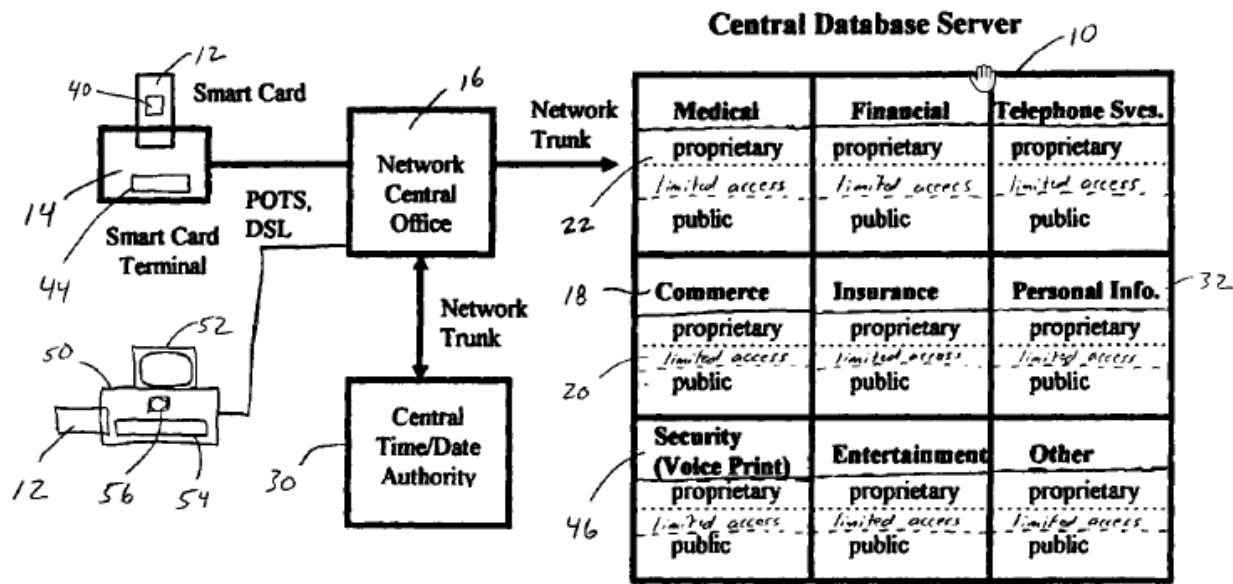


Figure 1

EX1005 (Bossemeyer), Figure 1.

98. 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.

99. 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.”).

100. 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.

101. 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 words, private or proprietary information is controlled by the owner of that

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

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.

102. 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.

103. In Bossemeyer, the information stored in the centralized database server is separated according to at least three distinct security levels: proprietary/restricted, limited access, or public/unrestricted. *See* EX1005 (Bossemeyer), 2:13-24:

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.

104. 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.

105. 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.

106. 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.

107. In addition, Bossemeyer explains that users and merchants use its system based on a subscription service. EX1005 (Bossemeyer), 5:23-31:

Data is stored in the server in several ways. Merchant profiles become populated ***when a merchant subscribes*** to the service. Default profiles

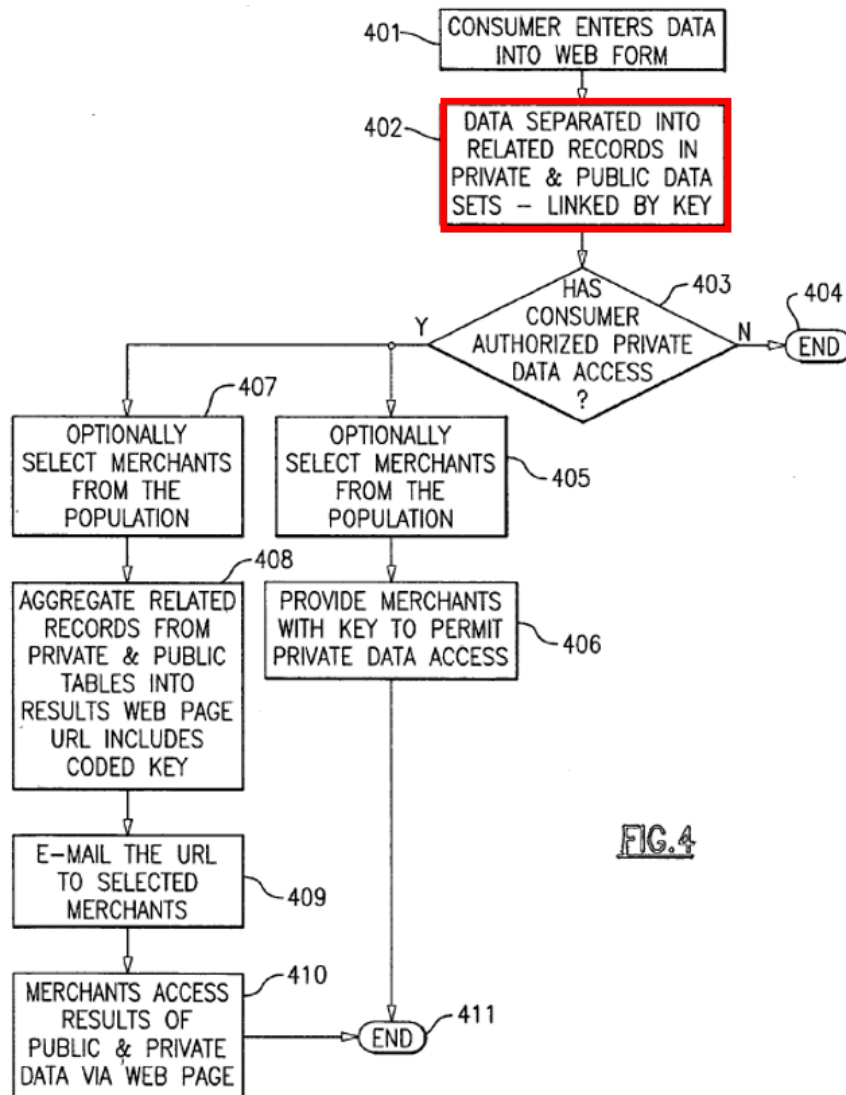
can exist for merchants until a sufficient number of transactions occur through that merchant to provide network use information which may be relevant to the system. Similarly, the user data becomes populated *when the user subscribes* as part of the smart card activation process. Additional data is created as the user and the merchants interact with the system.

B. Merenda (U.S. Publication No. 2004/0148290, “EX1006 (Merenda)”)

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

109. Merenda describes “a method, system and program product for allowing the viewer of a public data set to access related records in a private data set based upon a link which may be selectively provided to the viewer to authorize such access.” EX1006 (Merenda), ¶2. Specifically, Merenda describes that “data entered by a consumer into a Web form is separated into related records in a public and private data set. The public records would be available without restriction for read access by a population of merchants. The private records would be available only per the indication of the consumer to the merchant in the population.” *Id.*, ¶7.

110. For example, Merenda's Figure 4 illustrates that "[i]n step 402 the entered data is separated and inserted as data records in public and private data sets which records are linked by a common key value assigned thereto and which may be stored in the tables as part of the record." EX1006 (Merenda), ¶34, Figure 4:²



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

111. Merenda discloses that “[u]pon entering the data the consumer may be prompted to indicate whether they wish to provide merchants with access to their private data... The consumer may be offered and [sic] opportunity to choose among the population of merchant the select merchant to whom they wish their private data to be provided.” EX1006 (Merenda), ¶8. In addition, “[o]nce selected... the merchants may be provided with a pass code... With the pass code the merchants are provided with the ability to view the particular consumers private data record in the private data set.” *Id.*, ¶9.

112. For example, a user of Merenda’s system (*e.g.*, a merchant), who requests information, can have access only to certain portions of the private information. That is, a merchant can access certain selected private data sets (*e.g.*, private data sets having a first security level, such as ***name, address, phone number, e-mail***), but the merchant cannot access other private data sets (*e.g.*, private data sets having a second (higher) security level, such as ***revenue, credit card***). *See* EX1006 (Merenda), ¶29:

It is useful to note that the present invention contemplates that provision of ***access to the data elements in the private data*** set may be made on an element-by-element basis, that is to say, that ***the merchant may be provided with access to certain select pieces of private data within the single data record 214***, such as the ***contact information (name,***

address, phone number, e-mail) but not to other sensitive data such as revenue, credit card etc..

113. Merenda discloses using parsing to separate data into private and non-private (public) elements. EX1006 (Merenda), ¶23 (“Fundamental to the implementation of the present invention is the notion that a set of data may be *parsed into private and non-private elements.*”). Specifically, Merenda discloses different ways of parsing data from simple techniques to more sophisticated ones. *Id.*:

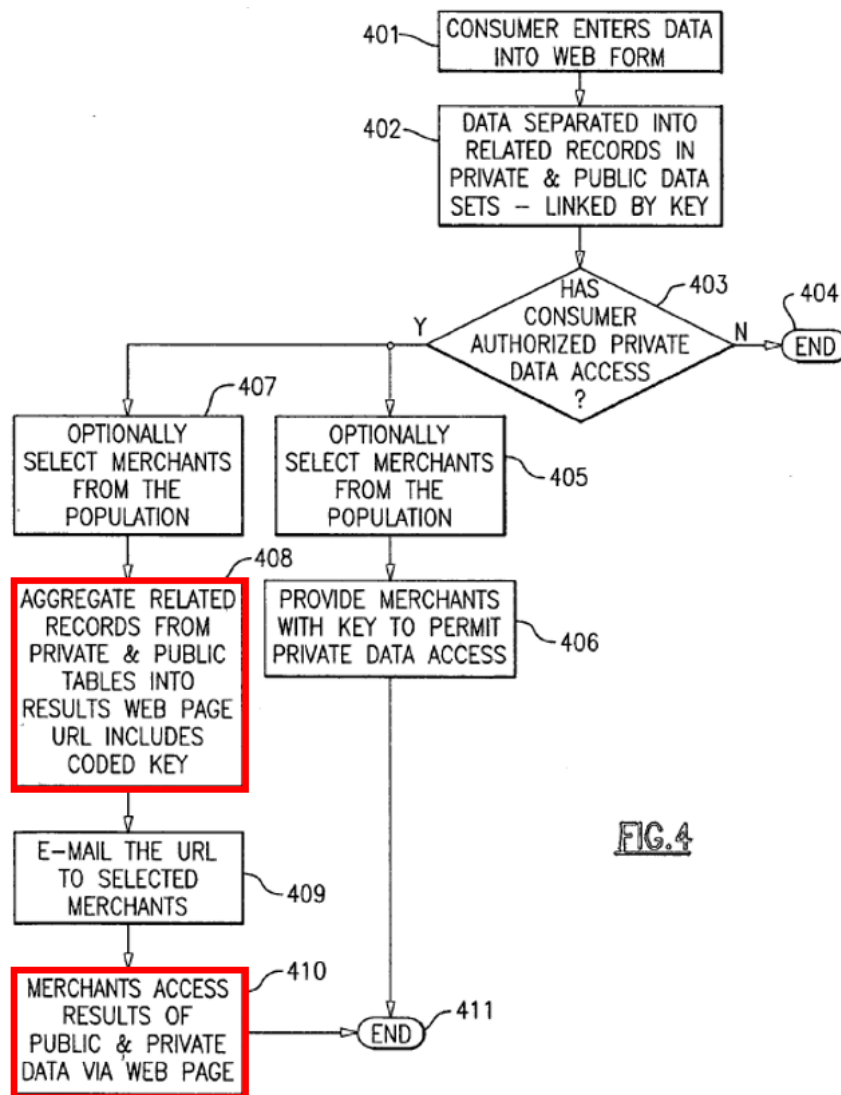
... At the most simplistic level this might entail, for example, identifying input fields on a Web page as requiring sensitive data input such as an address, credit card or social security number, versus non-sensitive information such as the name of the item being purchased, the date, time etc... At a more sophisticated level this notion might entail the combination of otherwise non-sensitive data elements into a combined sensitive data construct.

114. Merenda discloses aggregating information from private and public tables into a Web page and allowing selected merchants access to the aggregated (reconstructed) information. *See* EX1006 (Merenda), ¶36:

The remaining steps in accordance with the embodiment in FIG. 3 are similar: Once again the consumer may optionally select among the population of merchants with access to the public data, certain merchants to whom they wish to grant private data access 407 or access may be granted globally. *Next in step 408 the various tables of data 302a-d which may contain private or public information are*

aggregated into a query result web page having a URL which is coded with an identifier which in a preferred embodiment is the key value 123456789876 used to logically relate the records in the various tables 302a-d. In step 409 those vendors for whom access has been indicated by the consumer in step 407 are provided with an e-mail including a hyperlink to the key-coded URL through which *the merchant may access 410 the results of the combined consumer data*. The process is then ended 411.

115. These steps are illustrated in Merenda's Figure 4:



EX1006 (Merenda), Figure 4.

C. Chaganti (U.S. Patent No. 6,845,448, “EX1007 (Chaganti)”)

116. Chaganti is a U.S. Patent filed on January 7, 2000, and issued on January 18, 2005. I understand that Chaganti is prior art because it is a U.S. Patent that was filed prior to the earliest possible priority date of the '987 Patent.

117. Chaganti is directed to systems for “gathering, storing personal information on a server computer and releasing such information to authorized requesters.” EX1007 (Chaganti), Abstract, 2:23-43, 1:7-10 (“gathering, storing and disbursing personal information to authorized entities via a communication network”). In its background section, Chaganti states that businesses on the Internet “would like to have as much information about the user as possible, so that they could obtain a profile of the type of persons that are interested in their products or services” and that “[i]t would be useful to both the user and the provider if the user can store all his information at a single location and authorize the release of such information to any person or entity.” EX1007 (Chaganti), 1:26-33. Chaganti explains that there was no method where a user could store his information and “selectively authorize it to be distributed to a number of entities.” EX1007 (Chaganti), 1:48-49.

118. In Chaganti, a server computer “preferably includes a trusted computer base (TCB) comprising a secure kernel, which includes the security module 120.” EX1007 (Chaganti), 7:61-63. Chaganti further describes that “[s]everal types of information are stored for release to different entities with appropriate authorization.” EX1007 (Chaganti), Abstract, 2:21-22. As an example, Chaganti describes that a Personal Information Repository Service Provider (PIRSP) implements the features it discloses. *See, e.g.*, EX1007 (Chaganti), 5:29-33

(“Referring to FIG. 2, the steps included in a preferred embodiment of the invented System are described. During an initialization step (step 200), in a preferred embodiment, a Personal Information Repository Service Provider (PIRSP) operated the server computer 100.”). A user can enter his information such as “medical information” and store it in appropriate tables. EX1007 (Chaganti), 8:52-53.

119. Chaganti discloses that that its system allows storing and accessing information, but based on assessing charge fees for users and requesters. *See* EX1007 (Chaganti), 5:43-52:

Preferably, the PIRSP makes it known to a user 103 that it provides a trusted information repository service. In preferred and alternative embodiments, the PIRSP announces that its services are available free, or for a fee, and in the latter case, *the fee is calculated based on a per transaction basis, or on a subscription basis*, either from users that store information or from entities that request such information. Other embodiments comprise direct or vicarious payment methods for utilizing the services provided by the PIRSP.

120. Chaganti describes optional payment plans for rendering services. *See* EX1007 (Chaganti), 9:1-5:

The user account management module 112 optionally allows the user 103 to select *a payment plan for the services rendered by the PIRSP*, block any request if the user 103 is in default of a payment, obtain credit card or other verification, and the like.

121. Chaganti describes implementing payment plans for charging fees to requesters who seek to access the data in its system. EX1007 (Chaganti), 10:30-42:

In a preferred embodiment, potential requesters are also enrolled by the PIRSP in a similar manner as described for the user 103 (step 214). The server computer 100 establishes accounts for *potential requesters*, allocates identifiers, authenticates their trustworthiness and enables them to *establish a payment/billing plan for accessing information objects stored by the user 103*. In one embodiment, where there are a number of users, statistical information, rather than individual pieces of information objects is offered for sale to potential requesters. In other embodiments, the potential requesters do not establish accounts with the PIRSP, and will pay as they go for each access of information as described below.

122. Chaganti discloses details of exemplary charging models as well protection of information being sold: by accessed object, by subscription, or statistical. See EX1007 (Chaganti), 12:42-67:

Preferably, the requester 105 is forbidden from reselling or retransmitting the information, or using it beyond an expiration date set either by the user 103 or by the PIRSP. Preferably, to ensure this, *information objects are copyrighted or otherwise contractually protected*. Further, this could be a selling point to users, since the PIRSP not only guarantees the safety of the stored information, but in addition controls how this information is used.

In one embodiment, *the requester 105 is charged a fee for receiving the information objects, on a per-object basis, or on a subscription basis or for receiving statistical reports.* The PIRSP may provide an incentive to the user 103 by paying a portion of the fee to the user 103. In another embodiment, a requester may receive statistical report such as “how many male golf players between the ages 22 and 55 in the zip code 20006 are interested in trading stocks?” The statistics module 140 and report generation module 150 make appropriate queries in the database 108 and obtain the information. Preferably such statistical information is considered secure, unless it has a tendency to reveal too much about the private habits of the user 103. Thus, so long as information is aggregated and can remain anonymous, it will be released to potential requesters to assist marketing of products/services.

123. Chaganti illustrates examples for assessing charge fees in Figures 2a and 2b:

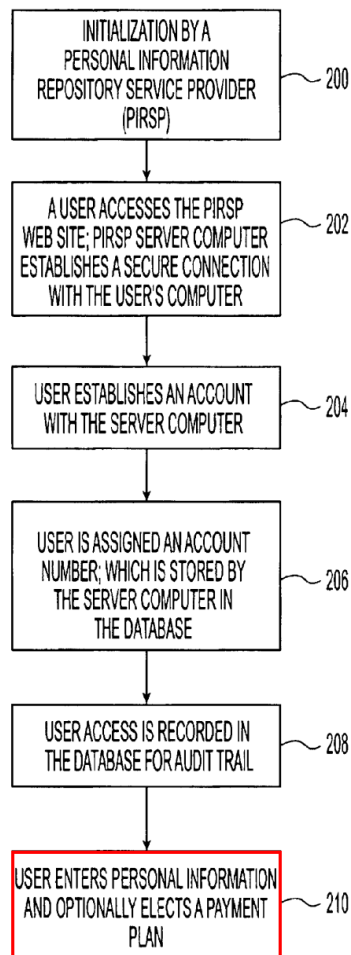


Fig. 2a

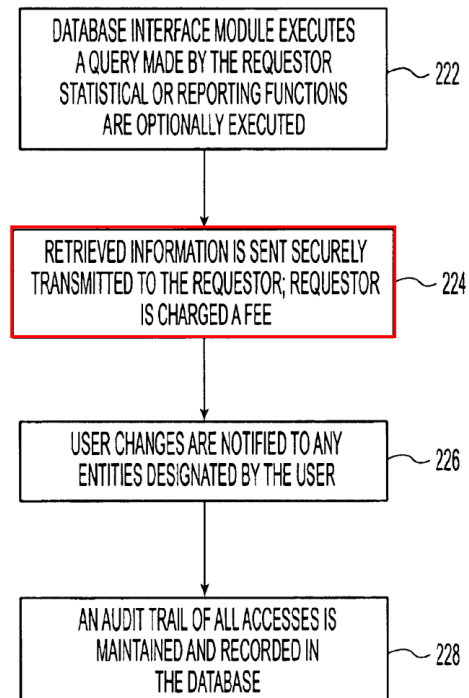


Fig. 2b

EX1007 (Chaganti), Figures 2a and 2b.

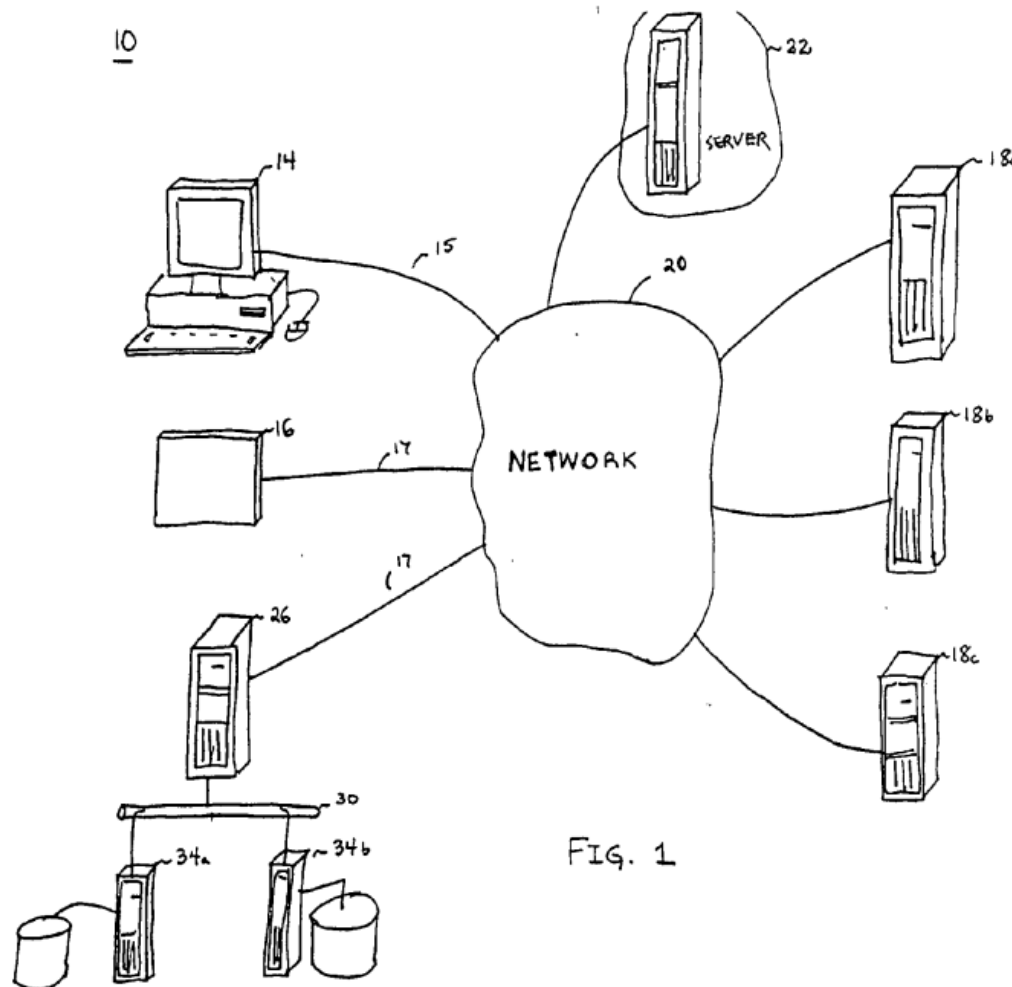
D. Kohane (U.S. Publication No. 2004/0199765, “EX1008 (Kohane)”)

124. U.S. Publication No. 2004/0199765 (EX1008, “Kohane”) filed on December 22, 2003, is a continuation application of U.S. Ser. No. 09/410,717, filed on October 1, 1999, and claims priority to Provisional Application No. 60/150,154,

filed on August 20, 1999. Kohane was published on October 7, 2004, and is prior art under at least 35 U.S.C. §102(e).

125. Kohane is directed to systems and methods for providing “adequate confidentiality of the confidential records, mobility of individual access to the records, security of the data in the records, individual control of the confidential records, and integration with institutional information systems.” EX1008 (Kohane), Abstract, ¶5. Kohane discloses that the “confidential record is encrypted and stored by the gateway system on the selected record server.” EX1008 (Kohane), Abstract. Records can be electronic medical, financial, and legal records. *See* EX1008 (Kohane), ¶¶3 (“[I]n an age of increased deployment of electronic medical records, the patient still has little access to their own complete record.”), 5 (“Examples of confidential records are medical records and financial records. Other types of confidential records are within the scope of the invention.”), 37 (“[T]he record can be a medical record pertaining to a particular patient (the record owner) produced by a health care institution (the record author). [T]he record can include other types of personal or confidential information, such as financial data, legal data, etc. The record can include a mixture of information types, such as a medical history combined with legal information.”). Kohane further describes that its computer system has a “record system 10 including client systems ([i.e.,] agent systems) in communication with servers 18a, 18b, 18c (collectively, server 18) through a

gateway server system 22 over a network 20.” EX1008 (Kohane), ¶23. Kohane explains that access to the confidential information can be allowed by tokens such as a “smart card,” where the agent systems can be “smart-card based.” EX1008 (Kohane), ¶¶7, 26, 30, 61. Kohane illustrates its system in Figure 1:



EX1008 (Kohane), Figure 1.

126. Kohane discloses that the agent systems 14, 15, 26 include devices such as a personal computer, workstation, smart card reader, a medical instrument, etc.,

and that the “agent can be the record owner, a member of an institution (*e.g.*, health care institution), university, research facility, financial institution, legal profession, the general public, or, government employee, etc.”). EX1008 (Kohane), ¶¶24-30, 32, Abstract. Kohane explains that, using the agent systems, the record owner connects to the gateway server system to store “record objects corresponding to the record of the record owner” on the system servers. *See* EX1008 (Kohane), ¶23:

FIG. 1 shows a record system 10 including client systems 14, 16, 26 (hereafter ***agent systems***) in communication with servers 18*a*, 18*b*, 18*c* (collectively, ***server 18***) through a ***gateway server system 22*** over a network 20. This network 20 can be a large international network (*e.g.*, the Internet, the World Wide Web, or Wide Area Network (WAN)) or a small local area network (LAN).

See also EX1008 (Kohane), ¶41:

Record objects, like the directory file representing the record, ***are stored on the servers 18***. Each record object is individually addressable through a unique URL. Also, each record object can include other record objects. Each server 18 can hold all or a portion of the record objects corresponding to the record of the record owner. For example, the complete record can reside on server 18*a*.

127. Moreover, Kohane explains that “the confidentiality of the information stored in the records is of utmost importance.” EX1008 (Kohane), ¶57. Kohane

discloses that “[b]efore transmitting the record objects to the servers 18, the gateway server system 22 encrypts the record objects.” EX1008 (Kohane), ¶58:

The gateway server system 22 stores the record objects on the servers 18. Before transmitting the record objects to the servers 18, the gateway server system 22 encrypts the record objects. Thus, such record objects traverse the network 20 in encrypted form when the gateway server system 22 uploads the record objects to the server 18. The servers 18 store the record objects in this encrypted form. In addition, the record objects traverse the network 20 in this encrypted form when subsequently downloaded by the gateway server system 22. ***Consequently, the information in the record objects remain unintelligible to anyone who intercepts the transmission of the record objects between the gateway server system 22 and the server 18 and does not possess the appropriate decryption key.***

128. Further, Kohane discloses that record objects that are stored in the gateway server system 22 remain in encrypted form. EX1008 (Kohane), ¶59:

On the gateway server system 22, each record objects remains in encrypted form except for those record objects that the authorized agent is privileged to access. Accordingly, not every record object may be decrypted, only those record objects for which the accessing agent retains a privilege. The gateway server system 22 possesses and uses the appropriate key to decrypt the record objects obtained from the servers 18. The gateway server system 22 decrypts those record objects for subsequent transmission to the accessing agent.

