

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 IPR2023-00973

U.S. Patent No. 8,468,244

Claim 1

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	13
A. Claim Construction.....	14
B. Obviousness.....	15
C. Ordinary Skill in the Art.....	17
IV. Summary of Opinions.....	17
V. Technology Overview	18
A. General Computer Operations.....	18
B. Data Storage Devices and Systems	20
C. Networked and Distributed Storage Systems.....	21
D. File and Data Security, Security Levels.....	24
VI. Overview Of The '244 Patent.....	29
A. Prosecution History of the '244 Patent	33
VII. Overview Of The Prior Art.....	38
A. Redlich (U.S. Patent Publication No. US2003/0182435, "EX1005 (Redlich)").....	38
B. Ozzie (U.S. Patent No. 8,601,598, "EX1006 (Ozzie)").....	54
VIII. Level of Ordinary Skill in the Art	58

IX.	Claim Construction.....	58
A.	“means for identifying plurality of select content data stores for respective ones of a plurality of security designated data in said server cloud”.....	59
B.	“an extractor for extracting and storing said security designated data in respective select content data stores of said server cloud”	61
C.	“means for parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores”	64
D.	“means for applying a reconstruction data process employing said respective access controls to combine one or more of said security designated data and remainder data”	68
X.	Specific Grounds For Challenge.....	72
A.	Ground 1: Claim 1 Is Obvious Over Redlich.....	72
1.	Independent Claim 1	72
i.	Claim 1 Preamble	72
a.	[1pre-i] A distributed computer system for organizing and processing data, the data to be processed having select content represented by one or more predetermined words, characters, images, data elements or data objects,.....	72
b.	[1pre-ii] said distributed computing system having (a) a plurality of select content data stores in a server cloud for respective ones of a plurality of security designated data and (b) a plurality of granular data stores,.....	79
c.	[1pre-iii] each said select content data store and granular data store having respective access controls thereat, said plurality of data stores and	

	said server cloud operatively coupled over a communications network, ...	85
ii.	[1a] means for identifying plurality of select content data stores for respective ones of a plurality of security designated data in said server cloud;	89
iii.	[1b] an extractor for extracting and storing said security designated data in respective select content data stores of said server cloud;.....	94
iv.	[1c] a processor activating at least one of said select content data stores in said server cloud thereby permitting access to said select content data stores and respective security designated data based upon an application of one or more of said access controls thereat;	101
v.	[1d] means for parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores;.....	107
vi.	[1e] said processor having means for applying a reconstruction data process employing said respective access controls to combine one or more of <i>said security designated data</i> and remainder data.....	115
B.	Ground 2: Claim 1 Is Obvious Over Redlich With Ozzie	122
1.	Independent Claim 1	122
i.	Claim 1 Preamble	122
a.	[1pre-i] A distributed computer system for organizing and processing data, the data to be processed having select content represented by one or more predetermined words, characters, images, data elements or data objects,.....	122

- b. [1pre-ii] said distributed computing system having
(a) a plurality of select content data stores in a
server cloud for respective ones of a plurality of
security designated data and (b) a plurality of
granular data stores,.....122
- c. 266.[1pre-iii] each said select content data store
and granular data store having respective access
controls thereat, said plurality of data stores and
said server cloud operatively coupled over a
communications network, ...127
- ii. [1a] means for identifying plurality of select
content data stores for respective ones of a
plurality of security designated data in said server
cloud; 127
- iii. [1b] an extractor for extracting and storing said
security designated data in respective select
content data stores of said server cloud;.....128
- iv. [1c] a processor activating at least one of said
select content data stores in said server cloud
thereby permitting access to said select content
data stores and respective security designated data
based upon an application of one or more of said
access controls thereat; 128
- v. [1d] means for parsing remainder data not
extracted from said data to be processed and
storing the parsed data as data segments in
respective granular data stores;.....129
- vi. [1e] said processor having means for applying a
reconstruction data process employing said
respective access controls to combine one or more
of said security designated data and remainder
data.....129
- vii. Reasons To Combine Redlich With Ozzie.....129

XI. Conclusion	148
XII. Availability for Cross-Examination	148
XIII. Right to Supplement	149
XIV. Jurat.....	149

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. 8,468,244 (the “’244 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 ’244 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 '244 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. 8,468,244 to Redlich et al.
1002	Prosecution History of U.S. 8,468,244
1004	My <i>Curriculum Vitae</i>
1005	U.S. Patent Publication No. 2003/0182435 to Redlich et al.
1006	U.S. Patent No. 8,601,598 to Ozzie et al.
1011	U.S. Patent No. 9,015,301 (Continuation-in-part Application No. 11/746,440)
1012	U.S. Provisional Application No. 60/883,522
1013	U.S. Patent No. 5,960,080 to Fahlman et al. (“Fahlman”)
1014	U.S. Patent Publication No. 2008/0087756 to Hoffberg et al. (“Hoffberg”)
1015	Microsoft Computer Dictionary, Fourth Edition, Copyright 1999, Excerpts
1016	Beck et al., Linux Kernel Internals, 2nd Ed., Copyright 1998, pp. 148-187

Exhibit No.	DESCRIPTION
1017	DOD Standard, Department of Defense Trusted Computer System Evaluation Criteria, December 26, 1985 (“Orange Book”)
1018	Director of Central Intelligence Directive No. 1/16, Security of Compartmented Computer Operations (“CIA”)
1019	Cheswick et al., Firewalls and Internet Security, Copyright 1994, p. 163

30. I understand that the '244 Patent has a filing date of April 29, 2009, claiming priority to applications Nos. 11/746,440, filed May 9, 2007, and 60/883,522, filed January 5, 2007. *See* EX1001 (the '244 Patent), 1; EX1011 (Patent Application No. 11/746,440); EX1012 (Provisional Application No. 60/883,522). Therefore, I assume that the earliest possible priority date of the '244 Patent is January 5, 2007. I understand that all prior art references used in this declaration predate the earliest possible priority date of the '244 Patent of January 5, 2007. Thus, I have considered certain issues from the perspective of a person of ordinary skill in the art as described below as of January 5, 2007.

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.

36. I have been informed that patent claims can be drafted in a so-called “means-plus-function” form and that, in such situations, the proper claim construction must include the claimed “function” and the “corresponding structure” that is disclosed in the specification of the patent (and equivalents).

B. Obviousness

37. 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.

38. 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.

39. 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.

40. 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.

41. 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.

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

43. 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

44. 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.

45. 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

46. It is my opinion that claim 1 of the ’244 Patent is rendered obvious by the prior art identified below:

Ground	References	Invalid Claim
1	Redlich	1
2	Redlich, Ozzie	1

V. Technology Overview

47. 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 January 5, 2007.

A. General Computer Operations

48. 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.

49. 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.

50. 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.

51. 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

52. 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. EX1016 (Microsoft Dictionary), p. 372 (“RAM”).

53. 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. EX1016 (Microsoft Dictionary), p. 212 (“hard disk”).

54. 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. EX1016 (Microsoft Dictionary), p. 188 (“flash memory”).

55. Moreover, any single device (*e.g.*, a hard disk) can be logically broken down into several units called “partitions.” EX1016 (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.”).

56. 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. EX1016 (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

57. 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. EX1016 (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.”).

58. 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). EX1016 (Microsoft Dictionary), p. 424 (“storage area network”), p. 432 (“system area network”), p. 398 (“SCSI network”).

59. 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.

60. 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.

61. 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." EX1016 (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.").

62. 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. EX1016 (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.”).

63. One example of a popular distributed system is that of databases, where different components are often distributed, stored, and managed separately. EX1016 (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

64. All modern file and storage systems include measures of security to protect their data from unauthorized access. EX1016 (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.”).

65. The POSIX standard, first started in the late 1980s, codifies the access application program interfaces (APIs) that operating systems export to user applications. EX1016 (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.”).

66. A simple data protection scheme defines whether users can only read files, only write files, or have both read and write access. EX1016 (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.”).

67. 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).

68. 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. EX1016 (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.”).

69. ACLs existed in Unix systems since at least the 1990s (and I personally used them). EX1017 (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 []”).

70. 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. EX1016 (Microsoft Dictionary), p. 323 (Orange Book).

71. 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.” EX1018 (Orange Book), p. 111.

72. The Orange Book detailed how data of different security levels has to be stored in separate compartments or locations, for example level C1. EX1018 (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. [].”

73. 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. EX1013 (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 [].”

74. 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).

75. Similarly, the U.S. National Security Agency (NSA) defined its own standard called the “Red Book”, again defining multiple security levels. EX1016 (Microsoft Dictionary), p. 377 (“Red Book”).

76. 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”).

77. 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).

78. 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

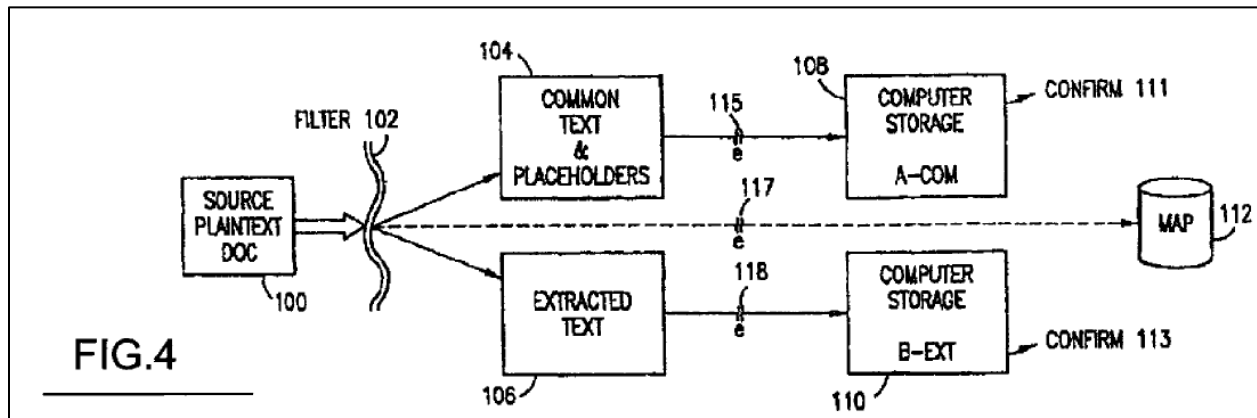
salespersons will not have access to that file. In such a way, a two-level security hierarchy is created, with sales-managers being logically at a higher security level than sales-people. The same mechanism can be used to create an arbitrarily long set of security levels.

79. 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 '244 Patent

80. The '244 Patent relates to “information management data processing modules and computer software system and method enabling protection of confidential information, identification of such information, identification of select content, classification for the same, and security system for the same.” EX1001 (the '244 Patent), 1:15-19. The '244 Patent purports to create a new system that is used to protect security sensitive content in a distributed computer system by storing the data in data stores in a server cloud and permitting access based upon an application of access controls. EX1001 (the '244 Patent), Abstract. According to the '244 Patent, prior systems did not adequately “automatically categorize[] information in unstructured information files and label[] the same and permit[] the enterprise to establish a policy for that information and implement the policy recommendation with specific actions to ensure that the information is properly handled, distributed,

retained, deleted (document retention) and otherwise managed.” EX1001 (the '244 Patent), 2:55-61. Figure 4, below, illustrates the disclosed information management system:



EX1001 (the '244 Patent), Figure 4.

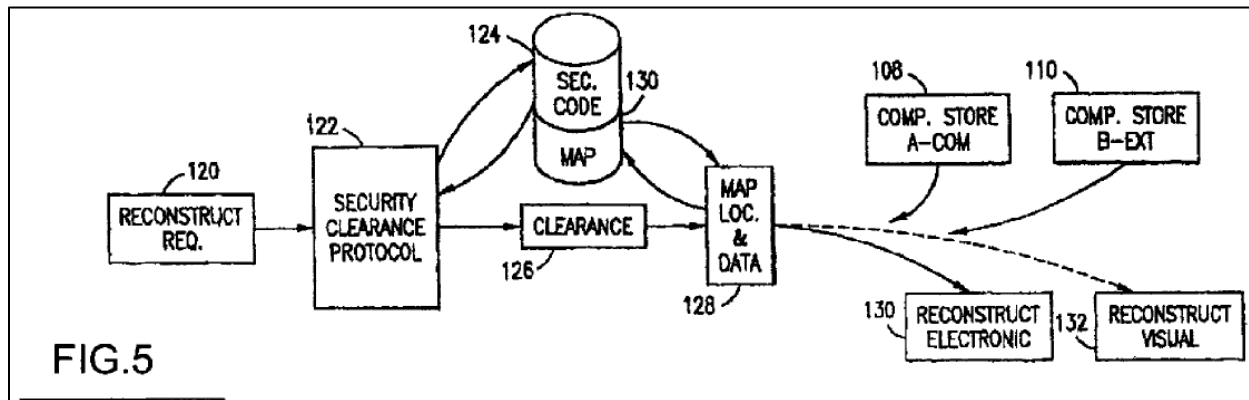
81. As shown, a source document 100 is sent to a filter 102 that “separates out common text or remainder data 104 from uncommon text, words, characters, or icons.” EX1001 (the '244 Patent), 435:40-42. Remainder data is the common text or data that is not extracted by the system. EX1001 (the '244 Patent), 435:42-44, 435:60-61, 442:33-36. The remainder data file 104 may “include[] place holders which enables the extracted data to be easily inserted or set back into the remainder data file.” EX1001 (the '244 Patent), 435:61-64. After the data is passed through the filter, the “security sensitive” words, characters, or icons are separated from remainder or common text 104 as extracted text 106. EX1001 (the '244 Patent), 435:40-44.

82. After the data is separated, it is placed in storage. EX1001 (the '244 Patent), 442:65-67. For storage, "the common text or the remainder data is stored in common storage memory 108." EX1001 (the '244 Patent), 443:2-3. "The extracted data file 106 is stored in a different memory computer storage 110," but is preferably stored at a "different location than computer storage memory segment 110." EX1001 (the '244 Patent), 443:17-20.

83. The security system is compatible with multiple security levels. EX1001 (the '244 Patent), 461:54-62, 490:1-4. "For select content systems having multiple security levels of importance (which may be multiple security levels or multiple levels of SC importance ...), a plurality of filters would be created, each filter associated with a different SC level." EX1001 (the '244 Patent), 461:54-60. Having multiple security levels "require[s]... a plurality of extracted data documents 106... [where] each extracted data document 106 would be stored in a respective, separate computer memory segment [] 110." EX1001 (the '244 Patent), 444:23-29. Having separate storage for extracted data of different security levels is "one of the many important features of the present invention." EX1001 (the '244 Patent), 444:29-32.

84. To enable secure storage of the data, the system reconstructs the data or data object that was previously in storage. EX1001 (the '244 Patent), 442:1-10.

Figure 5, shown below, illustrates the major features of the reconstruction routine/system.



EX1001 (the '244 Patent), Figure 5.

85. 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 '244 Patent), 447:2-7. 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 '244 Patent), 447:8-12. 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 '244 Patent), 447:12-14. "[M]ap 130 show[s] the location of [extracted and remainder] memory segments." EX1001 (the '244 Patent), 447:18-19. 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 ‘244 Patent), 447:29-31.

A. Prosecution History of the ‘244 Patent

86. I have reviewed the file history of the ‘244 patent. EX1002 (‘244 Prosecution History). I summarize the relevant information that I have reviewed pertaining to my opinion.

87. The ‘244 Patent was filed as U.S. Ser. No. 12/453,124 on April 29, 2009. EX1001 (‘244 Patent), 1. The application was filed with 4 total claims, containing 2 independent claims. EX1002 (‘244 Prosecution History), 1065-1066.

88. On November 24, 2010, the Examiner issued a non-final office action. First, the Examiner found that provisional application “60/883522 [] does not disclose or provide adequate support/description of several limitations claimed. Therefore, this application has not been accorded the priority date of the provisional application.” EX1002 (‘244 Prosecution History), 2221.

89. Second, the Examiner rejected claims 1-4 as not patently distinct from the claims of other patents and/or applications with common ownership. EX1002 (‘244 Prosecution History), 2223-2228.

90. Third, the Examiner rejected claims 1-4 as obvious over U.S. Patent Nos. 5,960,080 (EX1013, “Fahlman”) and U.S. Patent Publication No. 2008/0087756 (EX1014, “Hoffberg”). EX1002 (‘244 Prosecution History), 2223-

2230. The Examiner noted that Fahlman “teaches a distributed computer system for organizing and processing data having select content represented by one or more predetermined words,” a “distributed computing system having a plurality of select content data stores for respective ones of a plurality of security designated data and scarcity designated data, each with respective access controls,” “means for identifying a plurality of select content data stores for respective ones of a plurality of security designated data and scarcity designed data,” “a processor activating at least one of said select content data stores there by permitting access to said select content data stores,” and the processor “having means for applying a reconstruction data process employing said respective access control to combine one or more of said security designated data and scarcity designated data.” EX1002 (’244 Prosecution History), 2232.

91. The Examiner then noted that Hoffberg “teaches ... cloud based computing.” EX1002 (’244 Prosecution History), 2233.

92. The Examiner further noted that “[i]t would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the teachings of Hoffberg into those of Fahlman to make the system more efficient. By allowing the computing environment to be a cloud, the devices contained within the environment can communicate without the need for additional security clearances/credentials.” EX1002 (’244 Prosecution History), 2233.

93. In response to the obviousness rejection, Applicant amended application claim 3 (issued as claim 1) to recite “a plurality of granular data stores,” “an extractor for extracting and storing said security designated data in respective select content data stores of said server cloud,” and “means for parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores.” Applicant’s amendments are shown below:

3. (currently amended) A distributed computer system for organizing and processing data having, the data to be processed having select content represented by one or more predetermined words, characters, images, data elements or data objects, said distributed computing system having (a) a plurality of select content data stores in a server cloud for respective ones of a plurality of security designated data and (b) a plurality of granular data stores, each said select content data store and granular data store having ~~security designated data, each with~~ respective access controls thereat, said plurality of ~~select content~~ data stores and said server cloud operatively coupled over a communications network, comprising:

means for identifying plurality of select content data stores for respective ones of a plurality of security designated data ~~and security designated data~~ in said server cloud,

an extractor for extracting and storing said security designated data in respective select content data stores of said server cloud;

a processor activating at least one of said select content data stores in ~~a~~ said server cloud ~~there by~~ thereby permitting access to said select content data stores and respective security designated data ~~and security designated data~~ based upon an application of one or more of said access controls thereat;

means for parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores;

said processor having means for applying a reconstruction data process employing said respective access controls to combine one or more of said security designated data and ~~security designated~~ remainder data. ~~in said server cloud.~~

EX1002 ('244 Prosecution History), 2253.

94. Applicant argued that Fahlman did not include “(a) extraction to different Sec-Con or SC stores, each with a separate access control (which limits further access to the data stored therein) and (b) granular parsing of remainder data and (c) storage of the parsed data in granular data stores.” EX1002 (’244 Prosecution History), 2259.

95. Specifically, Applicant argued that Fahlman “does not discuss reconstruction or merger in the presence of any type of security clearance” whereas “the present invention requires multiple security clearances, each unique to a security level.” EX1002 (’244 Prosecution History), 2260.

96. Applicant also argued that “Fahlman does not seem to store granular data or non-secure data in a separate stores [sic] apart from Sec-Con or SC secure data” while “in the present invention, remainder, non-secret data is stored separately from secret data.” EX1002 (’244 Prosecution History), 2260.

97. Applicant further argued that “Fahlman does not discuss multiple security levels for Sec-con or SC data into multiple storage sites at each security level.” EX1002 (’244 Prosecution History), 2260.

98. Applicant also argued that there was no motivation to combine Fahlman with Hoffberg. EX1002 (’244 Prosecution History), 2261.

99. In response to the rejection of claims 1-4 over patents and/or applications with common ownership, Applicant filed a terminal disclaimer, which

allowed the applicant to overcome the rejections over the listed commonly owned patents and applications. EX1002 ('244 Prosecution History), 2376.

100. The Examiner issued a Notice of Allowance on February 19, 2013. EX1002 ('244 Prosecution History), 2390.

101. The '244 Patent issued on June 18, 2013. EX1001 (the '244 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. Redlich (U.S. Patent Publication No. US2003/0182435, “EX1005 (Redlich)”)

102. Redlich is a U.S. Patent Publication filed on March 19, 2003, and published on September 25, 2003. EX1005 (Redlich), 1. I understand that Redlich is prior art because it is a U.S. Patent Publication that was published prior to the earliest possible priority date of the '244 Patent.

103. The two inventors of Redlich (Ron Redlich and Martin Nemzow) are the same inventors of the '244 Patent. *Compare* EX1005 (Redlich), 1 *with* EX1001 (the '244 Patent), 1.

104. Redlich is directed to “a data security system and method and, more specifically, to a process, program and system which operates to secure files and data objects.” EX1005 (Redlich), ¶2. In particular, Redlich describes a “method for

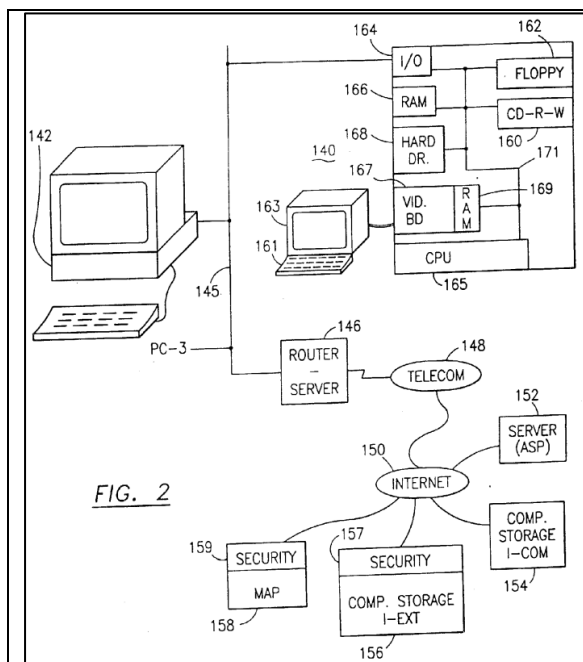
securing data in a computer system”¹ that “includes *establishing a group of security sensitive words, characters, icons, data streams or data objects*, filtering the data input from a data input device and *extracting the security sensitive data*. *The extracted data is separated from the remainder data and is separately stored.*” EX1005 (Redlich), ¶34. Redlich further describes the method as including “[r]econstruction of some or all of the data via one or more of the subsets of extracted data and the remainder data is permitted only in the presence of a predetermined security clearance from the plurality of security levels.” EX1005 (Redlich), ¶35.

105. Redlich discloses that the system and method described above “may be *arranged in a distributed computer system, interconnected by any suitable means* as would be known by one of ordinary skill in the art.” EX1005 (Redlich), ¶99. For example, Redlich discloses that “[i]n a *network implementation*, the extracted data may be stored in one computer and the remainder or common data may be stored in another computer.” EX1005 (Redlich), ¶34. For another example, Redlich discloses that “[i]n a *client-server implementation*, the server may direct *storage of the extracted data to a different location than the remainder data*, either on the server

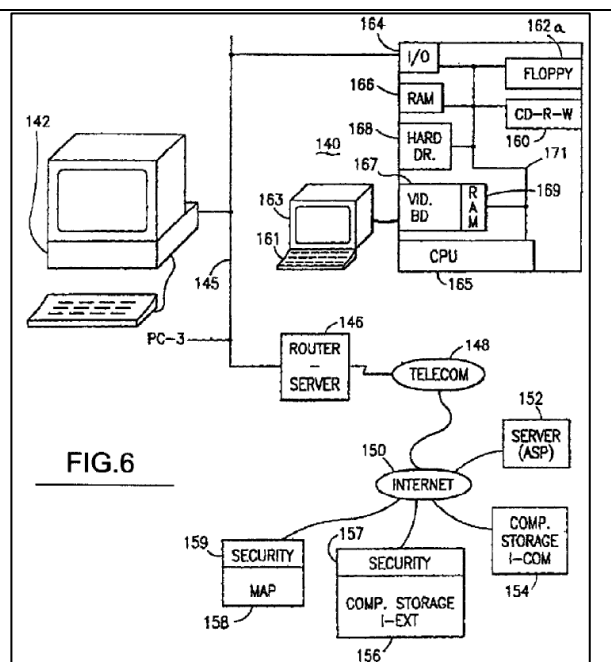
¹ All emphases (italicized bold text and/or colored text) have been added, unless noted otherwise.

or on a further memory system (computer) interconnected to the server or on the client computer and *in distributed memory segments*.” EX1005 (Redlich), ¶34.