129. In Kohane's system, the gateway server system 22 can also send (encrypted) record objects to the agent systems. EX1008 (Kohane), ¶60:

Before sending the record objects over the communication links (e.g., 15) to the agent system 14, the gateway server system 22 encrypts such record objects. A commercially available security protocol that the gateway server system 22 can use to encrypt the record objects is SSL (Secure Sockets Layer). During a typical SSL session, the Web browser of the agent system 14 sends its public key to the gateway server system 22 so that the gateway server system 22 can securely return a secret key to the browser. The Web browser and gateway server system 22 then communicate using encryption with the secret key during that SSL session. This same security protocol can operate between the gateway server system 22 and the servers 18.

130. Kohane discloses that the record objects in the agent systems 14, 16, 26 are deleted after being reviewed by those systems to further enhance data security. EX1008 (Kohane), ¶63:

Data security can be enhanced at the agent systems 14, 16, 26 by not storing any record objects at the agent systems 14, 16, 26. Accordingly, after the agent completes reviewing the record object, the agent system 14, 16, 26 *deletes the corresponding information* from the respective agent system, including all downloaded files and cached copies of the downloaded Web page. To secure information transmitted by the agent systems 14, 16, 26 to the gateway server system 22, such information

is transmitted over the network 20 in encrypted form, for example, by using SSL.

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 ’987 Patent as of its earliest possible priority date of November 13, 2000, 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 ’987 Patent.

IX. Claim Construction

133. I have reviewed the claims, specification, and file history of the ’987 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

A. Ground 1: Claims 1, 6, 9, 10-11, 15-16, 21-23, And 27 Are Obvious Over Bossemeyer

1. Independent Claims 1, 10, 16, and 22

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

135. To the extent that the preamble is limiting, Bossemeyer discloses or renders obvious the preambles of independent claims 1, 10, 16, and 22, as explained below.

a. [1pre-i] A method of securing **data** having one or more security sensitive words, characters or icons in a computer system³

136. Bossemeyer discloses and, alternatively, Bossemeyer renders obvious this limitation.

137. Bossemeyer discloses a method of securing **data**. Specifically, Bossemeyer discloses securing information (*e.g.*, user data) by separating sensitive data to control how the data is transferred. *See* EX1005 (Bossemeyer), 2:28-36:

Private or proprietary information is *partitioned* such that *the owner of the **information** has control over how the **information** is transferred*

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.

and used. Thus, for example, medical information 22 provided to a health professional may be considered private and *only available by way of special authorization from the owner of the information.* In this way, *the owner of the information contained within the central database server has control over how the information is transferred and used.*

138. A POSITA would have understood that here, “information” is data. EX1028 (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.”).

139. Bossemeyer further discloses securing information by restricting access to 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.

140. Figures 1 and 3 also illustrate Bossemeyer’s *data* access restrictions:

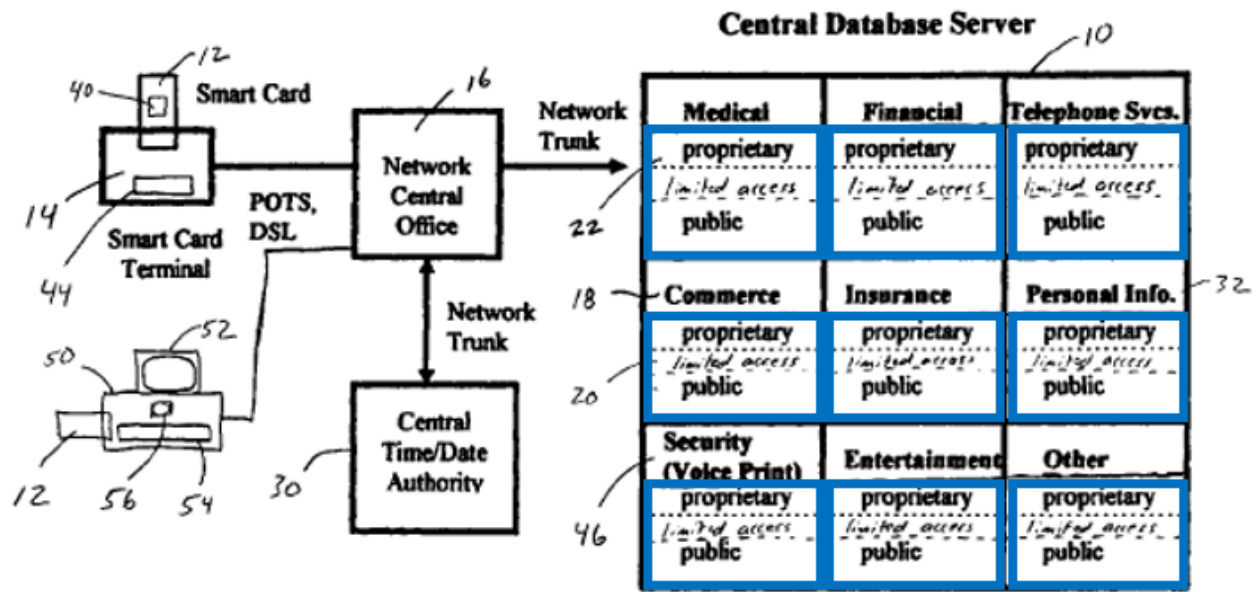


Figure 1

EX1005 (Bossemeyer), Figure 1.

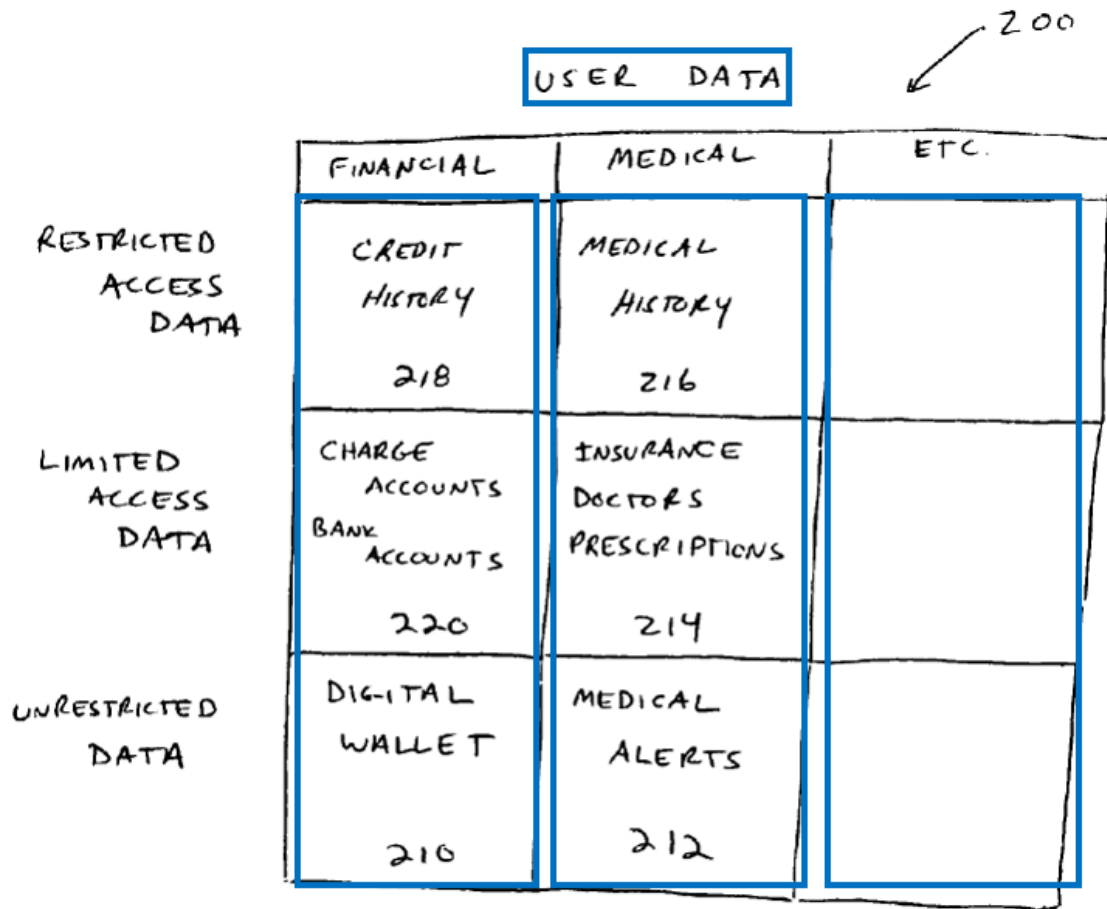


FIG. 3

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, or icons, 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

'987 Patent discusses the privacy of credit history, medical history, business trade secrets, and financial data (EX1001 (the '987 Patent), 1:35-38).

142. A POSITA would have understood that 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, or icons” under the meaning of this limitation.

143. 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.”); EX1006 (Merenda), ¶23 (“[F]or example, identifying input fields on a Web page... require[es] sensitive data input such as an address, credit card or social security number....”); EX1008 (Kohane), ¶5 (“[T]o maintain adequate confidentiality of the confidential records, [] security of the confidential records, control of the confidential records by the

individual... Examples of confidential records are medical records and financial records. Other types of confidential records are within the scope of the invention.”).

144. A POSITA would have found it obvious that Bossemeyer discloses other types of security sensitive words, characters, 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.

145. Bossemeyer discloses that its method is performed in a computer system. Specifically, 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.”). Thus, Bossemeyer’s network arrangement for securing data is implemented over an interconnected network of computers, *i.e.*, a computer system having a plurality of computers.

146. In sum, Bossemeyer discloses and/or renders obvious a method of securing data (“**information**”) by securing security sensitive content (*e.g.*, “*limited access information*” and/or “*proprietary information*”) that has one or more security sensitive words, characters or icons in a computer system.

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

147. Bossemeyer discloses and, alternatively, Bossemeyer renders obvious this limitation as explained below in addition to the reasons discussed in Section X.A.1.i.a (above).

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

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

150. As discussed in Section X.A.1.i.a (above), *limited access information* and/or *proprietary information* includes security sensitive content, such as, words, characters, or icons. For example, Figure 1 of Bossemeyer shows *medical information 22* stored in central database 10 as proprietary information. See EX1005 (Bossemeyer), Figure 1:

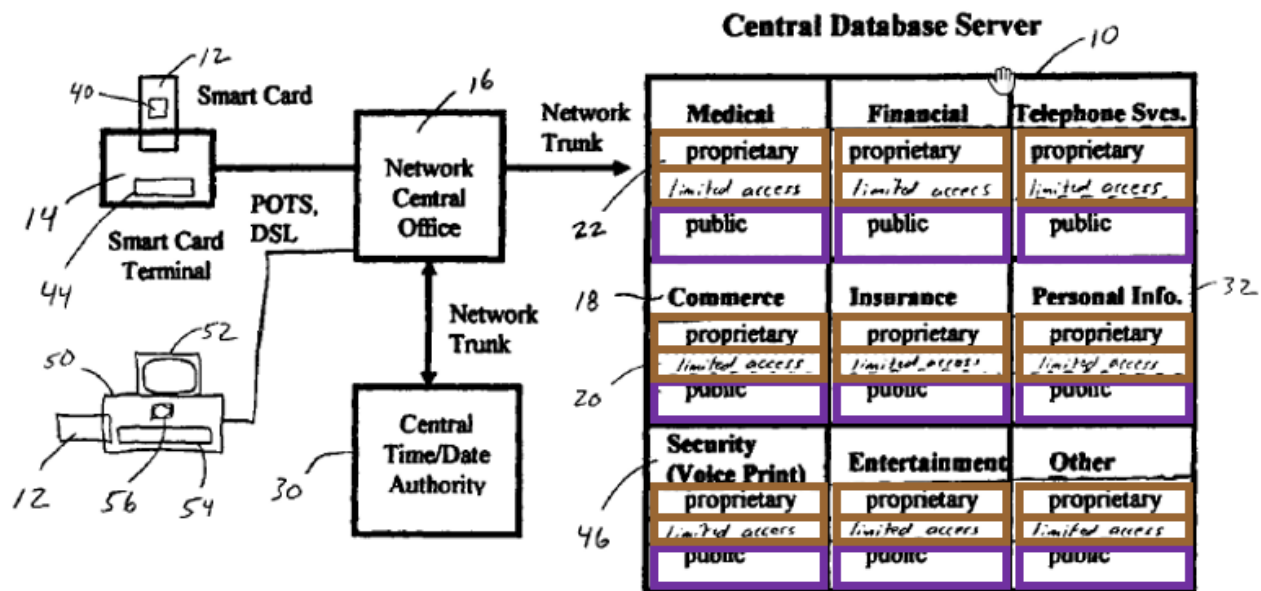


Figure 1

151. Bossemeyer describes examples of protection for such medical information. See EX1005 (Bossemeyer), 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.

152. Figure 3 of Bossemeyer provides another example of separating (e.g., extracting) *user data* into *extracted data* and *remainder data*. See EX1005 (Bossemeyer), Figure 3:

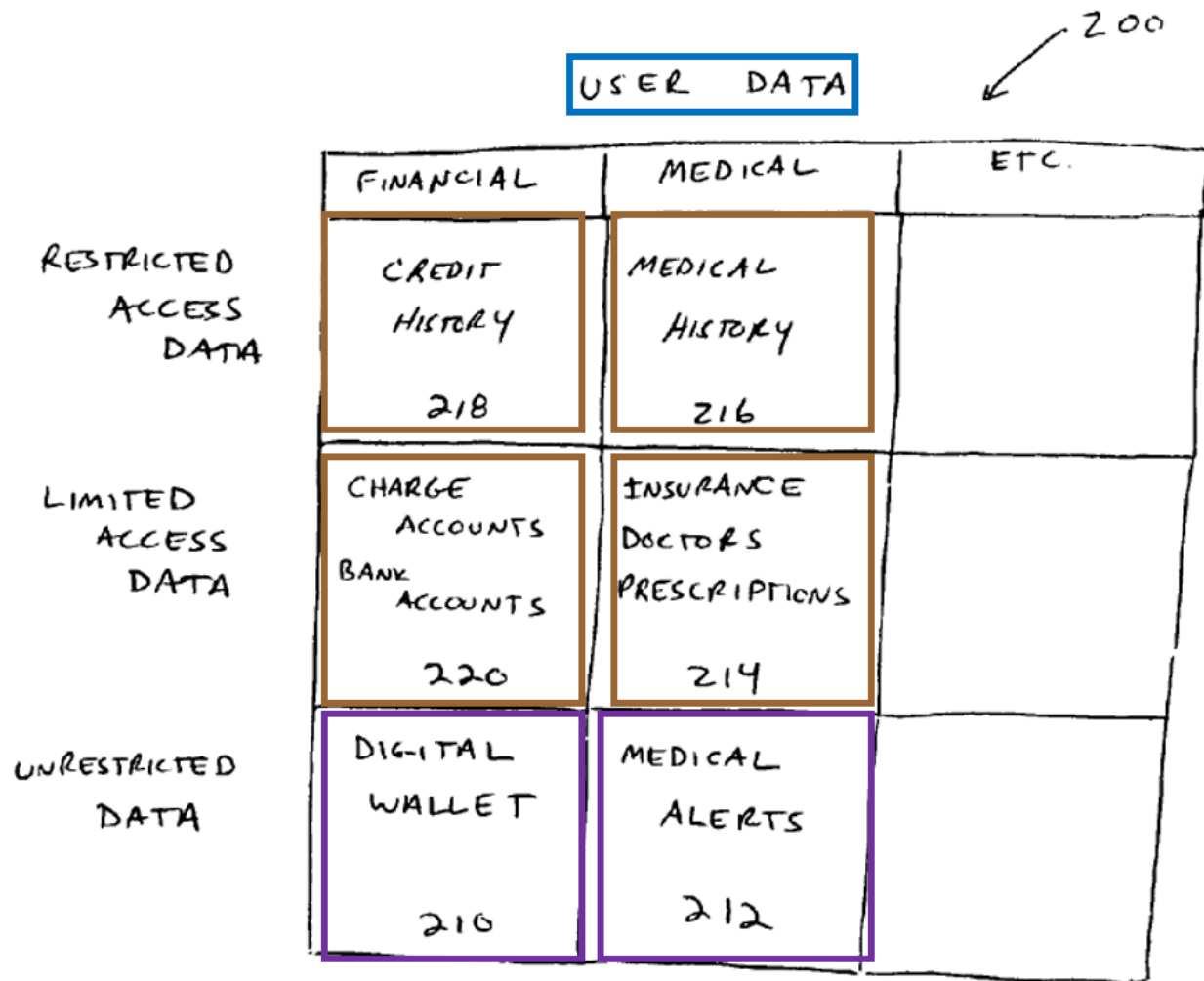


FIG. 3

153. In this figure, for example, a pharmacist would have access to the *user's digital wallet, medical alerts* (remainder data), and *insurance and prescription information* (extracted data). 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*.

154. Bossemeyer further discloses another example where a grocer has access to a user's *digital wallet* (remainder data) and *medical alerts* (remainder data), but not to any of the *other information, such as credit history or medical history* (extracted data). EX1005 (Bossemeyer), 5:16-19:

Similarly, 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*.

155. Another example Bossemeyer discloses is a loan officer at a bank or an automotive dealership that would have access to additional information compared to the grocer; such a person would also have access to the user's *credit history* (extracted data) and the user's *financial account balances* (extracted data). EX1005 (Bossemeyer), 5:20-22:

In contrast, a loan officer at a bank or automotive dealership would be allowed to access to the user's *credit history 218* as well as the user's *financial account balances 220*.

156. To the extent that Patent Owner argues that Bossemeyer does not explicitly disclose “extracting data,” a POSITA would have understood that when Bossemeyer’s “central database server partitions [user] information... in terms of... the accessibility of the information” (EX1005 (Bossemeyer), 2:17-20), Bossemeyer’s method would filter and extract the secure sensitive information, (*e.g.*, restricted- and/or limited-data), from the received user data, (*e.g.*, from a user data file), to store the restricted- and/or limited-data in the proper security-level store, and store the remaining information in the user data file as unrestricted data, (*e.g.*, public data).

157. For example, a POSITA would have understood that Bossemeyer’s method parses received information into private and non-private elements. *See e.g.*, EX1006 (Merenda), ¶7. (“[A] set of data may be parsed into private and non-private elements.”). *See also* EX1028 (Microsoft Dictionary), p. 333 (“**parse** *vb.* To break input into smaller chunks so that a program can act upon the information.”).

158. To illustrate, when Bossemeyer’s central database server receives a *user’s medical data file*, as shown in Bossemeyer’s Figure 3 below, Bossemeyer’s method separates (*e.g.*, extracts) the *user’s medical history information 216*, and

insurance, doctors, prescriptions information 214, and stores them into respective extract stores corresponding to the proper respective security level. As discussed in Section X.A.1.i.a (above), a POSITA would have understood that medical history information can include images of medical charts, insurance information can include icons of the user's insurance card, prescription information can include the names of the drugs prescribed to the user, etc. *See* EX1005 (Bossemeyer), Figure 3:

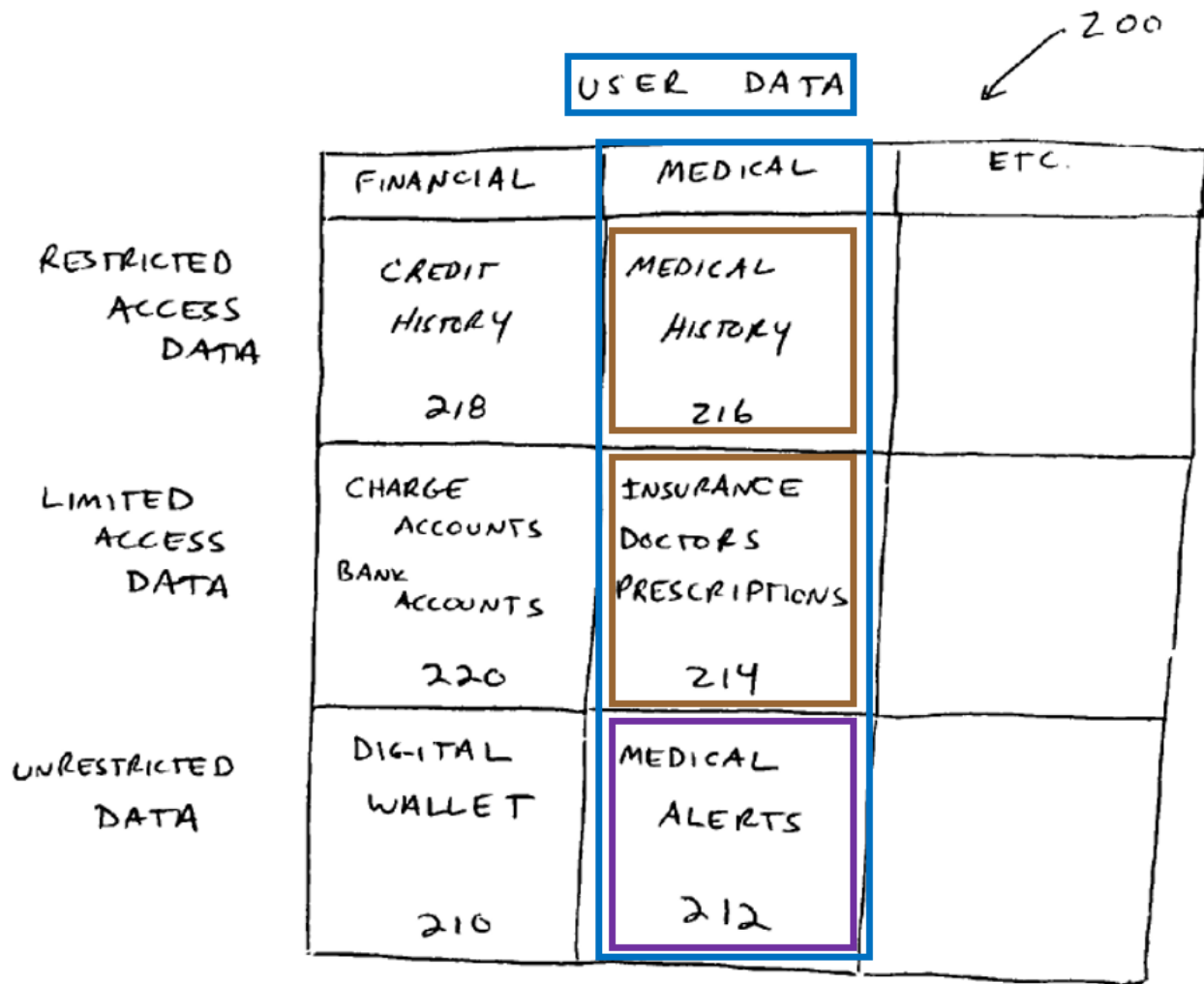


FIG. 3

159. A POSITA would have also understood that Bossemeyer's separation of user data utilized a parsing algorithm because Bossemeyer's method would filter and split the sensitive information, (e.g., restricted- and/or limited-data), from the received user data, (e.g., from a user data file), and store the restricted- and/or

limited-data in the appropriate security-level store, while storing the remaining information in the user data file as unrestricted data, (*e.g.*, public data).

160. For example, A POSITA would have understood that Bossemeyer teaches that its method parses received information into private (restricted, limited access data) and non-private (unrestricted data) elements because the information is split and separated by different categories and levels of security at different servers. *See e.g.*, 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).

161. A POSITA would have understood that Bossemeyer discloses keeping different security information stored in different locations and/or managed by different entities, because that would have decreased the surety risk (*i.e.*, if one server is broken into, the information that may be stolen is limited to just that server). *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 such cases, the central database server 10 acts as a network smart card server which facilitates data transfer between the database containing the desired information and the merchant or person requesting the information. In the same way, *insurance information would ultimately reside with the insurer, medical records with the health provider, financial records with the bank or broker, and so on.*

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

See also EX1005 (Bossemeyer), Figures 1, 3; EX1006 (Merenda), ¶7 (“[A] set of data may be parsed into private and non-private elements.”).

162. In fact, the '987 Patent describes the process to split and separate information as in Bossemeyer to be “parsing.” For example, the '987 Patent states that “parsing occurs with the filtering of the plain text source document 100 and the subsequent storage of extracted data apart from remainder data.” EX1001 (the '987 Patent), 19:11-13. The '987 Patent also describes that:

The parsing algorithm, as stated earlier, targets the plaintext document or data object 100 and *splits, cuts and segments (that is, parses)* the document by bit count, word, word count, page, line count, paragraph count, any identifiable document or icon characteristic, or other identifiable feature Such as capital letters, italics, underline, etc.

EX1001 (the '987 Patent), 39:8-13.

163. Such parsing algorithms were well known in the art. *See, e.g.*, EX1006 (Merenda), ¶7 (“[A] set of data may be parsed into private and non-private elements.”); EX1026 (Wylie), 64 (“Secret-sharing schemes can be thought of as a combination of splitting and replication techniques.”); EX1027 (Chaum), 3:33-36 (“Each new patient medical record entered by a physician into his terminal is split into two fragments: a fragment containing only medical information, and a fragment containing only patient identifying information.”).

164. In sum, Bossemeyer discloses and/or renders obvious a method of securing data (“**information**”) by parsing security sensitive content (*e.g.*, “**user’s medical history information 216**,” and “**insurance, doctors, prescriptions information 214**”) and unrestricted data (*e.g.*, “**medical alerts 212**”) based on a parsing algorithm that separates information by category (medical, financial, etc.) as well as level of security in a computer system (“network arrangement”).

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

165. Bossemeyer renders obvious this limitation as explained below in addition to the reasons discussed in Section X.A.1.i.a (above).

166. As discussed in Section X.A.1.i.a (above), Bossemeyer discloses a method for “securing data having one or more security sensitive words, characters

or icons” in a computer system. Bossemeyer’s network arrangement for securing data is implemented over an interconnected network of computers, *i.e.*, a computer system for performing Bossemeyer’s method. A POSITA would have understood that Bossemeyer’s method would have been implemented using programming instructions and that these programming instructions would be stored in a “computer readable storage medium.” Bossemeyer’s computer system would execute programming instructions, which requires storage (*i.e.*, in a “storage medium”). To implement its computerized method, Bossemeyer’s computer system would read the programming instructions from the storage medium and execute them, for example, in an execution unit. *See also* Section V.A above.