106. Figure 2 of Redlich, reproduced side-by-side with identical Figure 6 of the '244 Patent, shows a computer network system comprising a plurality of computers and servers:



EX1005 (Redlich), Figure 2



EX1001 (the '244 Patent), Figure 6

Compare EX1005 (Redlich), Figure 2 *with* EX1001 (the '244 Patent), Figure 6 (same figure).

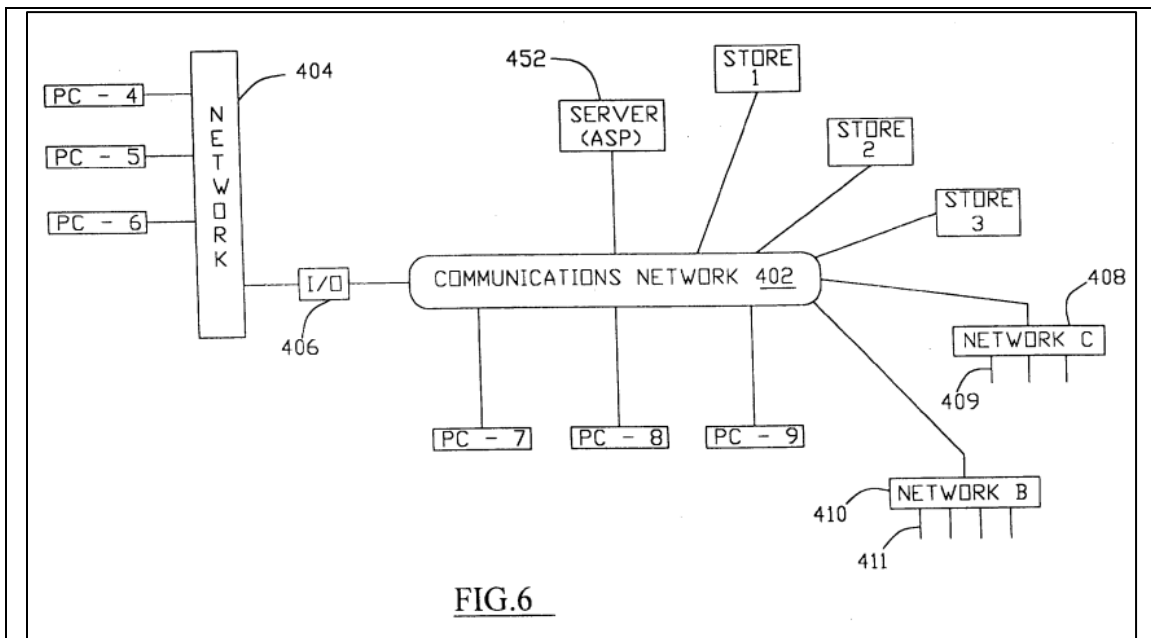
107. Similar to Figure 6 of the '244 Patent, Figure 2 of Redlich discloses a distributed computer system which comprises a plurality of computers (PC 140, PC 142, PC-3) that are connected to a network of servers, which include Internet 150

and Server (ASP) 152, via router or server 146 and a telecommunications system 148. In particular, similar to the '244 Patent, Redlich explains:

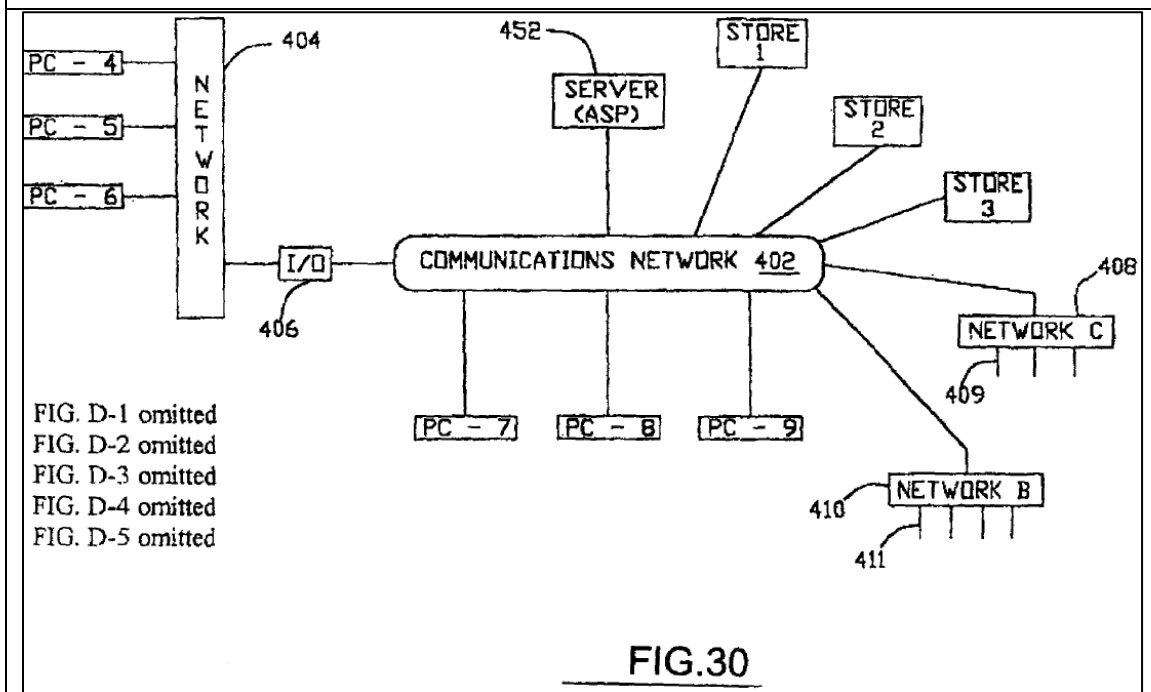
PCs 140, 142, and PC-3 are connected together via a network 145 (LAN or WAN) and are also connected to an input/output device 146 that may be generally described as a router or a server to an outside communications system. The input/output device 146 is connected to *a telecommunications system 148 which leads to Internet 150*. The Internet is a global computer network. *Internet 150 is coupled to a plurality of servers*, one of which is server 152. Server 152 may be designated as an application service processor ASP. *Internet 150 also includes various computer memory storage devices* such as computer storage I-com 154, computer storage I-ext 156 and computer storage map 158.

Compare EX1005 (Redlich), ¶124 with EX1001 (the '244 Patent), 439:4-15 (same disclosure).

108. Figure 6 of Redlich, reproduced below on top of structurally identical Figure 30 of the '244 Patent, shows another example of a computer network system comprising a plurality of computers and servers:



EX1005 (Redlich), Figure 6



EX1001 (the '244 Patent), Figure 30

Compare EX1005 (Redlich), Figure 6 *with* EX1001 (the '244 Patent), Figure 30 (same figure).

109. Similar to Figure 30 of the '244 Patent, Figure 6 of Redlich discloses a distributed computer system comprising a plurality of computers (PC-4, PC-5, PC-6, PC-6, PC-7, PC-8, PC-9), networks (Network A, Network B, Network C), and data stores (Store 1, Store 2, Store 3) interconnected by telecommunications network 402. In particular, similar to the '244 Patent, Redlich explains:

Fig. 6 is an exemplary computer network diagram showing various user communities. The telecommunications network 402 is connected to the server application server provider ASP 452 and *to various networks and personal computers* ... Network A [404] is coupled to various PCs identified in FIG. 6 as PC-4, PC-5 and PC-6. Of course, Network A could be coupled to other PCs not illustrated in FIG. 6. As described earlier, *server 452 can facilitate remote or offsite storage of extract data and remainder data in store 1, store 2 and/or store 3* ... If PC-6 is designated as the input computer, the extract data may be stored on PC-4. Of course, PC-4 could be designated as the server for Network A.

Compare EX1005 (Redlich), ¶177 *with* EX1001 (the '244 Patent), 490:25-58 (same disclosure).

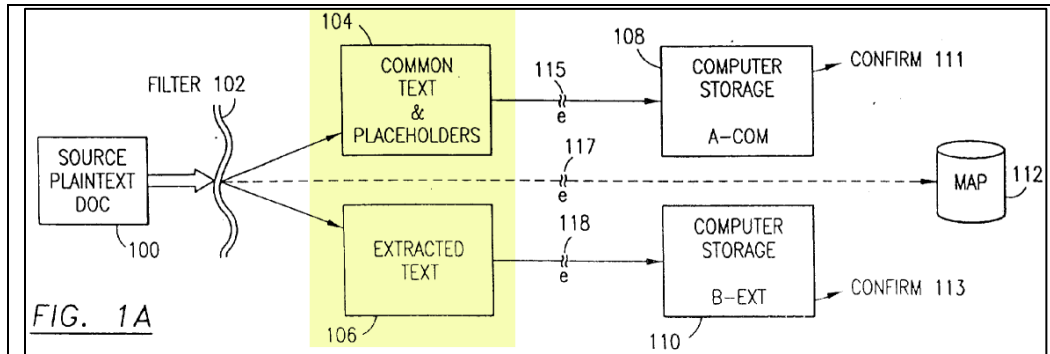
110. Similar to the '244 Patent, Redlich discloses extracting security sensitive data from the data to result in extracted data and remainder data. For example, Redlich explains that its “method for securing data in a computer system

in one embodiment includes establishing a group of security sensitive words, characters, icons, data streams or data objects, filtering the data input from a data input device and *extracting the security sensitive data. The extracted data is separated from the remainder data and is separately stored.*” EX1005 (Redlich), ¶34. Redlich further discloses that the security sensitive content that is extracted could be “security sensitive words, phrases, characters, icons, or data objects.” EX1005 (Redlich), ¶¶35 (“The method and the computer media containing programming instructions includes... *extracting security sensitive words, phrases, characters, icons, or data objects* and forming subsets of extracted data and remainder data.”); 38 (“The method *extracts the security sensitive words, characters or icons from said e-mail data* to obtain extracted data and remainder data therefrom.”).

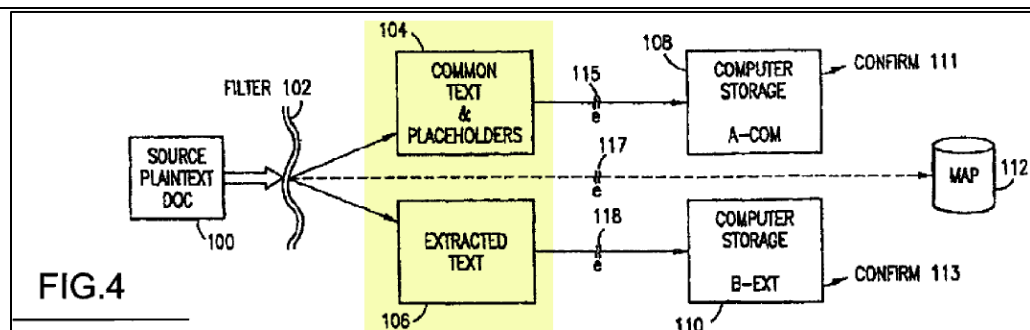
111. Similarly, the '244 Patent states that “[t]he method and system extracts security sensitive content from a data input to obtain extracted security sensitive data for a corresponding security level and remainder data.” EX1001 (the '244 Patent), 4:22-25, 413:14-17 (“[T]he method and system extracts security sensitive content TS or Sor C (FIG. 2) from a data input to obtain extracted security sensitive data for a corresponding security level and remainder data.”).

112. Figure 1A of Redlich, reproduced below on top of identical Figure 4 of the '244 Patent, discloses a diagram showing, with highlighting, extracting security

sensitive data to result in extracted data (106) and also separating the non-security sensitive data into remainder data (104):



EX1005 (Redlich), Figure 1A



EX1001 (the '244 Patent), Figure 4

Compare EX1005 (Redlich), Figure 1A with EX1001 (the '244 Patent), Figure 4 (same figure).²

113. Similar to Figure 4 of the '244 Patent, Figure 1A of Redlich illustrates the extraction of security sensitive data from the data (*i.e.*, Source Plaintext Doc 100)

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

to result in extracted data (*i.e.*, Extracted Text 106) and separating the non-security sensitive data into remainder data (*i.e.*, Common Text 104). In particular, similar to the '244 Patent, Redlich explains:

Filter 102, in a most basic sense, *separates out common text or remainder data 104 from uncommon text, words, characters, icons or data objects*. The security sensitive words, characters, icons or data objects are separated from remainder or common text 104 as extracted text 106 ... The uncommon words (extracted-security sensitive words), not found in the dictionary, would be placed in an extracted text or extracted data file 106 ... The common text or remainder data would be stored in remainder data file 104.

Compare EX1005 (Redlich), ¶104 *with* EX1001 (the '244 Patent), 435:40-61 (same disclosure).

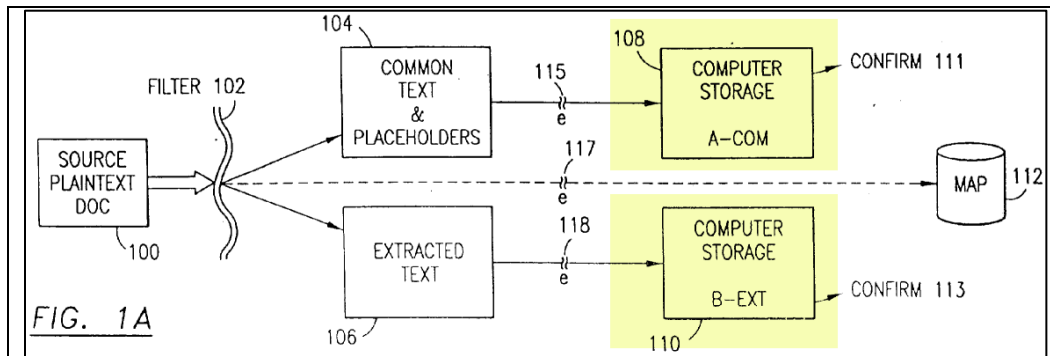
114. Similar to the '244 Patent, Redlich additionally discloses storing extracted data in different extract stores based on the extracted data's security level. Redlich discloses that the security sensitive extract data are stored in a plurality of different computer storage locations. EX1005 (Redlich), ¶172 ("Each filter could filter out different levels of security sensitive items and *each bundle or group of security sensitive items* (from each distinct filter) could be *stored at different computer storage locations.*"); *see also* EX1005 (Redlich), ¶35 ("The subsets of *extracted data are stored in one or more computer memories* in the network *identified as extracted stores*").

115. Redlich further explains that these different computer storage locations are differentiated by the security level of the stored data. EX1005 (Redlich), ¶245 (“[T]he extract store may comprise *a plurality of extract stores operative in conjunction with a plurality of security clearance levels.*”).

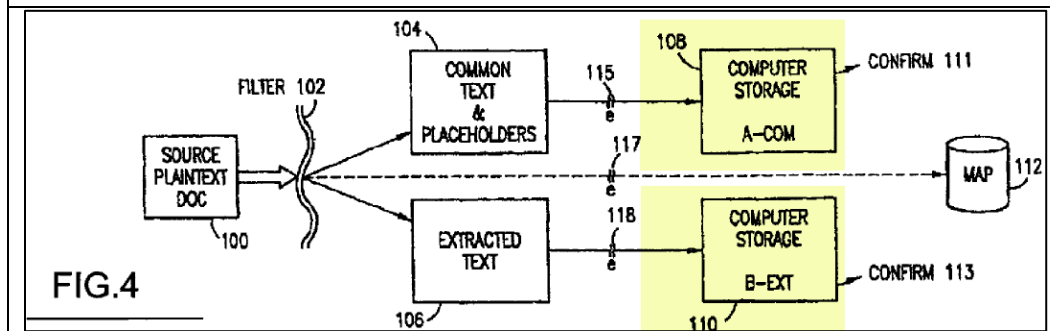
116. Similarly, the '244 Patent also discloses storing extracted data in different data stores based on the extracted data's security level. EX1001 (the '244 Patent), 413:22-25 (“This *extracted security sensitive data is stored for the corresponding security level in a respective security sensitive extract store* 6a, 6b or 6c. Remainder data is stored in the distributed computer system.”); 513:13-15 (“[T]he extract store may comprise *a plurality of extract stores operative in conjunction with a plurality of security clearance levels.*” (same disclosure as EX1005 (Redlich), ¶245)).

117. Similar to the '244 Patent, Redlich also discloses that the remainder data is stored separate from the extracted data. Compare EX1005 (Redlich), ¶34 (“The *extracted data is separated from the remainder data* and is *separately stored.*”) with EX1001 (the '244 Patent), 4:25-27 (“This *extracted security sensitive data is stored in a respective security sensitive extract store. Remainder data is stored in the distributed computer system.*”).

118. Figure 1A of Redlich, reproduced below on-top of identical Figure 4 of the '244 Patent, also discloses a diagram showing, with highlighting, storing the extracted and remainder data in separate data stores:



EX1005 (Redlich), Figure 1A



EX1001 (the '244 Patent), Figure 4

Compare EX1005 (Redlich), Figure 1A with EX1001 (the '244 Patent), Figure 4 (same figure).

119. Similar to Figure 4 of the '244 Patent, Figure 1A of Redlich illustrates the storing of extracted data in an extract store (*i.e.*, Computer Storage B-ext 110) and storing remainder data in a separate store (*i.e.*, Computer Storage A-com 108).

As noted above, Redlich explains that “*the extract store may comprise a plurality of extract stores* operative in conjunction with a plurality of security clearance levels.” EX1005 (Redlich), ¶245. Similar to the ’244 Patent, Redlich explains:

[T]he common text or the remainder data is stored in common storage memory 108 ... The extracted data file 106 is stored in a different memory computer storage 110 (B-ext). In a preferred embodiment, memory segment 108 (A-com) is at a different location than computer storage memory segment 110 (B-ext).

Compare EX1005 (Redlich), ¶107 with EX1001 (the ’244 Patent), 443:2-3, 17-20 (same disclosure).

120. Similar to the ’244 Patent, Redlich further describes parsing data into data segments. Redlich explains that its disclosed process “involves *parsing the documents or content into granular data groups* and optionally creating small groups of data wherein the data segments cannot be recognized even to the level of providing 2-4 data objects in each file.” EX1005 (Redlich), ¶238. Redlich further provides a specific parsing algorithm that could be used. The algorithm “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. Hence, the parsed document 100 constitutes

at least remainder data and data which is extracted or parsed or segmented out.”

EX1005 (Redlich), ¶231.

121. The '244 Patent includes the same disclosures, shown in the following comparison table:

EX1005 (Redlich)	EX1001 (the '244 Patent)
“The process involves <i>parsing the documents or content into granular data groups</i> and optionally creating small groups of data wherein the data segments cannot be recognized even to the level of providing 2-4 data objects in each file” EX1005 (Redlich), ¶231.	“The process involves <i>parsing the documents or content into granular data groups</i> and optionally creating small groups of data wherein the data segments cannot be recognized even to the level of providing 2-4 data objects in each file” EX1001 (the '244 Patent), 508:34-37.
“The parsing algorithm, as stated earlier, targets the plaintext document or data object 100 and <i>splits, cuts and segments (that is, parses) the document by bit count, word, word count, page, line count, paragraph count, any</i>	“The parsing algorithm, as stated earlier, targets the plaintext document or data object 100 and <i>splits, cuts and segments (that is, parses) the document by bit count, word, word count, page, line count, paragraph count, any</i>

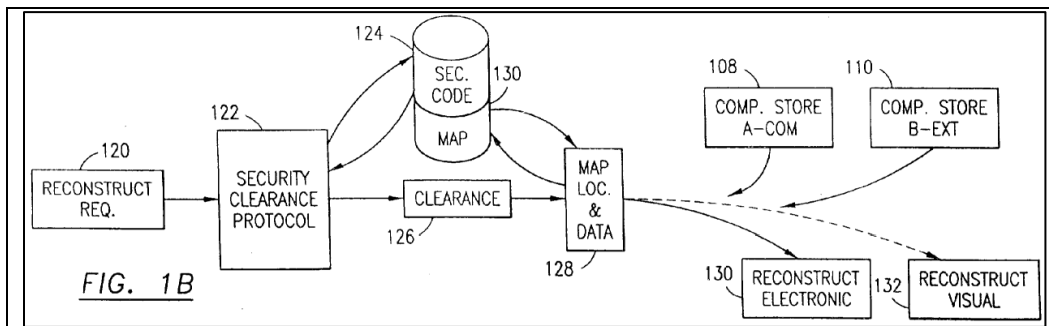
EX1005 (Redlich)	EX1001 (the '244 Patent)
<i>identifiable document or icon characteristic, or other identifiable feature such as capital letters, italics, underline, etc.</i> Hence, the parsed document 100 constitutes at least remainder data and data which is extracted or parsed or segmented out.” EX1005 (Redlich), ¶238.	<i>identifiable document or icon characteristic, or other identifiable feature such as capital letters, italics, underline, etc.</i> Hence, the parsed document 100 constitutes at least remainder data and data which is extracted or parsed or segmented out.” EX1001 (the '244 Patent), 506:65-507:5.

122. Similar to the '244 Patent, Redlich also discloses controlling access to all or some of the security sensitive data based on the requesting user's security clearance. Redlich explains that “[t]he classification level of a user will determine his right and ability to access and release the stored critical extracted content from the various storage locations for reconstruction.” EX1005 (Redlich), ¶200. Thus, “[a] user with top classification will view the entire document, while a user with a lower level classification will view a sanitized document, tailor made automatically for his clearance level.” EX1005 (Redlich), ¶200; *see also* EX1005 (Redlich), ¶35 (“Reconstruction of some or all of the data via one or more of the subsets of extracted

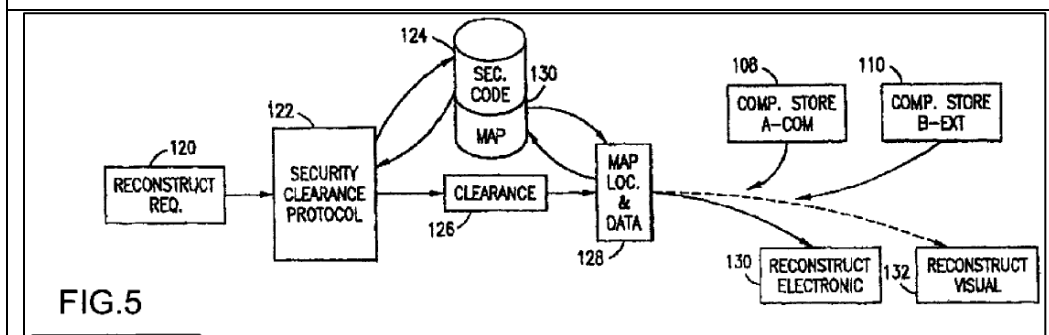
data and the remainder data is *permitted only in the presence of a predetermined security clearance* from the plurality of security levels.”).

123. Similarly, the '244 Patent also discloses controlling access to all or some of the security sensitive data based on the requesting user's security clearance. The '244 Patent discloses that “[a] low level security clearance results in only partial reconstruction of the plain text or source document,” but “each successively higher level of security clearance permits the user to see greater degrees of reconstructed plain text obtained from the extracted data stored in extract stores and the remainder data from the remainder stores.” EX1001 (the '244 Patent), 490:11-19; *see also* EX1001 (the '244 Patent), 496:7-13 (“*The classification level of a user will determine his right and ability to access* and release the stored critical extracted content from the various storage locations for reconstruction. A user with top classification will view the entire document, while a user with a lower level classification will view a sanitized document, tailor made automatically for his clearance level.” (same disclosure as EX1005 (Redlich), ¶200)).

124. Figure 1B of Redlich, reproduced below on-top of identical Figure 5 of the '244 Patent, discloses a diagram showing the controlling of access of security sensitive data:



EX1005 (Redlich), Figure 1B



EX1001 (the '244 Patent), Figure 5

Compare EX1005 (Redlich), Figure 1B with EX1001 (the '244 Patent), Figure 5 (same figure).

125. Similar to Figure 5 of the '244 Patent, Figure 1B of Redlich illustrates permitting full or partial reconstruction of data. After performing a security clearance protocol (122) to determine the security clearance of a user (126), the system would permit either full or partial reconstruction of that data based on that security clearance. The data would be reconstructed using remainder data from the remainder data store (Comp. Store A-com 108) and extracted data from the extract store (Comp. Store B-ext 110). Similar to the '244 Patent, Redlich explains:

The user, typically at a computer terminal, inputs a reconstruction request 120. The system *first executes a security clearance protocol* routine 122 in order *to determine whether the user has the proper security clearance*. The security clearance may be thought of as a security clearance control ... [T]he security clearance protocol determines the level of security clearance and, hence, the full or partial reconstruction of the plaintext.

Compare EX1005 (Redlich), ¶122 with EX1001 (the '244 Patent), 447:3-12 (same disclosure).

B. Ozzie (U.S. Patent No. 8,601,598, “EX1006 (Ozzie)”)

126. U.S. Patent No. 8,601,598 (EX1006, “Ozzie”) was filed on September 29, 2006 as U.S. Ser. No. 11/536,907. EX1006 (Ozzie), 1. Ozzie was published on April 3, 2008 as U.S. Patent Publication No. 2008/0083036, and is prior art under at least 35 U.S.C. §102(e).

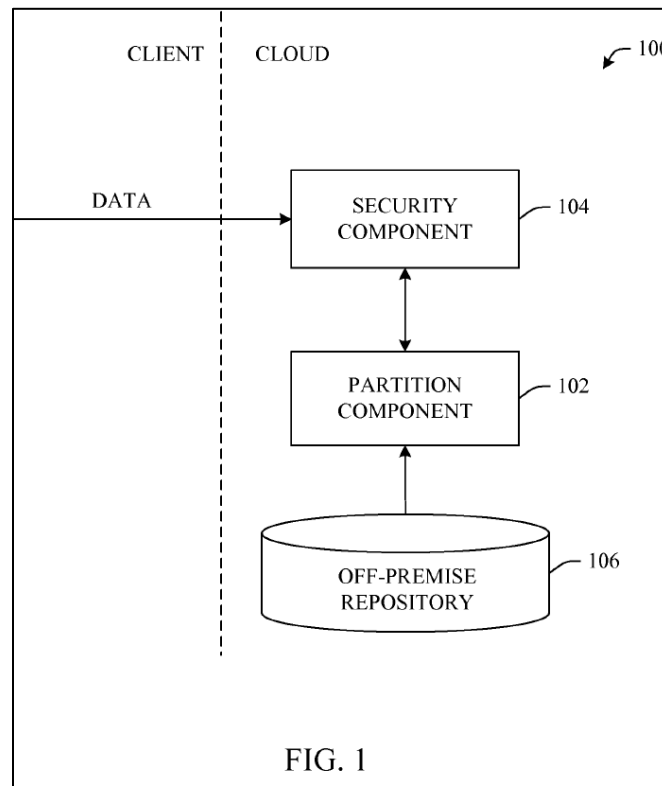
127. Ozzie describes “a system that can enable *a cloud-based data repository* to function as a secure ‘dropbox’ for data that corresponds to a user.” EX1006 (Ozzie), 2:6-9. In particular, Ozzie describes a system in which data is “stored in partitions within the cloud while preventing unwanted or unintended disclosure of the information.” EX1006 (Ozzie), 4:33-36.

128. The purpose of Ozzie’s invention is to “leverage[] the user-centric architecture of emerging ‘cloud-based’ systems.” EX1006 (Ozzie), 4:51-52. “For

instance, rather than housing applications and data locally, data can be offloaded to a ‘cloud’ such as a group of one or more communicatively coupled ‘off-premise’ servers. In this manner, a user’s data can be accessed from any network connected computing device.” EX1006 (Ozzie), 4:52-57.

129. For example, Ozzie discloses dividing a cloud-based repository into partitions based on any particular criteria. EX1006 (Ozzie), 4:64-5:1 (“[S]ystem 100 can include a partition component 104 that can *partition an off-site or ‘cloud-based’ repository 106 based upon any criteria*, including, but not limited to, user identity, data type, associated service, associated activity, date created/modified, etc.”). These partitions are viewed as “drop-boxes,” which are used “for data maintained within the ‘cloud.’” EX1006 (Ozzie), 5:1-3. Ozzie explains that “a user, application and/or service can ‘drop’ or save information into a respective segment based upon a particular partition operation.” EX1006 (Ozzie), 5:3-5.

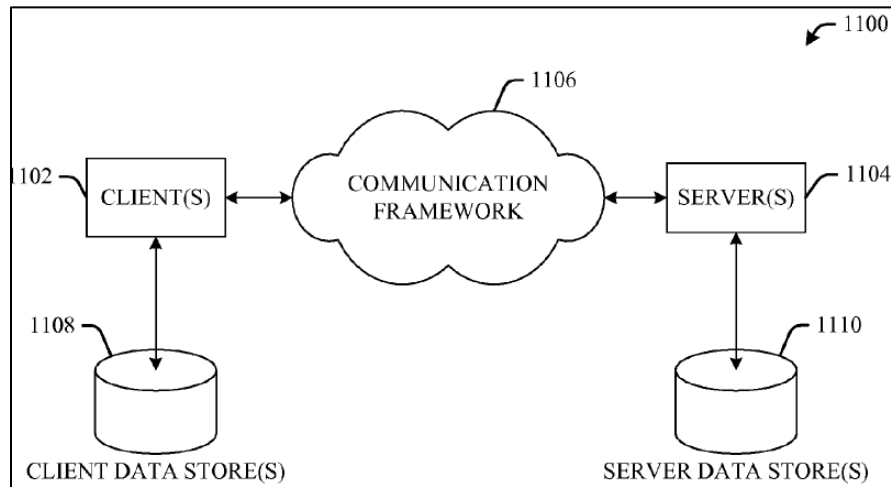
130. Figure 1 of Ozzie, reproduced below, illustrates a system for storing data in cloud-based repositories:



EX1006 (Ozzie), Figure 1.

131. Ozzie explains that “FIG. 1 illustrates a system 100 that includes a partition component 102 and a security component 104 that facilitate establishing a virtual ‘drop-box’ for encrypted data associated with an identity of an intended or target recipient. The partition component 102 can partition an off-site repository(ies) 106 into multiple partitions thereby establishing drop-boxes associated with an identity, type of data, etc.” As explained above, “off-site repositories” as disclosed in Ozzie are also known as cloud-based repositories. EX1006 (Ozzie), 4:65.

132. Figure 11 of Ozzie, reproduced below, illustrates a schematic block diagram of an exemplary computing environment on which Ozzie's invention could be implemented:



EX1006 (Ozzie), Figure 11.

133. Figure 11 of Ozzie discloses a system 1100 comprising of a plurality of clients (1102) and a plurality of servers (1104). “The system 1100 includes a communication framework 1106 (e.g., a global communication network such as the Internet) that can be employed to facilitate communications between the client(s) 1102 and the server(s) 1104.” EX1006 (Ozzie), 14:6-9.

134. Ozzie's System 1100 is also comprised of a plurality of client data stores (1108) and server data stores (1110). “The client(s) 1102 are operatively connected to one or more client data store(s) 1108 that can be employed to store information local to the client(s) 1102.” EX1006 (Ozzie), 14:12-15. “Similarly, the server(s) 1104 are operatively connected to one or more server data store(s) 1110

that can be employed to store information local to the servers 1104.” EX1006 (Ozzie), 14:16-18.

VIII. Level of Ordinary Skill in the Art

135. In my opinion, a person of ordinary skill in the art (“POSITA”) in the field of the ’244 patent as of its earliest possible priority date of January 5, 2007, 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.

136. I met these requirements for POSITA at the time of earliest possible priority date of the ’244 patent.

IX. Claim Construction

137. I have reviewed the claims, specification, and file history of the ’244 patent.

138. Other than the “means-plus function” terms analyzed below, I have not construed any terms in my analysis, and I have afforded the claim terms their ordinary and customary meaning.

A. “means for identifying plurality of select content data stores for respective ones of a plurality of security designated data in said server cloud”

139. This phrase appears in Claim 1 of the '244 Patent. As noted in Section III.A above, I understand that patent claims can be drafted in a so-called “means-plus-function” form and that, in such situations, the proper claim construction must include the claimed “function” and the “corresponding structure” that is disclosed in the specification of the patent (and equivalents). I am informed that this phrase is an example of “means-plus-function” claiming.

140. In my opinion, the “function” that is claimed by this phrase is “identifying plurality of select content data stores for respective ones of a plurality of security designated data in said server cloud.”

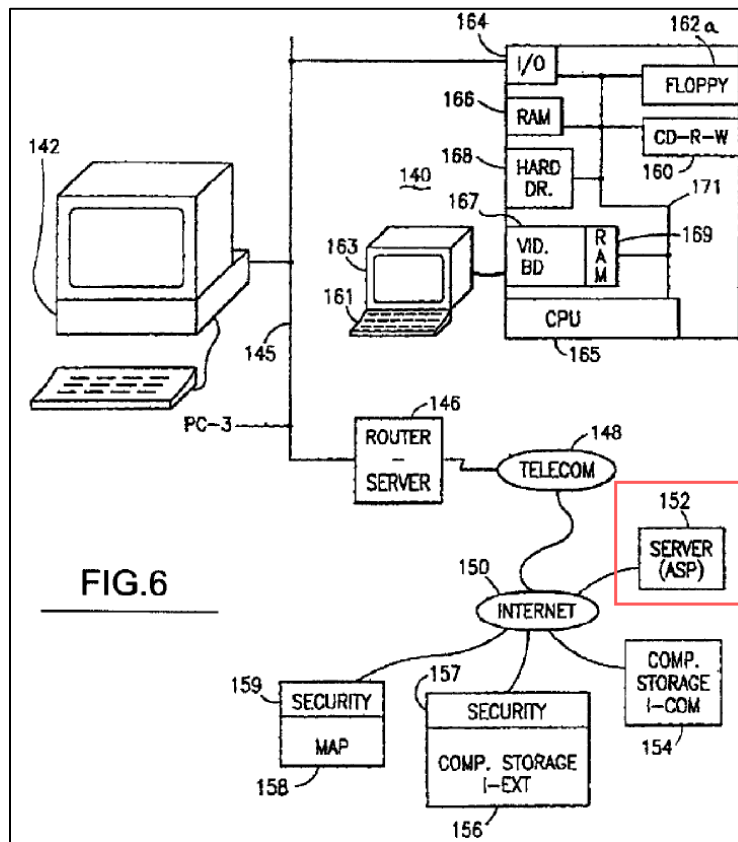
141. Based on my review of the '244 Patent, to the extent a corresponding structure is disclosed, the “structure” corresponding to claimed “function” is an application service provider (“ASP”) server, such as the server labeled as box 152 in Figure 6, performing the algorithm as described in EX1001 (the '244 Patent), 436:34-46, and structural equivalents thereof.

142. My opinion is based at least on the following disclosures in the '244 Patent:

- EX1001 (the '244 Patent), 436:34-46: “[A] client-server system over the Internet may have URLs designating storage sites and an *ASP 152*

(FIG. 6) controlling storage. In this pre-set system, the user does not select the sites. The sites may be randomly selected by ASP 152. The ASP may use artificial intelligence AI to locate secure extract data storage sites. AI or inference machines can ascertain (a) traffic on communications channels, (b) storage limit issues, (c) transmission failures in the communications links, and (d) the degree of security necessitated by exterior events, i.e., terrorism alerts, virus alerts, war, data security warnings posted by trusted sources, MicroSoft, Norton, NASA, DoD, CDC, FBI, etc.”

- EX1001 (the '244 Patent), Figure 6:



- EX1001 (the '244 Patent), 522:15 (“Abbreviations Table”): “ASP application service provider - server on a network”

B. “an extractor for extracting and storing said security designated data in respective select content data stores of said server cloud”

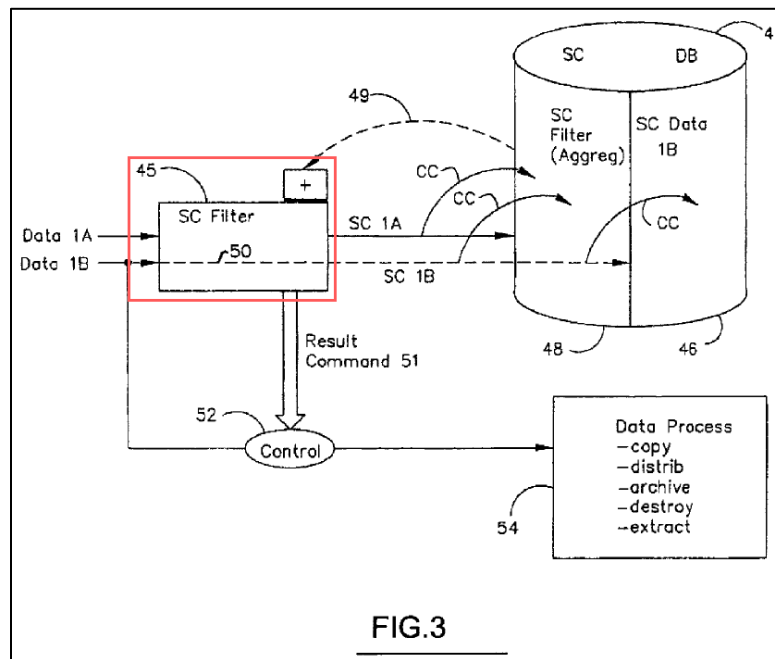
143. This phrase also appears in Claim 1 of the '244 Patent. As noted in Section III.A above, I understand that patent claims can be drafted in a so-called “means-plus-function” form and that, in such situations, the proper claim construction must include the claimed “function” and the “corresponding structure” that is disclosed in the specification of the patent (and equivalents). I am informed that this phrase is an example of “means-plus-function” claiming.

144. In my opinion, the “function” that is claimed by this phrase is “extracting and storing said security designated data in respective select content data stores of said server cloud.”

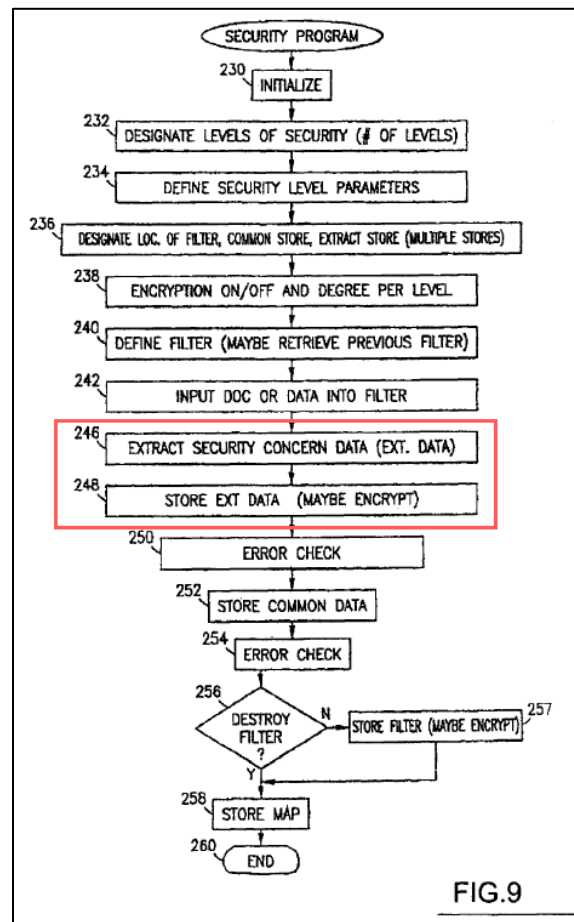
145. Based on my review of the '244 Patent, to the extent a corresponding structure is disclosed, the “structure” corresponding to claimed “function” is a filter, such as the filter labeled as box 45 in Figure 3, performing the algorithm as set forth in the boxes labeled as 246 and 248 in EX1001, Figure 9, and described in EX1001 (the '244 Patent), 437:1-5, and structural equivalents thereof.

146. My opinion is based at least on the following disclosures in the '244 Patent:

- EX1001 (the '244 Patent), 412:11-13: “SC filter 45 may be one or more of a content-based filter, contextual filter or a taxonomic classification filter.”
- EX1001 (the '244 Patent), Figure 3:



- EX1001 (the '244 Patent), 437:1-5: “In any event, the plaintext document is fed through the filter. Step 246 extracts the security data or SC data from the input document. Step 248 stores the extracted data. The extracted data may be encrypted prior to storage.”
- EX1001 (the '244 Patent), Figure 9:



C. “means for parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores”

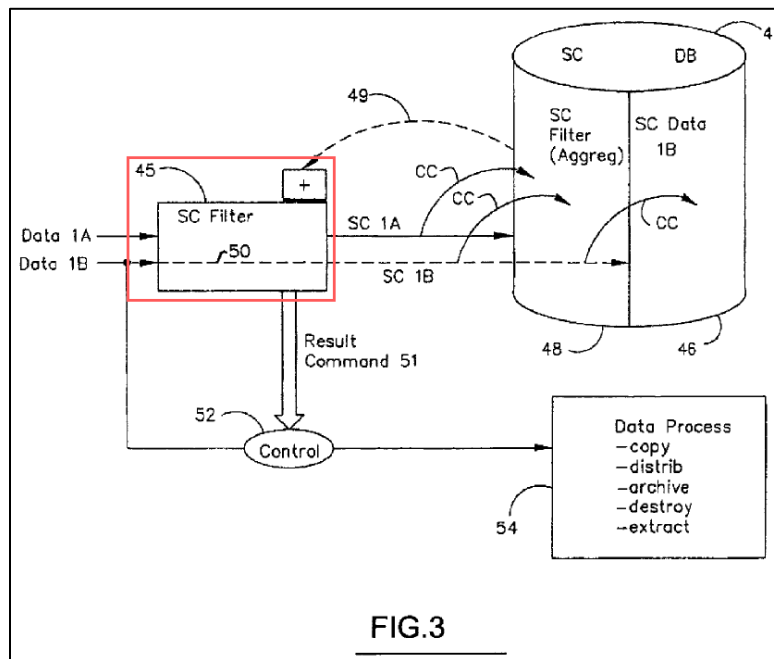
147. This phrase also appears in Claim 1 of the '244 Patent. As noted in Section III.A above, I understand that patent claims can be drafted in a so-called “means-plus-function” form and that, in such situations, the proper claim construction must include the claimed “function” and the “corresponding structure” that is disclosed in the specification of the patent (and equivalents). I am informed that this phrase is an example of “means-plus-function” claiming.

148. In my opinion, the “function” that is claimed by this phrase is “parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores.”

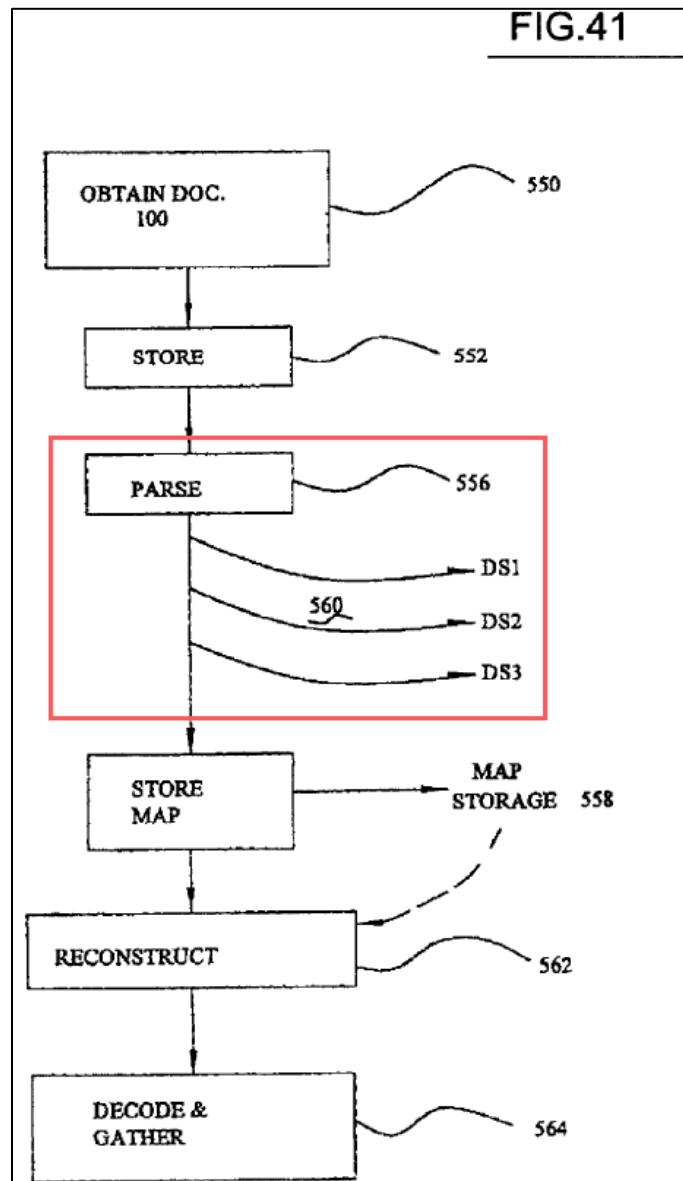
149. Based on my review of the '244 Patent, to the extent a corresponding structure is disclosed, the “structure” corresponding to claimed “function” is a filter, such as the filter labeled as box 45 in Figure 3, performing the algorithm as set forth in the box labeled as 556 in EX1001, Figure 41, and described in EX1001 (the '244 Patent), 506:63-507:8 and 442:55-67, and structural equivalents thereof.

150. My opinion is based at least on the following disclosures in the '244 Patent:

- EX1001 (the '244 Patent), 412:11-13: “SC filter 45 may be one or more of a content-based filter, contextual filter or a taxonomic classification filter.”
- EX1001 (the '244 Patent), Figure 3:



- EX1001 (the '244 Patent), 506:63-507:8: “A parsing algorithm function 554 is utilized in parsing step 556. The parsing algorithm, as stated earlier, targets the plain text 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. ... The parsed data [] is then dispersed into storage facilities data store DS 1, 2, 3, 4, etc.”
- EX1001 (the '244 Patent), Figure 41:



- EX1001 (the '244 Patent), 442:55-67: “The system and methodology described herein also encompasses parsing the plain text document by bit count, word, word count, page count, line count, paragraph count and parsing based upon any identifiable document characteristic, capital letters, italics, underline, etc. Parsing is a contextual filter using a content

as a marker and a range defines by certain file parameters. Algorithms may be implemented to parse the plain text document ... The 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 '244 Patent), 435:17-19: “A source document 100 containing data, sometimes referred to as a ‘plaintext,’ is passed through a filter 102.”

D. “means for applying a reconstruction data process employing said respective access controls to combine one or more of said security designated data and remainder data”

151. This phrase also appears in Claim 1 of the '244 Patent. As noted in Section III.A above, I understand that patent claims can be drafted in a so-called “means-plus-function” form and that, in such situations, the proper claim construction must include the claimed “function” and the “corresponding structure” that is disclosed in the specification of the patent (and equivalents). I am informed that this phrase is an example of “means-plus-function” claiming.

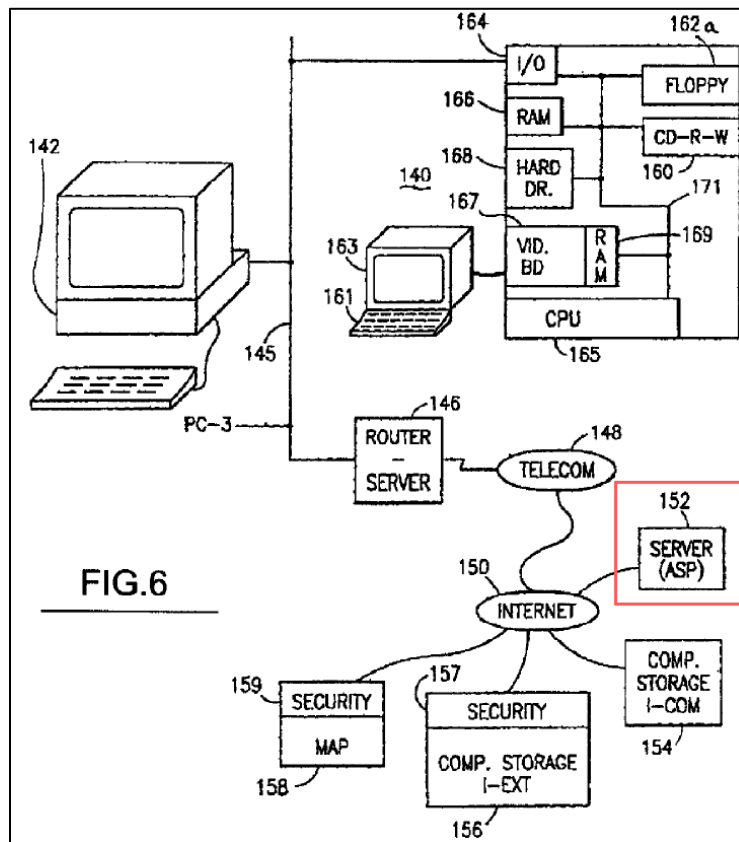
152. In my opinion, the “function” that is claimed by this phrase is “applying a reconstruction data process employing said respective access controls to combine one or more of said security designated data and remainder data.”