167. For example, Bossemeyer states that 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” (EX1005 (Bossemeyer), 2:13-16) and that the “network smart card server acts as a secured gatekeeper of such information and the smart card acts as the enabling key” (EX1005 (Bossemeyer), 3:16-18). Bossemeyer also disclose that “[s]mart card 12 is formed of plastic or other suitable material and contains circuitry 40 which includes ***a micro-processor and memory including random access memory (RAM) and read only memory (ROM).***” (EX1005 (Bossemeyer), 3:28-31)). *See also* EX1005 (Bossemeyer), 3:39-43 (“Smart card terminal 14 is capable of reading information

contained within the memory 40 of the smart card and is also capable of writing information to the smart card memory to update various records thereon.”), 3:56-6:6 (“Routing circuitry controlled by the *microprocessor* within the central database server 10 routes.... 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.”).

168. In sum, Bossemeyer renders obvious a computer readable storage medium encoded with programming instructions (required for “**networked computers**”) for securing data (“**information**”) having one or more security sensitive words, characters or icons in a computer system (“**networked computers**”).

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

169. Bossemeyer renders obvious this limitation for the reasons discussed in Sections X.A.1.i.a, X.A.1.i.b, and X.A.1.i.c (above).

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

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

170. Bossemeyer discloses and, alternatively, Bossemeyer renders obvious these limitations, as explained below in addition to the reasons discussed in Sections X.A.1.i.a and X.A.1.i.b (above).

171. As an initial matter, a POSITA would not have found any meaningful difference between “physically distinguishable” and “physically distinct” in these claims.

172. Bossemeyer discloses that its computer system has a plurality of physically distinguishable memories for storing various sensitive information (in **distinct extract stores**) and public information (in a **remainder store**). Specifically, Bossemeyer explains that subsets of sensitive information are stored respectively in a plurality of physically distinct memories by application “category (medical, financial, etc.) as well as level of security (unrestricted, or public limited access, restricted).” *See, e.g.,* 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).*

173. Bossemeyer provides several examples. For instance, Bossemeyer describes storing different types of sensitive information at separate memory locations (distinct **extract stores**) based on their respective categories (e.g., limited-access and/or restricted information for medical, financial, telephone services, commerce, insurance, personal info, security, entertainment, etc., as shown in Figure 1; and restricted data such as credit history 218, medical history 216, and limited-access data for bank accounts, insurance, etc., as shown in Figure 3). See, e.g., EX1005 (Bossemeyer), Figures 1, 3.

174. Bossemeyer also describes storing different types of public information at memory locations (**remainder store**) separate from the **extract stores** (e.g., public data for medical, financial, telephone services, commerce, insurance, personal info, security, entertainment, etc., as shown in Figure 1; and unrestricted data such as digital wallet 210, medical alerts 212, etc. as shown in Figure 3). See, e.g., EX1005 (Bossemeyer), Figures 1, 3. The separate storage locations in Bossemeyer lead to security access controls 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.

175. The above examples are illustrated in Figures 1 and 3 below:

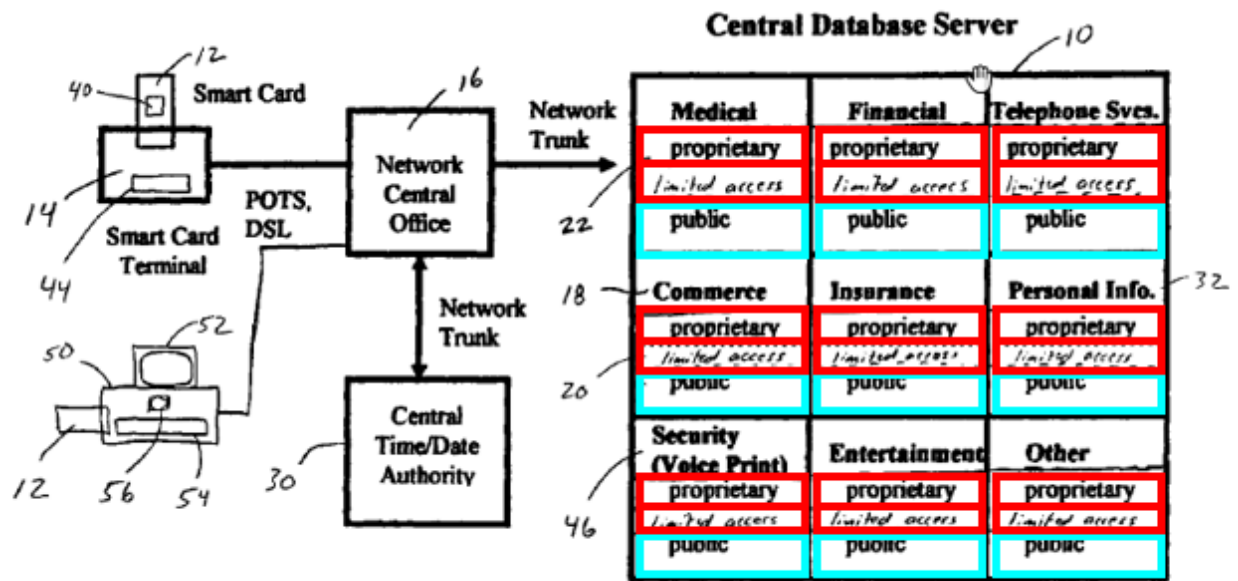


Figure 1

EX1005 (Bossemeyer), Figure 1.

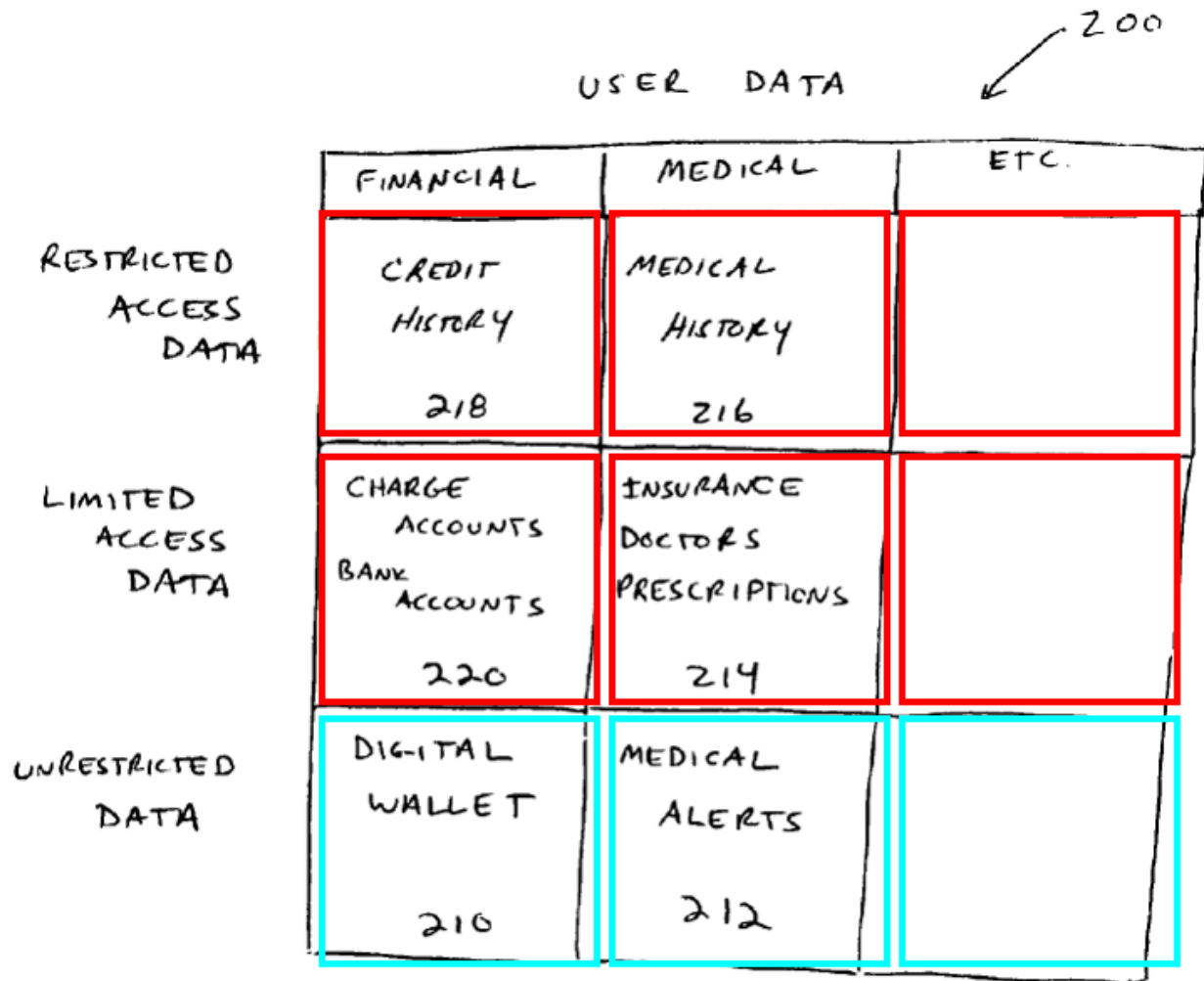


FIG. 3

EX1005 (Bossemeyer), Figure 3.

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

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

177. Bossemeyer’s computer system has a plurality of *physically distinct exact stores*. Specifically, Bossemeyer discloses that distinct servers at physically different locations collectively make up the central database server, and that a server in a particular location (e.g., remote location) can store sensitive information. For example, Bossemeyer explains:

Although the *central database server 10* is shown as a single server, *it is to be understood that multiple servers may comprise the central database server 10*. For example, in the merchant transaction discussed above, the *purchaser’s credit files* are more likely to be stored *in a database monitored by the credit reporting companies* such as *TransUnion* or *Equifax*, as opposed to the central database server 10. In such cases, the central database server 10 acts as a network smart card server which facilitates data transfer between the database containing the desired information and the merchant or person requesting the information. In the same way, *insurance information* would ultimately reside with the *insurer*, *medical records* with the *health provider*, *financial records* with the *bank or broker*, and so on. The network smart card server acts as a secured gatekeeper to such information and the smart card acts as the enabling key.

EX1005 (Bossemeyer), 3:3-18.

178. A POSITA would have understood in this example that the different entities (*e.g.*, credit reporting company, insurer, health provider, and bank or broker) would each control their own operations and hence store their secure information in physically distinct locations—not merely logically distinct ones. This is not just because these types of entities tend to be very different organizations from each other, but also because storing data in physically distinct location improves security considerably (*e.g.*, the compromise of secure information in one location does not implicate information in other locations).

179. Moreover, in the above example, a POSITA would have understood that the public information (*e.g.*, unrestricted data such as digital wallet 210 and medical alerts 212 in Figure 3) is stored in the central database server 10, in a way that the public information is physically separate from the extract stores, so as to be accessible by various applications (*e.g.*, credit card, bank applications). A POSITA would have understood that requested information is retrieved from databases at different locations depending on the application at issue. *See, e.g.*, EX1005 (Bossemeyer), 3:66-4:3 (“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.”). A POSITA would have further understood that

physically separating the public vs. secure information would have also enabled easier management of said data: secure data would be subject to stricter controls whereas public data made more easily accessible.

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

181. Based on Bossemeyer’s disclosure, a POSITA would have understood that each respective sensitive information is a subset of the entire sensitive information and is stored with its data owner. A POSITA would have also

understood that the subsets would have different security levels. For example, the health provider's *extract store* would save "medical history" with "*restricted access*" and the insurer's *extract store* would store "insurance" information with "*limited access*." EX1005 (Bossemeyer), Figure 3 (shown below). The "medical history" and "insurance" information are subsets of the secured information having sensitive words, characters, or icons.

182. A POSITA would have further understood that storing information of different security levels in different physical locations would have further improved security and eased the management of each time of data for two reasons. First, data requiring higher levels of security usually demands stronger access controls, which are often more complicated to use (e.g., a simple password is far easier to setup and use than, say, a biometric method such as a retinal eye scan). Second, compartmentalizing data of different security levels mitigates the possible damage that could be done if any one location is compromised.

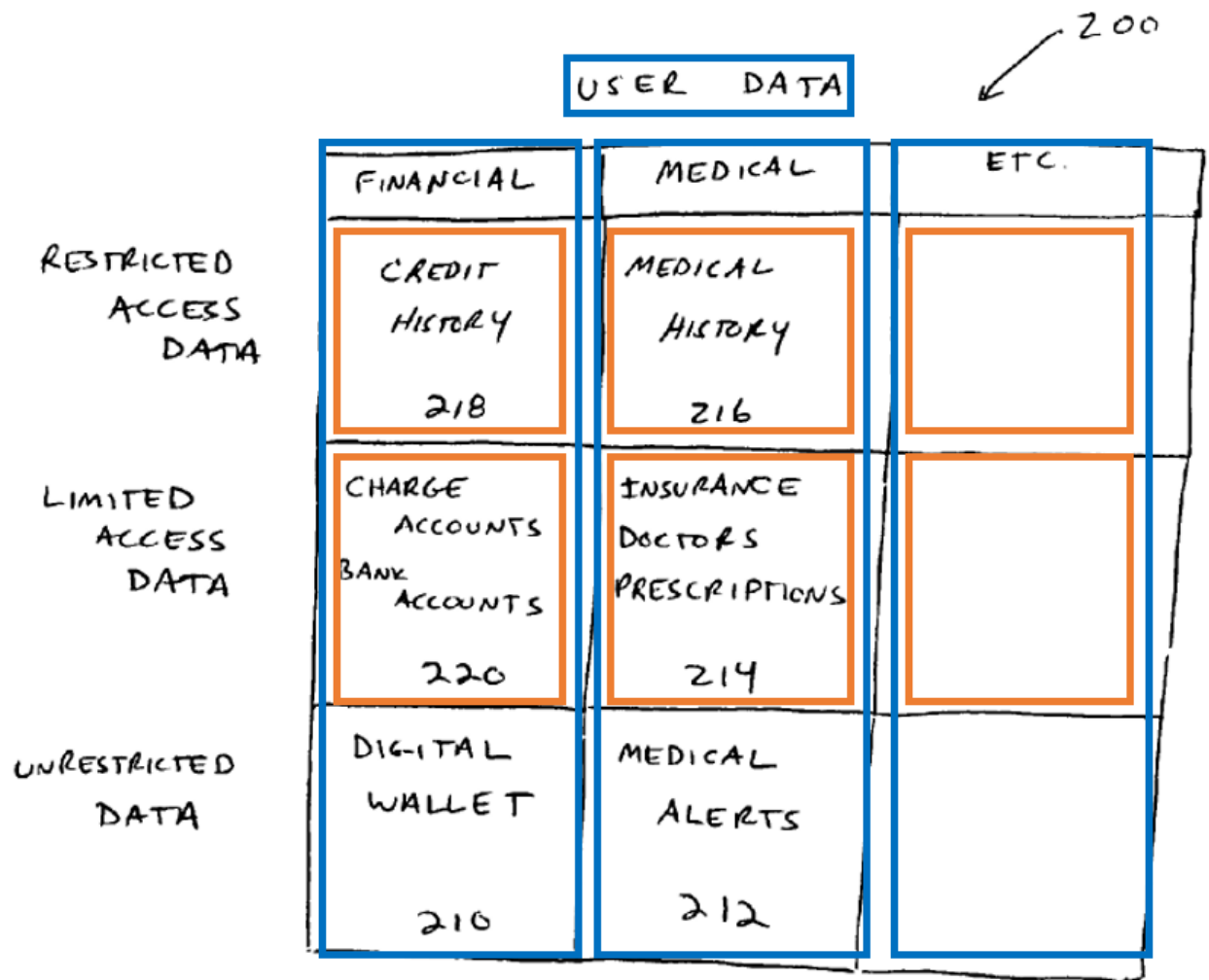


FIG. 3

EX1005 (Bossemeyer), Figure 3.

183. In sum, Bossemeyer discloses and/or renders obvious a plurality of physically distinguishable memories (locations storing remainder data in the **central database server**, **credit card company server**, **insurer server**, **health provider server**, **bank server**) respectively designated as a remainder store and a plurality of

physically distinct extract stores corresponding to a plurality of security levels (“**public limited access, restricted**” security levels) for respective subsets of said security sensitive words, characters or icons.

184. Bossemeyer also discloses and/or renders obvious having physically distinguishable memories (locations storing remainder data in the **central database server, credit card company server, insurer server, health provider server, bank server**) designated as a remainder store and a plurality of physically distinct extract stores corresponding to a plurality of security levels (“**public limited access, restricted**” security levels) for respective subsets of said security sensitive words, characters or icons.

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

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

185. Bossemeyer discloses and, alternatively, Bossemeyer renders obvious these limitations, as explained below in addition to the reasons discussed in Section X.A.1.i.b (above).

186. As an initial matter, I note that the '987 Patent uses the terms “extracting” and “parsing” to mean a process that separates different types of data.

187. As discussed in Sections X.A.1.i.b and X.A.1.i.e (above), Bossemeyer separates (e.g., extracts) and parses, *user data* into subsets of *extracted data* (e.g., *limited access information* and/or *proprietary information*), and *remainder data* (e.g., *public information*). 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.

188. Various information of the *extracted data* is associated with respective *levels of security/accessibility* (e.g., *public limited access*, *restricted*). 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.

189. In sum, Bossemeyer discloses and/or renders obvious securing data (“**information**”) by extracting said security sensitive content (*e.g.*, “**user’s medical history information 216**,” and “**insurance, doctors, prescriptions information 214**”) and extracting security sensitive words, characters or icons from said data to obtain extracted data (“**restricted**” or “**limited-access data**”) and remainder data (“**unrestricted data**”) therefrom.

190. Bossemeyer also discloses and/or renders obvious securing data (“**information**”) by parsing said data including security sensitive content (*e.g.*, “**user’s medical history information 216**,” and “**insurance, doctors, prescriptions information 214**”) and extracting security sensitive words, characters or icons from said data to obtain extracted data (“**restricted**” or “**limited-access data**”) and remainder data (“**unrestricted data**”) therefrom.

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

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

191. Bossemeyer discloses and, alternatively, Bossemeyer renders obvious these limitations, as explained below in addition to the reasons discussed in Section X.A.1.i.e (above).

192. As discussed in Sections X.A.1.i.b and X.A.1.i.e (above), Bossemeyer discloses separating (extracting) security sensitive content from user data to obtain *restricted access* data (*credit history 218* and *medical history 216*) and *limited access* data (*charge/bank accounts 220* and *insurance and prescriptions 214*) and *remainder data*. As also discussed, Bossemeyer discloses storing *extracted data*, e.g., *restricted access data* and *limited access data* in respective *extract stores* corresponding to their *security level* and the *remainder data* in the *remainder store*. This is illustrated in Figure 3 below. See EX1005 (Bossemeyer), Figure 3:

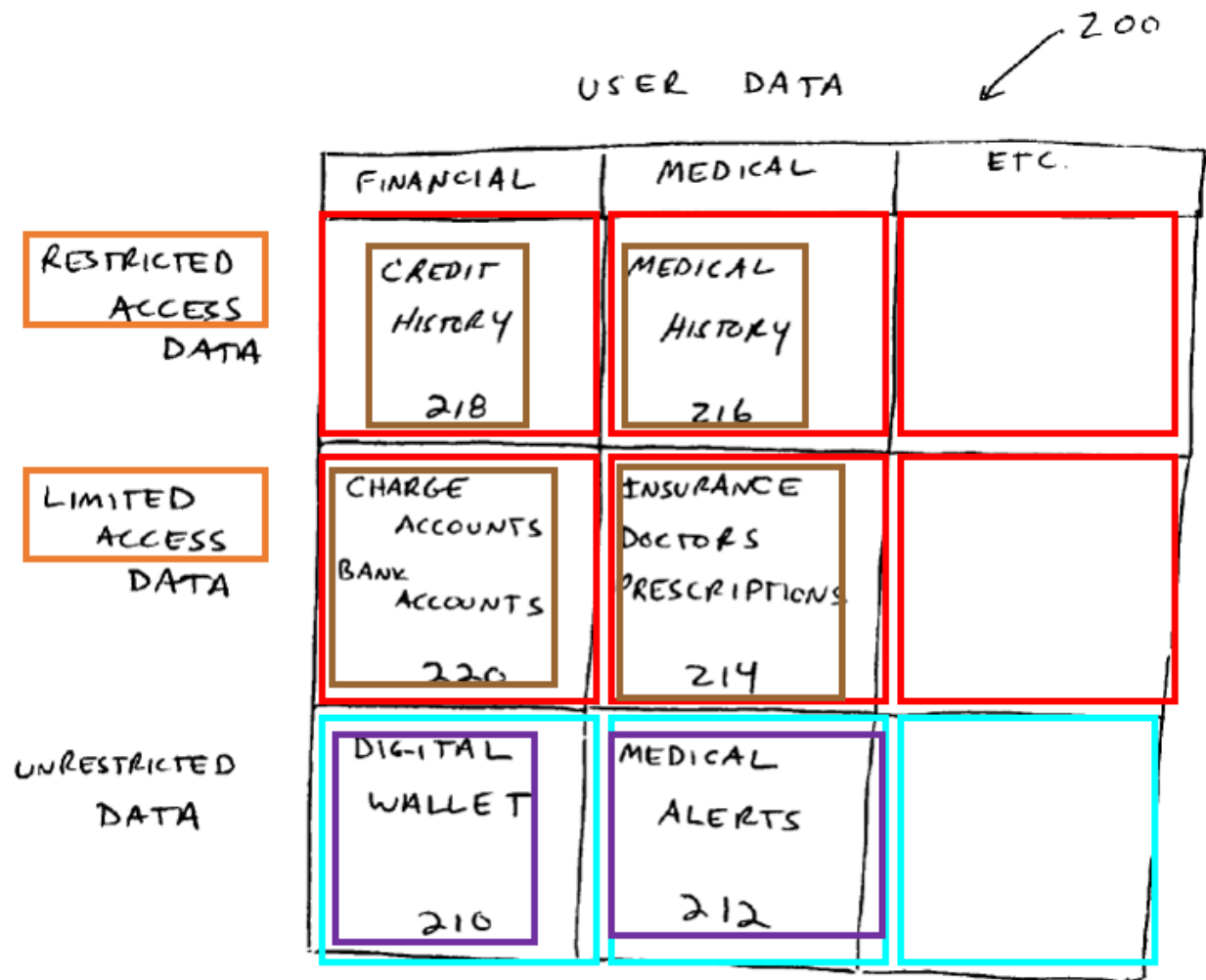


FIG. 3

See also EX1005 (Bossemeyer), Figure 1:

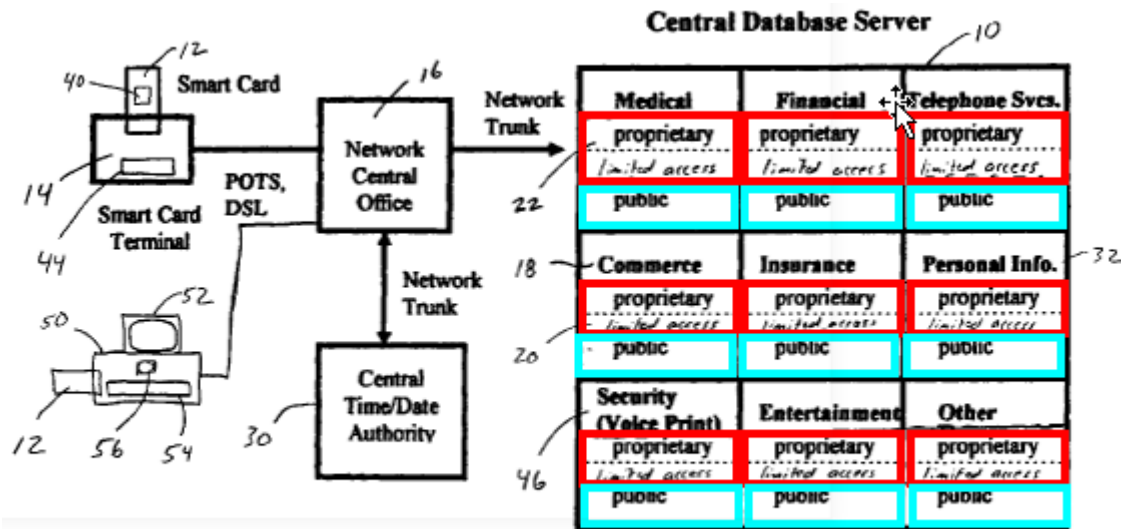


Figure 1

193. The extracted data and remainder data are stored by different categories and levels of security at different servers. *See e.g.*, 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).

194. Bossemeyer explains that different entities store and manage their own security data, and a POSITA would have understood those to use multiple (distinct) servers. *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 such cases, the central database server 10 acts as a network smart card server which facilitates data transfer between the database containing the desired information and the merchant or person requesting the information. In the same way, *insurance information would ultimately reside with the insurer, medical records with the health provider, financial records with the bank or broker, and so on.* The network smart card server acts as a secured gatekeeper to such information and the smart card acts as the enabling key.

195. In sum, Bossemeyer discloses and/or renders obvious storing said extracted data (e.g., *credit history 218, medical history 216, charge/bank accounts 220*, and *insurance doctor's prescriptions 214*) and said remainder data (e.g., *digital wallet 210* and *medical alerts 212*) in said respective *extract stores* (e.g., stores for “*restricted access data*” and “*limited access data*”), corresponding to an associated security level and said remainder store (“*unrestricted data*”), respectively.

196. Bossemeyer also discloses and/or renders obvious storing said extracted data (e.g., *credit history 218, medical history 216, charge/bank accounts 220*, and *insurance doctor's prescriptions 214*) and said remainder data (e.g., *digital wallet 210* and *medical alerts 212*) in said *extract stores* (e.g., stores for “*restricted access data*” and “*limited access data*”) and said remainder store (“*unrestricted data*”), respectively.

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

197. Bossemeyer discloses and, alternatively, Bossemeyer renders obvious this limitation.

198. As discussed in Sections X.A.1.i.e and X.A.1.ii (above), Bossemeyer discloses extracting **user data** to obtain **extracted data** and **remainder data** and storing **extracted data** in respective **extract stores** according to different levels of security.

199. As an initial matter, a POSITA would have understood that a system such as Bossemeyer separates (extracts or parses) 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.

200. Further, Bossemeyer discloses permitting the full or partial reconstruction of the user data, *e.g.*, permitting access to the data stored at different memory locations (*e.g.*, servers), using “user identification codes” or “data pointers.” *See* EX1005 (Bossemeyer), 2:37-47:

The structure of the central database server is similar to a UNIX-based file system. *Different user identification code*, or data pointers, provided by smart cards 12 *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.

201. Bossemeyer discloses transmitting information to authorized parties requesting said information, which a POSITA would have understood facilitates the merging (reconstruction) of that information. *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 such cases, *the central database server 10 acts as a network smart card server which facilitates data transfer between the database containing the desired information and the merchant or person requesting the information*. In the same way, insurance information would ultimately reside with the insurer, medical records with the health provider, financial records with the bank or broker, and so on.