153. Based on my review of the '244 Patent, to the extent a corresponding structure is disclosed, the “structure” corresponding to claimed “function” is the

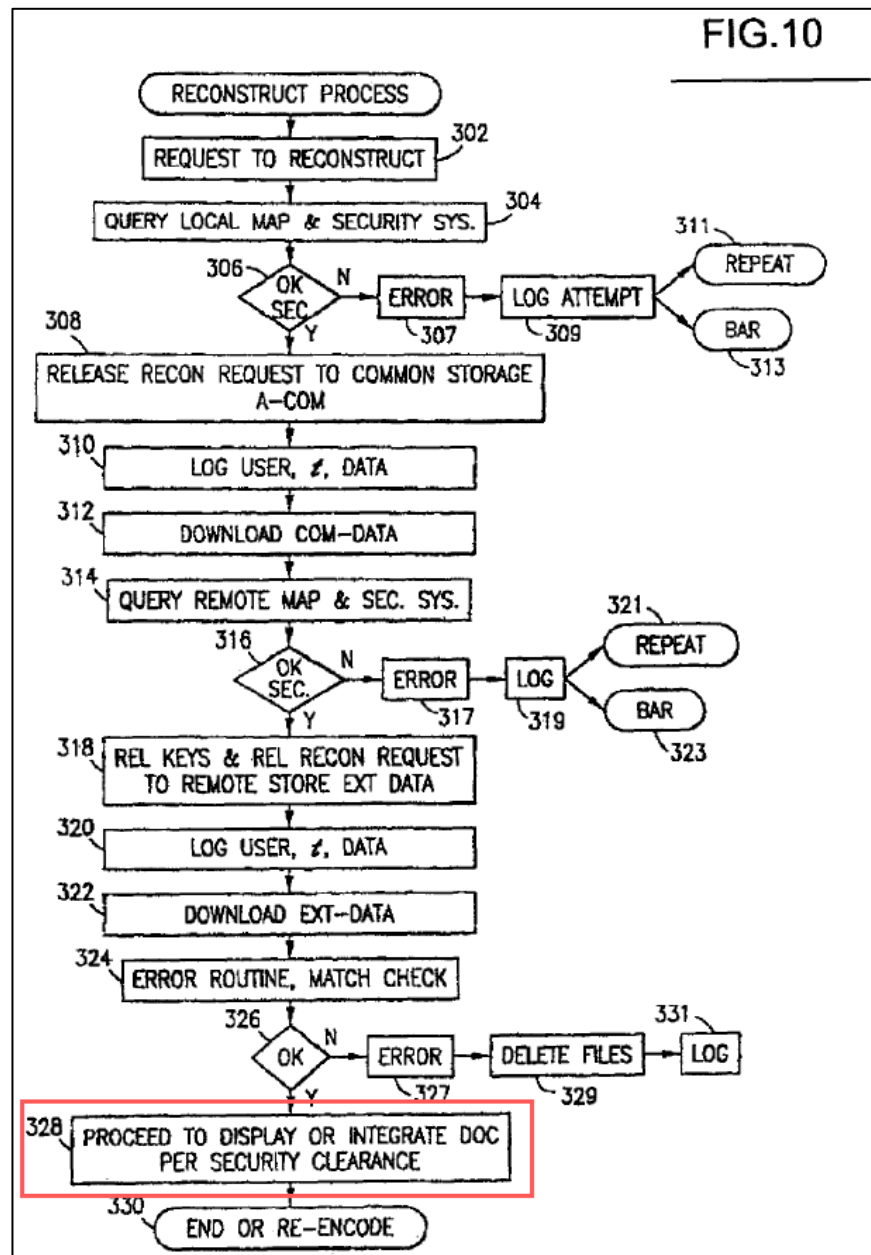
processor of an ASP server, such as the processor of the ASP server labeled as box 152 in EX1001, Figure 6, performing the algorithm as set forth in box 328 of EX1001, Figure 10, and described in EX1001, 438:9-15, and 441:16-30, and structural equivalents thereof.

154. My opinion is based at least on the following disclosures in the '244 Patent:

- EX1001 (the '244 Patent), 441:16-30: "To reconstruct the document, the user at computer 140 would be required to call up the URL of server 152 and input the appropriate security code. The server 152 would then call up and download data from various memory locations whether they be memory locations on computer 140 or memory locations I-com 154, I-ext 156 and map memory 158. The system compiles the entirety of the plaintext document by gathering the dispersed components thereof or compiles partial reconstructions for different levels of security. By implementing different security levels, the system is dynamic enough such that server 152 can easily locate the various extracted data levels based upon various security codes representing different security levels, as those codes are input by the user at computer 140."
- EX1001 (the '244 Patent), Figure 6:



- EX1001 (the '244 Patent), 522:15 (“Abbreviations Table”): “ASP application service provider - server on a network”
- EX1001 (the '244 Patent), 438:9-15: “If the error checking routine on the extracted data is acceptable, the YES branch is taken from decision step 326 and the system, in step 328, proceeds to display the plaintext document or to integrate the plaintext document pursuant to the security clearance initially input by the user.”
- EX1001 (the '244 Patent), Figure 10:



155. Additionally, a POSITA would understand that a server, such as an ASP server, comprises a processor because a processor would carry out the instructions for implementing and performing server applications and services. *See also* EX1015 (MS-Dict.), 403-404 (“server”).

X. Specific Grounds For Challenge

A. Ground 1: Claim 1 Is Obvious Over Redlich

1. Independent Claim 1

i. Claim 1 Preamble

156. To the extent the preamble is limiting, Redlich discloses or renders obvious the preamble of independent claim 1, as explained below.

a. [1pre-i] A distributed computer system for organizing and processing **data**, the **data** to be processed having select content represented by one or more predetermined words, characters, images, data elements or data objects,³

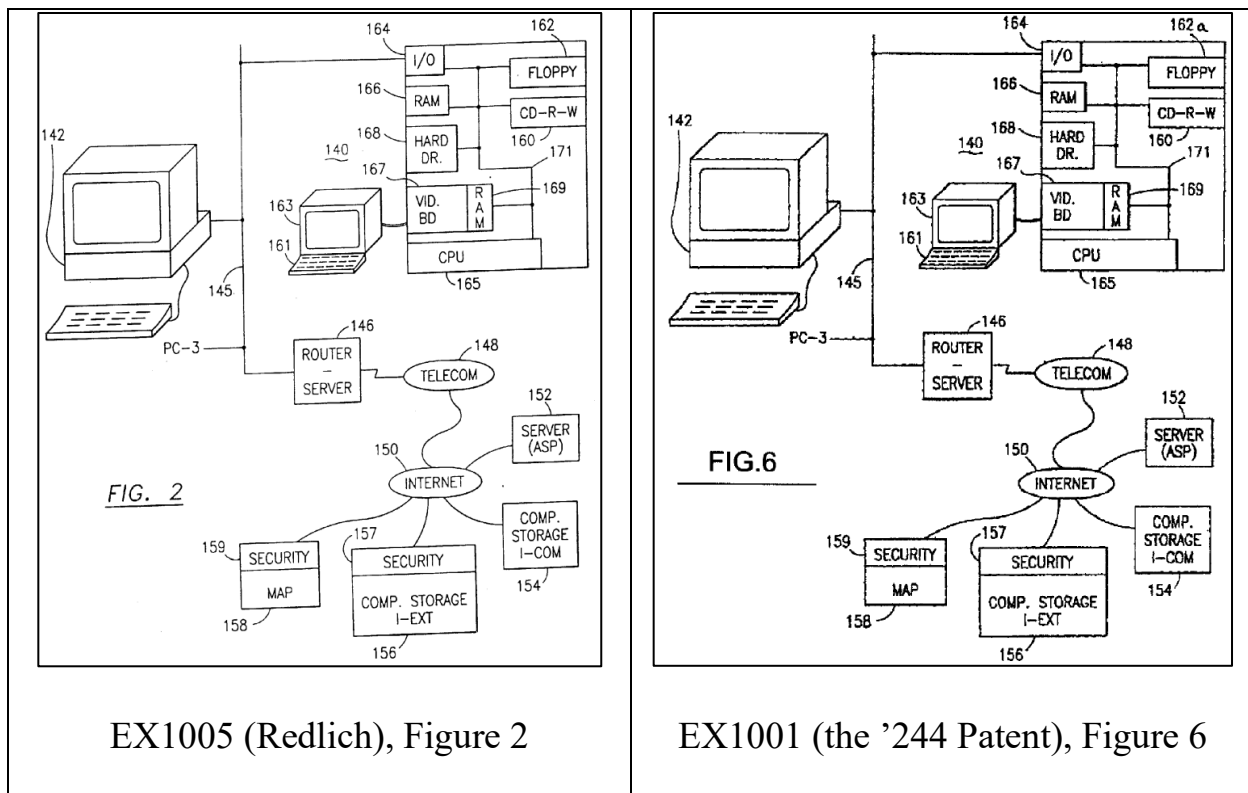
157. Redlich discloses this limitation.

158. Redlich discloses a distributed computer system. Specifically, Redlich discloses “*a distributed computer system*, interconnected by any suitable means.” EX1005 (Redlich), ¶99; *see also* EX1005 (Redlich), ¶¶231 (“[T]he dispersement 560 largely spreads out or distributes the parsed document 100 to a plurality of memories *in the distributed computer system.*”), 245 (“The method of securing e-mail data

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.

operates on *a distributed computer system* which at least includes a remote memory designated as an extract store.”).

159. Redlich also discloses examples of a distributed computer system. For example, Figure 2 of Redlich, reproduced below side-by-side identical Figure 6 of the '244 Patent, illustrates a distributed computer system comprising a plurality of computers (PC 140, PC 142, and PC-3) and a plurality of servers (Server 146 and Server (ASP) 152) connected via a network (Telecommunications Network 148 and Internet 150):



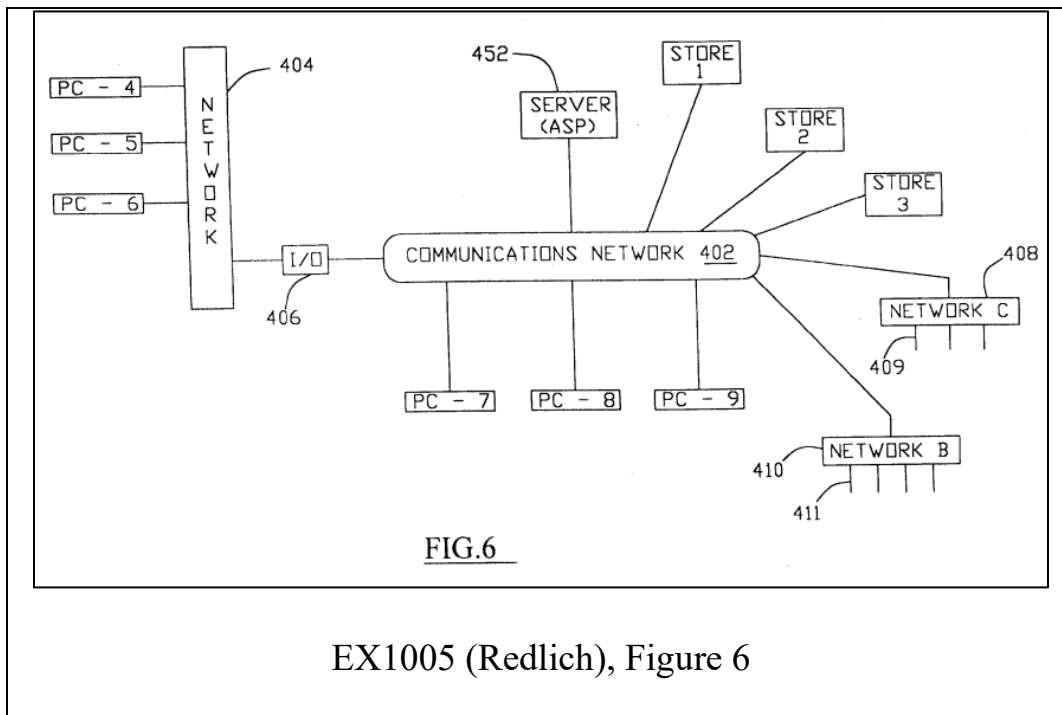
Compare EX1005 (Redlich), Figure 2 with EX1001 (the '244 Patent), Figure 6 (same figure); see Section VII.A above.

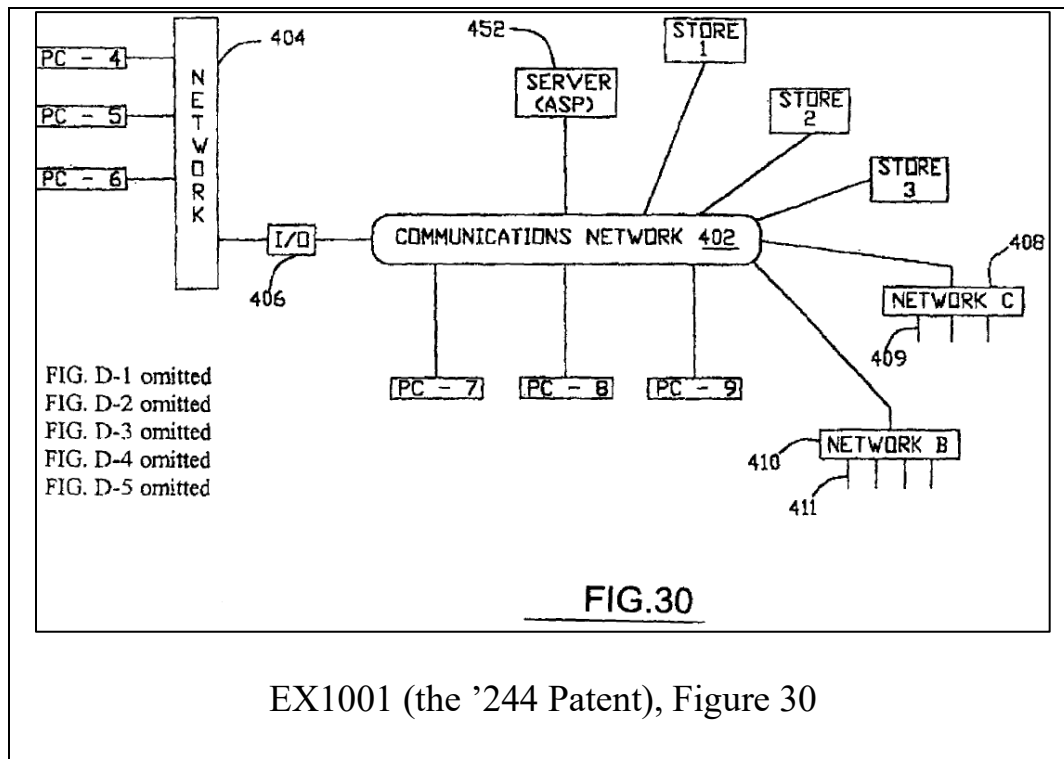
160. Similar to '244 Patent Figure 6, Figure 2 of Redlich shows a distributed computer system comprising a plurality of computers “PCs 140, 142, and PC-3” “connected together via a network” (*i.e.*, Telecommunications network 148). *Compare* EX1005 (Redlich), ¶124; *see also* EX1001 (the '244 Patent), 439:4-5 (same disclosure). The network is connected to Internet 150, which is further connected to “a plurality of servers,” including server 152, and “various computer memory storage devices such as computer storage I-com 154, computer storage I-ext 156....” *Compare* EX1005 (Redlich), ¶124 *with* EX1001 (the '244 Patent), 439:7-15 (same disclosure). In particular, similar to the '244 Patent, Redlich explains:

PCs 140, 142, and PC-3 are connected together via a network 145 (LAN or WAN) and are also connected to an input/output device 146 that may be generally described as a router or a server to an outside communications system. The input/output device 146 is connected to *a telecommunications system 148 which leads to Internet 150*. The Internet is a global computer network. *Internet 150 is coupled to a plurality of servers*, one of which is server 152. Server 152 may be designated as an application service processor ASP. *Internet 150 also includes various computer memory storage devices* such as computer storage I-com 154, computer storage I-ext 156 and computer storage map 158.

Compare EX1005 (Redlich), ¶124 *with* EX1001 (the '244 Patent), 439:4-15 (same disclosure).

161. For another example, Figure 6 of Redlich, reproduced below on top of identical Figure 30 of the '244 Patent, illustrates another distributed computer system comprising a plurality of computers (PC-4, PC-5, PC-6, PC-7, PC-8, PC-9) and a plurality of servers (server 452 and servers associated with networks 404, 408, and 410) connected via a network (Communications Network 402):





Compare EX1005 (Redlich), Figure 6 with EX1001 (the '244 Patent), Figure 30 (same figure); see Section VII.A above.

162. Similar to '244 Patent Figure 30, Figure 6 discloses a communications network 402 that connects “various networks and personal computers” such as a plurality of computers (PC-4 to PC-9), stores 1 to 3 for “remote or offsite storage of extract data and remainder data,” and server 452 and PC-4 when “designated as the server for Network A.” Compare EX1005 (Redlich), ¶177 with EX1001 (the '244 Patent), 490:25-58 (same disclosure).

163. Additionally, a POSITA would understand that each of the various networks (Networks A, B, C) each comprise a server computer that manages and

executes the functions, services, and applications of the network. Similar to the '244 Patent, regarding Figure 6, Redlich explains:

Fig. 6 is an exemplary computer network diagram showing various user communities. The telecommunications network 402 is connected to the server application server provider ASP 452 and *to various networks and personal computers* ... Network A [404] is coupled to various PCs identified in FIG. 6 as PC-4, PC-5 and PC-6. Of course, Network A could be coupled to other PCs not illustrated in FIG. 6. As described earlier, *server 452 can facilitate remote or offsite storage of extract data and remainder data in store 1, store 2 and/or store 3* ... If PC-6 is designated as the input computer, the extract data may be stored on PC-4. Of course, PC-4 could be designated as the server for Network A.

Compare EX1005 (Redlich), ¶177 with EX1001 (the '244 Patent), 490:25-58 (same disclosure).

164. Redlich further discloses that its distributed computing system is a system for organizing and processing **data**. Specifically, Redlich discloses a particular method for “securing **data** in a computer system” that includes “establishing a group of security sensitive words, characters, icons, data streams or data objects, filtering the data input from a data input device and extracting the security sensitive data. The extracted data is separated from the remainder data and is separately stored.” EX1005 (Redlich), ¶34.

165. Redlich further discloses that its method for organizing and processing **data** includes a step for limiting access to the data by permitting “[r]econstruction of some or all of the **data** via one or more of the subsets of extracted data and the remainder data ... only in the presence of a predetermined security clearance from the plurality of security levels.” EX1005 (Redlich), ¶35.

166. Redlich further discloses organizing and processing **data** having select content represented by one or more predetermined words, characters, images, data elements or data objects. In particular, Redlich discloses a method in which the data being secured includes an “establish[ed] [] group of security sensitive words, characters, icons, data streams, or data objects.” EX1005(Redlich), ¶34 (“The method for securing **data** in a computer system in one embodiment includes *establishing a group of security sensitive words, characters, icons, data streams or data objects....*”); *see also* EX1005 (Redlich), ¶105 (“The security sensitive words, characters, icons or data objects may be any *word, phrase, letter, character, icon, data object (full or partial), image or whatever, as pre-defined or as established by the user*. The user may specifically design the filter, begin with a dictionary to define common terms, identify any additional security sensitive *words, letters, images, icon, data objects*, partial versions of the foregoing or any other granular aspect of the plaintext.”); EX1005, Claim 124 (“An information processing system for securing **data** *having one or more security sensitive words, characters, data*

objects or icons in a computer system with memories designated as a remainder store and an extract store”).

167. Additionally, Redlich discloses organizing and processing **data** by categorizing security sensitive content into pre-set (*e.g.*, predetermined) categories. EX1005 (Redlich), ¶46 (“Some aspects of the present invention introduce a new method and apparatus to monitor security sensitive content through a process of analysis and categorization of **each word or character, in a document**. The invention enables processing of **every character, word, number**, as they are entered into a document and categorizes each into one of many *pre-set categories*. Categories can include surnames, locations, currency, defined terminology, and unknown words or phrases.”).

168. In sum, Redlich discloses a distributed computer system for organizing and processing **data**, the **data** to be processed having select content represented by one or more predetermined words, characters, images, data elements or data objects.

b. [1pre-ii] said distributed computing system having (a) a plurality of select content data stores in a server cloud for respective ones of a plurality of security designated data and (b) a plurality of granular data stores,

169. Redlich discloses and/or renders obvious this limitation.

170. As discussed in Section X.A.1.i.a above, Redlich discloses a “distributed computing system.”

171. In particular, Redlich discloses a distributed computing system having **a plurality of select content data stores** for respective ones of **a plurality of security designed data**. Specifically, Redlich discloses a plurality of **extract stores** for storing **security sensitive content** extracted from the **data**. For example, Redlich discloses “extracting **security sensitive words, phrases, characters, icons, or data objects**” to form **extracted data** that is then stored in **one or more computer memories**. EX1005 (Redlich), ¶¶35 (“The method and the computer media containing programming instructions includes filtering data from the data input computer, extracting **security sensitive words, phrases, characters, icons, or data objects** and forming subsets of **extracted data** and remainder data. The subsets of **extracted data** are stored in **one or more computer memories** in the network identified as **extracted stores**.”), 176 (“The separation is accomplished by *extraction pursuant to security levels*, dispersion of **data** into **secure storage facilities (memory stores)** and reconstruction based upon the assigned security level.”).

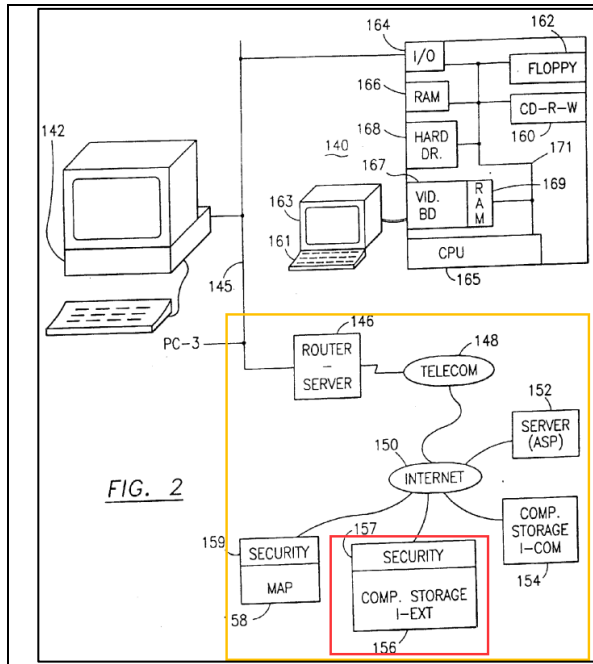
172. Redlich further discloses a **plurality of extract stores** wherein each **extract store** stores **security sensitive data** at a different security level. Redlich explains that “**the extract store** may comprise **a plurality of extract stores**” corresponding to “a plurality of security clearance levels.” EX1005 (Redlich), ¶245 (“[T]he **extract store** may comprise **a plurality of extract stores** operative in

conjunction with a plurality of security clearance levels.”). **Security sensitive content** of different security levels are stored at **different computer storage locations** corresponding to those levels. EX1005 (Redlich), ¶172 (“Each filter could filter out different levels of **security sensitive items** and each bundle or group of **security sensitive items** (from each distinct filter) could be stored at **different computer storage locations**.”).

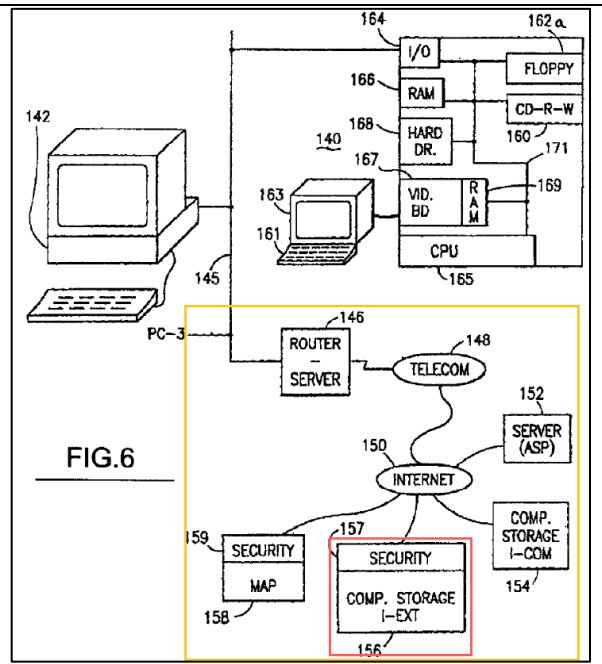
173. Redlich further discloses and/or renders obvious that the **plurality of select content stores** are in a **server cloud**. The specification of the '244 Patent does not mention the term “server cloud.” The '244 Patent does, however, disclose that a “‘cloud’ consists of many servers and the sensitive extracts may be dispersed all over the cloud to achieve high level security.” EX1001, 62:15-17. A POSITA would understand a **server cloud** as disclosed in the '244 Patent to thus be synonymous with the '244 Patent’s description of a cloud.