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

202. Specifically, Bossemeyer discloses that the extracted data and remainder data are retrieved from different memory locations of its computer system, and are presented, *e.g.*, at a terminal, based on a particular user's authorization. *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.*

203. Bossemeyer then explains that by supplying the requested information to authorized parties, merchants can view it to, say, complete a transaction. A POSITA would have understood that when a merchant is viewing of information, it is only after the relevant pieces of information were merged (reconstructed). *See* EX1005 (Bossemeyer), 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.

204. A POSITA would have understood that for a, say, 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 merge 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 have understood 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).

205. 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, thus resulting in a failed transaction.

206. 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.

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

See also EX1005 (Bossemeyer), Figure 3:

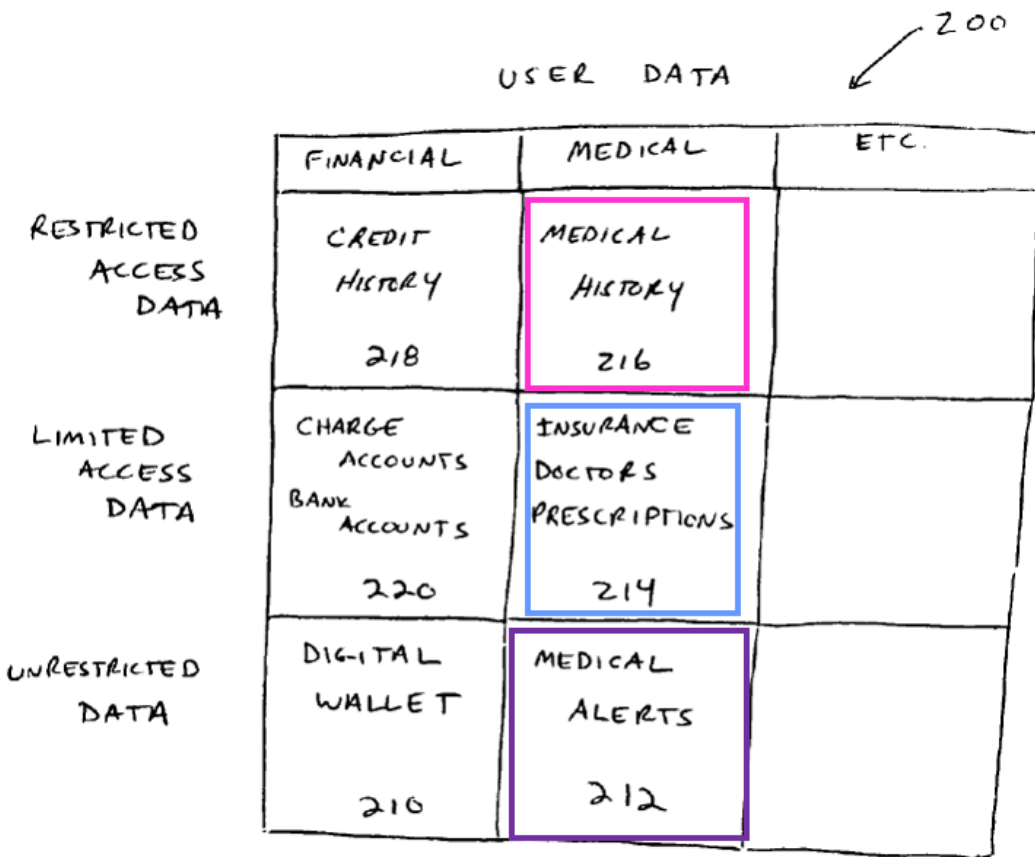


FIG. 3

208. 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.

209. In sum, Bossemeyer discloses and/or renders obvious permitting full or partial reconstruction (e.g., presenting data to the terminal) of said **data** via one or

more of said subsets of *extracted data* from respective *extract stores* and *remainder data*.

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

210. Bossemeyer discloses and, alternatively, Bossemeyer renders obvious this limitation.

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

212. In Bossemeyer, access to the relevant data is provided only after the user's *authorization* has been verified. *See also* 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.

213. Bossemeyer describes the mechanisms that enable predetermining which user has access to what level of information: authentication codes, authorization codes, and access codes. *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*. This code, in turn, is transmitted over the communication network 100, 102 along with the merchant identification code to the server 10, 110. Thus, the digital signature of the card does not change, but an *authorization code* generated by an encryption scheme known to the server provides a unique *access code* each time the card is involved in a transaction with the network.

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

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

214. *Second*, Bossemeyer's *user identification codes* correspond to respective *security levels*. As I discussed earlier in Sections X.A.1.i.e, X.A.1.ii, and X.A.1.iii (above), these security levels that require identification codes correspond to respective *extract stores*.

215. For example, Bossemeyer discloses accessing a user's medical data by permitting partial reconstruction (*e.g.*, presentation of some) or full reconstruction (*e.g.*, presentation of all) of the user's medical data based on the *security level* of the *user identification codes*. Specifically, Bossemeyer discloses allowing access to the user's medical data with "*unrestricted*" and "*limited access*" security levels only with a proper *user authentication code* (*e.g.*, the user's *medical alerts 212* and *insurance and prescription information 214*) but requiring *further authorization* to allow access to data with a "restricted access" security level, such as the user's medical data (*e.g.*, the user's *medical history 216*). *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.

See also EX1005 (Bossemeyer), Figure 3:

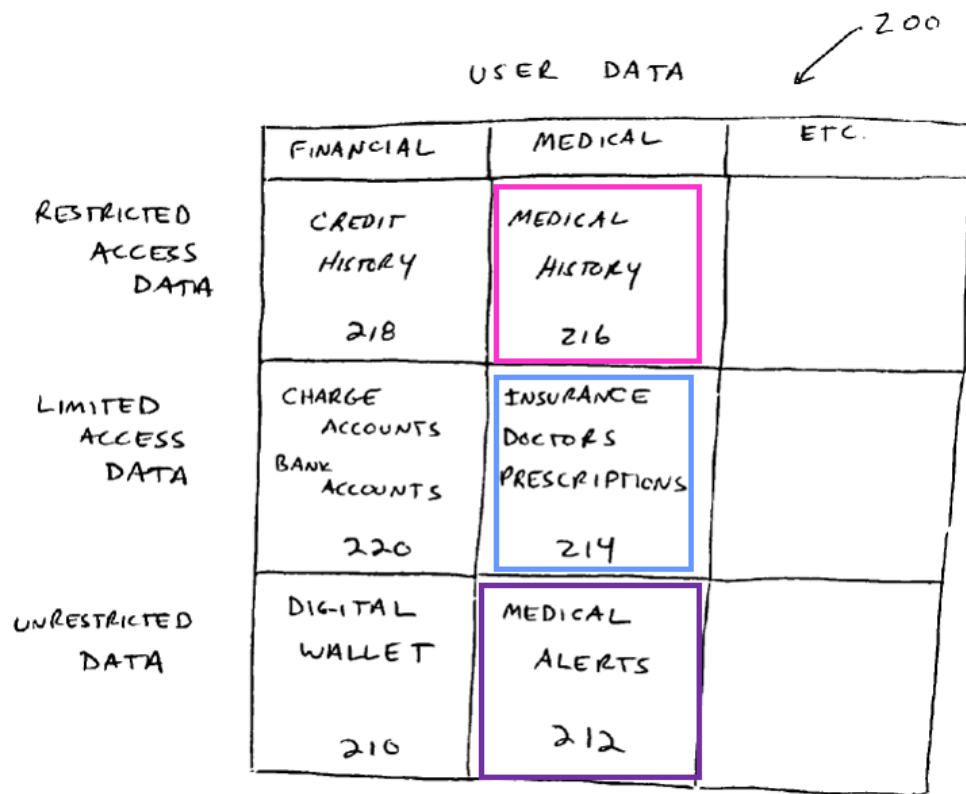


FIG. 3

216. Moreover, a POSITA would have understood that “*further authorization*” would be in the form of a different (or an additional) *user authorization code* that allows 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.*”).

217. 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 be permitted to access only data that corresponds to that person’s security clearance, such that other 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.

218. 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.

219. In sum, Bossemeyer discloses and/or renders obvious permitting the reconstruction only in the presence of predetermined security clearance (“*user authorization code* or *user identification code*”) corresponding to said associated security level (“*restricted*,” or “*limited access*”) for said respective extract stores (*insurer server, health provider server, and bank server*).

2. Dependent Claims 6 and 21

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

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

220. Bossemeyer renders obvious claims 1 and 16. *See* Section X.A.1 (above).

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

221. Bossemeyer discloses this limitation.

222. As discussed in Section X.A.1.ii (above), Bossemeyer discloses establishing a plurality of security levels.

223. Further, Bossemeyer teaches that each *security level* has a *security clearance*, e.g., *user identification/authentication code* or *authorization/access code* associated with a particular *security level*. Specifically, Bossemeyer teaches that “[d]ifferent *user identification codes*, or data pointers, provided by smart cards 12 *allow access to partitions in the database*.” A POSITA would have understood that these multiple codes help protect the privacy of the data. *See* EX1005 (Bossemeyer), 2:38-40; 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.

224. Bossemeyer teaches that *data* (or “*information*”) with a *limited access security level* is “available to *persons or selected groups with a user authentication code*,” while data with a *proprietary information security level* is “accessible only by the *owner of the information or a group with privileges* to that directory information.” EX1005 (Bossemeyer), 2:44-47; *see also id.*, 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.

225. For example, a merchant with a corresponding merchant code can access information available to the particular merchant. *See* EX1005 (Bossemeyer), 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), Figure 2:

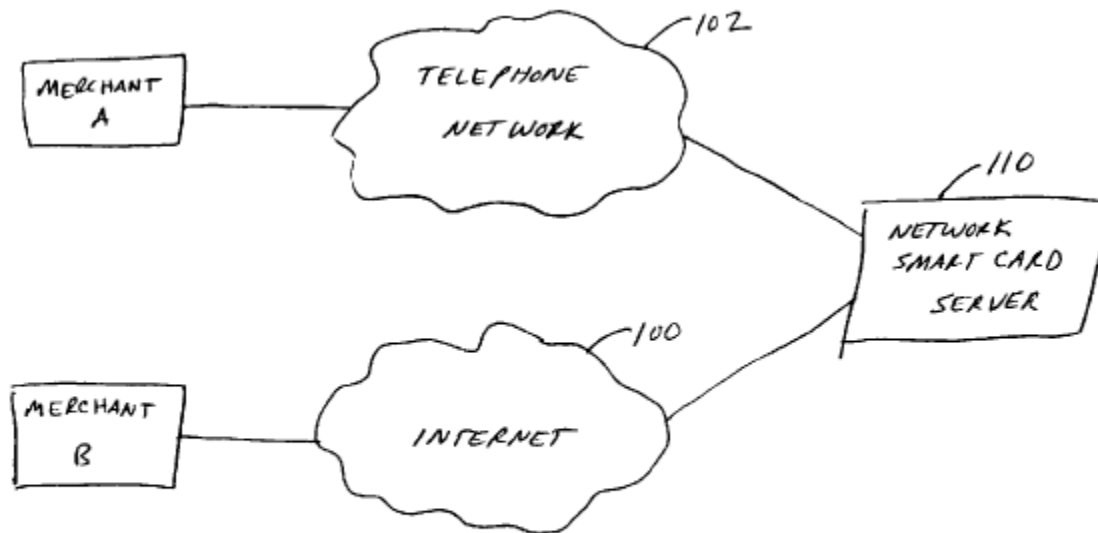


FIG. 2

226. In another example, Bossemeyer explains that a pharmacist will have clearance to access data with *limited access security level*, e.g., a user's *insurance and prescription information 214*, but will not have clearance to access data with *proprietary information security level*, e.g., a user's *medical history 216*. See EX1005 (Bossemeyer), 5:8-15:

[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*.

See also EX1005 (Bossemeyer), Figure 3:

200 ↙

USER DATA

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

FIG. 3

227. In sum, Bossemeyer discloses establishing a plurality of security levels (“**public limited access, restricted**” security levels), each with a respective security clearance a predetermined security clearance (“**user identification code**” or “**authorization code**”).

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

228. Bossemeyer discloses this limitation.

229. As I discussed in Sections X.A.1.i.e and X.A.1.ii (above), Bossemeyer discloses that each subset of the security sensitive words, characters or icons are stored in the plurality of physically distinct extract stores (credit card company server, insurer server, health provider server, bank server) corresponding to the plurality of security levels (“**public limited access, restricted**” security levels). Thus, each subset is correlated with the plurality of security levels (“**public limited access, restricted**” security levels).

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

230. Bossemeyer discloses this limitation.

231. As I discussed in Sections X.A.1.iv and X.A.1.v (above), Bossemeyer discloses permitting a partial reconstruction of the user data in the presence of a predetermined security clearance levels.

232. Moreover, Bossemeyer teaches using its computer system to reconstruct the user data from transactions involving multiple partial reconstructions. Specifically, Bossemeyer describes reconstructing user data, for

example, by a pharmacist's request to access "insurance and prescription information 214" (correlated with the "limited access" level) and a request by other merchants (*e.g.*, automotive dealership, bank officer) to access the user's "credit history" (correlated with the "restricted access" level). *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 such cases, the central database server 10 acts as a network smart card server which facilitates data transfer between the database containing the desired information and the merchant or person requesting the information. In the same way, *insurance information would ultimately reside with the insurer, medical records with the health provider, financial records with the bank* or broker, and so on. The network smart card server acts as a secured gatekeeper to such information and the smart card acts as the enabling key.

233. Bossemeyer then explains how multiple requested pieces of data are routed to multiple different locations, for each respective application or user (*e.g.*, medical, financial, etc.). *See* EX1005 (Bossemeyer), 3:53-4:6:

In operation, the smart card 12 is inserted into the smart card terminal 14 and a personal identification number (PIN) is optionally entered using an input device 44 such as a keypad, mouse, or a track ball provided on the terminal 14. A digital signature or a voice print or other security measure 46 which is stored in the central database server 10 can optionally be verified as well. The desired application is then selected which relates to a memory partition of the central database server 10 such as: medical treatment, financial transaction, telephone services, commercial transaction, insurance, personal information, security access/authorization, entertainment, or other application. 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.

234. Bossemeyer provides examples of how different users (e.g., pharmacist, grocer, loan officer) would each have access to some information based on their respective security clearance levels. See EX1005 (Bossemeyer), 5:6-22:

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.

Similarly, *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.

In contrast, *a loan officer at a bank or automotive dealership would be allowed to access to the user's credit history 218 as well as the user's financial account balances 220*.

235. A POSITA would have understood that Bossemeyer's system utilized transactions with different requesters (e.g., pharmacists, commercial merchants, financial officers) and thus permitted a plurality of partial reconstructions. *See* EX1005 (Bossemeyer), 3:6-22, 3:53-4:6, 5:6-22, 4:23-42. In particular, Bossemeyer discloses that multiple merchants can use Bossemeyer's system. *See* EX1005 (Bossemeyer), 4:23-42:

Referring to FIG. 2, another embodiment of the network arrangement for smart card applications is shown. In contrast to FIG. 1, the 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. In this example, ***Merchant A can be identified to the network smart card server 110*** via the dial-up network of the telephone network 102. For example, the “caller ID” feature of the telephone network 102 could identify the merchant to the network smart card server 110. Alternatively, ***the server 110 can identify the merchant, such as Merchant B***, by way of a digital certificate or access code associated with the particular merchant transmitted over the Internet. ***The merchant record at the server 110 identifies the nature of the transaction, i.e., pharmacy, dentist/doctor, insurance, financial, travel, retail, etc.*** This link between the merchant and server 110 may be established at the start of each business day, at the time of the transaction, or may be continuously established until the merchant has “logged off” the system.

236. Moreover, as another example, when a user visits a health provider (e.g., dentist, doctor), the user’s transaction with the health provider would concern requesting medical history information and charge/credit or bank information that have different security levels (e.g., restricted access data such as medical history, vs. limited access data such as charge/bank accounts). See EX1005 (Bossemeyer), Figure 3:

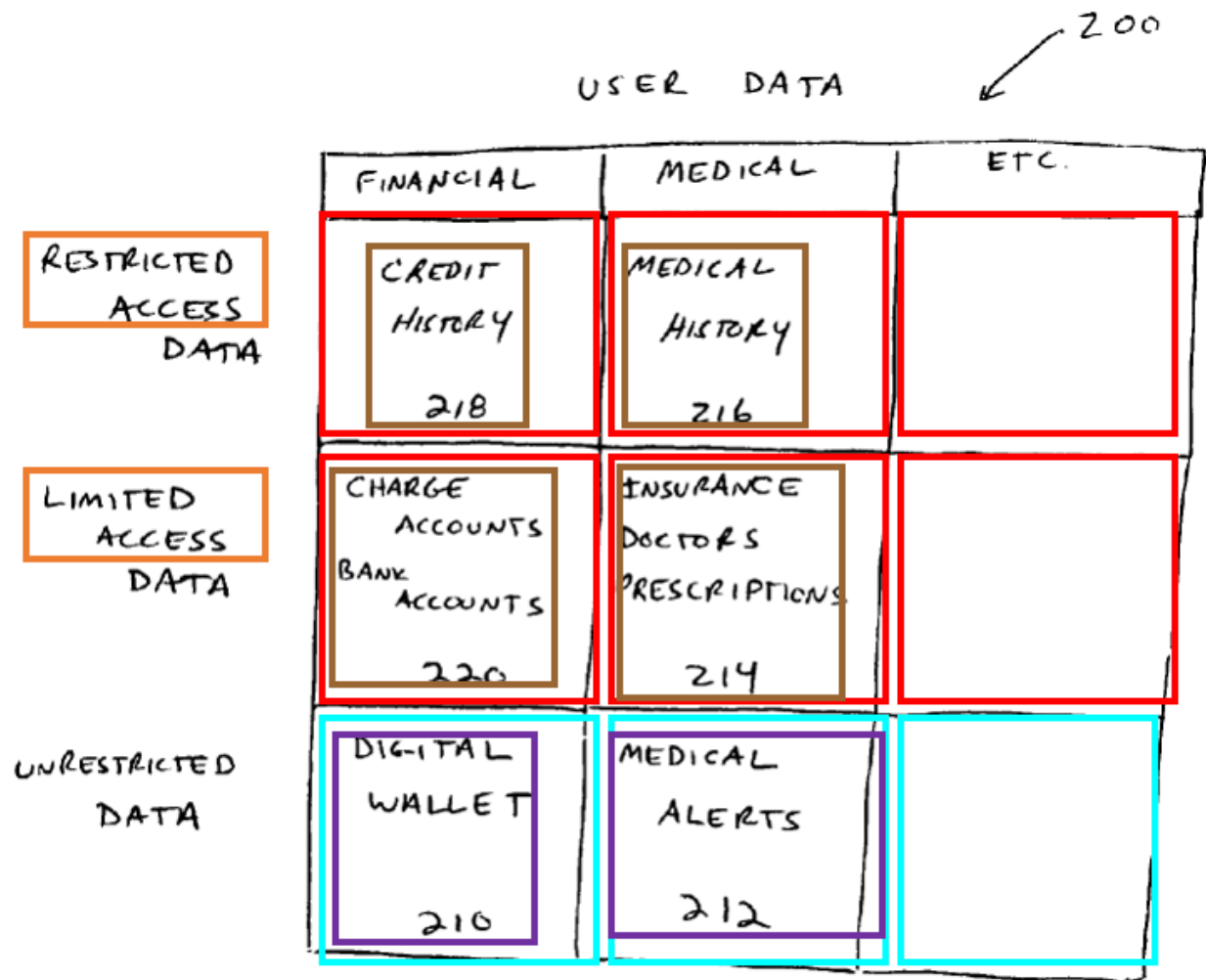


FIG. 3

237. A POSITA would thus have understood that such a medical service transaction requires a plurality of reconstructions from information received from servers (e.g., credit card company, bank, hospital) with different security levels.

238. In sum, Bossemeyer discloses and/or renders obvious the step of permitting reconstruction including the step of permitting a plurality of partial reconstructions of said data (e.g., presenting data to the terminal from requests to

different transactions or servers) in the presence of respective ones of said plurality of security clearance levels (“**public limited access, restricted**” security levels, for multiple users).

3. Dependent Claim 9

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

239. Bossemeyer renders obvious claim 1. *See* Section X.A.1 (above).

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

240. Bossemeyer renders obvious this limitation.

241. I note that this claim can be met by just one of extracting, storing, and/or permitting reconstruction; Bossemeyer renders obvious all three as discussed below.

242. As an initial matter, the '987 Patent itself states that assessing a charge to a merchant or user over the Internet, during the data-securing stage or reconstruction stage, was well known in the art. *See, e.g.,* EX1001 (the '987 (Patent)), 45:34-46:17:

FIG. 13 diagrammatically shows several revenue systems which may be employed with the data security systems described herein....

FIG. 13 shows two basic systems, one at the data input stage and the second at the data output or reconstruction phase. Within each revenue subsystem are two types of revenue generators, an advertising revenue generator and a user charge generator. The user charge system contemplates charging or assessing a fee to the user's employer or

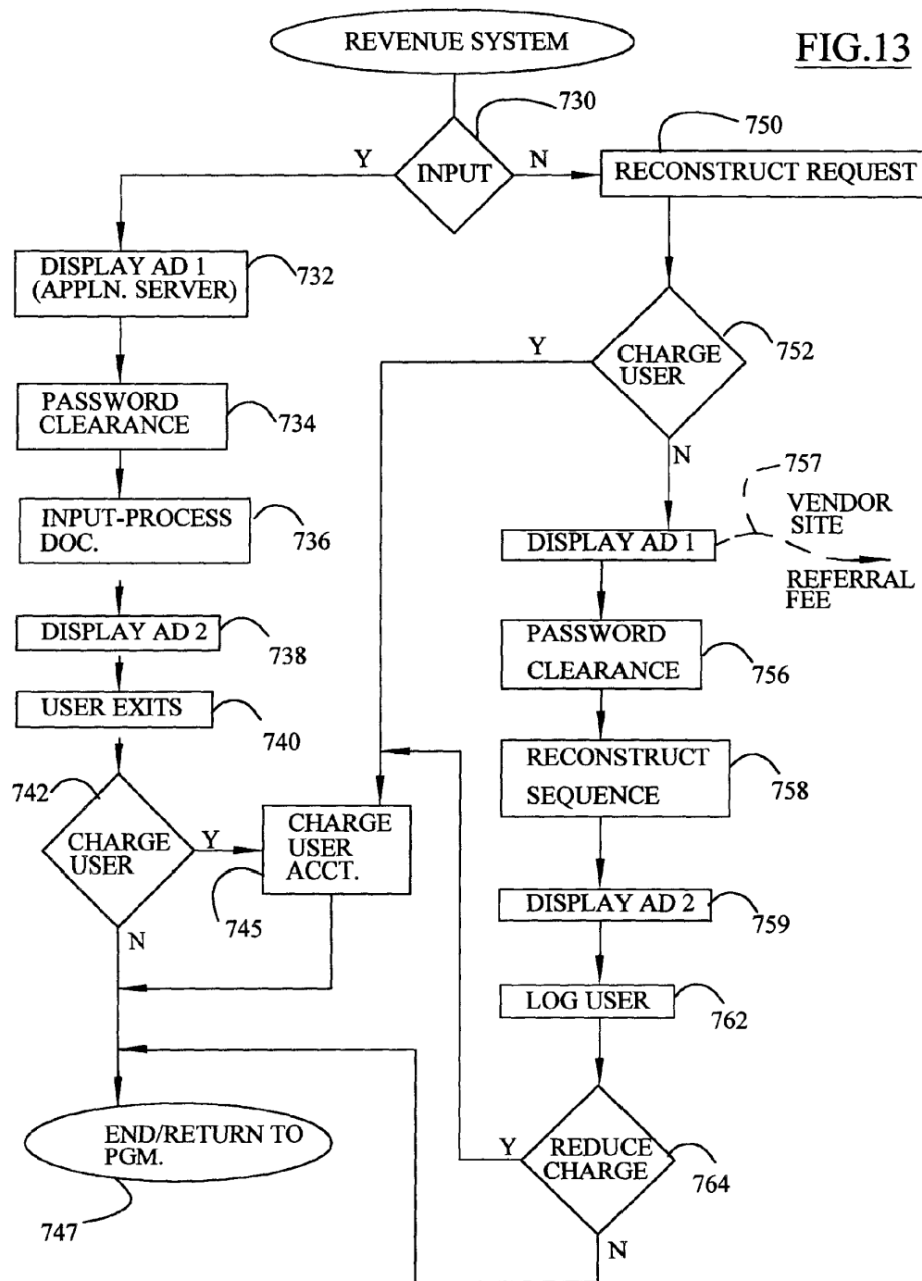
organization. Therefore, the system operator may select up to four (4) revenue generation systems (ads at the input, charges at the input, ads at the output and charges at the output). *It is well known that vendors selling goods and services over the Internet are willing to pay a certain percentage of their sales revenue to other entities referring customers to the vendor's web sites.* The concept of display ads in FIG. 13 includes this revenue stream.... Other revenue system may also be utilized. The steps in the revenue system described herein may be reorganized to attain higher consumer and user acceptance and/or to maximize the revenue to the system operator.

...

Step 738 shows display ad 2 to the user thereby potentially generating referral revenue for the system operator. Step 740 notes that the user exits the revenue system. Step 742 determines whether the system charges the user for the security service. If YES, the program processes the charge in step 745 (*charge systems are known*). If [] NO, the system ends or returns to other programs in step 747.

...

See EX1001 (the '987 (Patent)), Figure 13:



243. For example, the '987 Patent explains that “*charge systems are known*” for “security service.” EX1001 (the '987 (Patent)), 46:11-16. The '987 Patent also states that “[i]t is well known that *vendors* selling goods and services over the Internet *are willing to pay a certain percentage of their sales revenue* to other

entities referring customers to the vendor's web sites." EX1001 (the '987 Patent), 45:46-49.

244. As the '987 Patent states, using charging systems was well known in the art. Indeed, Bossemeyer specifically teaches that data is stored based on a subscription of merchants and users of its system. *See* EX1005 (Bossemeyer), 5:23-31:

Data is stored in the server in several ways. Merchant profiles become populated *when a merchant subscribes* to the service. Default profiles can exist for merchants until a sufficient number of transactions occur through that merchant to provide network use information which may be relevant to the system. Similarly, the user data becomes populated *when the user subscribes* as part of the smart card activation process. Additional data is created as the user and the merchants interact with the system.