174. Redlich discloses a **plurality of extract stores** in a **server cloud**. In particular, Redlich discloses a distributed computer system comprising of many servers and **extracted data** dispersed in **extract stores** to achieve high level security. For example, Figure 2 of Redlich, reproduced below side-by-side identical Figure 6 of the '244 Patent, illustrates a distributed computer system comprising a “plurality of servers,” including servers 146 and 152, and “various memory storage devices such as computer storage I-com 154, [and] **computer storage I-ext 156**.”

Compare EX1005 (Redlich), ¶124 *with* EX1001 (the '244 Patent), 439:4-15 (same disclosure).



EX1005 (Redlich), Figure 2



EX1001 (the '244 Patent), Figure 6

Compare EX1005 (Redlich), Figure 2 *with* EX1001 (the '244 Patent), Figure 6 (same figure); *see also* Section VII.A above.

175. Additionally, similar to in the '244 Patent, Redlich discloses that “the **extracted data** (that is, the **high security data**), may be stored on **computer storage I-ext memory unit 156** via Internet 150, telecommunications system 148 and router/server 146. In this manner, the common data or remainder data is stored on hard drive 168 and the **highly sensitive data** is stored off site in a secured location.”

Compare EX1005 (Redlich), ¶127 *with* EX1001 (the '244 Patent), 439:61-67 (same disclosure).

176. In light of the '244 Patent's disclosure of a cloud, a POSITA would have understood that Redlich's disclosure of a group of servers and data stores is a **server cloud** as claimed in Claim 1 of the '244 Patent. The '244 Patent provides two descriptions relating to a **server cloud**. First, Claim 1 itself requires “a **plurality of select content data stores in a server cloud**.” EX1001 (the '244 Patent), Claim 1. Second, the '244 Patent explains that “[t]he ‘**cloud**’ consists of many servers and the sensitive **extracts** may be dispersed all over the cloud to achieve high level security.” EX1001 (the '244 Patent), 62:15-17. Redlich's disclosure of a group of servers and data stores in a distributed computer system as illustrated in Figure 2 meets these descriptions of a **server cloud**.

177. In particular, as explained above, the distributed computer system shown in Figure 2 of Redlich “consists of many servers” (*i.e.*, a plurality of servers, including servers 146 and 152), a **plurality of select content data stores** (*i.e.*, **extract stores**), and “**sensitive extracts**” (*i.e.*, **extracted data**) is dispersed all over (*i.e.*, in the **extract stores**).

178. Therefore, Redlich discloses and/or renders obvious “a **plurality of select content data stores** in a **server cloud**.”

179. Redlich's distributed computing system also comprises a plurality of **granular data stores**. Specifically, Redlich discloses **data stores that store granular data segments**. Redlich discloses that when data is parsed into "granular data groups," those groups of data are dispersed into "different storage locations" that store the granular data. EX1005 (Redlich), ¶238 ("The process involves parsing the documents or content into granular data groups and optionally creating small groups of data wherein the data segments cannot be recognized even to the level of providing 2-4 data objects in each file; *dispersing the granular data groups into different storage locations*"). Redlich further distinguishes data stores that store content (*i.e.*, **select content data stores**) and data stores that store granular content (*i.e.*, **granular data stores**). EX1005 (Redlich), ¶64 ("The present invention, in certain configurations, provides a controlled release security mechanism to enable the release of *content and granular content from storage locations* in a centralized and decentralized environment.").

180. In sum, Redlich discloses and/or renders obvious said distributed computing system having (a) a **plurality of select content data stores** (*i.e.*, **extract stores**) in a **server cloud** for respective ones of a **plurality of security designated data** (*i.e.*, **extracted data**) and (b) a **plurality of granular data stores**.

c. [1pre-iii] each said **select content data store** and **granular data store** having respective **access controls** thereat, said plurality of data stores and said **server cloud** operatively coupled over a communications network,

181. Redlich discloses and/or renders obvious this limitation.

182. As an initial matter, the '244 Patent explains that “[g]ranularity is achievable at word, character, symbol, or image bit levels.” EX1001 (the '244 Patent), 66:9-10. Redlich discloses the same level of granularity. *See* EX1005 (Redlich), ¶¶22 (“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...”), 34 (“The method for securing data in a computer system in one embodiment includes establishing a group of security sensitive words, characters, icons, data streams or data objects...”).

183. Redlich discloses **select content data stores** and **granular data stores** having respective **access controls**. Redlich discloses that access to select content data stores and to granular data stores is permitted based upon appropriate **security clearances**. For example, Redlich discloses that its system must determine whether a user has the right **security clearance**, such as the **correct password**, prior to being granted access to **extracted data** stored in the **extract store** and/or remainder data stored in the **remainder store**. EX1005 (Redlich), ¶¶122 (“The system first executes a security clearance protocol routine 122 in order to determine whether the

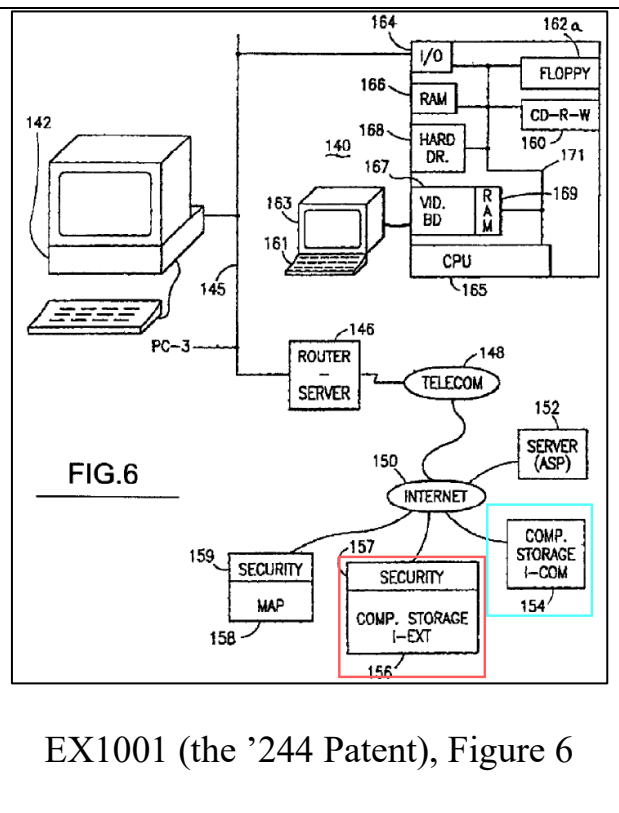
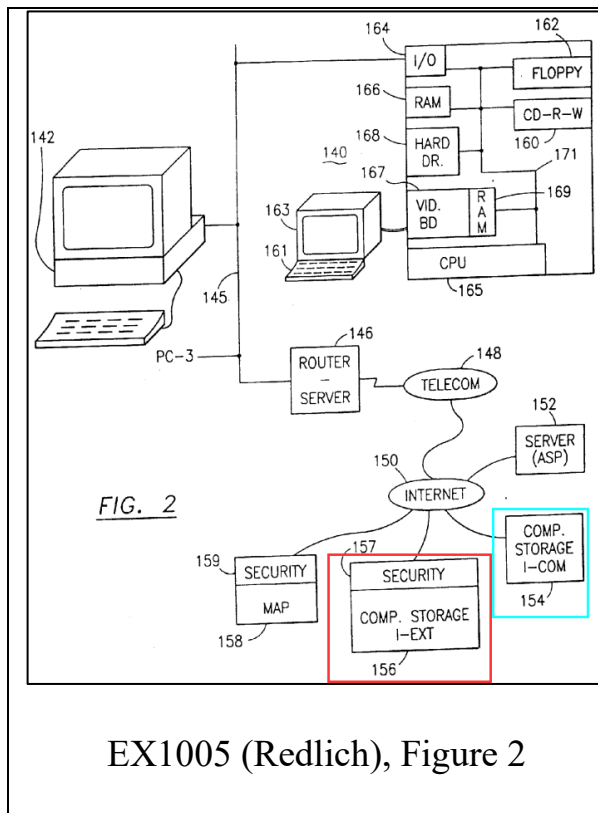
user has the proper **security clearance** ... Clearance is provided in Step 126. The location of the map and, hence, the location of the remainder data (**A-com 108**) and **extraction** [**B-ext 110**] is provided to the user's computer in step 128... The common or remainder data is downloaded or transferred or made available to the user's computer as shown at the output of map location and data step 128. Typically, the extracted or security sensitive data from B-ext is downloaded."), 144-145 ("In a preferred embodiment the user would have to input several passwords, one of them being a **local password** on computer 140 ... if the **password** is locally acceptable, the YES branch is taken and the system executes Step 308 which releases a reconstruction request to the common storage facility **I-com 154** or **A-com 108** (FIGS. 2 and 1A-B)."), 64 ("The present invention, in certain configurations, provides a controlled release **security mechanism** to enable the release of **content** and granular content from storage locations in a centralized and decentralized environment.").

184. Redlich also discloses providing limited access to **extract data stores** depending on the level of a user's **security clearance**. In particular, Redlich discloses that users with a **high security clearance** would be granted access to all of the **extracted data** and remainder data of the requested data, whereas users with a **security clearance** that is lower than the security level of the **extracted data** would be granted access to a "sanitized document" comprising of only the remainder

data. EX1005 (Redlich), ¶¶200 (“The classified granular content is dispersed to different secure, distributed storage locations. The **classification level of a user** will determine his right and ability to access and release the stored critical extracted content from the various storage locations for reconstruction. A user with **top classification** will view the entire document, while a user with a **lower level classification** *will view a sanitized document*, tailor made automatically for his clearance level.”), 35 (“Reconstruction of some or all of the data via one or more of the subsets of **extracted data** and the remainder data is permitted only in the presence of a **predetermined security clearance** from the plurality of security levels.”), 38 (“The addressee is permitted to retrieve the **extracted data** from **said extract store** only in the presence of a **predetermined security clearance** and hence, reconstruct the e-mail data with said **extracted data** and remainder data.”).

185. Redlich further discloses that the plurality of data stores and the **server cloud** are operatively coupled over a communications network. For example, Figure 2 of Redlich, reproduced below side-by-side identical Figure 6 of the '244 Patent, discloses a plurality of data stores (*i.e.*, data stores such as **computer storage I-com 154** and **computer storage I-ext 156**) and a **server cloud** (*i.e.*, the “plurality of servers” and “various memory storage devices”) that are operatively coupled over a communications network (*i.e.*, telecommunications system 148 and/or Internet 150). *Compare* EX1005 (Redlich), ¶124 (“The input/output device 146 is connected

to a *telecommunications system 148* which leads to *Internet 150* ... *Internet 150* is coupled to a plurality of servers ... *Internet 150* also includes various computer memory storage devices such as **computer storage I-com 154** [and] **computer storage I-ext 156**[.]” with EX1001 (the '244 Patent), 439:61-63 (same disclosure); see also Section VII.A above.



Compare EX1005 (Redlich), Figure 2 with EX1001 (the '244 Patent), Figure 6 (same figure).

186. As discussed in Section X.A.1.i.b above, Redlich discloses and/or renders obvious a **plurality of select content data stores** in a **server cloud**.

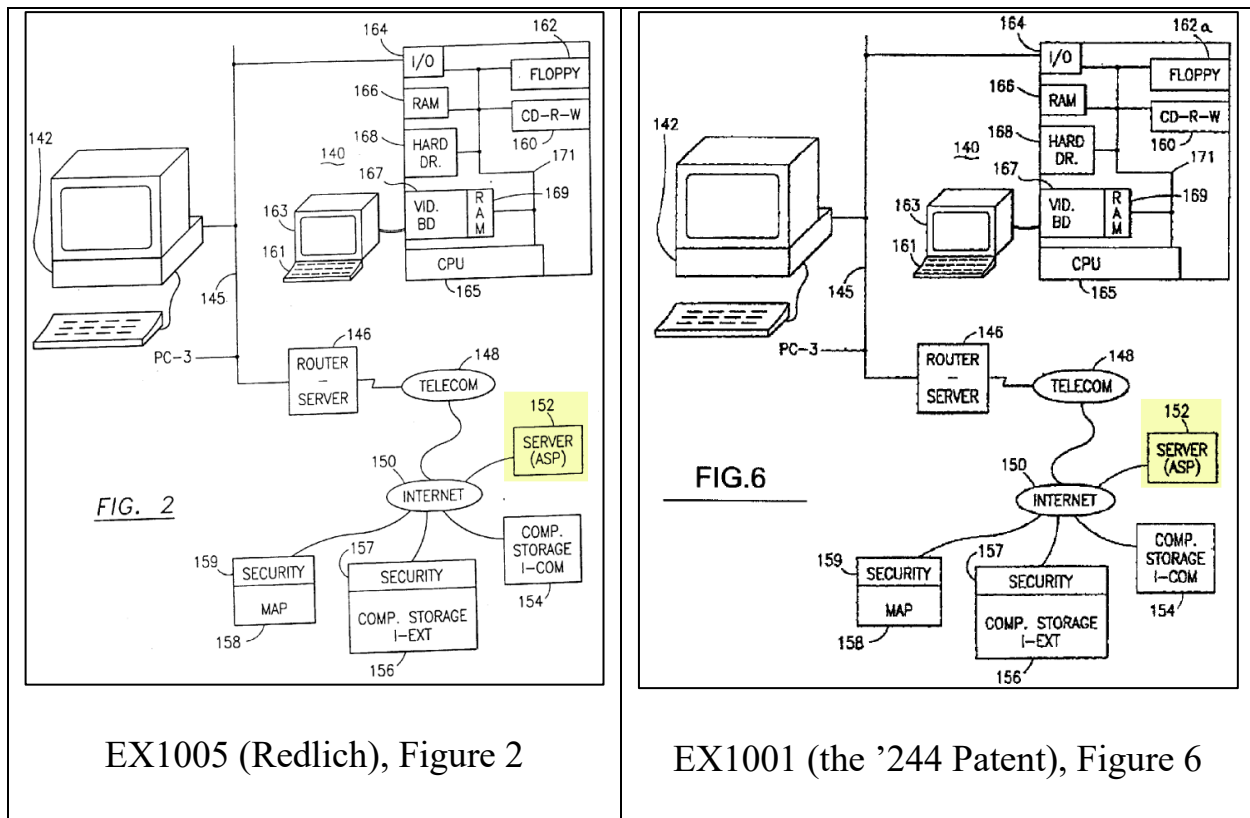
187. In sum, Redlich discloses and/or renders obvious each said **select content data store** (*i.e.*, **extract store**) and **granular data store** (*i.e.*, **remainder store**) having respective **access controls** (*i.e.*, **security clearance** or **password**) thereat, said plurality of data stores and said **server cloud** operatively coupled over a communications network.

ii. [1a] means for identifying **plurality of select content data stores** for respective ones of a **plurality of security designated data** in said **server cloud**;

188. The claimed function is “identifying plurality of select content data stores for respective ones of a plurality of security designated data in said server cloud” and the corresponding structure is an application service provider (“ASP”) server, such as the server labeled as box 152 in Figure 6, performing the algorithm as described in EX1001 (the ’244 Patent), 436:34-46. *See* Section IX.A above.

189. Redlich discloses and/or renders obvious this limitation.

190. Redlich discloses the structure of this limitation. In fact, Redlich discloses the same ASP server and algorithm as the ’244 Patent. Figure 2 of Redlich, reproduced below side-by-side identical Figure 6 of the ’244 Patent, discloses the ASP server:



Compare EX1005 (Redlich), Figure 2 at box 152 with EX1001 (the '244 Patent), Figure 6 at box 152.

191. Similarly, the algorithm performed by the ASP server described in EX1005 (Redlich), ¶142 is the same algorithm disclosed in the '244 Patent, at EX1001 (the '244 Patent), 436:34-46. This is shown in the following comparison table:

EX1005 (Redlich)	EX1001 (the '244 Patent)
“[A] client-server system over the Internet may have URLs designating	“[A] client-server system over the Internet may have URLs designating

EX1005 (Redlich)	EX1001 (the '244 Patent)
storage sites and an <i>ASP 152</i> (FIG. 6) controlling storage. In this pre-set system, the user does not select the sites. The sites may be randomly selected by ASP 152. The ASP may use artificial intelligence AI to locate secure extract data storage sites. AI or inference machines can ascertain (a) traffic on communications channels, (b) storage limit issues, (c) transmission failures in the communications links, and (d) the degree of security necessitated by exterior events, i.e., terrorism alerts, virus alerts, war, data security warnings posted by trusted sources, MicroSoft, Norton, NASA, DoD, CDC, FBI, etc.” EX1005 (Redlich), ¶142.	storage sites and an <i>ASP 152</i> (FIG. 6) controlling storage. In this pre-set system, the user does not select the sites. The sites may be randomly selected by ASP 152. The ASP may use artificial intelligence AI to locate secure extract data storage sites. AI or inference machines can ascertain (a) traffic on communications channels, (b) storage limit issues, (c) transmission failures in the communications links, and (d) the degree of security necessitated by exterior events, i.e., terrorism alerts, virus alerts, war, data security warnings posted by trusted sources, MicroSoft, Norton, NASA, DoD, CDC, FBI, etc.” EX1001 (the '244 Patent), 436:34-46.

192. Redlich also discloses the function of this term, *i.e.*, identifying a plurality of select content data stores for respective ones of a plurality of security designated data in said server cloud. In fact, Redlich provides nearly identical disclosures for this function as the '244 Patent. This is shown in the following comparison table:

EX1005 (Redlich)	EX1001 (the '244 Patent)
“The sites may be randomly <i>selected by ASP 152</i> . The ASP may use artificial intelligence AI to locate secure extract data storage sites . AI or inference machines can ascertain (a) traffic on communications channels, (b) storage limit issues, (c) transmission failures in the communications links, and (d) the degree of security necessitated by exterior events, <i>i.e.</i> , terrorism alerts, virus alerts, war, data security warnings posted by trusted sources, Microsoft, Norton, NASA, DoD, CDC, FBI, etc.”	“The sites may be randomly <i>selected by ASP 152</i> . The ASP may use artificial intelligence AI to locate secure extract data storage sites . AI or inference machines can ascertain (a) traffic on communications channels, (b) storage limit issues, (c) transmission failures in the communications links, and (d) the degree of security necessitated by exterior events, <i>i.e.</i> , terrorism alerts, virus alerts, war, data security warnings posted by trusted sources, Microsoft, Norton, NASA, DoD, CDC, FBI, etc.”

EX1005 (Redlich)	EX1001 (the '244 Patent)
EX1005 (Redlich), ¶142.	EX1001 (the '244 Patent), 436:37-46
“[T]he extract store may comprise a plurality of extract stores operative in conjunction with a plurality of security clearance levels.”	“[T]he extract store may comprise a plurality of extract stores operative in conjunction with a plurality of security clearance levels.”
EX1005 (Redlich), ¶245.	EX1001 (the '244 Patent), 513:13-15.
“Each filter could filter out different levels of security sensitive items and each bundle of group of security sensitive items (from each distinct filter) <i>could be stored at</i> different computer storage locations. ”	“Each filter could filter out different levels of security sensitive (or select content) items and each bundle of group of security sensitive items (from each distinct filter) <i>could be stored at</i> different computer storage locations. ”
EX1005 (Redlich), ¶172.	EX1001 (the '244 Patent), 489:45-48.

193. Redlich additionally discloses that “[t]he **subsets of extracted data** are stored in **one or more computer memories** in the network *identified* as **extracted stores.**” EX1005 (Redlich), ¶35.

194. As discussed in Section X.A.1.i.b above, Redlich discloses and/or renders obvious a **plurality of select content data stores** in a **server cloud**.

195. In sum, Redlich discloses and/or renders obvious means for identifying **plurality of select content data stores** (*i.e.*, **extract stores**) for respective ones of a **plurality of security designated data** in said **server cloud**.

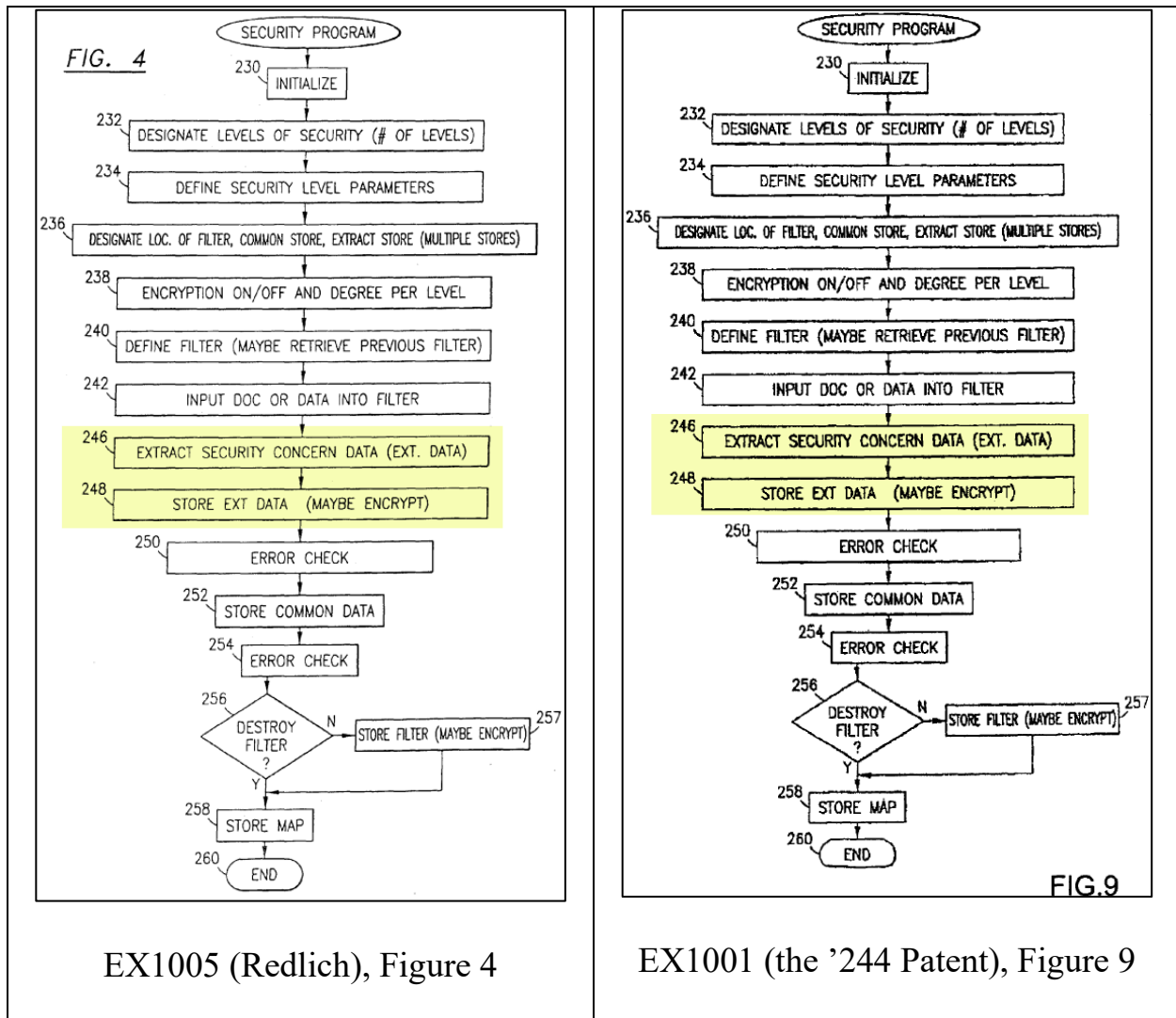
iii. [1b] an extractor for extracting and storing said **security designated data in respective select content data stores of said server cloud**;

196. The claimed function is “extracting and storing said security designated data in respective select content data stores of said server cloud” and the corresponding structure is a filter performing the algorithm as set forth in the boxes labeled as 246 and 248 in EX1001 (the '244 Patent), Figure 9 and described in EX1001 (the '244 Patent), 437:1-5. *See* Section IX.B above.

197. Redlich discloses and/or renders obvious this limitation.

198. Redlich discloses the structure of this limitation. Redlich discloses “***a data filter*** for the data input from the data input computer.” EX1005 (Redlich), ¶35 (“The information processing system which secures data per the community of interest security level in the [sic] includes ***a data filter*** for the data input from the data input computer which extracts the security sensitive words, phrases, icons or data objects.”).