245. Bossemeyer does not explicitly state that subscriptions are for pay. However, first, a POSITA would have understood that the term "subscription," in this context means a paid one. Second, a POSITA would have understood that Bossemeyer's computer system could assess a subscription charge to merchants and users for extracting, storing, or permitting reconstruction of the user data during their transactions. Indeed, the information that Bossemeyer's system manages is highly valuable as much of it requires high security to maintain privacy. Therefore, a POSITA would have found obvious for an operator of Bossemeyer's system to try

and monetize the access to such data (especially as much of this data could never be made fully public). Second, a POSITA would have understood that charging a fee was a well-known technique. *See* EX1005 (Bossemeyer), 5:23-31; EX1001 (the '987 Patent), 45:34-46:34. Indeed, as I discuss in Section X.C.2 (below), systems that assess and charge fees for subscription services for monetization were common and well known. *See* Section X.C.2 (discussing EX1021 (Paltenghe), EX1022 (Baker), EX1023 (Clark), EX1024 (OceanStore)).

246. In sum, Bossemeyer renders obvious assessing a charge (*e.g.*, subscription fee) for extracting, storing or permitting reconstruction.

4. Dependent Claims 11 and 23

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

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

247. Bossemeyer renders obvious claims 10 and 22. *See* Section X.A.1 (above).

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

248. Bossemeyer renders obvious this limitation for the reasons discussed in Sections X.A.1.i.b and X.A.1.ii (above).

249. I note that the '987 Patent does not describe what it means by “parsing ... granularly.” A POSITA would have understood that the granularity of data can

be any, from fine to coarse and anything in between. *See* EX1028 (Microsoft Dictionary), p. 206 (“**granularity** *n.* A description, from ‘coarse’ to ‘fine’, of a computer activity or feature (such as screen resolution, searching and sorting, or time slice allocation) in terms of the size of the units it handles (pixels, sets of data, or time slices). The larger the pieces, the coarser the granularity.”). Absent additional information, the term “granularly” in these two claims appears to be superfluous. A POSITA would have therefore understood that the data Bossemeyer parses is necessarily at *some* granularity (*e.g.*, fine, coarse), because it is smaller than the whole of the original data prior to parsing.

5. Dependent Claims 15 and 27

i. [15pre] A method as claimed in claim 10 including

[27pre] A storage medium as claimed in claim 22 including

250. Bossemeyer renders obvious claims 10 and 22. *See* Section X.A.1 (above).

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

251. Bossemeyer renders obvious this limitation.

252. At the outset, I note that the claimed “further data security step” does not impose a narrowing limitation on the claimed “data.” That is, the “data” will either exist (stored with or without encryption) or will not exist (get destroyed).

253. Moreover, I understand that one may meet this claim by practicing only one option out of a group of three: (1) data stored unencrypted, (2) data stored encrypted, or (3) data is destroyed. Nevertheless, below I show how Bossemeyer independently renders obvious each of the three options.

254. *First*, in some examples, Bossemeyer discloses that the user data is “stored on the smart card.” EX1005 (Bossemeyer), 3:52-4:6:

In operation, the smart card 12 is inserted into the smart card terminal 14 and a personal identification number (PIN) is optionally entered using an input device 44 such as a keypad, mouse, or a track ball provided on the terminal 14.... 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.

255. Bossemeyer also teaches that the user inputs user data upon subscription. See EX1005 (Bossemeyer), 5:28-31 (“[T]he user data becomes populated when the user subscribes as part of the smart card activation process. Additional data is created as the user and the merchants interact with the system.”).

256. In the above examples, a POSITA would have understood that Bossemeyer’s smart card stores user data (as it could be later “updated”), for example, by the user’s entry of data upon activation, before sending the data to the network smart card server (central database server). EX1005 (Bossemeyer), 4:3-6, 5:28-30.

257. Moreover, Bossemeyer describes that the data stored in the smart card may or may not be encrypted because it optionally has an “encryption capability.” EX1005 (Bossemeyer), 3:28-38:

Smart card 12 is formed of plastic or other suitable material and contains circuitry 40 which includes a microprocessor and memory including random access memory (RAM) and read only memory (ROM). The face of the smart card 12 may have information printed or embossed on it such as a photograph, in addition to the name of the card holder. The same information can alternatively or additionally be provided in the memory contained within the card 12. The card memory also preferably includes a users [sic] “certificate” or “digital signature” as well as *encryption capability* for security.

258. Thus, a POSITA would have understood that Bossemeyer's smart card can store user data with or without encryption, and that such storing is independent of parsing, storing, and reconstruction using parsed data because the storing is unrelated to the separation of sensitive content at the central database server. Accordingly, Bossemeyer teaches this limitation.

259. ***Second***, Bossemeyer, alternatively, teaches destroying the smart card's user data after it is sent to the network smart card server because Bossemeyer's system could "reduce[] the amount of information which must be stored... to each smart card 12 and enable[] data to be shared across groups of cards" by using data pointers to access information in remote servers. Bossemeyer explains that such an approach facilitates "complex applications which may otherwise require more resources than could be economically stored or transferred to the smart card 12" by deleting user data in the card and storing data elsewhere. Specifically, Bossemeyer states:

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 and enables data to be shared across groups of cards that may be treated as a single unit.*** These pointers *facilitates* [sic] ***more complex applications which may otherwise require more resources than could be economically stored*** or transferred to the smart

card 12. Thus, the network augments or replaces the amount of card memory typically associated with smart cards. ***This allows greater capacity than could otherwise be achieved by storing information on the cards alone.***

See EX1005 (Bossemeyer), 2:58-3:2.

260. Thus, because the smart card itself does not always store the user data, Bossemeyer further explains that the secured data can be accessed through the network arrangement. See EX1005 (Bossemeyer), 4:7-17:

Because the majority of the information is stored at a central location, namely the central database server 10, the present network arrangement allows for advance 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 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. Smart card 12, in such a case, provides access to the authorization procedure, user profile information, and pointers to relevant data within the partitioned central database server 10.

261. Bossemeyer's smart cards, as a POSITA would have known, have limited storage capacity. Hence it is desirable to limit how much and which data is stored on smart cards (*e.g.*, by deleting older data to make room for new one). See *also* EX1005 (Bossemeyer), Abstract:

A network for smart card applications using a smart card in combination with a smart card terminal. The network arrangement includes a communications network connected to at least one smart card terminal, and a central database server in operative communication with the network central office.... The information contained in the partitioned memory locations is accessible by data pointers stored on the individual smart cards. ***In this manner, the amount of data stored on the smart cards using the system is reduced and all of the information relating to a smart card user is centralized in one location.*** The central database server includes means for distinguishing between public information and proprietary information stored in the partitioned memory locations.

262. Thus, a POSITA would have understood that in some examples Bossemeyer at least suggests to delete the user data in the smart card that is transferred to and stored in remote servers to avoid requiring a large (and more expensive) storage capacity in the card, and that the deletion is independent of parsing, storing, and reconstruction using parsed data because the storing is unrelated to the separation of sensitive content at the central database server. Accordingly, Bossemeyer teaches this limitation.

263. In sum, Bossemeyer renders obvious a further data security step of one from the group of storing said data (e.g., user data in the smart card) without encryption, storing said data with encryption (e.g., user data in the smart card, using

optional encryption) and destroying said data (*e.g.*, deleting user data in the smart card). Bossemeyer renders obvious that the further data security step is independent of said parsing, storing and permitting reconstruction.

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

1. Independent Claims 1, 10, 16, and 22

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

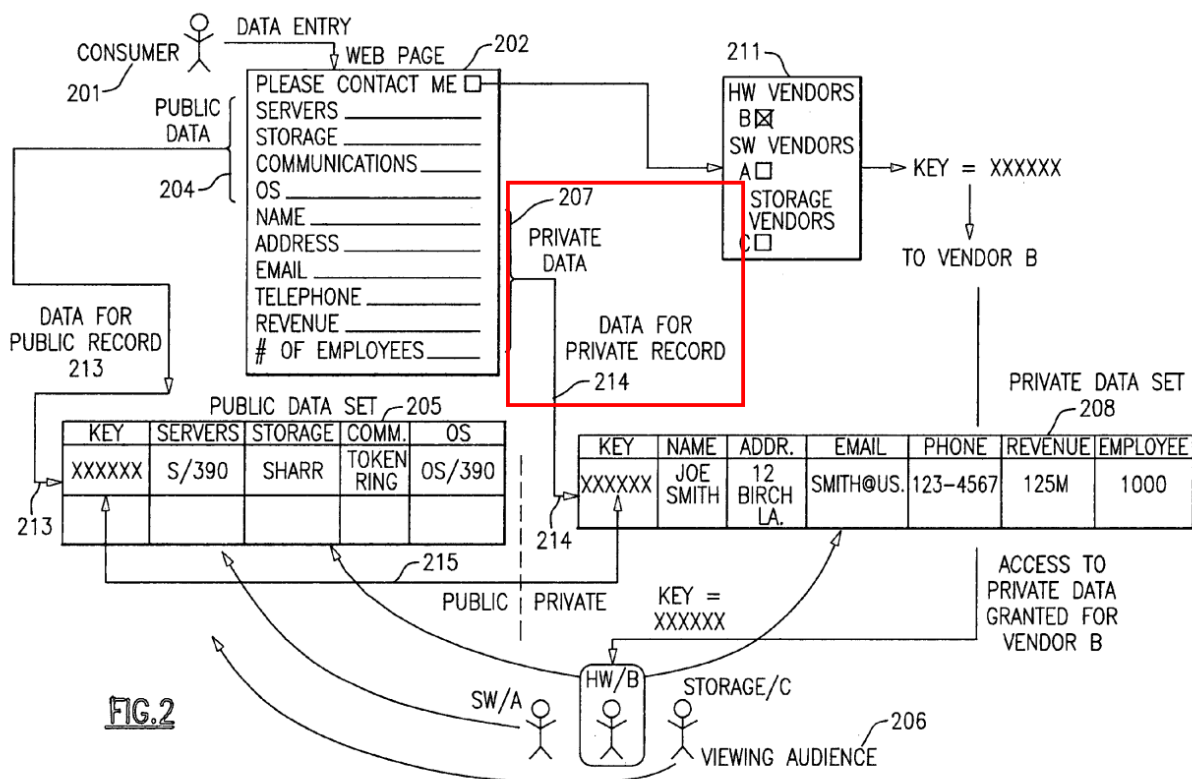
264. To the extent that the preamble is limiting, Bossemeyer in combination with Merenda renders obvious the preambles of independent claims 1, 10, 16, and 22, as explained below.

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

265. As I explained in Section X.A.1.i.a (above), Bossemeyer discloses and, alternatively, renders obvious this limitation. Bossemeyer combined with Merenda renders obvious this limitation for the same reasons discussed in Section X.A.1.i.a (above) and as explained below.

266. To the extent that Patent Owner argues that Bossemeyer does not teach this limitation, Merenda discloses a method for securing *data* that has security sensitive content represented by one or more security sensitive words, characters, or icons. EX1006 (Merenda), ¶23 (“Fundamental to the implementation of the present invention is the notion that a set of *data* may be parsed into private and non-private

elements. At the most simplistic level this might entail, for example, identifying input fields on a Web page as requiring *sensitive data input* such as an address, credit card or social security number, versus non-sensitive information such as the name of the item being purchased, the date, time etc.), ¶24 (“As previously noted, such separation of data elements may be accomplished using known techniques to any desired level of granularity, resulting potentially in multiple public and private data sets and in the combination of individually public data sets 103, 104 into a combined private data set 105.”); Figures 1, 2, 6. For example, Merenda’s Figure 2 illustrates securing private data of the user’s data entry:



EX1006 (Merenda), Figure 2.

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

268. In sum, Bossemeyer combined with Merenda renders obvious a method of securing data (Bossemeyer’s and/or Merenda’s “*information*”) having one or more security sensitive words, characters (*e.g.*, Bossemeyer’s and/or Merenda’s credit card number, Merenda’s social security number) or icons (*e.g.*, Bossemeyer’s insurance cards).

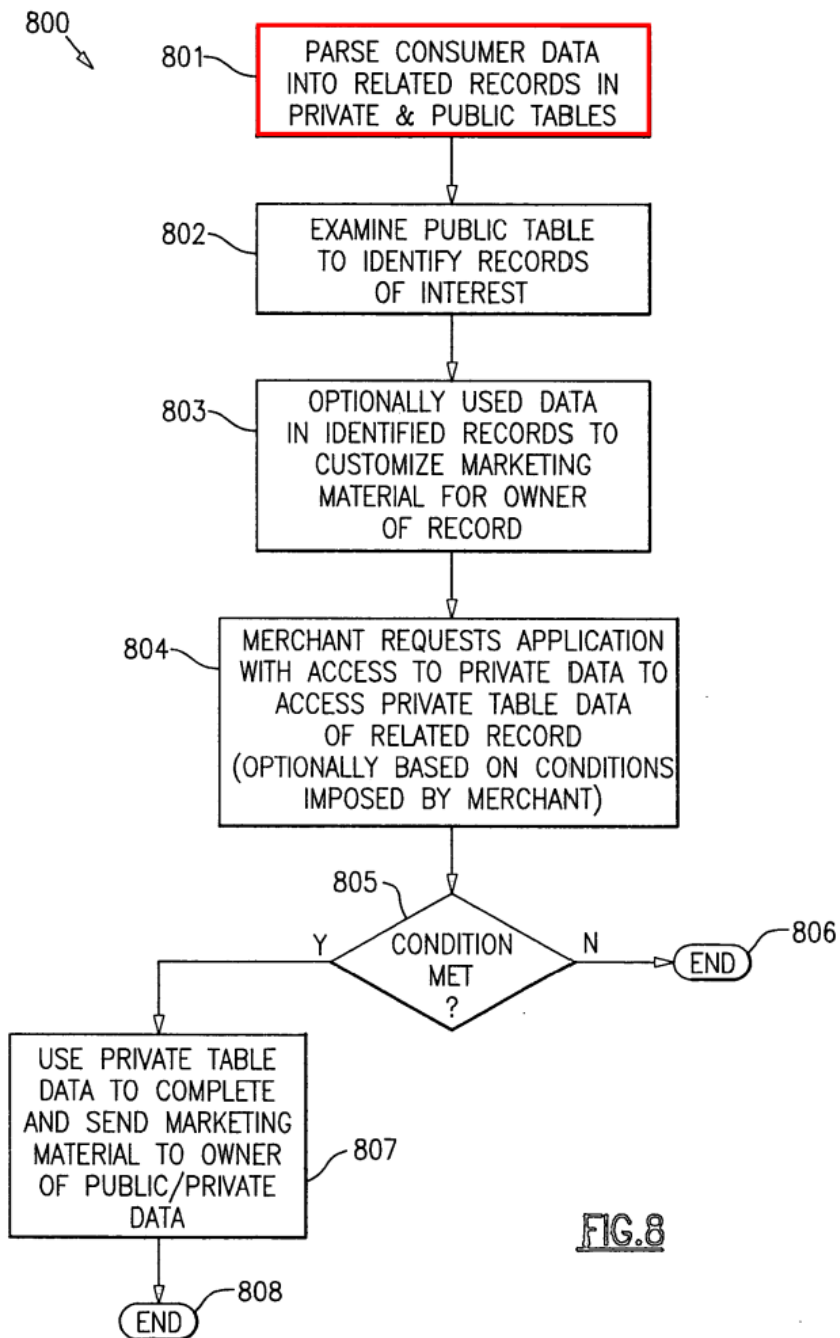
b. [10pre-i] A method of securing *data* with a parsing algorithm via a computer system

269. As I explained in Section X.A.1.i.b (above), Bossemeyer discloses and, alternatively, renders obvious this limitation. Bossemeyer combined with Merenda renders obvious this limitation for the same reasons discussed in Section X.A.1.i.b (above) and as explained below.

270. To the extent that Patent Owner argues that Bossemeyer does not teach using a “parsing algorithm” to secure data, Merenda teaches it. Merenda specifically discloses parsing security sensitive content (*e.g.*, *private elements*) from *user data* to obtain subsets of *extracted data* (*e.g.*, *address*, *credit card* or *social security*

number) and *remainder data* (e.g., *non-private elements*). EX1006 (Merenda), ¶23 (“[A] set of *data* may be parsed into *private* and *non-private elements*. At the most simplistic level this might entail, for example, identifying input fields on a Web page as requiring sensitive data input such as an *address*, *credit card* or *social security number*, versus non-sensitive information such as the *name of the item being purchased*, the *date*, *time* etc.”), ¶24 (“It is of course understood that the source of such data may come from any number of sources, including without limitation, surveys, transactional data, etc. and is not limited to customer interactions over the World Wide Web. As previously noted, such separation of data elements may be accomplished *using known techniques to any desired level of granularity*, resulting potentially in multiple public and private data sets and in the combination of individually public data sets 103, 104 into a combined private data set 105.”), ¶31 (“Turning to FIG. 3 it is seen that a web form may generate a number of data sets 301*a-d* including demographics 301*a*, server data 301*b*, user data 301*c*, and cost data 301*d*. Any of these data sets may be designated as including private data, and the *remaining data sets* include public data.”), Figures 1, 2, 3.

271. Merenda specifically discloses parsing as illustrated in Figure 8, step 801:



EX1006 (Merenda), Figure 8, ¶47 (“Starting at step 801 data from a consumer is *parsed* into related records in public and private tables.”).

272. Accordingly, a POSITA would have understood that Merenda discloses parsing data into *public data* (e.g., *remainder data*) and *private data* (e.g., *extracted data*) and storing that data as respective public data sets (e.g., *remainder store*) and private data sets (e.g., *extract stores*), which results from utilizing a parsing algorithm. EX1006 (Merenda), ¶¶23-24, ¶31 (“Turning to FIG. 3 it is seen that a web form may generate a number of data sets 301*a-d* including demographics 301*a*, server data 301*b*, user data 301*c*, and cost data 301*d*. Any of these data sets may be designated as including private data, and the remaining data sets include public data.”), Figures 1, 2, 3, ¶15 (“FIG. 1 illustrates a set of data elements *parsed* into private and public data sets.”), ¶47. It would have been obvious to combine Merenda’s teaching with Bossemeyer to use a parsing algorithm to extract sensitive content. *See* Section X.B.2 (below).

273. In sum, Bossemeyer combined with Merenda renders obvious a method of securing data (Bossemeyer’s and/or Merenda’s “*information*”) with a parsing algorithm (Bossemeyer’s and/or Merenda’s splitting the data using known techniques to any desired level of granularity) via a computer system (Bossemeyer’s “interconnected network of computers”).

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

274. As I explained in Section X.A.1.i.c (above), Bossemeyer renders obvious this limitation. Bossemeyer combined with Merenda renders obvious this limitation for the same reasons discussed in Section X.A.1.i.c (above) and as explained below.

275. Merenda discloses “at least one *program storage device readable by a machine*, tangibly embodying at least one *program of instructions* executable by the machine to perform the capabilities of the present invention can be provided.” EX1006 (Merenda), ¶50, ¶49.

276. As discussed in Section X.B.2 (below), a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in combining Bossemeyer with Merenda and meet this limitation.

277. In sum, Bossemeyer combined with Merenda renders obvious a computer readable storage medium (Bossemeyer’s and/or Merenda’s “*program storage device readable by a machine*”) encoded with programming instructions (Bossemeyer’s and/or Merenda’s “*program of instructions*”) for securing data (Bossemeyer’s and/or Merenda’s “*information*”) having one or more security

sensitive words, characters (*e.g.*, Bossemeyer's and/or Merenda's credit card number, Merenda's social security number) or icons (*e.g.*, Bossemeyer's insurance cards) in a computer system (Bossemeyer's "interconnected network of computers").

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

278. As I explained in Section X.A.1.i.d (above), Bossemeyer renders obvious this limitation. Bossemeyer combined with Merenda renders obvious this limitation for the same reasons discussed in Sections X.A.1.i.d, X.B.1.i.b, and X.B.1.i.c (above).

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

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

279. As I explained in Section X.A.1.i.e (above), Bossemeyer discloses and, alternatively, renders obvious these limitations. Bossemeyer combined with

Merenda renders obvious these limitations for the same reasons discussed in Section X.A.1.i.e (above) and as explained below.

280. As an initial matter, a POSITA would not have found any meaningful difference between “physically distinguishable” and “physically distinct” in these claims.

281. To the extent that Patent Owner argues that Bossemeyer does not disclose a plurality of security levels, Merenda discloses, or at minimum renders obvious, a plurality of security levels for the private data sets. For example, a person requesting information (*e.g.*, a merchant) can have access only to certain segments of the private information. That is, a merchant can access certain selected private data sets (*e.g.*, private data sets having a first security level, such as *name, address, phone number, e-mail*), but cannot access other private data sets (*e.g.*, private data sets having a second (higher) security level, such as *revenue, credit card*). See EX1006 (Merenda), ¶29:

It is useful to note that the present invention contemplates that provision of *access to the data elements in the private data* set may be made on an element-by-element basis, that is to say, that *the merchant may be provided with access to certain select pieces of private data within the single data record 214*, such as the *contact information (name, address, phone number, e-mail)* but *not to other sensitive data* such as *revenue, credit card etc..*

282. As discussed in Section X.B.2 (below), a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in combining Bossemeyer with Merenda.

283. In sum, Bossemeyer combined with Merenda renders obvious a plurality of physically distinguishable memories (Bossemeyer's **central database server**, **credit card company server**, **insurer server**, **health provider server**, **bank server**) respectively designated as a remainder store and a plurality of physically distinct extract stores corresponding to a plurality of security levels (Bossemeyer's "**limited access**, **restricted**" security levels and/or Merenda's **security levels of private data**) for respective subsets of said security sensitive words, characters or icons.

284. Bossemeyer combined with Merenda also renders obvious having physically distinguishable memories (Bossemeyer's **central database server**, **credit card company server**, **insurer server**, **health provider server**, **bank server**) designated as a remainder store and a plurality of physically distinct extract stores corresponding to a plurality of security levels (Bossemeyer's "**limited access**, **restricted**" security levels and/or Merenda's **security levels of private data**) for respective subsets of said security sensitive words, characters or icons.

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

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

285. As I explained in Section X.A.1.ii (above), Bossemeyer discloses and, alternatively, renders obvious these limitations. Bossemeyer combined with Merenda renders obvious these limitations for the same reasons discussed in Sections X.A.1.ii and X.B.1.i.b (above) and as explained below.

286. As an initial matter, I note that the '987 Patent uses the terms “extracting” and “parsing” to mean a process that separates different types of data.

287. To the extent that Patent Owner argues that Bossemeyer does not teach these limitations, Merenda discloses extracting by parsing security sensitive words, characters or icons (e.g., *private elements*) from *user data* to obtain subsets of *extracted data* (e.g., *address*, *credit card* or *social security number*) and *remainder data* (e.g., *non-private elements*). EX1006 (Merenda), ¶23 (“[A] set of *data* may be *parsed* into *private* and *non-private elements*. At the most simplistic level this might entail, for example, identifying input fields on a Web page as requiring sensitive data input such as an *address*, *credit card* or *social security number*, versus non-sensitive information such as the *name of the item being purchased*, the *date*, *time* etc.”), ¶24 (“It is of course understood that the source of such data may come from any number

of sources, including without limitation, surveys, transactional data, etc. and is not limited to customer interactions over the World Wide Web. As previously noted, such separation of data elements may be accomplished using known techniques to any desired level of granularity, resulting potentially in multiple public and private data sets and in the combination of individually public data sets 103, 104 into a combined private data set 105.”), ¶31 (“Turning to FIG. 3 it is seen that a web form may generate a number of data sets 301*a-d* including demographics 301*a*, server data 301*b*, user data 301*c*, and cost data 301*d*. Any of these data sets may be designated as including private data, and the *remaining data sets* include public data.”), Figures 1, 2, 3.

288. In sum, Bossemeyer combined with Merenda renders obvious securing data (Bossemeyer’s and/or Merenda’s “**information**”) by extracting said security sensitive content (*e.g.*, Bossemeyer’s “**user’s medical history information 216**,” and “**insurance, doctors, prescriptions information 214**”) and extracting security sensitive words, characters or icons from said data to obtain extracted data (Bossemeyer’s “**restricted**” or “**limited-access data**” and/or Merenda’s **private data**) and remainder data (Bossemeyer’s “**unrestricted data**” and/or Merenda’s **public data**) therefrom.

289. Bossemeyer combined with Merenda also renders obvious securing data (Bossemeyer’s and/or Merenda’s “**information**”) by parsing said data

including security sensitive content (e.g., Bossemeyer's "user's medical history information 216," and "insurance, doctors, prescriptions information 214") and extracting security sensitive words, characters or icons from said data to obtain extracted data (Bossemeyer's "restricted" or "limited-access data" and/or Merenda's private data) and remainder data (Bossemeyer's "unrestricted data" and/or Merenda's public data) therefrom.

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

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

290. As I explained in Section X.A.1.iii (above), Bossemeyer discloses and, alternatively, renders obvious these limitations. Bossemeyer combined with Merenda renders obvious these limitations for the same reasons discussed in Section X.A.1.iii (above) and as explained below.

291. To the extent that Patent Owner argues that Bossemeyer does not teach these limitations, Merenda discloses parsing data into public data (e.g., remainder data) and private data (e.g., extracted data) and storing that data as respective public data sets (e.g., remainder store) and private data (e.g., extract stores).

292. Merenda discloses that its data stores are preferably databases. *See* EX1006 (Merenda), ¶24 (“The public 101 and private 102 data sets are, in a preferred embodiment, relational databases such as DB2 (DB2 is a registered trademark of IBM Corporation.”). A POSITA, however, would have understood that these claims are not limited to databases and other suitable storage systems and techniques may be used. *See also* Sections V.B and V.C (above).

293. As I explained in Sections X.B.1.i.a, X.B.1.i.b, and X.B.1.ii (above), Merenda discloses separating the data elements at any desired level of granularity resulting in multiple private data sets. *See* EX1006 (Merenda), ¶24 (“As previously noted, such separation of data elements may be accomplished using known techniques to *any desired level of granularity*, resulting potentially in multiple public and private data sets and in the combination of individually public data sets 103, 104 into a combined private data set 105.”).

294. Merenda also contemplates providing differing levels of access, including determining access level on an element-by-element basis. A POSITA would have understood that when access to some sensitive information can be granted, but not access to other (more) sensitive information, that this represents at least two different security levels. *See, e.g.*, EX1006 (Merenda), ¶29:

[T]he present invention contemplates that provision of access to the data elements in the *private data set* may be made on an element-by-

element basis, that is to say, that the merchant may be provided with access to certain select pieces of private data within the single data record 214, such as the *contact information (name, address, phone number, e-mail)* but not to other sensitive data such as *revenue, credit card* etc..”).

295. In sum, Bossemeyer combined with Merenda renders obvious storing said extracted data (e.g., Bossemeyer’s *credit history 218, medical history 216, charge/bank accounts 220, and insurance doctor’s prescriptions 214*) and said remainder data (e.g., Bossemeyer’s *digital wallet 210* and *medical alerts 212*) in said respective *extract stores* (e.g., stores for Bossemeyer’s “*restricted access data*” and “*limited access data*” and/or Merenda’s *private data*), corresponding to an associated security level and said remainder store (e.g., store for Bossemeyer’s “*unrestricted data*” and/or Merenda’s *public data*), respectively.

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

296. As I explained in Section X.A.1.iv (above), Bossemeyer discloses and, alternatively, renders obvious these limitations. Bossemeyer combined with Merenda renders obvious these limitations for the same reasons discussed in Section X.A.1.iv (above) and as explained below.

297. To the extent that Patent Owner argues that Bossemeyer does not teach this limitation, Merenda discloses providing partial access to data (for example,

access to public data or access to a subset of public and private data) and/or providing complete access to the data.

298. As an initial matter, a POSITA would have understood that a system such as Bossemeyer or Merenda 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 and/or Merenda disclose(s) 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.

299. Merenda discloses providing access to public data (*e.g.*, remainder data) without restriction. EX1006 (Merenda), ¶7 (“The public records would be available without restriction for read access by a population of merchants.”).

300. Merenda also discloses accessing fully reconstructed data by combining the public and private data when the requester provides a certain predetermined security clearance. For example, a predetermined security clearance can be satisfied when the consumer has indicated that the requester, such as a merchant, can access private data. *Id.*, ¶7 (“The private records would be **available**

only per the indication of the consumer to the merchant in the population.”). See also EX1006 (Merenda), ¶10:

*[U]pon designation by the consumer, the various logically linked records in public and private tables for that consumer may be collected and assembled into an output Web page.... The merchant for whom access has been indicated is provided either via e-mail or otherwise, with a hyperlink to the coded URL **thereby enabling the selected merchant to access both the public and private data.***

301. Merenda also discloses accessing reconstructed (combined) data. See EX1006 (Merenda), ¶30:

[T]he **combined information** including the contact information from the private data set and the technical data from the public data set may be provided to the merchant by way of a customized Web page using a uniform resource locator (URL) that includes the command required for accessing the restricted data set.

302. In addition, Merenda discloses providing access to fully or partially reconstructed data based on any desired level of granularity. See EX1006 (Merenda), ¶29:

It is useful to note that the present invention contemplates that provision of access to the data elements in the private data set may be made **on an element-by-element basis**, that is to say, that the merchant may be provided with access to certain select pieces of private data within the single data record 214, such as the contact information (name, address,

phone number, e-mail) but not to other sensitive data such as revenue, credit card etc..

303. Merenda describes passcode mechanisms that, for example, permit users to share their private data with select merchants, thus enabling the reconstruction of data. *See also* EX1006 (Merenda), ¶¶8-9:

Upon entering the data the consumer may be prompted to indicate whether they wish to provide merchants with access to their private data. This may, in a preferred embodiment, take the form of a box on the Web form which may be checked to indicate that the consumer wishes to be contacted. The consumer may be offered and [sic] opportunity to choose among the population of merchant the *select merchant to whom they wish their private data to be provided*.

Once selected, in accordance with an embodiment of the invention, the *merchants may be provided with a pass code*, which may in a preferred implementation, be the key value linking the public and private data records in their respective data sets. With the pass code *the merchants are provided with the ability to view the particular consumers private data record in the private data set*.

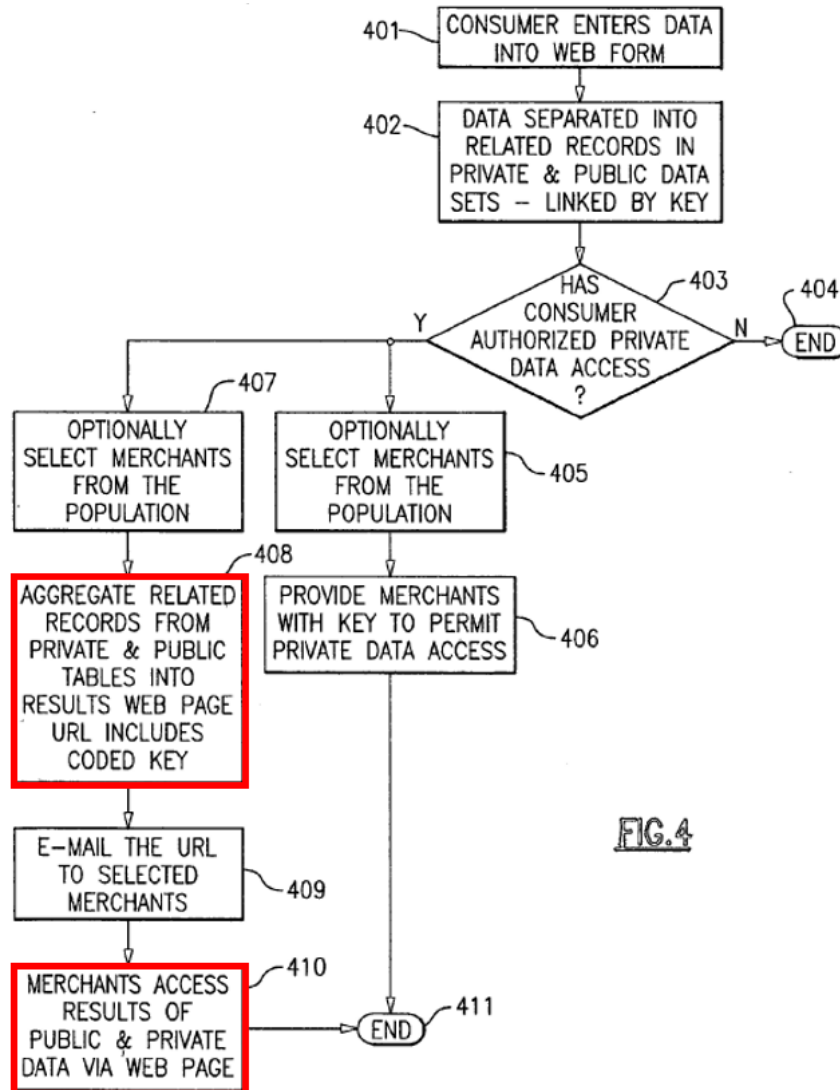
304. Merenda describes how the split but logically linked data can be assembled (reconstructed) later on and presented into an output Web page. A POSITA would have understood that if a merchant is presented with information on a web page, that the presentation would include previously split information that has now been merged. *See* EX1006 (Merenda), ¶10:

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

305. Similarly, Merenda discloses aggregating information from private and public tables into a Web page and allowing selected merchants access to the aggregated (reconstructed) information. *See* EX1006 (Merenda), ¶36, Figure 4:

The remaining steps in accordance with the embodiment in FIG. 3 are similar: Once again the consumer may optionally select among the population of merchants with access to the public data, certain merchants to whom they wish to grant private data access 407 or access may be granted globally. *Next in step 408 the various tables of data 302a-d which may contain private or public information are aggregated into a query result web page having a URL* which is coded with an identifier which in a preferred embodiment is the key value 123456789876 used to logically relate the records in the various tables 302a-d. In step 409 those vendors for whom access has been indicated by the consumer in step 407 are provided with an e-mail including a hyperlink to the key-coded URL through which *the merchant may*

access 410 the results of the combined consumer data. The process is then ended 411.



EX1006 (Merenda), Figure 4.

306. In sum, Bossemeyer combined with Merenda renders obvious permitting full or partial reconstruction (e.g., Bossemeyer's and/or Merenda's presenting data to the terminal/web page) of said **data** via one or more of said subsets of *extracted data* from respective *extract stores* and *remainder data*.

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

307. As I explained in Section X.A.1.v (above), Bossemeyer discloses and, alternatively, renders obvious these limitations. Bossemeyer combined with Merenda renders obvious these limitations for the same reasons discussed in Sections X.A.1.v, X.B.1.i.e, and X.B.1.iv (above) and as explained below.

308. To the extent that Patent Owner argues that Bossemeyer does not teach this limitation, Merenda discloses providing partial access and/or complete access to the data only in the presence of predetermined security clearance for a respective security level. As I discussed in Sections X.A.1.v (above) and X.B.2 (below), Merenda discloses that private data sets can be assigned different security levels.

309. For example, a POSITA would have understood that in Merenda, a person requesting information (e.g., a merchant) can have access *only to certain portions of the private information*. In other words, after a merchant is “provided with access” (e.g., **a first predetermined security clearance**) to selected private data sets, the merchant can access those selected private data sets (e.g., private data sets having a **first security level**, such as **name, address, phone number, e-mail**). But, without further authorization (e.g., **a second predetermined security clearance**), a POSITA would have understood that the merchant *does not have access to other*

private data sets (e.g., private data sets requiring a *second (higher) security level*, such as *revenue, credit card*). See EX1006 (Merenda), ¶29:

It is useful to note that the present invention contemplates that provision of access to the data elements in the private data set may be made on an element-by-element basis, that is to say, that *the merchant may be provided with access to certain select pieces of private data within the single data record 214*, such as the contact information (*name, address, phone number, e-mail*) *but not to other sensitive data* such as *revenue, credit card* etc..

310. In Merenda, the predetermined security clearance can be in the form of an indication, designation, or explicit direction by the owner of the information, e.g., a consumer. EX1006 (Merenda), ¶7 (“The private records would be *available only per the indication of the consumer* to the merchant in the population.”), ¶10 (“[U]pon *designation by the consumer, the various logically linked records in public and private tables for that consumer may be collected and assembled into an output Web page....* The merchant for whom access has been indicated is provided either via e-mail or otherwise, with a hyperlink to the coded URL *thereby enabling the selected merchant to access both the public and private data.*”), ¶25 (“The present invention is directed toward providing the level of control 108 required in keeping the public and private data separate, and *allowing access to the private data either at the explicit direction of the consumer 109* (the individual that

is the subject of the public and private data) or in such a manner as to protect the privacy concerns of the consumer.”); ¶¶8-10, 23-26, 29-30, 34-36.

311. The predetermined security clearance can also be in the form of a pass code provided to a merchant. EX1006 (Merenda), ¶9 (“[T]he merchants may be provided with *a pass code*... With the pass code the merchants are provided with the ability to view the particular consumers private data record in the private data set.”).

312. In sum, Bossemeyer combined with Merenda renders obvious permitting the reconstruction only in the presence of predetermined security clearance (Bossemeyer’s “*user authorization code* or *user identification code*” and/or Merenda’s “*indication*,” “*designation*,” or “*explicit direction*”) corresponding to said to said associated security level (Bossemeyer’s and/or “*restricted access*,” “*limited access*” and/or Merenda’s *private data*) for said respective extract stores (Bossemeyer’s *insurer server, health provider server, and bank server*).

2. Reasons To Combine Bossemeyer With Merenda

313. A POSITA would have been motivated to combine Bossemeyer and Merenda to parse user data that includes private and non-private elements using a parsing algorithm, as taught by Merenda, in Bossemeyer’s system, to extract the private elements and subsequently store them separately from the non-private elements, for at least the five reasons I discuss below. My discussion below applies

to the entirety of Grounds 2, 4, and 6 regarding the combination of Bossemeyer with Merenda.

314. A POSITA would have understood that to “parse” is to segment or break up the data. *See* EX1001 (the ’987 Patent), 39:8-10 (“The parsing algorithm, as stated earlier, targets the plaintext document or data object 100 and splits, cuts and *segments (that is, parses)*...”). *See also* EX1028 (Microsoft Dictionary), p. 333 (“**parse** *vb.* To break input into smaller chunks so that a program can act upon the information.”).

315. **First**, the combination of Bossemeyer and Merenda represents the use of known techniques according to known methods in the same way to yield predictable results. Bossemeyer and Merenda relate to the same field of providing multiple users access to information, and both Bossemeyer and Merenda address the same problem of controlling access to secure information. *Compare* EX1005 (Bossemeyer), 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*.”) and 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”) *with* EX1006 (Merenda), Claim 1 (“A method for accessing *data records* in a *private data set having restricted access*, the records in the private data set being accessible only by authorized *users*.”).

316. The Bossemeyer and Merenda combination would merely involve using Merenda's data parsing technique (parsing algorithm) in Bossemeyer's system, both of which were known, according to Merenda's methods for separating private and non-private elements within user data.

317. For example, Bossemeyer's system separates security sensitive content (private data) from public data and stores the private and public data in a database, while allowing the owner of the data to control access to the data. *See* EX1005 (Bossemeyer), 2:17-20 ("The central database server 10 is a centralized partitioned database server which partitions information both in terms of the smart card application as well as the accessibility of the information."), 1:49-52 ("With a centralized server architecture, data related to an individual can be accessed by an individual smart card, predefined groups of smart card users, or the general public."), 2:28-30 ("Private or proprietary information is partitioned such that the owner of the information has control over how the information is transferred and used."), 2:38-40 ("Different user identification codes, or data pointers, provided by smart cards 12 allow access to partitions in the database.").

318. In Bossemeyer's system, user data "can be classified as *public information* available to all the world; *limited access information* available to persons or selected groups with a user authentication code, or *proprietary information* accessible only by the owner of the information or a group with

privileges to that directory information....” EX1005 (Bossemeyer), 2:40-55.

Bossemeyer’s Figure 3 provides examples of the type of information stored in Bossemeyer’s system, wherein the “information is stored in three levels of security:

unrestricted, *limited access*, and *restricted*.” *Id.*, 5:6-9, Figure 3:

	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	

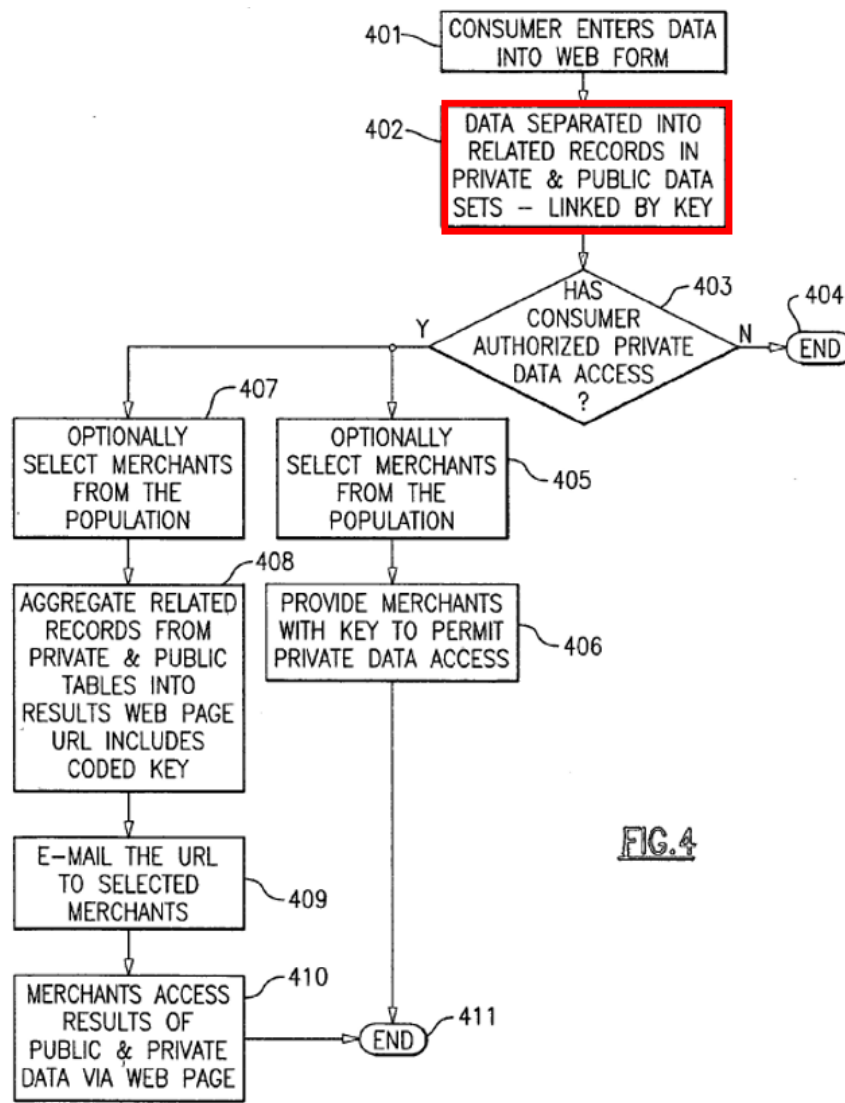
FIG. 3

See also, EX1005 (Bossemeyer).

319. Merenda similarly discloses a way of separating user data using a parsing technique which separates private and public elements and allows control over access to the private and public elements. See EX1006 (Merenda), ¶23 (“Fundamental to the implementation of the present invention is the notion that *a set*

*of data may be parsed into private and non-private elements.”), ¶25 (“As a result of the distribution of data elements among various public and private data sets, **it is desirable to establish a level of control over access to the public and private data stored therein**.... The present invention is directed toward providing the level of control 108 required in keeping the public and private data separate, and allowing access to the private data either at the explicit direction of the consumer 109 (the individual that is the subject of the public and private data) or in such a manner as to protect the privacy concerns of the consumer.”), ¶26 (“The public data set does not impose any access restrictions to its viewing audience 206. Other items of information, [may be] designated as ... private data elements 207 and as such will be stored separately in a private data set 208 which imposes certain restrictions on access by the viewing audience 206.”)*

320. Merenda’s Figure 4 illustrates that “[i]n step 402 the entered data is separated and inserted as data records in public and private data sets which records are linked by a common key value assigned thereto and which may be stored in the tables as part of the record.” EX1006 (Merenda), ¶34, Figure 4:



321. Moreover, the combination would merely use Merenda's methods of entering data such as using a Web form, in Bossemeyer's system, where both teach populating data by the user's actions. *Compare* EX1005 (Bossemeyer), 5:23-31:

Data is stored in the server in several ways. ***Merchant profiles become populated when a merchant subscribes to the service.*** Default profiles can exist for merchants until a sufficient number of transactions occur through that merchant to provide network use information which may

be relevant to the system. Similarly, *the user data becomes populated when the user subscribes as part of the smart card activation process.* Additional data is created as the user and the merchants interact with the system.

with EX1006 (Merenda), ¶7:

In an embodiment of the invention, *data entered by a consumer into a Web form is separated into related records in a public and private data set.* The public records would be available without restriction for read access by a population of merchants. The private records would be available only per the indication of the consumer to the merchant in the population. The records may, in an embodiment, be logically linked by the inclusion of a common key value into each of these records to indicate, for example, that these records emanated from a common source.

322. Merenda further describes in detail the usefulness of data entry by a user, where the user can also indicate preferences on security of the data. See EX1006 (Merenda), ¶31 (“*Each time a new customer enters web form data, a record is created* in the respective DB2 tables 302a-d associated with the segmented data 301a-d.”), ¶34 (“In step 401 a consumer enters data into a web form. In step 402 the entered data is separated and inserted as data records in public and private data sets....”), ¶8 (“Upon entering the data *the consumer may be prompted to indicate whether they wish to provide merchants with access to their private data.*”)

This may, in a preferred embodiment, take the form of a box on the Web form which may be checked to indicate that the consumer wishes to be contacted.”), ¶26 (“In a first embodiment of the invention, illustrated in FIG. 2, *a consumer 201, upon entering information to a Web page 202, is given an option 203 to designate that they wish to be contacted regarding the particular Web transaction....*”), ¶32 (“The related *records* in these tables *may be aggregated through a tool 303 which, in response to a designation by the consumer who has entered the data* (John Doe in our example) will aggregate the related records in the various tables 302*a-d* into an output web page 304 which will present an analysis of the data that will entice the customer to request that he be contacted by a merchant.”).

323. ***Second***, a POSITA would have been motivated to combine Bossemeyer with Merenda, because Merenda identifies a known problem (*e.g.*, controlling access to private information) and provides a solution to address the problem (*e.g.*, parsing user data to extract the private elements and store private elements and non-private elements in separate memory stores).

324. Both Bossemeyer and Merenda acknowledge the problems with mass information sharing and the importance of data security, for example when merchants attempt to access user information to conduct business. *Compare* EX1005 (Bossemeyer), 3:5-18 (“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 The network smart card server *acts as a secured gatekeeper to such information* and the smart card acts as the enabling key.”) and 5:9-22 (“*In the pharmacy example*, once the user’s authentication code and merchant code have been verified by the system, *the pharmacist may have access* to the user’s digital wallet 210, medical alerts 212, and insurance and prescription information 214. Without further authorization, however, the pharmacy *would not have access* to the user’s medical history 216.... Similarly, 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*. ... In contrast, a loan officer at a bank or automotive dealership would be allowed to access to the user’s credit history 218 as well as the user’s financial account balances 220.”) with EX1006 (Merenda), ¶5:

From the foregoing it can be seen that solutions which provide a *means for merchants to make use of customer data while still protecting the privacy interests of individual user’s engender considerable interest from the participants in the Internet economy*. ... the solution should provide the requisite flexibility to allow an Internet user to proactively indicate their desire to selectively provide their private data to selected merchants while their public data (i.e., *data which does not reasonably compromise the privacy concerns of the user*) is provided to the general audience of merchants on the Internet. Another desirable

feature of such a system would be the ability to *enable a merchant to target an unidentified consumer via access to such public data*, and to provide a “blind” access to private data enabling the merchant to perform target marketing to the unknown consumer based upon public data and the “blind” private data access. Finally, the system should provide access to the private database for performing data mining operations or other types of analysis which do not expose the individual records therein and accordingly *raise no privacy concerns. At the present such a system does not exist, and its absence has created a difficult commercial landscape for on-line merchants.*

325. A POSITA would have known that when users consider security measures, they decide on how much security or what level of security to have. While each of Bossemeyer and Merenda provide security measures, their combination yields better, more versatile, and stronger security, thus better control of access to private information. For example, a home owner can start with a simple key to lock their home, and then add more locks and keys to increase the security, then add security cameras and burglar alarms to increase security even further, followed by adding a tall fence around the property, and so on. Merenda’s parsing technique adds security to Bossemeyer’s system in a similar way.

326. Merenda explicitly discloses parsing data to extract private elements and store the private elements separately from non-private elements, thereby controlling access to sensitive/proprietary information. EX1006 (Merenda) ¶23

(“[A] set of data may be *parsed* into private and non-private elements. At the most simplistic level this might entail, for example, identifying input fields on a Web page as requiring sensitive data input such as an address, credit card or social security number, versus non-sensitive information such as the name of the item being purchased, the date, time etc.”), ¶14 (“FIG.1 illustrates a set of data elements *parsed* into private and public data sets.”). This would have been a motivation known to a POSITA in the field of providing users with access to information; it also improves the technology, by ensuring that access to the sensitive/proprietary information is only limited to specific users (e.g., merchants that have been granted access to the information).

327. **Third**, a POSITA would have been motivated to use Merenda’s parsing technique to identify private elements within user data, because it would improve Bossemeyer’s system for controlling access to sensitive/proprietary information. Using Merenda’s technique to improve Bossemeyer’s system would enable the splitting or separation of private and non-private elements where “such separation [can occur] at *various levels of sophistication and granularity...*” EX1006 (Merenda), ¶23. That is, the combination would merely be a use of a known technique (e.g., parsing user data) to improve similar methods (e.g., controlling access to information) in the same way (e.g., by allowing access to information at the appropriate granularity level).

328. As discussed in Section X.B.1.i.e (above), Bossemeyer discloses extracting security sensitive content in terms of the data's level of security or accessibility. Adding Merenda's teachings of parsing user data to identify various private elements would be an improvement to the security and access control afforded to users of Bossemeyer's system, because it would allow the versatile separation of the private elements "at various levels of sophistication and granularity..." (EX1006 (Merenda), ¶23) and therefore could allow a greater number of security levels to correspond to the different private elements as needed. For example, implementing Merenda's technique in Bossemeyer's system could allow access to groups of users (*e.g.*, merchants) that, otherwise, would not have access to portions of the user data (*e.g.*, merchants not having access to revenue, medical, or other unrelated private data).

329. A POSITA would have understood that Merenda's splitting data into more levels of granularity would enable better security than Bossemeyer alone, because data could be controlled more granularly. For example, all medical records could be split into sensitive (*e.g.*, blood type, useful for blood banks seeking blood donors), moderately sensitive (*e.g.*, cholesterol medications taken, useful for pharmacists refilling prescriptions), and highly sensitive (*e.g.*, terminal disease diagnosis that patients often keep secret).

330. This finer grained security separation also comports with a POSITA's understanding of the "least privilege" principle, which states "Do not give [] any more power than they need."—meaning that security is improved when various entities are given the least amount of privilege needed to accomplish the task. EX1032 (Cheswick), p. 163. *See also* Section V.D above. *Compare* EX1006 (Merenda), ¶29:

Once the consumer 201 has selected the set of merchants with whom contact is desired, a number of mechanisms may be employed to *provide access to the designated merchants*. In a preferred embodiment, the merchants may be provided with a [sic] the value of the key XXXXXX identifying the records 213, 214 with which access to the designated contact information may be enabled. It is useful to note that the present invention contemplates that provision of access to the data elements in the private data set may be made on an element-by-element basis, that is to say, that the merchant may be provided with access to *certain select pieces of private data* within the single data record 214, such as the contact information (name, address, phone number, e-mail) *but not to other sensitive data* such as revenue, credit card etc..

with 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.

331. Moreover, the combination of Bossemeyer and Merenda would also permit users of Bossemeyer's system to enter data more conveniently using Merenda's techniques (*e.g.*, web form entry) and to indicate user preferences such as whether the user wishes to be contacted by select merchants. *See, e.g.*, EX1006 (Merenda), ¶31, ¶34:

A flow diagram 400 provided in FIG. 4 illustrates the steps undertaken in practicing the foregoing embodiments. In step 401 a consumer enters data into a web form. In step 402 the entered data is separated and inserted as data records in public and private data sets which records are linked by a common key value assigned thereto and which may be stored in the tables as part of the record. ***At decision point 403 it is determined whether the consumer has indicated (via an entry on the web form or otherwise) a desire to be contacted by a merchant (or for that matter more specifically a willingness to permit a view of their private data).*** If the consumer has indicated a desire to have their private data remain private, the "no" path is traversed and [sic] the process is ended 404. Alternatively, if the consumer indicates that their

data may be accesses [sic] the “yes” path is traversed and the process continues either in accordance with the embodiment described in FIG. 2 (steps 405-406) or FIG. 3 (steps 407-410).

332. *Fourth*, a POSITA would have been motivated to combine Bossemeyer with Merenda, because the combination would involve applying a known technique (e.g., using Merenda’s parsing of user information and data entry) to a known device (e.g., Bossemeyer’s network arrangement with a central database server storing user information), which was ready for improvement to yield predictable results.