199. The algorithm performed by the filter in Redlich is the same algorithm disclosed in the '244 Patent. Figure 4 of Redlich, reproduced below side-by-side identical Figure 9 of the '244 Patent, identifies the algorithm performed by the filter:



Compare EX1005 (Redlich), Figure 4 at boxes/steps 246 and 248 with EX1001 (the '244 Patent), Figure 9 at boxes/steps 246 and 248.

200. Similarly, the algorithm performed by the filter described in EX1005 (Redlich), ¶143 and represented by boxes/steps 246 and 248 above is the same

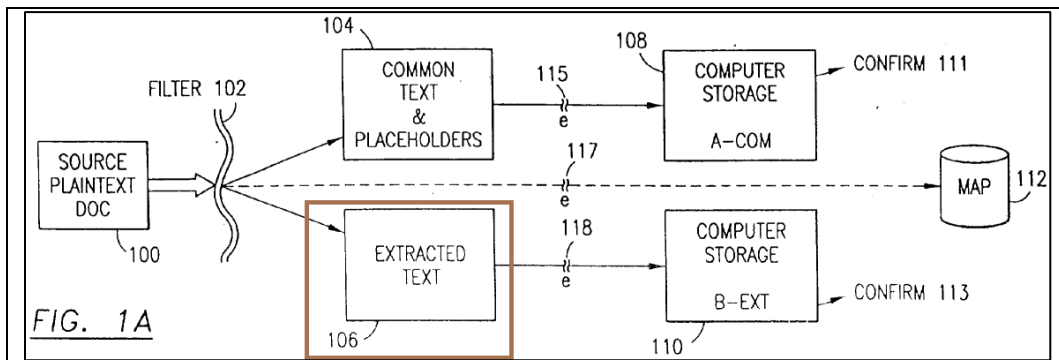
algorithm disclosed in the '244 Patent, at EX1001 (the '244 Patent), 437:1-45. This is shown in the following comparison table:

EX1005 (Redlich)	EX1001 (the '244 Patent)
“In any event, the plaintext document is fed through the filter. Step 246 extracts the security data from the input document. Step 248 stores the extracted data. The extracted data may be encrypted prior to storage.” EX1005 (Redlich), ¶143.	“In any event, the plaintext document is fed through the filter. Step 246 extracts the security data or SC data from the input document. Step 248 stores the extracted data. The extracted data may be encrypted prior to storage.” EX1001 (the '244 Patent), 437:1-5.

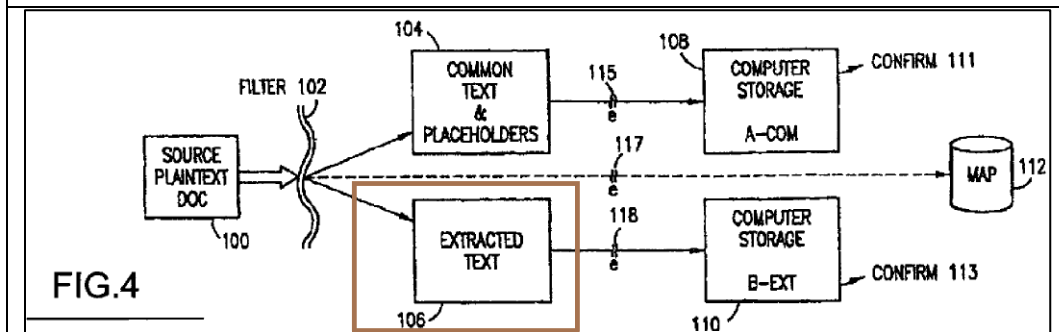
201. Redlich also discloses the function of this term, *i.e.*, extracting and storing said security designated data in respective select content data stores of said server cloud. First, Redlich discloses extracting security sensitive data from the data to separate the extracted data from the remainder data. EX1005 (Redlich), ¶¶34 (“The method for securing data in a computer system in one embodiment includes ... **extracting security sensitive data**. The **extracted data** is *separated from* the remainder data and is separately stored.”), 35 (“The method and the computer media containing programming instructions includes ... **extracting security sensitive**

words, phrases, characters, icons, or data objects and forming subsets of **extracted data** and remainder data.”), 38 (“The method *extracts the security sensitive words, characters or icons* from said e-mail data to obtain **extracted data** and remainder data therefrom.”), 134 (“[S]erver 152 maybe [sic] involved in ... *extracting the security sensitive words, characters, icons or data objects* to obtain **extracted data** and remainder data thereat, separately storing the **extracted data** from the remainder data (**extracted data** being placed in **computer memory I-ext 156** and remainder data being stored in **common remainder data memory I-com 154**) and then permitting reconstruction via separate or combined downloads of the remainder data and the **extracted data** into computer 140.”), Claim 138 (“[M]eans for extracting *extracts said security sensitive words, data objects, characters or icons* from said **data** to obtain (a) *subsets of extracted data* and (b) remainder data.”).

202. Figure 1A of Redlich, reproduced below on top of identical Figure 4 of the '244 Patent, also illustrates extracting *security sensitive content* from **data** to separate **extracted data** (106) from remainder data (*i.e.*, common text (104)).



EX1005 (Redlich), Figure 1A



EX1001 (the '244 Patent), Figure 4

Compare EX1005 (Redlich), Figure 1A with EX1001 (the '244 Patent), Figure 4.

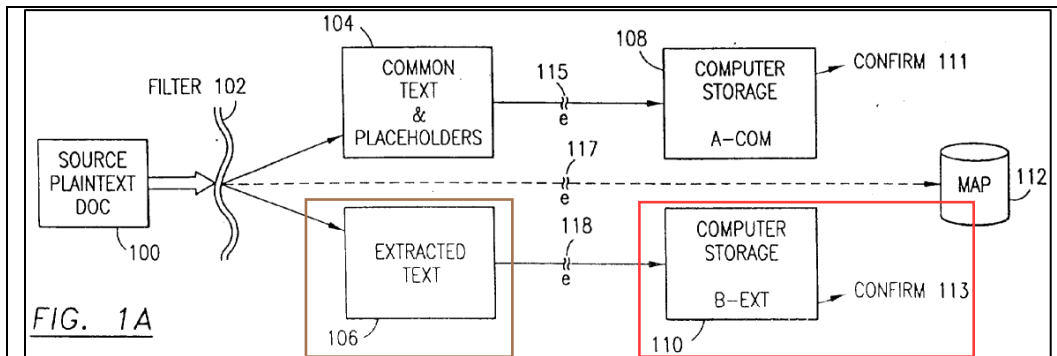
203. Redlich and the '244 Patent explain that in the above figures, “Filter 102 ... separates out common text or remainder data 104 from *uncommon text, words, characters, icons or data objects*. The *security sensitive words, characters, icons or data objects* are separated from remainder or common text 104 as *extracted text 106*.” Compare EX1005 (Redlich), ¶104 with EX1001 (the '244 Patent), 435:40-44 (identical disclosure).

204. Second, Redlich discloses storing the *extracted data* in a **plurality of extract stores**. In fact, Redlich provides nearly identical disclosures for this function as the '244 Patent, as shown in the following comparison table:

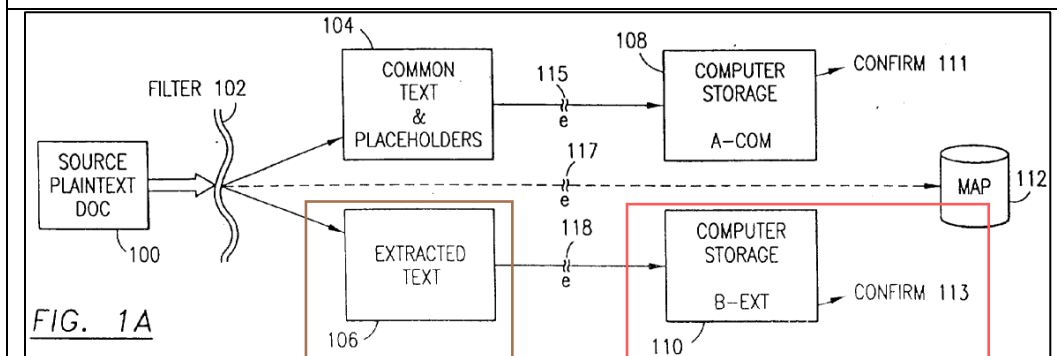
EX1005 (Redlich)	EX1001 (the '244 Patent)
“[T]he extract store may comprise a plurality of extract stores operative in conjunction with a plurality of security clearance levels.” EX1005 (Redlich), ¶245.	“[T]he extract store may comprise a plurality of extract stores operative in conjunction with a plurality of security clearance levels.” EX1001 (the '244 Patent), 513:13-15.
“Each filter could filter out different levels of security sensitive items and each bundle of group of security sensitive items (from each distinct filter) <i>could be stored at</i> different computer storage locations.” EX1005 (Redlich), ¶172.	“Each filter could filter out different levels of security sensitive (or select content) items and each bundle of group of security sensitive items (from each distinct filter) <i>could be stored at</i> different computer storage locations.” EX1001 (the '244 Patent), 489:45-48.

205. Redlich additionally discloses that “[t]he *subsets of extracted data* are *stored* in **one or more computer memories in the network identified as extracted stores.**” EX1005 (Redlich), ¶35.

206. Figure 1A of Redlich, reproduced below on top of identical Figure 4 of the '244 Patent, also illustrates the storing of *extracted data* in an **extract store**, which “may comprise a **plurality of extract stores** operative in conjunction with a plurality of security clearance levels.” EX1005 (Redlich), ¶245.



EX1005 (Redlich), Figure 1A



EX1001 (the '244 Patent), Figure 4

Compare EX1005 (Redlich), Figure 1A with EX1001 (the '244 Patent), Figure 4.

207. Redlich and the '244 Patent explain that the figures above show “[t]he *extracted data file 106* [] stored in a **different memory computer storage 110**.” Compare EX1005 (Redlich), ¶104 with EX1001 (the '244 Patent), 443:17-18 (identical disclosure).

208. As discussed in Section X.A.1.i.b above, Redlich discloses and/or renders obvious a **plurality of select content data stores** in a **server cloud**.

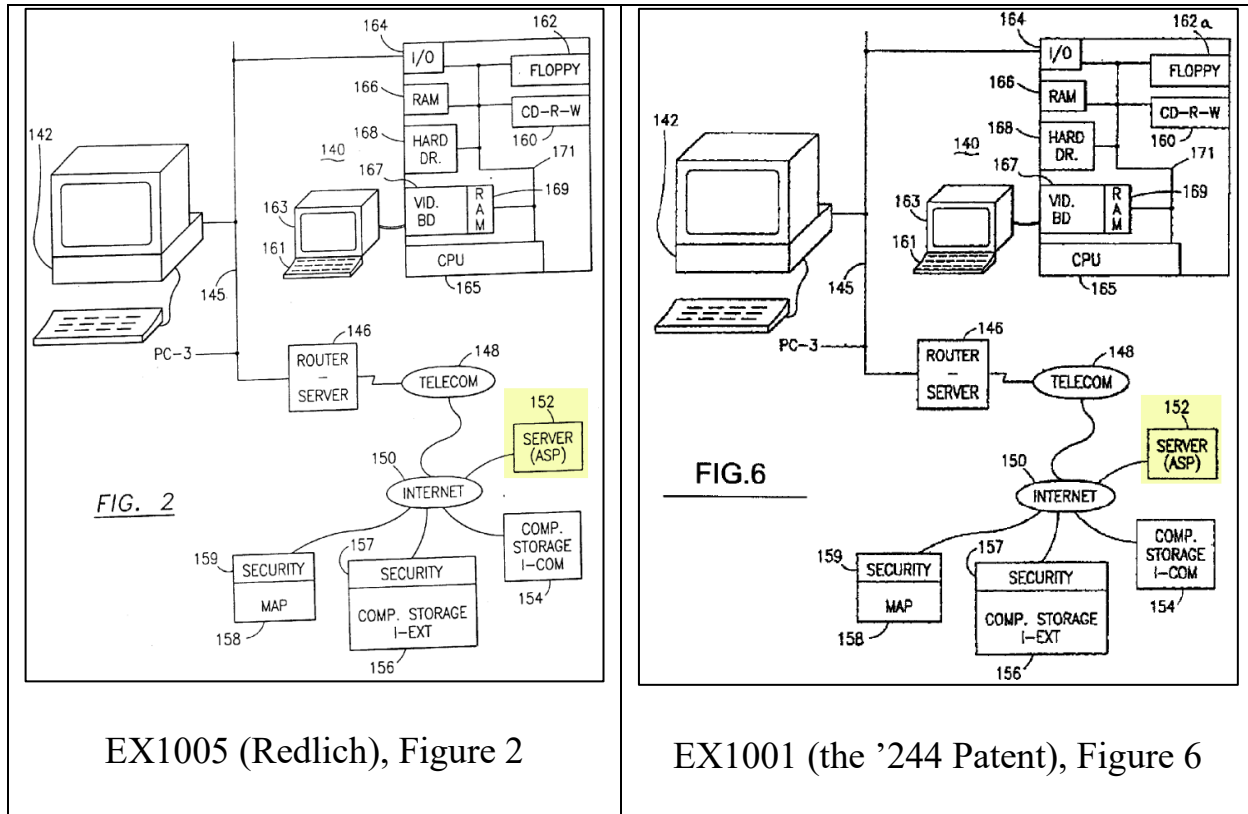
209. In sum, Redlich discloses and/or renders obvious an extractor for extracting and storing said **security designated data** in **respective select content data stores** (*i.e.*, **extract stores**) of said **server cloud**.

iv. [1c] a processor activating at least one of said **select content data stores** in said **server cloud** thereby permitting access to said **select content data stores** and respective **security designated data** based upon an application of one or more of said **access controls** thereat;

210. Redlich discloses and/or renders obvious this limitation.

211. A POSITA would have understood that Redlich discloses a processor in the same manner as the '244 Patent. In particular, a POSITA would have understood that the application provider (“ASP”) server disclosed in Redlich and in the '244 Patent is a computer that comprises a processor that carries out and executes the instructions for implementing the various application, functions, and services provided by the server.

212. Figure 2 of Redlich, reproduced below side-by-side identical Figure 6 of the '244 Patent, discloses the ASP server that comprises the processor:



Compare EX1005 (Redlich), Figure 2 at box 152 with EX1001 (the '244 Patent), Figure 6 at box 152.

213. Redlich and the '244 Patent both explain that the ASP server is an “application service provider” that is a “server on a network.” *Compare* EX1005 (Redlich), ¶103 *with* EX1001 (the '244 Patent), 522:15 (“Abbreviations Table”).

214. Redlich and the '244 Patent further explain that a server, such as the ASP server, is a computer. *Compare* EX1005 (Redlich), ¶¶177 (“Of course, ***PC-4 could be designated as the server*** for Network A.”), 221 (“[D]uring high utilization

of the computer network (high utilization in a *server computer* in a server-client environment)”) with EX1001 (the ’244 Patent), 490:57-58, 511:39-41 (same disclosures).

215. A POSITA would have also understood a server to be a computer. See EX1015 (MS-Dict.), 403-404:

Server n. 1. On a local area network (LAN), *a computer running administrative software* that controls access to the network and its resources, such as printer and disk drives, and provides resources to computers functioning as workstations on the network.

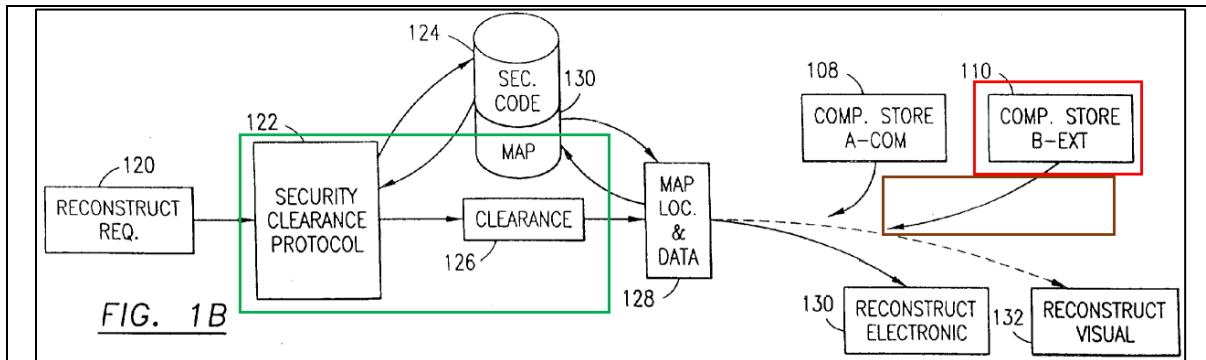
2. On the Internet or other network, a computer or program that responds to commands from a client. For example, a file server may contain an archive of data or program files; when a client submits a request for a file, the server transfers a copy of the file to the client.

216. Moreover, Redlich and the ’244 Patent both disclose that a computer includes a CPU, which a POSITA would have understood to be a processor. Compare EX1005 (Redlich), ¶125 (“PCs include a keyboard or data input device 161, a display 163, *a central processing unit CPU 165*”) with EX1001 (the ’244 Patent), 523:36-37.

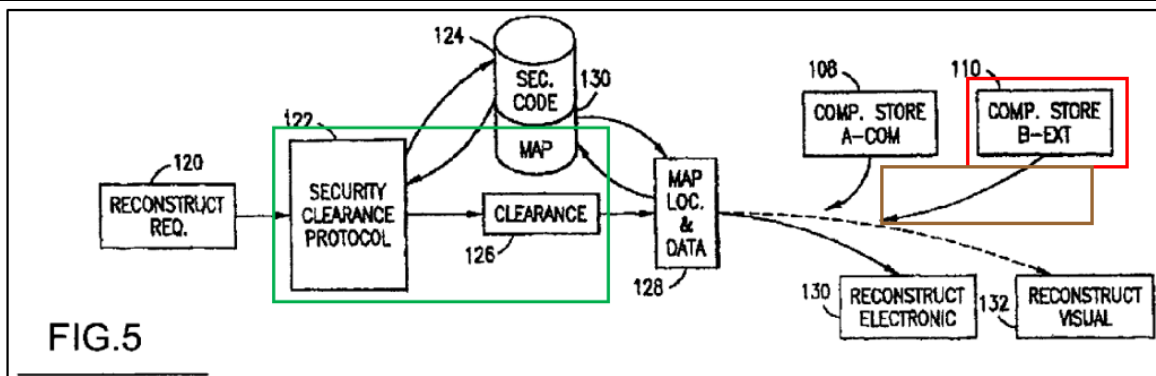
217. A POSITA would therefore have understood that the ASP server disclosed in Redlich is a computer that would include a processor (*i.e.*, a CPU).

218. Redlich further discloses the step of activating **extract stores** to retrieve **extracted data** from the **extract stores** in the presence of a **predetermined security clearance**, thereby permitting access to **extract stores** and their respective **extracted data**. Redlich discloses that when a user provides the appropriate **security clearance** and/or **additional access controls**, **extracted data** of the security level corresponding to the provided **security clearance** and/or **additional access controls** are received from the associated **extract store**. EX1005 (Redlich), ¶¶38 (“The *addresse[e]* is permitted to retrieve the **extracted data** from **said extract store** only in the presence of a **predetermined security clearance** and hence, reconstruct the e-mail data with said **extracted data** and remainder data.”), 200 (“The **classification level of a user** will determine his right and ability *to access and release* the stored critical **extracted content** from the various storage locations for reconstruction.”), 35 (“Reconstruction of some or all of the data via one or more of the subsets of **extracted data** and the remainder data is *permitted only* in the presence of a **predetermined security clearance** from the plurality of security levels.”), 55 (“*In order to view the reconstructed critical information* the user would need to be verified by **additional access controls** at the data storage level.”), Claim 124 (“means for *permitting* full or partial reconstruction of said data via said **extracted data** and remainder data only in the presence of a **predetermined security clearance**.”).

219. Figure 1B of Redlich, reproduced below on top of identical Figure 5 of the '244 Patent, further illustrates activating **extract stores** to retrieve **extracted data** from the **extract stores** in the presence of a **predetermined security clearance**:



EX1005 (Redlich), Fig. 1B



EX1001 (the '244 Patent), Fig. 5

Compare EX1005 (Redlich), Figure 1B with EX1001 (the '244 Patent), Figure 5.

220. Redlich and the '244 Patent explain that in the above figures, “[t]he system first executes a security clearance protocol routine 122 in order to determine whether the user has the proper security clearance. The **security clearance** may be

thought of as a **security clearance control** ... [T]he security clearance protocol determines the level of security clearance and, hence, the full or partial reconstruction of the plaintext. ... Typically, the **extracted** or **security sensitive data** from **B-ext** is downloaded.” Compare EX1005 (Redlich), ¶122 with EX1001 (the ’244 Patent), 447:3-12.

221. Redlich discloses that the step of activating **extract stores** to retrieve **extracted data** from the **extract stores** in the presence of a **predetermined security clearance** discussed above is performed by ASP server 152. EX1005 (Redlich), ¶131 (“The *server 152* would then call up and download data from various memory locations whether they be memory locations on computer 140 or memory locations **I-com 154** [and] **I-ext 156**”), 134 (“*[S]erver 152* maybe [sic] involved in ... permitting reconstruction via a separate or combined downloads of the remainder data and the extracted data into computer 140.”).

222. A POSITA would have understood that the processor of ASP 152 performs the activating step because a POSITA would have understood that processors typically execute instructions for implementing the various services and functions of a server, such as the activating step discussed above.

223. As discussed in Section X.A.1.i.b above, Redlich discloses and/or renders obvious a **plurality of select content data stores** in a **server cloud**.

224. In sum, Redlich discloses and/or renders obvious a processor activating at least one of said **select content data stores** (*i.e.*, **extract stores**) in **said server cloud** thereby permitting access to said **select content data stores** (*i.e.*, **extract stores**) and respective *security designated data* based upon an application of one or more of said **access controls** thereat.

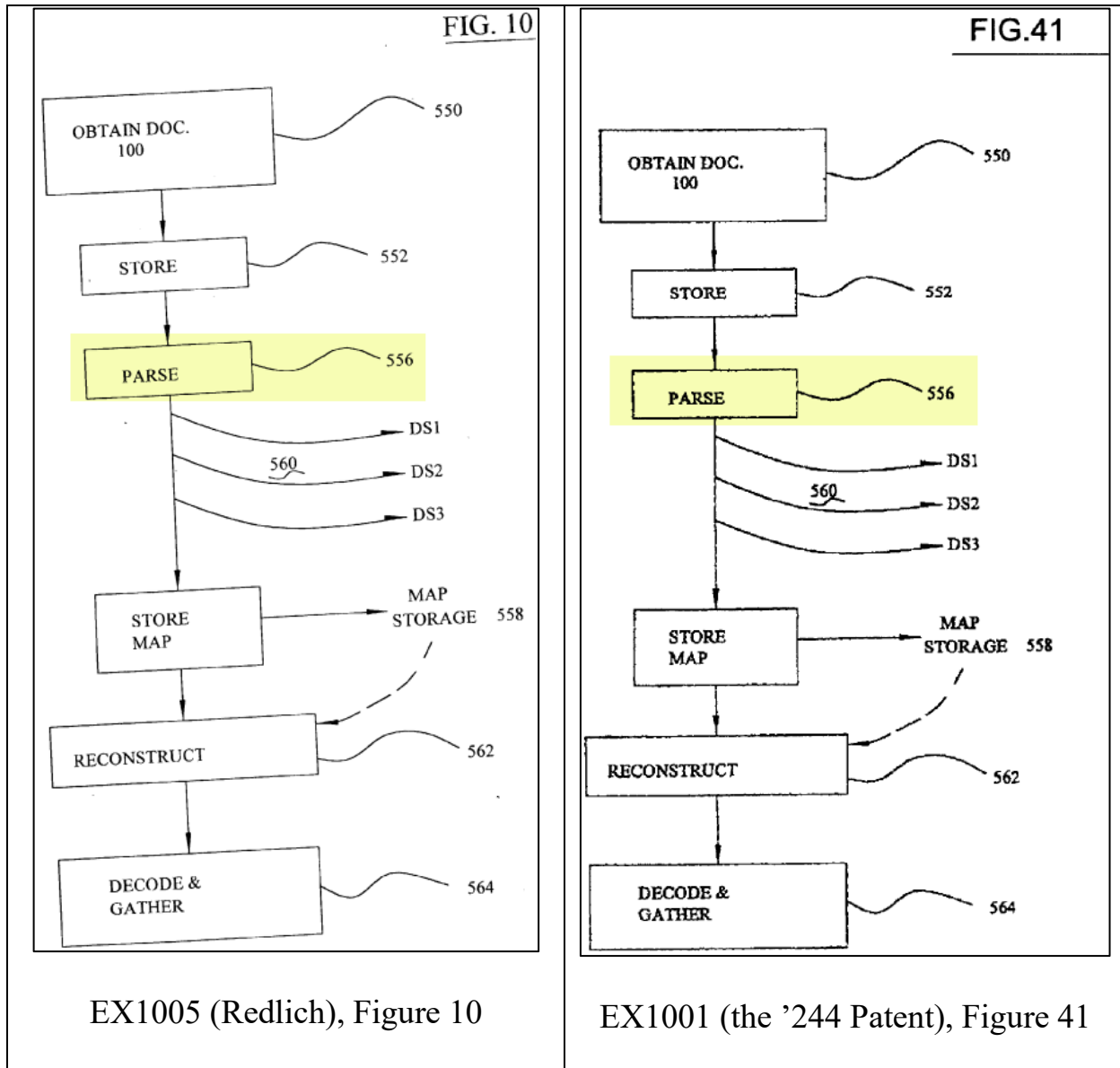
- v. [1d] means for parsing **remainder data** not extracted from **said data** to be processed and storing the **parsed data** as data segments in respective **granular data stores**;

225. The claimed function is “parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores” and the corresponding structure is a filter performing the algorithm as set forth in the box labeled as 556 in EX1001 (the '244 Patent), Figure 41 and described in EX1001 (the '244 Patent), 506:63-507:8 and 442:55-67. *See* Section IX.C above.

226. Redlich discloses and/or renders obvious this limitation.

227. Redlich discloses “*a data filter* for the data input from the data input computer.” EX1005 (Redlich), ¶35 (“The information processing system which secures data per the community of interest security level in the [sic] includes *a data filter* for the data input from the data input computer which extracts the security sensitive words, phrases, icons or data objects.”).

228. The algorithm performed by the filter in Redlich is the same algorithm disclosed in the '244 Patent. Figure 10 of Redlich, reproduced below side-by-side identical Figure 41 of the '244 Patent, identifies the algorithm performed by the filter:



Compare EX1005 (Redlich), Figure 10 at box 556 with EX1001, Figure 41 at box 556.

229. Similarly, the algorithm performed by the filter described in EX1005 (Redlich), ¶¶231, 106 and represented by box 556 above is the same algorithm disclosed in the '244 Patent, at EX1001 (the '244 Patent), 506:63-507:8 and 442:55-67. This is shown in the following comparison table:

EX1005 (Redlich)	EX1001 (the '244 Patent)
“A <i>parsing algorithm</i> function 554 is utilized in <i>parsing step 556</i> . The <i>parsing algorithm</i> , as stated earlier, targets the plain text 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. ... The parsed data [] is then dispersed into	“A <i>parsing algorithm</i> function 554 is utilized in <i>parsing step 556</i> . The <i>parsing algorithm</i> , as stated earlier, targets the plain text 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. ... The parsed data [] is then dispersed into

EX1005 (Redlich)	EX1001 (the '244 Patent)
storage facilities data store DS 1, 2, 3, 4, etc.” EX1005 (Redlich), ¶231.	storage facilities data store DS 1, 2, 3, 4, etc.” EX1001 (the '244 Patent), 506:63-507:8.
“The system and methodology described herein also encompasses <i>parsing the plain text document</i> by bit count, word, word count, page count, line count, paragraph count and parsing based upon any identifiable document characteristic, capital letters, italics, underline, etc. <i>Algorithms may be implemented to parse the plain text document ... The parsing occurs</i> with the filtering of the plain text source document 100 and the subsequent storage of <i>extracted data</i> apart from remainder data .”	“The system and methodology described herein also encompasses <i>parsing the plain text document</i> by bit count, word, word count, page count, line count, paragraph count and parsing based upon any identifiable document characteristic, capital letters, italics, underline, etc. Parsing is a contextual filter using a content as a marker and a range defines by certain file parameters. <i>Algorithms may be implemented to parse the plain text document ... The parsing occurs</i> with the filtering of the plain text source document 100 and

EX1005 (Redlich)	EX1001 (the '244 Patent)
EX1005 (Redlich), ¶106.	the subsequent storage of <i>extracted data</i> apart from <i>remainder data</i> .” EX1001 (the '244 Patent), 442:55-67.

230. A POSITA would have understood that Redlich discloses and/or renders obvious the function of this term, *i.e.*, parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores.

231. Redlich discloses parsing of **data** granularly into data segments. Redlich discloses that “[t]he *parsing* and dispersion aspects of the present invention enable the user to *parse*, disperse, and reconstruct the **data or data object** thereby enabling secure storage of the **data**.” EX1005 (Redlich), ¶37; *see also* EX1005 (Redlich), ¶143 (“*Granular extraction of data elements* in a data object may be permitted.”).

232. Redlich further discloses examples of the parsing of **data** granularly into data segments. As one example, Redlich discloses that for “financial data,” “a copy thereof can be parsed with *an algorithm*, the *parsed segments* dispersed off-site, (that is, separated and stored in extract and remainder stores or computer memories), away from the financial institute, and, upon appropriate security

clearance, the dispersed data can be reconstructed to duplicate the data.” EX1005 (Redlich), ¶37; *see also* EX1005 (Redlich), ¶¶106 (“The parsing occurs with the filtering of the plain text source document 100 and the subsequent storage of extracted data apart from remainder data.”), 238 (“The process involves *parsing the documents or content into granular data groups* and optionally creating small groups of data wherein the data segments cannot be recognized even to the level of providing 2-4 data objects in each file; dispersing the granular data groups into different storage locations; creation of a map of dispersal to the different storage locations (wherein the map is secured and encrypted and stored); and reconstructing the documents or data content.”).

233. Redlich also discloses parsing a plain text document in the same level of granularity as disclosed in the '244 Patent. This is shown in the following comparison table:

EX1005 (Redlich)	EX1001 (the '244 Patent)
“The system and methodology described herein also encompasses <i>parsing the plain text document</i> by bit count, word, word count, page count, line count, paragraph count and parsing	“The system and methodology described herein also encompasses <i>parsing the plain text document</i> by bit count, word, word count, page count, line count, paragraph count and parsing

EX1005 (Redlich)	EX1001 (the '244 Patent)
based upon any identifiable document characteristic, capital letters, italics, underline, etc. Algorithms may be implemented to parse the plain text document.” EX1005 (Redlich), ¶106.	based upon any identifiable document characteristic, capital letters, italics, underline, etc. Parsing is a contextual filter using a content as a marker and a range defines by certain file parameters. Algorithms may be implemented to parse the plain text document.” EX1001 (the '244 Patent), 442:55-67.

234. A POSITA would have understood that the parsing algorithm disclosed in Redlich could be applied to the remainder data. In particular, after the **security sensitive data** is extracted from the **data** as disclosed by Redlich, the **remainder data** would also need to be stored in data stores to allow for subsequent retrieval and reconstruction of the **data**.

235. One way that a POSITA would consider for storing the **remainder data** is by dividing the **remainder data** into smaller data segments and dispersing those resulting data segments to available **granular data stores** to ensure that there is sufficient capacity in the data stores. A POSITA would have also understood that distributing data across multiple data stores, and possibly multiple computers, also

improves overall throughput (*e.g.*, multiple servers can serve multiple client requests in parallel) as well as improving overall system resiliency (*e.g.*, a single downed node does not make all the data unavailable). Redlich discloses one particular way of dividing data, by parsing “by bit count, word, word count, page count, line count, paragraph count and parsing based upon any identifiable document characteristic, capital letters, italics, underline, etc.” EX1005 (Redlich), ¶106.

236. Redlich further discloses storing parsed data in **granular data stores**. For example, Redlich discloses that financial data “can be parsed with an algorithm [and] the *parsed segments dispersed off-site*, (that is, separated and stored in extract and remainder stores or computer memories)” EX1005 (Redlich), ¶37.

237. For another example, Redlich discloses the storing of granular data segments into different **storage locations**. *See, e.g.*, EX1005 (Redlich), ¶¶64 (“The present invention, in certain configurations, provides a controlled release security mechanism to enable the release of content and **granular content** from **storage locations** in a centralized and decentralized environment.”), 238 (“The process involves parsing the documents or content into granular data groups ... *dispersing the granular data groups into different storage locations*”), 2 (“The invention extracts, disperses, via a controlled release of *data segments to storage locations*, and permits reconstruction utilizing security protocols to provide a security system for **data**.”).

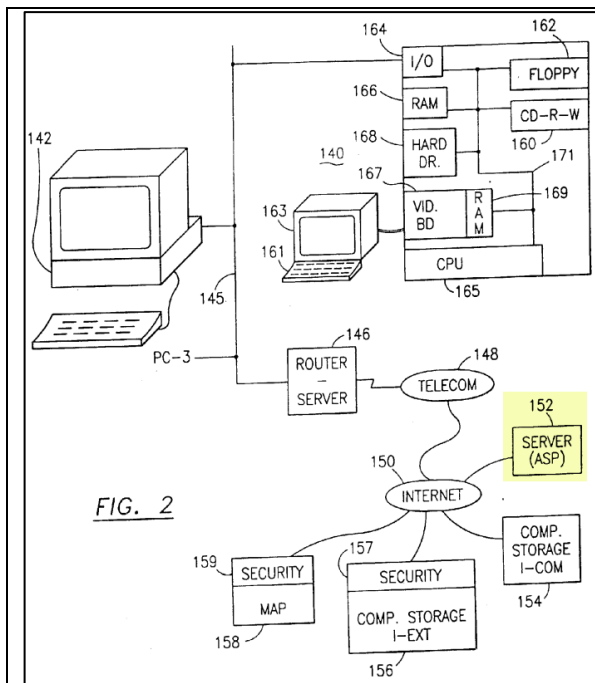
238. In sum, Redlich discloses and/or renders obvious means for parsing **remainder data** not extracted from **said data** to be processed and storing the **parsed data** as data segments in respective **granular data stores**.

- vi. [1e] said processor having means for applying a reconstruction data process employing said respective **access controls** to combine one or more of *said security designated data* and **remainder data**.

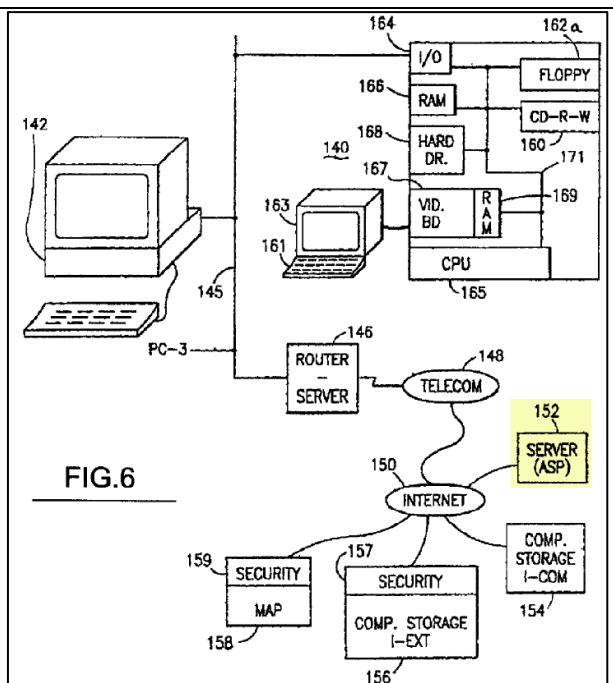
239. The claimed function is “applying a reconstruction data process employing said respective access controls to combine one or more of said security designated data and remainder data” and the corresponding structure is the processor of the ASP server performing the algorithm as set forth in box 328 of EX1001 (the ’244 Patent), Figure 10 and described in EX1001 (the ’244 Patent), 438:9-15 and 441:16-30. *See* Section IX.D above.

240. Redlich discloses this limitation.

241. Specifically, Redlich discloses the structure of this limitation. As explained in Section X.A.1.iv above, a POSITA would have understood that Redlich discloses a processor, the same processor as disclosed in the ’244 Patent. In particular, Figure 2 of Redlich, reproduced below side-by-side identical Figure 6 of the ’244 Patent, discloses the ASP server, which a POSITA would have understood comprises a processor.



EX1005 (Redlich), Figure 2



EX1001 (the '244 Patent), Figure 6

Compare EX1005, Figure 2 at box 152 with EX1001, Figure 6 at box 152.

242. Similarly, the algorithm performed by the processor of the ASP server described in EX1005 (Redlich), ¶¶131, 146 is the same algorithm disclosed in the '244 Patent, at EX1001 (the '244 Patent), 438:9-15, 441:16-30. This is shown in the following comparison table:

EX1005 (Redlich)	EX1001 (the '244 Patent)
"To reconstruct the document, the user at computer 140 would be required to call up the URL of server 152 and input	"To reconstruct the document, the user at computer 140 would be required to call up the URL of server 152 and input

EX1005 (Redlich)	EX1001 (the '244 Patent)
the appropriate security code. The server 152 would then call up and download data from various memory locations whether they be memory locations on computer 140 or memory locations I-com 154, I-ext 156 and map memory 158. The system compiles the entirety of the plaintext document by gathering the dispersed components thereof or compiles partial reconstructions for different levels of security.” EX1005 (Redlich), ¶131.	the appropriate security code. The server 152 would then call up and download data from various memory locations whether they be memory locations on computer 140 or memory locations I-com 154, I-ext 156 and map memory 158. The system compiles the entirety of the plaintext document by gathering the dispersed components thereof or compiles partial reconstructions for different levels of security.” EX1001 (the '244 Patent), 441:16-25.
“If the error checking routine on the extracted data is acceptable, the YES branch is taken from decision step 326 and the system, in step 328, proceeds to display the plaintext document or to	“If the error checking routine on the extracted data is acceptable, the YES branch is taken from decision step 326 and the system, in step 328, proceeds to display the plaintext document or to

EX1005 (Redlich)	EX1001 (the '244 Patent)
integrate the plaintext document pursuant to the security clearance initially input by the user.” EX1005 (Redlich), ¶146.	integrate the plaintext document pursuant to the security clearance initially input by the user.” EX1001 (the '244 Patent), 438:9-15.

243. Redlich also discloses the function of this term, *i.e.*, applying a reconstruction data process employing said respective access controls to combine one or more of said security designated data and remainder data. In particular, Redlich discloses applying a reconstruction data process in the presence of a **predetermined security clearance** in which one or more of the **extracted data** is combined with the **remainder data**. For example, Redlich discloses applying a reconstruction process to combine **extracted data** and **remainder data** of stored **email data** “only in the presence of a **predetermined security clearance**.” EX1005 (Redlich), ¶38 (“The addresse[e] is *permitted* to retrieve the **extracted data** from said **extract store** only in the presence of a **predetermined security clearance** and hence, *reconstruct the e-mail data* with said **extracted data** and **remainder data**.”).

244. For another example, Redlich discloses that the reconstruction data process that is applied could be full or partial reconstruction depending on the user’s **security clearance**. In particular, Redlich explains that “[r]econstruction of some

or all of the **data**” is permitted based on “the presence of a **predetermined security clearance** from the plurality of security levels.” EX1005 (Redlich), ¶35 (“*Reconstruction of some or all of the data* via one or more of the subsets of **extracted data** and the **remainder data** *is permitted* only in the presence of a **predetermined security clearance** from the plurality of security levels.”); *see also* EX1005 (Redlich), Claim 124 (“means *for permitting full or partial reconstruction of said data* via said **extracted data** and **remainder data** only in the presence of a **predetermined security clearance**.”), ¶200 (“The **classification level of a user** will determine his right and ability to access and release the stored **critical extracted content** from the various storage locations for reconstruction. A user with **top classification** will view the **entire document**, while a user with a **lower level classification** will view a *sanitized document, tailor made automatically for his clearance level*.”).

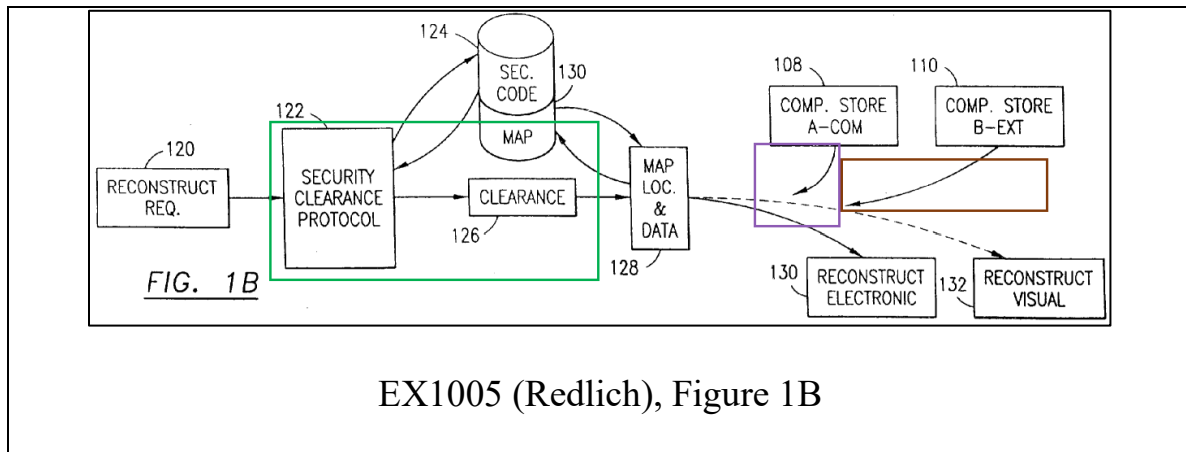
245. Redlich further discloses an example of reconstruction data process that could be applied:

To reconstruct the **document**, the user at computer 140 would be required to call up the URL of server 152 and input the **appropriate security code**. The server 152 would then call up and download data from various memory locations whether they be memory locations on computer 140 or memory locations **I-com 154**, **I-ext 156** and map memory 158. The system compiles the entirety of the **plaintext**

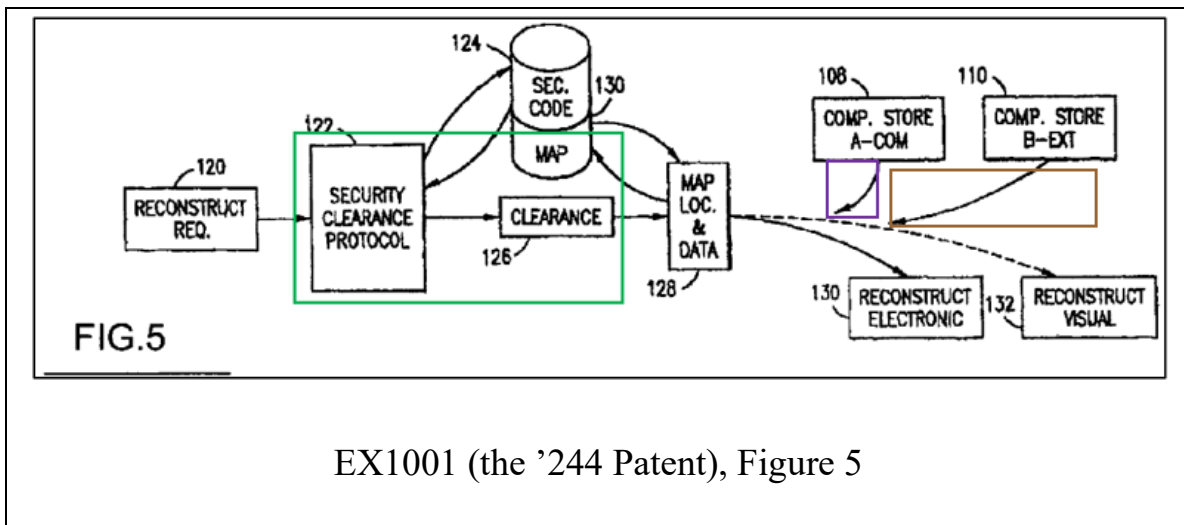
document by gathering the dispersed components thereof or compiles partial reconstructions for different levels of security. By implementing different security levels, the system is dynamic enough such that server 152 can easily locate the various extracted data levels based upon various **security codes** representing different security levels, as those codes are input by the user at computer 140.

EX1005 (Redlich), ¶131.

246. Figure 1B of Redlich, reproduced below on top of identical Figure 5 of the '244 Patent, further illustrates applying a reconstruction data process in the presence of a **predetermined security clearance** to combine one or more of the **extracted data** and the **remainder data**:



EX1005 (Redlich), Figure 1B



Compare EX1005 (Redlich), Figure 1B with EX1001 (the '244 Patent), Figure 5.

247. Figure 1B of Redlich shows the reconstruction process for a **plaintext document**. Similar to the '244 Patent, Redlich explains that “[t]he system first executes a security clearance protocol routine 122 in order to determine whether the user has the **proper security clearance**,” then permits a “full or partial reconstruction of the **plaintext**.” Compare EX1005 (Redlich), ¶122 with EX1001 (the '244 Patent), 447:5-12. The reconstruction of the **plaintext** is performed by “gather[ing] the **extracted data** and **remainder data** into a **single plaintext document**.” Compare EX1005 (Redlich), ¶122 with EX1001 (the '244 Patent), 447:29-31.

248. In sum, Redlich discloses said processor having means for applying a reconstruction data process employing said respective **access controls** to combine one or more of said **security designated data** and **remainder data**.

B. Ground 2: Claim 1 Is Obvious Over Redlich With Ozzie

1. Independent Claim 1

i. Claim 1 Preamble

249. To the extent the preamble is limiting, Redlich combined with Ozzie renders obvious the preamble of independent claim 1, as explained below.

a. [1pre-i] A distributed computer system for organizing and processing data, the data to be processed having select content represented by one or more predetermined words, characters, images, data elements or data objects,

250. As I explained in Section X.A.1.i.a above, Redlich discloses this limitation. Redlich combined with Ozzie renders obvious this limitation for the same reasons discussed in Section X.A.1.i.a above.

b. [1pre-ii] said distributed computing system having (a) a plurality of select content data stores in a server cloud for respective ones of a plurality of security designated data and (b) a plurality of granular data stores,

251. As I explained in Section X.A.1.i.b above, Redlich discloses and/or renders obvious this limitation. Redlich combined with Ozzie renders obvious this limitation for the same reasons discussed in Section X.A.1.i.b above.

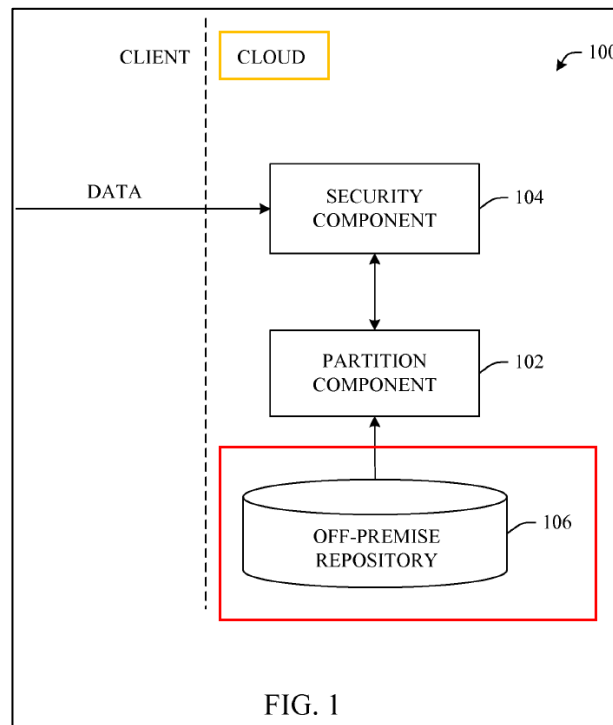
252. To the extent Patent Owner argues that Redlich does not disclose a plurality of select content stores in a server cloud, Ozzie discloses a system comprising a plurality of data stores for storing data in a server cloud.

253. As discussed in Section X.A.1.i.b above, the specification of the '244 Patent does not mention the term “server cloud.” However, the '244 Patent does disclose descriptions relating to a “**cloud**.” See EX1001 (the '244 Patent), 62:15-17 (“The ‘cloud’ consists of many servers and the sensitive extracts may be dispersed all over the cloud to achieve high level security.”).

254. In particular, the '244 Patent explains that that “[t]he ‘cloud’ consists of many servers.” EX1001 (the '244 Patent), 62:15. Claim 1 of the '244 Patent further requires that there be “a plurality of select content data stores *in* a server cloud.” The '244 Patent further explains that “sensitive extracts may be dispersed all over the cloud.” EX1001 (the '244 Patent), 62:15-17.

255. Ozzie discloses the same “**cloud**” of the '244 Patent. In particular, Ozzie describes a “**cloud**” that comprises of “many servers,” *i.e.*, “a group of one or more communicatively coupled ‘off-premise’ servers,” to which “**data** can be offloaded.” EX1006 (Ozzie), 4:53-55.