333. For example, it would be a trivial change to implement Merenda’s parsing technique to separate the data that is provided to Bossemeyer’s system, which already includes a central database server that separates data and can store data in the server in several ways. *See* EX1005 (Bossemeyer), 2:17-20 (“The central database server 10 is a centralized partitioned database server which partitions information both in terms of the smart card application as well as the accessibility of the information.”), 5:23-31 (“Data is stored in the server in several ways. ... [T]he user data becomes populated when the user subscribes as part of the smart card activation process. Additional data is created as the user and the merchants interact with the system.”).

334. Merenda discusses different ways of parsing data entered by a user into private and non-private elements, from simplistic to more sophisticated ones.

EX1006 (Merenda), ¶23 (“Fundamental to the implementation of the present invention is the notion that *a set of data may be parsed into private and non-private elements*. At the most simplistic level this might entail, for example, identifying input fields on a Web page as requiring sensitive data input such as an address, credit card or social security number, versus non-sensitive information such as the name of the item being purchased, the date, time etc.. At a more sophisticated level this notion might entail the combination of otherwise non-sensitive data elements into a combined sensitive data construct.”), ¶8 (Upon entering the data the consumer may be prompted to indicate whether they wish to provide merchants with access to their private data.”).

335. *Fifth*, Merenda provides express motivations that would have led a POSITA to combine Merenda’s and Bossemeyer’s teachings. Merenda acknowledges that “[t]he incredible growth of the Internet has provided ready access to a wealth of information. The World Wide Web is an ever-expanding repository of information spanning any and all conceivable topics limited only by the imagination of the information content provider.” EX1006 (Merenda), ¶3.

336. However, Merenda recognizes that “ready access to a wealth of information” can come with a cost of privacy. *See* EX1006 (Merenda), ¶3 (“The overwhelming benefits attendant to this ubiquity, however, are *counterbalanced to*

some extent by the inevitable loss of privacy associated with accessing a global computer network.”). See also EX1006 (Merenda), ¶4:

As the Internet evolves into the dominant commercial medium, merchants seeking to leverage data about Internet user’s to better focus their marketing efforts must do so in a manner that *respects the privacy interests of their intended customer*. Such interests have been the focal point of messages from leaders in government and in the high technology industry. The common theme being that in order to assure the unimpeded commercial growth of the Internet, it is vital that the *protection of individual privacy interests is accorded paramount importance*.

337. Merenda provides examples of the benefits of its methods for respecting the privacy interests of the public. For example, Merenda illustrates that companies would be incentivized to utilize a data system with a higher level of security. *See EX1006 (Merenda), ¶4:*

In fact, many leading technology companies refuse [sic] do business on-line with firms that do not have a satisfactorily articulated policy on privacy concerns. Industry-backed organizations such as Trust-E help businesses and consumers *ensure that they are dealing with companies that have placed the proper importance on on-line privacy rights*. Moreover, recent *public outcries over intrusive Internet advertising practices are cautionary tales for overzealous Internet marketers*.

338. In another example, Merenda teaches that a user's private information will be available to merchants only if the user indicates that a particular merchant can access their private information. *See* EX1006 (Merenda), ¶7:

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

See also EX1006 (Merenda), ¶8 (“Upon entering the data the ***consumer may be prompted to indicate*** whether they wish to provide merchants with access to their private data.”).

339. In fact, Merenda's method allows consumers to allow access to private data only to selected merchants among the available merchants. EX1006 (Merenda), ¶8 (“The consumer may be offered and [sic] opportunity to choose among the population of merchant the select merchant to whom they wish their private data to be provided.”). Merenda's disclosed method also allows merchants to data mine or statistically process the customer's private information. *Id.*, ¶12 (“In an exemplary embodiment the merchants ... are provided with the ability to data mine or statistically process the whole of the private data set while being restricted from reading any of the individual data records therein.”), ¶5 (“[T]he system should

provide access to the private database for performing data mining operations or other types of analysis which do not expose the individual records therein and accordingly raise no privacy concerns.”).

340. ***Finally***, a POSITA would have found that Bossemeyer and Merenda were analogous to the '987 Patent. All three pertain to the same field of endeavor, *i.e.*, securing security-sensitive information. *Compare* EX1001 (the '987 Patent), 6:48-58 (“It is an additional object of the present invention to enable the user to establish (a) the scope of the security sensitive words, characters or icon, data objects, (b) the future use ... of a filter enabling extraction of security sensitive data, (c) the selection of storage locations ... for extracted data and remainder or common data and (d) one or multiple levels of security limiting full reconstruction and enabling partial reconstruction of the extracted data and the remainder or common data.”) *with* EX1005 (Bossemeyer), 1:8-11 (“This invention relates to smart card applications and, more particularly, to a network arrangement to provide access to an architecture that supports a variety of advanced smart card applications.”), 1:44-47 (“[T]he present invention describes a network arrangement which is readily accessible from different types of smart card terminals supporting various smart card applications.”) *and* EX1006 (Merenda), ¶2 (“The present invention in [sic] relates in general to the field of data processing, and in particular to a method, system and program product for allowing the viewer of a public data set to access related records

in a private data set based upon a link which may be selectively provided to the viewer to authorize such access.”).

341. To the extent that Patent Owner argues that the references are not in the same field of endeavor as the '987 Patent, Bossemeyer and Merenda are still reasonably pertinent to the particular problem with which the purported '987 Patent's invention is involved, *i.e.*, securing digital information. *Compare* EX1001 (the '987 Patent), 6:30-33 (“It is an object of the present invention to provide a data security system, and information processing system and a method for securely storing data and rebuilding that data in the presence of an adequate security clearance.”), 7:3-5 (“It is an object of the present invention to parse, disperse and reconstruct the data or data object thereby enabling secure storage of the data.”) *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).”) *and* EX1006 (Merenda), ¶23 (“Fundamental to the implementation of the present invention is the notion that a set of data may be parsed into private and non-private elements.”), ¶37 (“The separation of data into public and private data sets creates a volume of public data which is generally usable

by the viewing public 206. This data has value by itself for marketing purposes, as it can be used for data mining to spot trends, in IT purchasing etc.”).

342. A POSITA would also have had a reasonable expectation of success in combining Bossemeyer with Merenda. Combining Bossemeyer with Merenda would merely involve including known data entry methods (*e.g.*, Merenda’s user’s web form entry), parsing user data in Bossemeyer’s system using Merenda’s more flexible and granular parsing, and storing private elements within the user data according to their respective security level in Bossemeyer’s various extract stores. EX1006 (Merenda), ¶23 (“Fundamental to the implementation of the present invention is the notion that *a set of data may be parsed into private and non-private elements.*”).

343. Merenda provides different ways for such parsing, all of which are within the reach of a POSITA. *See* EX1006 (Merenda), ¶23:

... At the most simplistic level this might entail, for example, identifying input fields on a Web page as requiring sensitive data input such as an address, credit card or social security number, versus non-sensitive information such as the name of the item being purchased, the date, time etc. ... At a more sophisticated level this notion might entail the combination of otherwise non-sensitive data elements into a combined sensitive data construct.

344. In fact, Merenda acknowledges that the exact mechanics of the parsing technique is not critical, as long as appropriate separation is achieved. This would suggest to a POSITA that different ways of parsing that were available and known to a POSITA can be employed for separating the data. *See* EX1006 (Merenda), ¶23:

... For purposes of the present invention the mechanics by which the various data elements are parsed into sensitive and public data sets is not critical, however the notion that such separation, at various levels of sophistication and granularity can, and does occur, is essential to the practice of the invention.

3. Dependent Claims 6 and 21

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

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

345. As I explained above in Section X.A.1 (above), Bossemeyer renders obvious claims 1 and 16. *See* Section X.A.1 (above). Bossemeyer in combination with Merenda renders obvious this limitation for the same reasons as discussed in Section X.B.2 (above).

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

346. As I explained above in Section X.A.1 (above), Bossemeyer discloses this limitation. *See* Section X.A.1 (above). Bossemeyer in combination with

Merenda renders obvious this limitation for the same reasons as discussed in Sections X.B.2 and X.B.1.v (above) and as explained below.

347. Specifically, Merenda discloses a method for securing data by separating the data into *public* and *private*, or sensitive, data sets and allowing access to the data based on predetermined security clearances. EX1006 (Merenda), ¶25 (“As a result of the distribution of data elements among various public and private data sets, it is desirable to establish a level of control over access to the public and private data stored therein.”).

348. In Merenda, public data may be accessible without restriction, while private or sensitive data would only be accessible based on the predetermined level(s) indicated, for example, by the consumer (*e.g.*, the individual who provides the data) or the level of control indicated for the data set. *See* EX1006 (Merenda), ¶25:

For purposes of the present invention it will suffice to assume that *a public data set is available, without restriction*, to the entire population of Internet users, or, as will more likely be the case, to a select subset of merchants 107 who subscribe to a marketing service that accumulates such data. With the public data elements, however, as opposed to data elements in the private data sets, there are no discrete access restrictions in place which would prevent a general member of the potential population from viewing the data from undertaking such access. The present invention is directed toward providing the level of

control 108 required in keeping the public and private data separate, and *allowing access to the private data either at the explicit direction of the consumer 109 (the individual that is the subject of the public and private data) or in such a manner as to protect the privacy concerns of the consumer.*

349. Merenda further clarifies the difference between public and private data sets. *See also* EX1006 (Merenda), ¶26:

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

350. Merenda discloses several embodiments where, for example, third-party applications could access public and private data without violating the consumer's privacy. EX1006 (Merenda), ¶10:

In another embodiment of the invention upon designation by the consumer, the various logically linked records in *public and private tables* for that consumer may be collected and assembled into an output Web page. The Web page is provided at a uniform resource locator (URL) which has been coded with the common key value linking the related records or with another pass code. The merchant for whom access has been indicated is provided either via e-mail or otherwise,

with a hyperlink to the coded URL thereby enabling the selected merchant to access both the public and private data.

351. In another example, Merenda describes limiting read access to the private data record to protect the consumer's privacy. EX1006 (Merenda), ¶¶11-12:

In yet another set of embodiments, read access is not provided to the private data record, however, an application with access to the private data allows the merchant to make use of the data without being able to read the data. In this manner the consumer need not decide whether or not to allow some or all of the merchants to view their private data, however all of the merchants are given the advantage of the *ability to use the private data without compromising the privacy of the consumer*.

In an exemplary embodiment the merchants are afforded unrestricted read access to the data records in the public data set and are provided with the ability to data mine or statistically process the whole of the private data set while being restricted from reading any of the individual data records therein.

352. Merenda explains other methods for allowing merchants to use the private data while protecting consumer privacy. EX1006 (Merenda), ¶13:

In another embodiment the merchants are provided with read access to the data records in the public data set, and based on such read access may make a request of an application which has access to the related

private data records in the private data sets. The application permits the merchants to use data in the related private records to target, customize and transmit marketing materials to the consumer audience based on their public data and using ***but not revealing their private data***. In this manner the consumer population is benefited by a system which respects their privacy interests and the merchant population is permitted to make use of the large and growing pool of data available about their potential customers.

353. Merenda describes mechanisms to split (extract) data into private and non-private parts, as well as combine (reconstruct) the data later on as needed. EX1006 (Merenda), ¶23:

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

which the various data elements are parsed into sensitive and public data sets is not critical, however the notion that such separation, at various levels of sophistication and granularity can, and does occur, is essential to the practice of the invention.

354. Merenda describes mechanisms for permitting access to sensitive data.

EX1006 (Merenda), ¶¶34-35:

A flow diagram 400 provided in FIG. 4 illustrates the steps undertaken in practicing the foregoing embodiments. In step 401 a consumer enters data into a web form. In step 402 the entered data is separated and inserted as data records in *public and private* data sets which records are linked by a common key value assigned thereto and which may be stored in the tables as part of the record. At decision point 403 it is determined whether the consumer has indicated (via an entry on the web form or otherwise) a desire to be contacted by a merchant (or for that matter more specifically a willingness to permit a view of their private data). If the consumer has indicated a desire to have their private data remain private, the “no” path is traversed and [sic] the process is ended 404. Alternatively, if the consumer indicates that their data may be accessed [sic] the “yes” path is traversed and the process continues either in accordance with the embodiment described in FIG. 2 (steps 405-406) or FIG. 3 (steps 407-410).

The remaining steps in accordance with the embodiment for FIG. 2 are as follows: The consumer may optionally select 405 particular merchants from the population of merchants with access to the public

data set 205. Of course, the consumer may merely indicate that they wish their data to be *accessible or restricted* on a global basis as well. The selected merchants are provided with a key which enables them to access the private information 406. Optionally, the key may be the logical link between the data in the public and private data sets. The process is then ended 411.

355. Next, Merenda discloses, or at least renders obvious, a plurality of security levels for the private data sets. For example, a person requesting information (*e.g.*, a merchant) can have access only to certain segments of the private information. That is, a merchant can access certain selected private data sets (*e.g.*, private data sets having a first security level, such as *name, address, phone number, e-mail*), but cannot access other private data sets (*e.g.*, private data sets having a second (higher) security level, such as *revenue, credit card*). A POSITA would have understood that when access to some sensitive information can be granted, but not access to other (more) sensitive information, that this represents at least two different security levels. *See* EX1006 (Merenda), ¶29:

It is useful to note that the present invention contemplates that provision of *access to the data elements in the private data* set may be made on an element-by-element basis, that is to say, that *the merchant may be provided with access to certain select pieces of private data within the single data record 214*, such as the *contact information (name,*

address, phone number, e-mail) but *not to other sensitive data* such as *revenue, credit card etc..*

356. As discussed in Section X.B.2 (above), a POSITA would have been motivated to combine Bossemeyer with Merenda and would also have had a reasonable expectation of success in combining Bossemeyer with Merenda.

357. In sum, Bossemeyer combined with Merenda renders obvious establishing a plurality of security levels (Bossemeyer's and/or Merenda's "*public limited access, restricted*" security levels, or *public, private, or sensitive data*) each with a respective security clearance (Bossemeyer's "*user identification code*," "*authorization code*," or "*restrictions*" and/or Merenda's "*indication*," "*designation*," or "*explicit direction*").

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

358. As I explained above in Section X.A.1 (above), Bossemeyer discloses this limitation. *See* Section X.A.1 (above).

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

359. As I explained above in Section X.A.1 (above), Bossemeyer discloses this limitation. *See* Section X.A.1 (above).

4. Dependent Claim 9

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

360. As I explained above in Section X.A.1 (above), Bossemeyer renders obvious claim 1. *See* Section X.A.1 (above). Bossemeyer in combination with Merenda renders obvious this limitation for the same reasons as discussed in Section X.B.2 (above).

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

361. As I explained above in Section X.A.1 (above), Bossemeyer discloses and, alternatively, Bossemeyer renders obvious this limitation. Bossemeyer in combination with Merenda renders obvious this limitation for the same reasons as discussed in Section X.A.1 (above).

5. Dependent Claims 11 and 23

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

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

362. As I explained above in Section X.A.1 (above), Bossemeyer renders obvious claims 10 and 22. *See* Section X.A.1 (above). Bossemeyer in combination with Merenda renders obvious this limitation for the same reasons as discussed in Section X.B.2 (above).

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

363. As I explained above in Section X.A.1 (above), Bossemeyer renders obvious this limitation. Bossemeyer in combination with Merenda renders obvious this limitation for the same reasons as discussed in Sections X.B.1.i.b, X.B.1.ii, X.B.1.iii, and X.B.1.iv (above) and as explained below.

364. I note that the '987 Patent does not describe what it means by “parsing ... granularly.” A POSITA would have understood that the granularity of data can be any, from fine to coarse and anything in between. See EX1028 (Microsoft Dictionary), p. 206 (“**granularity** *n.* A description, from ‘coarse’ to ‘fine’, of a computer activity or feature (such as screen resolution, searching and sorting, or time slice allocation) in terms of the size of the units it handles (pixels, sets of data, or time slices). The larger the pieces, the coarser the granularity.”). Absent additional information, the term “granularly” in these two claims appears to be superfluous, a nonce. A POSITA would have therefore understood that the data that Bossemeyer and/or Merenda parses is necessarily at *some* granularity (*e.g.*, fine, coarse), because it is smaller than the whole of the original data prior to parsing.

365. Specifically, Merenda explicitly discloses parsing the data elements at any desired level of granularity resulting in multiple private data sets. See EX1006 (Merenda), ¶24 (“It is of course understood that the source of such data may come

from any number of sources, including without limitation, surveys, transactional data, etc. and is not limited to customer interactions over the World Wide Web. As previously noted, such separation of data elements may be accomplished using known techniques to *any desired level of granularity*, resulting potentially in multiple public and private data sets and in the combination of individually public data sets 103, 104 into a combined private data set 105.”); EX1006 (Merenda), ¶23 (“[T]he notion that such separation, *at various levels of sophistication and granularity can*, and does occur, is essential to the practice of the invention.”).

366. Merenda further discloses providing differing levels of access, including determining access level on an element-by-element basis. EX1006 (Merenda), ¶29:

[T]he present invention contemplates that provision of access to the data elements in the *private data set* may be made on an element-by-element basis, that is to say, that the merchant may be provided with access to certain select pieces of private data within the single data record 214, such as the *contact information (name, address, phone number, e-mail)* but not to other sensitive data such as *revenue, credit card* etc..”).

367. In sum, Bossemeyer combined with Merenda renders obvious the step of parsing the data granularly.

6. Dependent Claims 15 and 27

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

368. As I explained above in Section X.A.1 (above), Bossemeyer renders obvious claims 10 and 22. *See* Section X.A.1 (above). Bossemeyer in combination with Merenda renders obvious this limitation for the same reasons as discussed in Section X.B.2 (above).

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

369. As I explained above in Section X.A.1 (above), Bossemeyer renders obvious claims this limitation. Bossemeyer in combination with Merenda renders obvious this limitation as I explain below. *See* Section X.B.2.

370. At the outset, I note that the claimed “further data security step” does not impose a narrowing limitation on the claimed “data.” That is, the “data” will either exist (stored with or without encryption) or will not exist (get destroyed).

371. Moreover, I understand that one may meet this claim by practicing only one option out of a group of three: (1) data stored unencrypted, (2) data stored encrypted, or (3) data is destroyed. For the reasons I explained in Section X.A.5.ii, a combined Bossemeyer/Merenda system would meet all three options; nevertheless,

such a system would also meet the third option (data destruction) in light of Merenda, as I explain below.

372. I begin this discussion by establishing that Merenda discloses user data entry methods, and that Bossemeyer could use those methods. In Section X.A.1 (above), I explained how Bossemeyer meets at least the elements of parsing, storing, and permitting reconstruction. I note that Bossemeyer discloses that “the user data becomes populated when the user subscribes as part of the smart card activation process.” EX1005 (Bossemeyer), 5:28-30. Similarly, Merenda discloses that a user enters data through a website on the user’s computer device. EX1006 (Merenda), ¶7 (“[D]ata entered by a consumer into a Web form is separated into related records in a public and private data set.”). A POSITA would have recognized the similarities between Bossemeyer and Merenda: in both cases, some raw user data is ingested initially, then separated or split into one or more public and private data sets.

373. Moreover, Merenda discloses that the user data provided by the user is “separated” into parts, like Bossemeyer. See EX1006 (Merenda), ¶7:

[D]ata entered by a consumer into a Web form *is separated* into related records in a public and private data set. The public records would be available without restriction for read access by a population of merchants. The private records would be available only per the indication of the consumer to the merchant in the population.

See also EX1006 (Merenda), ¶23:

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

374. As an example, Merenda explains that a user can input data in a web form although the methods are not limited to the World Wide Web. Merenda further discloses that techniques to separate data into different parts were well known. See EX1006 (Merenda), ¶24:

FIG. 1 illustrates such *a distribution of data which may emanate from a customer input source* such as common gateway interface (CGI) fields on *a Web page* 100 into public 101 and private 102 data sets. It is of course understood that *the source of such data* may come from any number of sources, including without limitation, surveys, transactional data, etc. and *is not limited to customer interactions over the World Wide Web*. As previously noted, *such separation of data elements may be accomplished using known techniques* to any desired level of granularity, resulting potentially in multiple public and private data sets and in the combination of individually public data sets 103, 104 into a combined private data set 105. The public 101 and private 102 data sets are, in a preferred embodiment, relational databases such as DB2 (DB2 is a registered trademark of IBM Corporation).

375. Merenda provides examples where the entered data is separated. EX1006 (Merenda), ¶34 (“In step 402 the entered data is separated and inserted as data records in public and private data sets....”), Figures 1, 4.

376. A POSITA would have understood that using a website and the Internet was a ubiquitous way of signing up to different services from different providers. Thus, it would have been obvious to a POSITA to use Merenda’s method of entering user data through a website when a user subscribes to Bossemeyer’s smart card services.

377. Having established that Merenda discloses user data entry methods, and that Bossemeyer could use those methods, I now explain how Merenda also meets the third, data-destruction option. Consider first an original data set D that got ingested, and then parsed into two parts: X (public) and Y (private). Merenda discloses that X and Y (or parts thereof) can be later merged/reconstructed to (fully or partially) reproduce part or even all of the original data; let’s call that reconstructed data set D’. Given that with X and Y, one can generate D’ to reproduce all of what D originally had, there is little reason to keep the original D around. A POSITA would have understood that after a successful ingestion, D can be deleted to save space and minimize the risk of exposure, should the original D be compromised.

378. Therefore, a POSITA would have reasonably inferred that the user data, including the originally entered (ingested) data, is later destroyed because it could always be reconstructed by later “aggregate[ing]” its separated elements. EX1006 (Merenda), ¶32:

The related records in these tables may be aggregated through a tool 303 which, in response to a designation by the consumer who has entered the data (John Doe in our example) will ***aggregate the related records*** in the various tables 302a-d into an output web page 304 which will present an analysis of the data that will entice the customer to request that he be contacted by a merchant. The consumers information will be made accessible to a merchant with whom the designated contact is designated, for example, by way of an e-mail 305 provided to the merchant and including a hyperlink to the key-coded URL. Via the key-coded URL the merchant may access the query page 306 including the combined related records for John Doe joined by the logical relationship of the key value 123456789876. In a preferred embodiment the Web access to ***this combined table data*** may be accomplished by use of the IBM Net.Data software product.

379. Moreover, the destruction would have been needed to preserve the privacy of the user signing up for Bossemeyer’s smart card services, when, for example, the user signs up for services from public computers. For example, in the combined Bossemeyer/Merenda system, the user data, being moved from the user’s

computer device to the central database server would cease to exist in its original form (which I denoted as “D” in the above example).

380. The destruction (*e.g.*, in the user’s computer) is independent of parsing, storing, and reconstruction using parsed data (*e.g.*, that occurs in the central database). Indeed, deletion of the original data, after the data is processed, was well known in the art. *See, e.g.*, EX1001 (the ’987 Patent), 24:1-2 (“Deletion systems are known to persons of ordinary skill in the art.”); EX1025 (Aichelen), 6:57-60 (“After the object is copied and restriped across all of the volumes of the expanded array, the original copy of the object can be deleted which allows the space to be reclaimed without disrupting operations.”). Therefore, a POSITA would have understood that the entered user data is destroyed.

381. In sum, Bossemeyer combined with Merenda renders obvious a further data security step of one from the group of storing said data without encryption (*e.g.*, in Bossemeyer’s smart card), storing said data with encryption (*e.g.*, in Bossemeyer’s smart card) and destroying said data (*e.g.*, in Bossemeyer’s smart card, entered from a website as taught by Merenda). The further data security step is independent of said parsing, storing and permitting reconstruction.

C. Ground 3: Claim 9 Is Obvious Over Bossemeyer With Chaganti

1. Dependent Claim 9

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

382. As I explained above in Section X.A.1 (above), Bossemeyer renders obvious claim 1. *See* Section X.A.1 (above).

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

383. As I explained above in Section X.A.1 (above), Bossemeyer discloses and, alternatively, Bossemeyer renders obvious this limitation. Moreover, Bossemeyer in combination with Chaganti renders obvious this limitation as I explain below.

384. I note that this claim can be met by just one of extracting, storing, or permitting reconstruction. Bossemeyer renders obvious all three as discussed below.

385. Chaganti discloses “assessing a charge for extracting, storing or permitting reconstruction.”

386. First, Chaganti discloses a computer system, for example, a Personal Information Repository Service Provider (PIRSP), for storing personal information assigned with a plurality of security levels and providing the information upon a request. *See, e.g.*, EX1007 (Chaganti), 2:23-43:

In one aspect, the present invention is directed toward a method of [sic] for automatically disbursing personal information belonging to a user

to a requester that is authorized by the user by transmitting said personal information from a server computer operated by a service provider, said server computer coupled to a database, the method comprising the steps of establishing an account for the user with the server computer; assigning an identifier to the user; ***entering personal information belonging to the user***, said personal information comprising at least one of a plurality of information objects; ***assigning at least one of a plurality of security levels to each information object***; storing in the database the user identifier, the information object and the security level assigned to the information object; receiving a request message from the requester, said request message comprising at least the user identifier; ***retrieving from the database the information object pertaining to the user identifier***; securely transmitting the information object to the requester. In a further aspect, the invention comprises the steps of presenting an authorization by the requester; and verifying the requester's authorization.

387. Chaganti discloses an example of the PIRSP, in relation to its Figure 2 of a system, that provides for securing information. *See also* EX1007 (Chaganti), 5:29-42:

Referring to FIG. 2, the steps included in a preferred embodiment of the invented system are described. During an initialization step (step 200), in a preferred embodiment, ***a Personal Information Repository Service Provider (PIRSP) operates the server computer 100***. In alternative embodiments, there is no service provider such as the PIRSP; and there are other methods of providing such service, such as

establishing a personal web site for each user 103, said personal web site comprising information that can be accessed only by an authorized requester 105 in a secure manner; establishing a personal database coupled either directly to the Internet or accessible via the Internet or other communication network; or retrieving information stored elsewhere manually or in an automatic fashion.

388. Second, Chaganti discloses that the operation of its system is based on assessing and charging fees to users or data requestors to store and/or reconstruct information. EX1007 (Chaganti), 5:43-56:

Preferably, the PIRSP makes it known to a user 103 that it provides a trusted information repository service. In preferred and alternative embodiments, the PIRSP announces that its *services are available* free, or *for a fee*, and in the latter case, *the fee is calculated based on a per transaction basis, or on a subscription basis, either from users that store information or from entities that request such information*. Other embodiments comprise direct or vicarious *payment methods for utilizing the services* provided by the PIRSP. These payment methods include an agreement between the PIRSP and the user 103 to generate additional or alternative sources of revenue for the PIRSP via advertisements, referrals, introductions, chain marketing methods and the like.

389. Chaganti describes that the user can select a variety of payment plans to pay for the charged fees for storing and extracting information in its multi-level security system. *See* EX1007 (Chaganti), 9:1-14:

The user account management module 112 optionally allows the user 103 to select *a payment plan for the services rendered by the PIRSP*, block any request if the user 103 is in default of a payment, obtain credit card or other verification, and the like. In a preferred embodiment, the payment plans for the user 103 depend on the number of security classifications the user 103 has chosen, the number and nature of the information objects stored by the user 103, the number of requests for information received, the number of accesses or updates made by the user 103 to view and/or change the information objects, the type of customer service requested, the number of entities to which any changes are to be notified, the resources utilized by the user 103, or a combination of these and similar types of activities.

390. For example, Chaganti discloses extracting information and that its system is a multi-level security system. *See* EX1007 (Chaganti), 3:44-49 (“[T]he CGI programs 107 are configured to perform other tasks such as communicate with a database 108 coupled to the server computer 100, and *extract or store information* in the database 108 according to the software instructions provided within the server computer 100 or in the packets received from the network 102.”), 9:33-39 (“After the user 103 fills out the web page forms displayed on the client computer 100, the

web pages are transmitted to the server computer 100, whereupon the CGI programs 107 receive, *parse*, and deliver portions of data to the database interface module 130 which stores portions of data entered by the user 103 as information objects in the database 108 in appropriate tables.”), 10:23-25 (“Other methods of ensuring security include establishing access control lists for each level of a *multi-level security system....*”).

391. Similarly, Chaganti describes that the requesters who seek to access the data in the PIRSP use a payment plan to pay for the fees charged for accessing the stored information that a POSITA would have understood would occur by reconstruction. *See* EX1007 (Chaganti), 10:30-42:

In a preferred embodiment, potential requesters are also enrolled by the PIRSP in a similar manner as described for the user 103 (step 214). The server computer 100 establishes accounts for potential *requesters*, allocates identifiers, authenticates their trustworthiness and enables them to *establish a payment/billing plan for accessing information objects stored by the user 103*. In one embodiment, where there are a number of users, statistical information, rather than individual pieces of information objects is offered for sale to potential requesters. In other embodiments, the potential requesters do not establish accounts with the PIRSP, and will pay as they go for each access of information as described below.

392. Finally, Chaganti describes several charging models: by object received, according to a subscription, or statistically. *See* EX1007 (Chaganti), 12:52-67:

In one embodiment, *the requester 105 is charged a fee for receiving the information objects, on a per-object basis, or on a subscription basis* or for receiving statistical reports. The PIRSP may provide an incentive to the user 103 by paying a portion of the fee to the user 103. In another embodiment, a requester may receive statistical report such as “how many male golf players between the ages 22 and 55 in the zip code 20006 are interested in trading stocks?” The statistics module 140 and report generation module 150 make appropriate queries in the database 108 and obtain the information. Preferably such statistical information is considered secure, unless it has a tendency to reveal too much about the private habits of the user 103. Thus, so long as information is aggregated and can remain anonymous, it will be released to potential requesters to assist marketing of products/services.

393. Accordingly, like Bossemeyer, Chaganti discloses an information storing and retrieving system with a plurality of security levels that assesses and charge fees to users and requesters. It would have been obvious to combine Chaganti’s teaching with Bossemeyer to assessing a charge for extracting, storing or permitting reconstruction. *See* Section X.C.2 (below).

2. Reasons To Combine Bossemeyer With Chaganti

394. A POSITA would have been motivated to include in Bossemeyer's system capabilities to assess and charge fees to generate revenue and improve the database of the computer system for securing data, including to share a portion of the revenue with the user, based on Chaganti's teaching. EX1007 (Chaganti), 5:52-56 ("These payment methods include an agreement between the PIRSP and the user 103 to generate additional or alternative sources of revenue for the PIRSP via advertisements, referrals, introductions, chain marketing methods and the like.").

395. The payments in Chaganti refer to fees based on a transaction, subscription basis, direct or indirect payment methods. *Id.* For example, fees assessed and charged to users are used to secure user data by extracting sensitive content and storing the data. EX1007 (Chaganti), 9:1-14, 5:43-56.

396. As another example, Chaganti explains that its system (*e.g.*, PIRSP) "may provide an incentive to the user 103 by paying a portion of the fee to the user 103," for example, to facilitate collecting information for a database and "assist marketing of products/services," where such a fee would be assessed and charged to requesters for reconstruction of secured data. *See* EX1007 (Chaganti), 12:52-67:

In one embodiment, ***the requester 105 is charged a fee for receiving the information objects***, on a per-object basis, or on a subscription basis or for receiving statistical reports. ***The PIRSP may provide an incentive to the user 103 by paying a portion of the fee to the user 103.***

In another embodiment, a requester may receive statistical report such as “how many male golf players between the ages 22 and 55 in the zip code 20006 are interested in trading stocks?” The statistics module 140 and report generation module 150 make appropriate queries in the database 108 and obtain the information. Preferably such statistical information is considered secure, unless it has a tendency to reveal too much about the private habits of the user 103. Thus, so long as information is aggregated and can remain anonymous, it will be released to potential requesters to assist marketing of products/services.

397. Indeed, charging a subscription fee was well known and a routine system design choice as taught by Bossemeyer and Chaganti. *See, e.g.*, EX1005 (Bossemeyer), 5:23-30 (“Merchant profiles become populated when a merchant subscribes to the service.... Similarly, the user data becomes populated when the user subscribes as part of the smart card activation process.”); EX1007 (Chaganti), 12:52-54 (“[T]he requester 105 is charged a fee for receiving the information objects, on a per-object basis, or on a subscription basis or for receiving statistical reports.”). A POSITA thus would have found it obvious to try and place and assessment and fee charging system in the computer system.

398. After all, the information that Bossemeyer’s and Merenda’s systems manage is highly valuable as much of it requires high security to maintain privacy. Therefore, a POSITA would have found that it made perfect sense for an operator of

such a system to try and monetize the access to such data (especially as much of this data could never be made fully public)

399. Moreover, a POSITA would have had a reasonable expectation of success to make the combination because it amounts to a simple combination of known techniques and components to build a system with a subscription on charge-by-transaction service. For example, systems for assessing and charging fees were known, as disclosed in Bossemeyer and Chaganti. *See, e.g.*, EX1005 (Bossemeyer), 5:23-31; EX1007 (Chaganti), 5:43-56, 10:30-42, 12:42-67.

400. Indeed, such systems were well known as shown in multiple references. For example, Paltenghe describes methods for charging a fee to merchants or service providers who request information stored in a computer system to facilitate efficient targeted marketing. *See* EX1021 (Paltenghe), ¶48:

FIG. 1 also shows a third type of data known as “dynamic demographic information data” which is kept in a value generation account 25. This file or account 35 is provided as a means for the consumer 25 to define certain demographic data, including a generic consumer profile, interests and hobbies, and the types of information the consumer would like to receive from third parties. This information is stored in the value generation account 35. ***Upon request by a third party merchant or service provider 27, a profile or aggregate of consumer information may be provided to the third party merchant or service provider by the information bank 23 for a fee.*** The profile or aggregate of information

about participating consumers will not provide information which identifies individual participating consumers, but will rather provide the third party merchant or service provider with sufficient information to determine if it will request that the information bank provide consumers with advertisements of its merchandise or services. Merchants or service providers 27 will likely agree to pay for this aggregate consumer data and for indirect access to the consumers whose information is contained in the data bank because *it will enable the merchant or service provider 27 to direct specific offers to a targeted market in an efficient manner.*

See also EX1021 (Paltenghe), ¶¶61-63.

401. Baker similarly describes charging a fee for collecting, organizing, and distributing data. *See* EX1022 (Baker), 8:64-67:

By participating in the massive archival of all firm data at a central service bureau 20, a service bureau 20 can organize all these data and coordinate dissemination of such data *for a rental fee or user fee.*

402. As another example, Clark discloses controlling access of data based on a fee system. *See* EX1023 (Clark), 6:59-63:

“To implement a peaceful mode the periodic key is transmitted along with the encrypted high precision navigational data from all satellites. When used in conjunction with the registration key this allows for *fee based* or commercial control of access to the high precision navigational data.

403. OceanStore also describes a fee system for accessing stored information. *See* EX1024 (OceanStore), p.1:

We envision a cooperative utility in which consumers *pay a monthly fee* in exchange for access to persistent storage.

404. Similar to Bossemeyer, Chaganti concerns multiple security levels and controlling the storing and access to secured information. *Compare* EX1005 (Bossemeyer), 2:40-50 (“The information... 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.”), 2:17-20 (“The central database server 10 is a centralized partitioned database server which partitions information both in terms of the smart card application as well as the accessibility of the information.”), 1:49-52 (“With a centralized server architecture, data related to an individual can be accessed by an individual smart card, predefined groups of smart card users, or the general public.”), 2:28-30 (“Private or proprietary information is partitioned such that the owner of the information has control over how the information is transferred and used.”) *with* EX1007 (Chaganti), 10:23-25 (“Other methods of ensuring security include establishing access control lists for each level of a multi-level security system.”), 9:22-32, 11:61-65 (“[N]umerical values representing security levels are also

assigned to the requester's computer...”), claim 1 (“a plurality of security levels”). Thus, a POSITA would have had a reasonable expectation of success to combine Bossemeyer and Chaganti because they are both directed to similar systems for securing information at multiple security levels.

405. To the extent that Patent Owner argues that Chaganti is not in the same field of endeavor as the '987 Patent, Chaganti is still reasonably pertinent to the particular problem with which the '987 Patent's invention is involved, *i.e.*, securing digital information. *Compare* EX1001 (the '987 Patent), 6:30-33 (“It is an object of the present invention to provide a data security system, and information processing system and a method for securely storing data and rebuilding that data in the presence of an adequate security clearance.”), 7:3-5 (“It is an object of the present invention to parse, disperse and reconstruct the data or data object thereby enabling secure storage of the data.”) *with* EX1007 (Chaganti), 2:18-22 (“The present invention is directed toward a method and system for gathering, storing personal information on a server computer and releasing such information to authorized requesters. Several types of information are stored for release to different entities with appropriate authorization.”), 3:44-49 (“[T]he CGI programs 107 are configured to perform other tasks such as communicate with a database 108 coupled to the server computer 100, and extract or store information in the database 108 according to the software instructions provided within the server computer 100 or in the

packets received from the network 102.”), 7:47-50 (“Tables to store such audit information are designed in the database 108, preferably in a secure partition reachable only by persons with a very high security clearance.”).

406. Accordingly, it would have been obvious to modify Bossemeyer to charge a fee for securing data (by extracting sensitive content), storing it, or reconstructing it, as taught by Chaganti. For the same reasons, it would have been obvious to modify the combined Bossemeyer/Merenda system for Ground 4 (see Section X.D below).

407. In sum, Bossemeyer combined with Chaganti renders obvious assessing a charge (*e.g.*, subscription fee) for extracting, storing or permitting reconstruction.

D. Ground 4: Claim 9 Is Obvious Over Bossemeyer With Merenda And Chaganti

1. Dependent Claim 9

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

408. As I explained above in Section X.A.1 (above), Bossemeyer renders obvious claim 1. *See also* Section X.A.1 (above). Bossemeyer in combination with Merenda renders obvious this limitation for the same reasons as discussed in Section X.B.2 (above).

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

409. As I explained above in Section X.A.1 (above), Bossemeyer discloses and, alternatively, Bossemeyer renders obvious this limitation. Bossemeyer in combination with Merenda renders obvious this limitation for the same reasons as discussed in Section X.A.1 (above).

410. Moreover, Bossemeyer in combination with Merenda and Chaganti renders obvious this limitation. It would have been obvious to modify the combine the Bossemeyer/Merenda system with Chaganti to charge a fee for securing data (by extracting sensitive content), storing it, or reconstructing it, for the same reasons as discussed in Sections X.C.1.ii and X.C.2 above.

E. Ground 5: Claims 15 And 27 Are Obvious Over Bossemeyer With Kohane

1. Dependent Claims 15 and 27

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

411. As I explained above in Section X.A.1 (above), Bossemeyer renders obvious claims 10 and 22. *See* Section X.A.1 (above).

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

412. As I explained above in Section X.A.1 (above), Bossemeyer renders obvious this limitation. Moreover, Bossemeyer in combination with Kohane renders obvious this limitation as I explain below.

413. At the outset, I note that the claimed “further data security step” does not impose a narrowing limitation on the claimed “data.” That is, the “data” will either exist (stored with or without encryption) or will not exist (get destroyed).

414. Moreover, I understand that one may meet this claim by practicing only one option out of a group of three: (1) data stored unencrypted, (2) data stored encrypted, or (3) data is destroyed. Nevertheless, below I show how Bossemeyer combined with Kohane renders obvious at least two of the three options.

415. Kohane discloses “a further data security step of one from the group of storing said data without encryption, storing said data with encryption and destroying said data,” where “said further data security step being independent of said parsing, storing and permitting reconstruction.”

416. *First*, Kohane discloses a networked computer system. The gateway server system 22 in the systems receives “object records” (e.g., user data such as dental, medical, legal information) from various agent systems, encrypts the records,

and sends them to servers 18 (e.g., remote storage locations). *See generally* EX1008 (Kohane), ¶¶24, 26, 32, 30, 37, 42.

417. Specifically, Kohane explains that “gateway server system 22 encrypts the record objects” to secure transmission to the servers 18, as illustrated in Figure 1 below. EX1008 (Kohane), ¶58:

The gateway server system 22 stores the record objects on the servers 18. ***Before transmitting the record objects to the servers 18, the gateway server system 22 encrypts the record objects.*** Thus, such record objects traverse the network 20 in encrypted form when the gateway server system 22 uploads the record objects to the server 18. The servers 18 store the record objects in this encrypted form. In addition, the record objects traverse the network 20 in this encrypted form when subsequently downloaded by the gateway server system 22. Consequently, ***the information in the record objects remain unintelligible to anyone who intercepts the transmission of the record objects between the gateway server system 22 and the server 18*** and does not possess the appropriate decryption key.

See also EX1008 (Kohane), Figure 1:

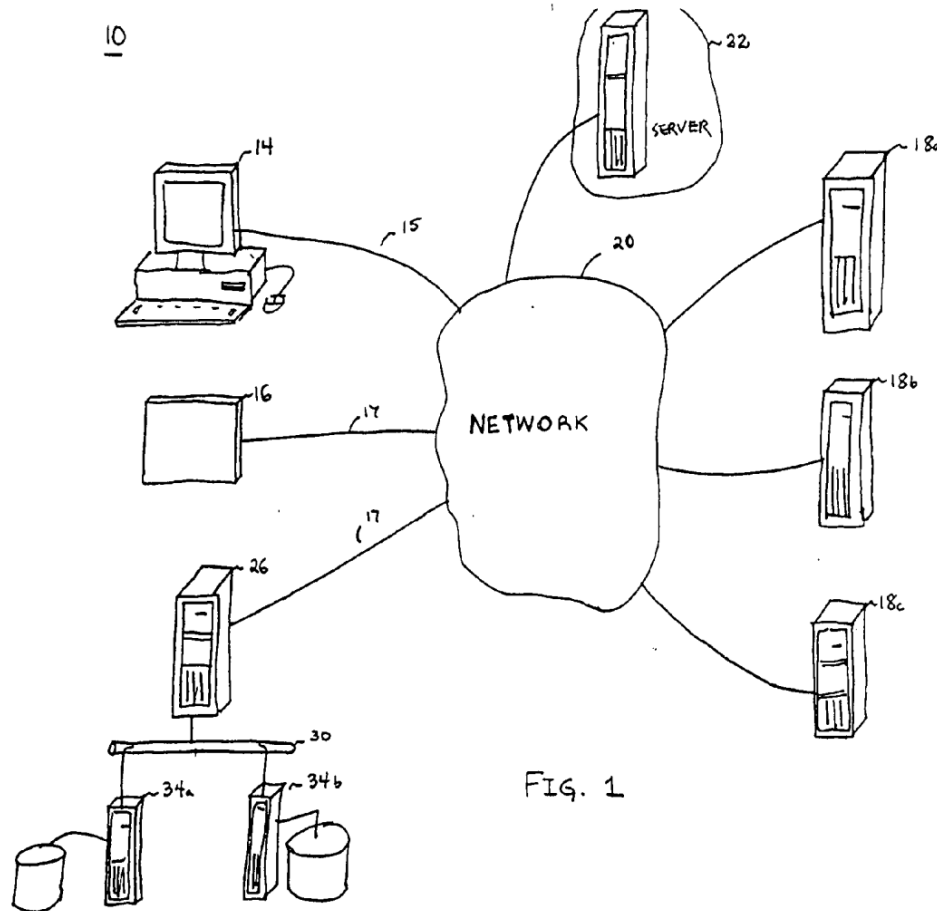


FIG. 1

418. Kohane further discloses that, “[o]n the gateway server system 22, *each record objects remains in encrypted form*” except when certain record objects are “decrypted” when an authorized agent accesses them. EX1008 (Kohane), ¶59:

On the gateway server system 22, each record objects remains in encrypted form except for those record objects that the authorized agent is privileged to access. Accordingly, not every record object may be decrypted, only those record objects for which the accessing agent retains a privilege. The gateway server system 22 possesses and uses the appropriate key to decrypt the record objects obtained from the

servers 18. The gateway server system 22 decrypts those record objects for subsequent transmission to the accessing agent.

419. Thus, Kohane discloses that the gateway server system 22 maintains the record objects only in encrypted form. A POSITA thus would have reasonably inferred that the original unencrypted data would have been deleted (destroyed) after encryption to ensure that such unencrypted (cleartext) data would never fall into the wrong hands. Accordingly, as discussed in Section X.E.2 (below), it would have been obvious to combine Bossemeyer and Kohane to store the user data with encryption and then destroy the unencrypted version for confidentiality and prevent unauthorized access of the data. For the same reasons, it would have been obvious to modify the combined Bossemeyer/Merenda system for Ground 6 (see Section X.F below).

420. **Second**, Kohane discloses that, in some examples, the agent systems (e.g., personal computer, smart card, measurement equipment) destroy (do not keep) its user data to secure information. EX1008 (Kohane), ¶63:

Data security can be enhanced at the agent systems 14, 16, 26 **by not storing any record objects at the agent systems** 14, 16, 26. Accordingly, after the agent completes reviewing the record object, **the agent system 14, 16, 26 deletes the corresponding information** from the respective agent system, including all downloaded files and cached copies of the downloaded Web page.

421. As discussed in Section X.E.2 (below), it would have been obvious to combine Bossemeyer with Kohane to meet this limitation. For the same reasons, it would have been obvious to modify the combined Bossemeyer/Merenda system for Ground 6 (see Section X.F below).

2. Reasons To Combine Bossemeyer With Kohane

422. A POSITA would have been motivated to encrypt the data and destroy the original unencrypted data to secure and maintain confidentiality when transmitting the parsed data between Bossemeyer's network smart card server and other remote databases (e.g., servers at credit card companies, insurers, health care providers). *See, e.g.,* EX1008 (Kohane), ¶58:

The gateway server system 22 stores the record objects on the servers 18. Before transmitting the record objects to the servers 18, the gateway server system 22 encrypts the record objects. Thus, ***such record objects traverse the network 20 in encrypted form when the gateway server system 22 uploads the record objects to the server 18.*** The servers 18 store the record objects in this encrypted form. In addition, the record objects traverse the network 20 in this encrypted form when subsequently downloaded by the gateway server system 22. ***Consequently, the information in the record objects remain unintelligible to anyone who intercepts the transmission of the record objects between the gateway server system 22 and the server 18 and does not possess the appropriate decryption key.***

423. Kohane further emphasizes the need for storing only encrypted data. EX1008 (Kohane), (“[T]he confidentiality of the information stored in the records is of utmost importance.”). A POSITA would have understood that the storing of encrypted data and destruction of the original unencrypted data are independent of parsing the user data, storing of, and reconstruction using the parsed data. A POSITA would also have been motivated to destroy the user data residing in the agent system devices (*e.g.*, smart card, personal computers) to reduce their needed storage capacity (*e.g.*, higher storage capacity costs more) and increase data security (*e.g.*, prevent unencrypted data from ever falling into the wrong hands). See EX1005 (Bossemeyer), 2:58-3:2:

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 and enables data to be shared across groups of cards that may be treated as a single unit.*** These pointers *facilitates* [sic] ***more complex applications which may otherwise require more resources than could be economically stored or transferred to the smart card 12.*** Thus, the network augments or replaces the amount of card memory typically associated with smart cards. This allows greater capacity than could otherwise be achieved by storing information on the cards alone.

424. Kohane similarly recognizes that security is improved by deleting data. *See also* EX1008 (Kohane), ¶63 (“Data security can be enhanced at the agent systems 14, 16, 26 by... delet[ing] the corresponding information.”).

425. A POSITA would have understood that the destruction of the user data in the agent system devices is independent of parsing the user data and storing of and reconstruction using the parsed data. In fact, it is well understood that the best way to protect data from ever being compromised is, somewhat counterintuitively, to never keep that data in the first place. This also comports with a POSITA’s understanding of the “least privilege” principle, which states “Do not give [] any more power than they need.”—meaning that security is improved when access to deleted data is nearly impossible. EX1032 (Cheswick), p. 163. *See also* Section V.D above.

426. A POSITA would have had a reasonable expectation of success in making the combination because it amounts to a simple combination of known techniques and components to encrypt information and remove unencrypted information to secure the system. Encryption techniques were well known in the art. *See, e.g.,* EX1008 (Kohane), ¶60 (“A commercially available Security protocol that the gateway Server System 22 can use to encrypt the record objects is SSL (Secure Sockets Layer).”); EX1005 (Bossemeyer), 3:36-38 (“The card memory also

preferably includes a user[']s 'certificate' or 'digital signature' as well as encryption capability."). *See also* Section V.D above.

427. A POSITA would also have had a reasonable expectation of success to make the combination because it amounts to a simple combination of known techniques and components for deleting information in computers. Such techniques were routine practice. *See, e.g.*, EX1001 (the '987 Patent), 24:1-2 ("Deletion systems are known to persons of ordinary skill in the art."); EX1025 (Aichelen), 6:57-60 ("After the object is copied and restriped across all of the volumes of the expanded array, the original copy of the object can be deleted which allows the space to be reclaimed without disrupting operations.").

428. Indeed, deleting user data residing in devices where the data is stored in remote servers was well known. EX1008 (Kohane), ¶63 ("[T]he agent system 14, 16, 26 deletes the corresponding information [(record objects)]..."), ¶41 ("Record objects, like the directory file representing the record, are stored on the servers 18.").

429. Moreover, similar to Bossemeyer, Kohane concerns providing multiple security levels and granting different privileges for accessing secured information, where access can be given using a smart card. *Compare* EX1005 (Bossemeyer), 2:40-50 ("The information... 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.”), 2:17-20 (“The central database server 10 is a centralized partitioned database server which partitions information both in terms of the smart card application as well as the accessibility of the information.”), 1:49-52 (“With a centralized server architecture, data related to an individual can be accessed by an individual smart card, predefined groups of smart card users, or the general public.”), 2:28-30 (“Private or proprietary information is partitioned such that the owner of the information has control over how the information is transferred and used.”) *with* EX1008 (Kohane), ¶76 (“For example, the privilege sections 86, 90 of Record-objects 84 and 88, respectively, give read, modify and annotate privileges to the record owner, read, delete, and annotate privileges to the group called ‘staff,’ and read privileges to the group called ‘other.’”), ¶49 (“The class of ‘other’ can be used, for example, to specify the privileges of the public or a research organization collecting data.”), ¶¶7 (“The agent system 14 can include a device (e.g., smart card reader, a fingerprint reader, etc.) to accept a token that authenticates the identity of the agent using the agent system 14.”), 26, 30, 61. Thus, a POSITA have had a reasonable expectation of success to combine Bossemeyer and Kohane because they use similar components to achieve a multilevel security storage system.

430. To the extent that Patent Owner argues that Kohane is not in the same field of endeavor as the ’987 Patent, Kohane is still reasonably pertinent to the

particular problem with which the '987 Patent's invention is involved, *i.e.*, securing digital information. *Compare* EX1001 (the '987 Patent), 6:30-33 ("It is an object of the present invention to provide a data security system, and information processing system and a method for securely storing data and rebuilding that data in the presence of an adequate security clearance."), 7:3-5 ("It is an object of the present invention to parse, disperse and reconstruct the data or data object thereby enabling secure storage of the data.") *with* EX1008 (Kohane), ¶5 ("The present invention features a system and method for maintaining confidential records of an individual on a network. Objectives of the invention are to maintain adequate confidentiality of the confidential records, mobility of the individual for accessing the records, security of the confidential records, control of the confidential records by the individual, and integration with institutional information systems."), ¶26 ("The agent system 14 is an exemplary embodiment of an agent system by which an agent can access records stored on the servers 18 according to the principles of the invention.").

431. Accordingly, it would have been obvious to combine Bossemeyer and Kohane to store the user data with encryption and then destroy the unencrypted version to improve confidentiality and to prevent unauthorized access of the data. Furthermore, it would have been obvious to delete the user data in the devices (*e.g.*, Bossemeyer's and/or Kohane's smart card, Kohane's personal computers)

connected to Bossemeyer's central database server, once the devices finish utilizing the data, as taught by Kohane. For the same reasons, it would have been obvious to modify the combined Bossemeyer/Merenda system for Ground 6 (see Section X.F below).

432. In sum, Bossemeyer combined with Kohane renders obvious a further data security step of one from the group of storing said data without encryption, storing said data with encryption (*e.g.*, in Bossemeyer's central database server) and destroying said data (*e.g.*, in Bossemeyer's central database server, Bossemeyer's and/or Kohane's smart card, Kohane's personal computers,). The further data security step is independent of said parsing, storing and permitting reconstruction.

F. Ground 6: Claims 15 And 27 Are Obvious Over Bossemeyer With Merenda And Kohane

1. Dependent Claims 15 and 27

i. [15pre] A method as claimed in claim 10 including

[27pre] A storage medium as claimed in claim 22 including

433. As I explained above in Section X.A.1 (above), Bossemeyer renders obvious claims 10 and 22. *See* Section X.A.1 (above). Bossemeyer in combination with Merenda renders obvious this limitation for the same reasons as discussed in Section X.B.1 (above). *See* Section X.B.1.

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

434. As I explained above in Section X.A.1 (above), Bossemeyer renders obvious this limitation. Bossemeyer in combination with Merenda renders obvious this limitation for the same reasons as discussed in Section X.A.1 (above).

435. Moreover, Bossemeyer in combination with Merenda and Kohane renders obvious this limitation. It would have been obvious to modify the combined Bossemeyer/Merenda system with Kohane to secure and maintain confidentiality, for the same reasons as discussed in Section X.E.1.ii.

XI. Conclusion

436. In my opinion, the challenged claims 1, 6, 9, 10-11, 15-16, 21-23, and 27 of the '987 Patent are unpatentable.

XII. Availability for Cross-Examination

437. 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

438. 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

439. 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.



Date: June 9, 2023

Dr. Erez Zadok