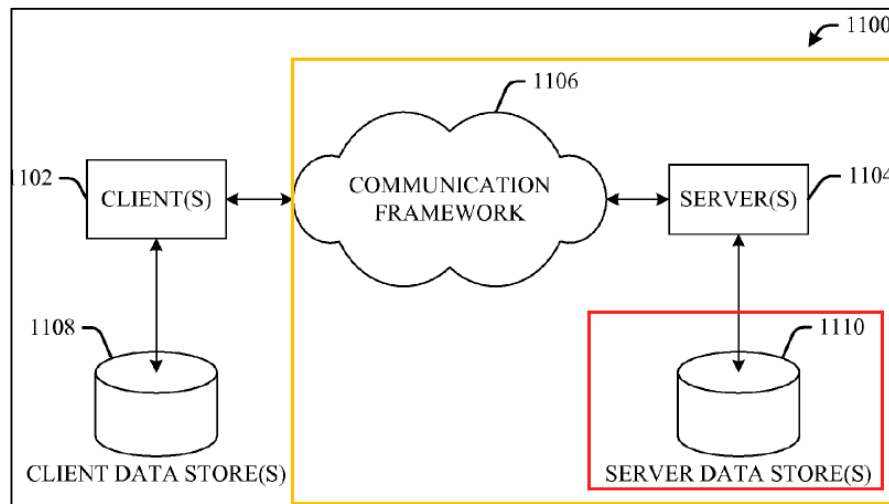
256. Figure 1 of Ozzie, reproduced below, illustrates such a “**cloud**,” comprising “cloud-based repositories” (EX1006 (Ozzie), 4:64-5:1) for storing **data**:



EX1006 (Ozzie), Figure 1.

257. Ozzie explains that the ***“off-site or ‘cloud-based’ repository 106”*** of Figure 1 of Ozzie can be partitioned into individual segments, which are “viewed as ‘drop-boxes’ for data maintained within the ‘cloud,’” thus allowing users to store **data** in these individual segments. EX1006 (Ozzie), 5:1-3 (“These individual segments can be viewed as ‘drop-boxes’ for **data** maintained within the **cloud**.”).

258. Figure 11 of Ozzie, reproduced below, provides another example of a **server cloud** “consist[ing] of ‘many servers’” and a **plurality of data stores** to which data may be dispersed:



EX1006 (Ozzie), Figure 11.

259. Figure 11 of Ozzie discloses a system 1100 comprising of a plurality of clients (1102) and a plurality of servers (1104). Ozzie explains that “system 1100 includes a communication framework 1106 (e.g., a global communication network such as the Internet) that can be employed to facilitate communications between the client(s) 1102 and the server(s) 1104.” EX1006 (Ozzie), 14:6-9.

260. Ozzie’s System 1100 of Figure 11 of Ozzie is also comprised of a plurality of server data stores (1110). Ozzie explains that “the server(s) 1104 are operatively connected to one or more server data store(s) 1110 that can be employed to store information local to the servers 1104.” EX1006 (Ozzie), 14:16-18.

261. As discussed above, the ’244 Patent discloses that in a **cloud**, “sensitive extracts may be dispersed all over the cloud.” EX1001 (the ’244 Patent), 62:15-17. Ozzie also discloses that **data** can be dispersed throughout its cloud. In particular,

Ozzie discloses that “**data** can be offloaded to a ‘**cloud**,’ such as a group of one or more communicatively coupled “off-premise servers.” EX1006 (Ozzie), 4:53-55. Specifically, Ozzie explains that to offload **data** to the **cloud**, “a user, application and/or service can ‘drop’ or save information into a respective segment based upon a particular operation.” EX1006 (Ozzie), 5:3-5.

262. Ozzie, therefore, discloses the **server cloud** as required in Claim 1 of the '244 Patent.

263. As discussed in Section X.B.1.vii below, a POSITA would have been motivated to combine Redlich with Ozzie to implement Ozzie’s server cloud in Redlich’s system and would also have had a reasonable expectation of success in combining Redlich with Ozzie.

264. In sum, Redlich combined with Ozzie renders obvious said distributed computing system having (a) a **plurality of select content data stores** in a **server cloud** for respective ones of a **plurality of security designated data** and (b) a **plurality of granular data stores**.

c. [1pre-iii] each said **select content data store** and **granular data store** having respective **access controls** thereat, said plurality of data stores and said **server cloud** operatively coupled over a communications network,

265. As I explained in Section X.A.1.i.c above, Redlich discloses and/or renders obvious this limitation. Redlich combined with Ozzie renders obvious this limitation for the same reasons discussed in Section X.A.1.i.c above.

266. To the extent Patent Owner argues that Redlich does not disclose a **plurality of select content stores** in a **server cloud**, Ozzie discloses a system comprising a **plurality of data stores** for storing **data** in a **server cloud** for the same reasons discussed in Section X.B.1.i.b above.

ii. [1a] means for identifying **plurality of select content data stores** for respective ones of a **plurality of security designated data** in said **server cloud**;

267. As I explained in Section X.A.1.ii above, Redlich discloses and/or renders obvious this limitation. Redlich combined with Ozzie renders obvious this limitation for the same reasons discussed in Section X.A.1.ii above.

268. To the extent Patent Owner argues that Redlich does not disclose a **plurality of select content stores** in a **server cloud**, Ozzie discloses a system comprising a **plurality of data stores** for storing **data** in a **server cloud** for the same reasons discussed in Section X.B.1.i.b above.

- iii. [1b] an extractor for extracting and storing said security designated data in respective select content data stores of said server cloud;

269. As I explained in Section X.A.1.iii above, Redlich discloses and/or renders obvious this limitation. Redlich combined with Ozzie renders obvious this limitation for the same reasons discussed in Section X.A.1.iii above.

270. To the extent Patent Owner argues that Redlich does not disclose a plurality of select content stores in a server cloud, Ozzie discloses a system comprising a plurality of data stores for storing data in a server cloud for the same reasons discussed in Section X.B.1.i.b above.

- iv. [1c] a processor activating at least one of said select content data stores in said server cloud thereby permitting access to said select content data stores and respective security designated data based upon an application of one or more of said access controls thereat;

271. As I explained in Section X.A.1.iii above, Redlich discloses and/or renders obvious this limitation. Redlich combined with Ozzie renders obvious this limitation for the same reasons discussed in Section X.A.1.iii above.

272. To the extent Patent Owner argues that Redlich does not disclose a plurality of select content stores in a server cloud, Ozzie discloses a system comprising a plurality of data stores for storing data in a server cloud for the same reasons discussed in Section X.B.1.i.b above.

- v. [1d] means for parsing remainder data not extracted from said data to be processed and storing the parsed data as data segments in respective granular data stores;

273. As I explained in Section X.A.1.v above, Redlich discloses and/or renders obvious this limitation. Redlich combined with Ozzie renders obvious this limitation for the same reasons discussed in Section X.A.1.v above.

- vi. [1e] said processor having means for applying a reconstruction data process employing said respective access controls to combine one or more of said security designated data and remainder data.

274. As I explained in Section X.A.1.vi above, Redlich discloses this limitation. Redlich combined with Ozzie renders obvious this limitation for the same reasons discussed in Section X.A.1.vi above.

vii. Reasons To Combine Redlich With Ozzie

275. A POSITA would have been motivated to combine Redlich and Ozzie to organize and process data in a computer system comprising of a plurality of data stores in a server cloud, as taught by Ozzie, in Redlich's system, to extract security sensitive information and subsequently store it separately from the remainder data, for at least the five reasons I discuss below.

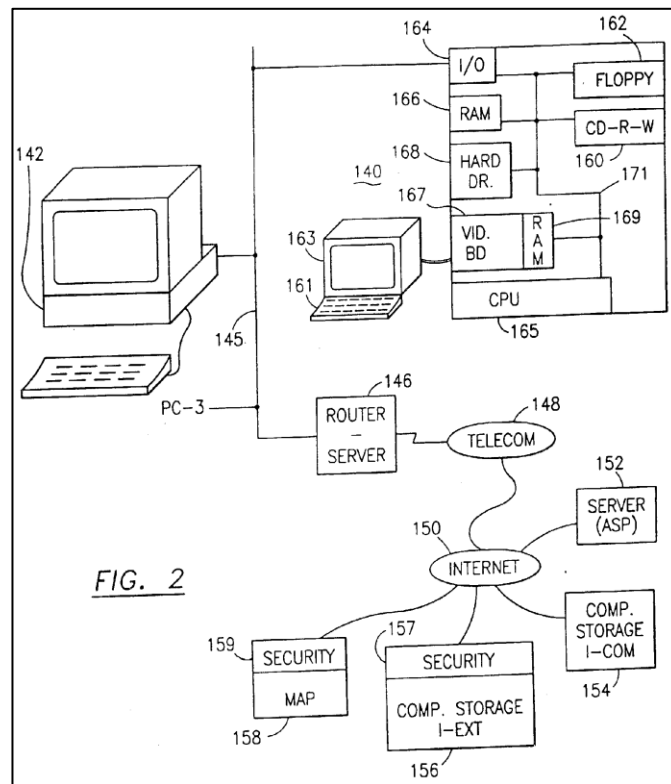
276. *First*, the combination of Redlich and Ozzie represents the use of known techniques according to known methods in the same way to yield predictable results. Redlich and Ozzie relate to the same field of storing information and both

Redlich and Ozzie address the same problem of maintaining security and efficient storage of the information. *Compare* EX1005 (Redlich), ¶18 (“It is an object of the present invention to provide a ***data security system***, an information processing system and a method for ***securely storing data*** and ***rebuilding that data in the presence of an adequate security clearance.***”) with EX1006 (Ozzie), 2:6-9 (“The innovation disclosed and claimed herein, in one aspect thereof, comprises a system that can enable a cloud-based data repository to function as a ***secure ‘drop-box’ for data that corresponds to a user.***”).

277. The Redlich and Ozzie combination would merely involve using Ozzie’s method of storing data in a cloud partitioned based on user identity with Redlich’s system for separating sensitive and non-sensitive elements within user data and storing the sensitive elements in a plurality of extract stores corresponding to a plurality of security levels. For example, Redlich’s system discloses a particular way of storing information, comprising extracting security sensitive content from data and separately storing the resulting extracted data from the remainder data. *See* EX1005 (Redlich), ¶¶35 (“The subsets of extracted data are stored in one or more computer memories in the network identified as extracted stores”), 172 (“Each filter could filter out different levels of security sensitive items and each bundle or group of security sensitive items (from each distinct filter) could be stored at different computer storage locations.”).

278. Redlich discloses that its system can be implemented in a distributed computer system. See EX1005 (Redlich), ¶¶99 (“The system, or method, according to the inventive principles as disclosed in connection with the preferred embodiment ... may be arranged in a distributed computer system, interconnected by any suitable means as would be known by one of ordinary skill in the art.”), 231(“[T]he dispersement 560 largely spreads out or distributes the parsed document 100 to a plurality of memories *in the distributed computer system.*”), 245 (“The method of securing e-mail data operates on *a distributed computer system* which at least includes a remote memory designated as an extract store.”).

279. Redlich discloses examples of such distributed computer systems. For example, Figure 2 of Redlich, reproduced below, shows a computer network system comprising a plurality of computers and servers:



EX1005 (Redlich).

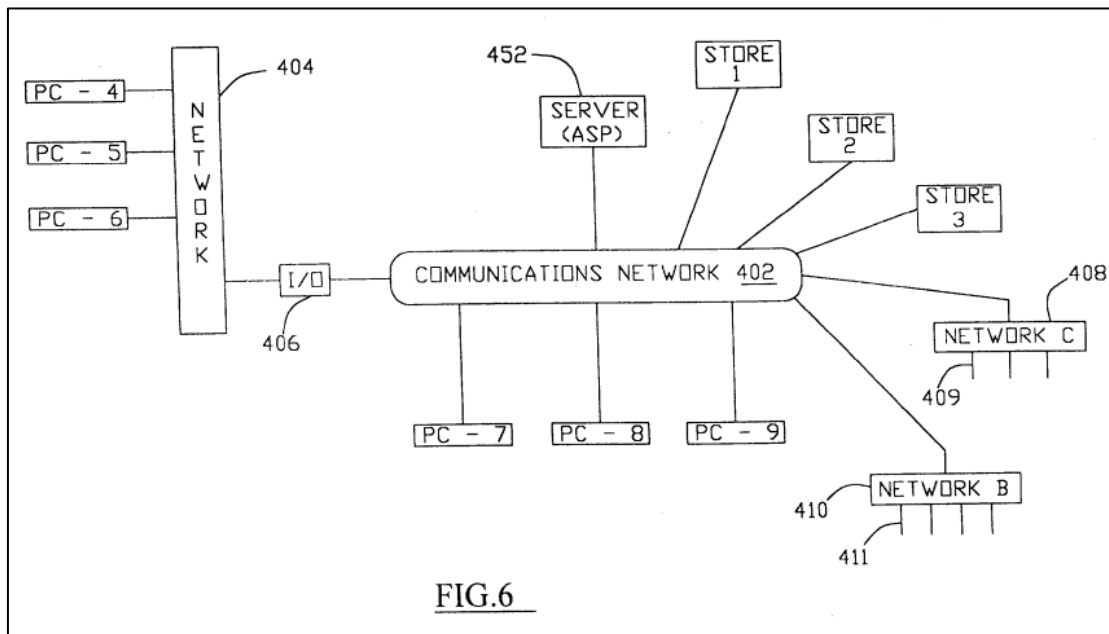
280. Figure 2 of Redlich discloses a distributed computer system which comprises a plurality of computers (PC 140, PC 142, PC-3) that are connected to a network of servers, which include Internet 150 and Server (ASP) 152, via router or server 146 and a telecommunications system 148. In particular, Redlich explains:

PCs 140, 142, and PC-3 are connected together via a network 145 (LAN or WAN) and are also connected to an input/output device 146 that may be generally described as a router or a server to an outside communications system. The input/output device 146 is connected to *a telecommunications system 148 which leads to Internet 150*. The Internet is a global computer network. *Internet 150 is coupled to a plurality of servers*, one of which is server 152. Server 152 may be

designated as an application service processor ASP. ***Internet 150 also includes various computer memory storage devices*** such as computer storage I-com 154, computer storage I-ext 156 and computer storage map 158.

EX1005 (Redlich), ¶124.

281. Figure 6 of Redlich, reproduced below, shows another example of a computer network system comprising a plurality of computers and servers:



EX1005 (Redlich), Figure 6.

282. Figure 6 of Redlich discloses a distributed computer system comprising a plurality of computers (PC-4, PC-5, PC-6, PC-6, PC-7, PC-8, PC-9), networks (Network A, Network B, Network C), and data stores (Store 1, Store 2, Store 3) interconnected by telecommunications network 402. In particular, Redlich explains:

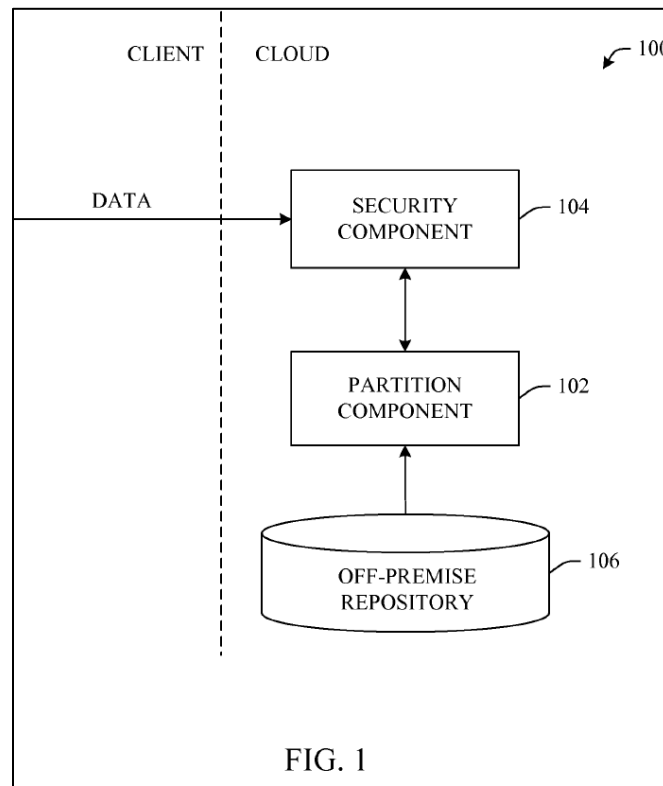
Fig. 6 is an exemplary computer network diagram showing various user communities. The telecommunications network 402 is connected to the server application server provider ASP 452 and *to various networks and personal computers* ... Network A [404] is coupled to various PCs identified in FIG. 6 as PC-4, PC-5 and PC-6. Of course, Network A could be *coupled to other PCs not illustrated in FIG. 6*. As described earlier, *server 452 can facilitate remote or offsite storage of extract data and remainder data in store 1, store 2 and/or store 3* ... If PC-6 is designated as the input computer, the extract data may be stored on PC-4. Of course, PC-4 could be designated as the server for Network A.

EX1005 (Redlich), ¶177.

283. Ozzie similarly discloses a particular way of storing data, by enabling storage of data in secure “drop-boxes” partitioned from cloud-based data repositories based on user identity. See EX1006 (Ozzie), 2:6-9 (“The innovation disclosed and claimed herein, in one aspect thereof, comprises a system that can *enable a cloud-based data repository to function as a secure ‘drop-box’ for data that corresponds to a user.*”), 4:51-57 (“[T]he subject innovation leverages the user-centric architecture of emerging ‘cloud-based’ system. For instance, rather than housing applications and data locally, *data can be offloaded to a ‘cloud’ such as a group of one or more communicatively coupled ‘off-premise’ servers.* In this manner, a user’s data can be accessed from any network connected computing device.”), 5:13-

21 (“Because storage occurs within the ‘cloud’, it can be useful to *partition or segment the cloud* in order to enhance organization and ease of locating resources. Thus, the partition component 102 can be employed to *segment, or virtually segment, the cloud storage (e.g., data repositories 106)* as desired. For example, the cloud can be *partitioned in accordance with an identity of a user*. Thus, all data that corresponds to a particular identity of a user can be located within the same segment of the cloud.”), 4:33-36 (“The system 100 can effectively enable *information to be stored in partitions within the cloud* while preventing unwanted or unintended disclosure of the information.”), 4:64-5:12 (“As shown, system 100 can include *a partition component 104 that can partition an off-site or ‘cloud-based’ repository 106* ... These individual segments can be viewed as ‘drop-boxes’ for data maintained within the ‘cloud.’ ... In accordance with the distributed ‘cloud-based’ model, partitioning of the off-premise data as well as securing transmissions and storage of the data is particularly important to the overall integrity of the architecture.”), 13:64 (“The system 1100 also includes one or more server(s) 1104.”), 14:16-18 (“Similarly, the server(s) 1104 are operatively connected to one or more server data store(s) 1110 that can be employed to store information local to the servers 1104.”).

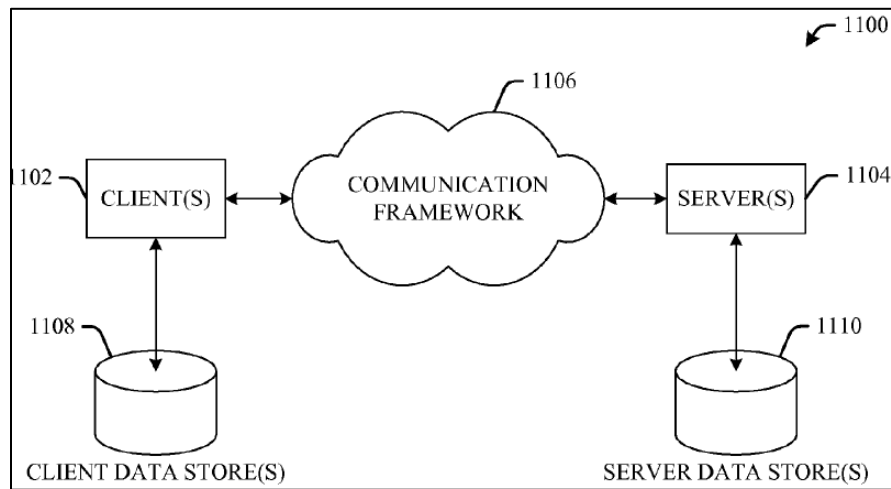
284. For example, Figure 1 of Ozzie reproduced below, illustrates Ozzie’s system for storing data in cloud-based data repositories:



EX1006 (Ozzie), Figure 1.

285. Ozzie explains that “system 100 [] includes a partition component 102 and a security component 104 that facilitate establishing a virtual ‘drop-box’ for encrypted data associated with an identity of an intended or target recipient. The partition component 102 can *partition an off-site repository(ies) 106 into multiple partitions thereby establishing drop-boxes* associated with an identity, type of data, etc.” As explained in Section X.B.1.i.b above, “off-site repositories” as disclosed in Ozzie are also known as cloud-based repositories. EX1006 (Ozzie), 4:65.

286. Figure 11 of Ozzie, reproduced below, also illustrates Ozzie’s system for storing data in cloud-based data repositories:



EX1006 (Ozzie), Figure 11.

287. Figure 11 of Ozzie discloses a system 1100 comprising of a plurality of clients (1102) and a plurality of servers (1104). “The system 1100 includes a communication framework 1106 (e.g., a global communication network such as the Internet) that can be employed to facilitate communications between the client(s) 1102 and the server(s) 1104.” EX1006 (Ozzie), 14:6-9.

288. Ozzie’s System 1100 is also comprised of a plurality of client data stores (1108) and server data stores (1110). “The client(s) 1102 are operatively connected to one or more client data store(s) 1108 that can be employed to store information local to the client(s) 1102.” EX1006 (Ozzie), 14:12-15. “Similarly, the server(s) 1104 are operatively connected to one or more server data store(s) 1110 that can be employed to store information local to the servers 1104.” EX1006 (Ozzie), 14:16-18.

289. Moreover, the combination would merely incorporate Ozzie's method of storing data in partitions of a cloud-based repository based on user identity, in Redlich's system, which also disclose storage of data in a cloud. *Compare* EX1005 (Redlich), ¶124:

FIG. 2 diagrammatically illustrates a personal computer or PC computer system 140, a second PC or computer 142, and a third PC-3. PCs 140, 142, and PC-3 are connected together via a network 145 (LAN or WAN) and are also connected to an input/output device 146 that may be generally described as a router or a server to an outside communications system. The input/output device 146 is connected to *a telecommunications system 148 which leads to Internet 150*. The Internet is a global computer network. *Internet 150 is coupled to a plurality of servers*, one of which is *server 152*. Server 152 may be designated as an application service processor ASP. *Internet 150 also includes various computer memory storage devices* such as *computer storage I-com 154, computer storage I-ext 156* and computer storage map 158.

with EX1006 (Ozzie), 4:11-18:

FIG. 1 illustrates a system 100 that includes a partition component 102 and a security component 104 that facilitate *establishing a virtual 'drop-box' for encrypted data associated with an identity of an intended or target recipient*. The partition component 102 can *partition an off-site repository(ies) 106 into multiple partitions*

thereby establishing drop-boxes associated with an identity, type of data, etc.

290. *Second*, a POSITA would have been motivated to combine Redlich with Ozzie, because Ozzie identifies a known problem (e.g., securely and efficiently managing data storage across multiple devices and services) and provides a solution to address the problem (e.g., storing data in a cloud partitioned in accordance with user identities).

291. Both Redlich and Ozzie acknowledge the problems with mass information sharing and the importance of data security. *Compare* EX1005 (Redlich), ¶3 (“Although the production, distribution and publication of documents is generally beneficial to society, there is a *need to limit the distribution and publication of security sensitive words, characters or icons*. Concerns regarding the privacy of certain data (for example, an individual’s social security number, credit history, medical history, business trade secrets and financial data) is an important issue in society. In another [sic] words, individuals and businesses have *a greater concern regarding maintaining the secrecy of certain information* in view of the increasing ease of distribution of documents through computer networks and the Internet.”) *with* EX1006 (Ozzie), 1:14-22:

[T]he conventional computing paradigm is beginning to shift as *maintaining security, indexing data, and the like on each client device*

can be quite expensive. As network connectivity has continued to improve, it has become apparent that a more efficient computing model includes light weight (e.g., inexpensive) clients that continuously communicate with third-party computing devices to achieve substantially similar end results when compared to the conventional computing paradigm.

292. A POSITA would have known that when users consider security measures for storage, they decide on the level and type of security to implement. While each of Redlich and Ozzie provide security measures, their combination yields versatile secure storage that is more efficient and more secure, thus allowing better control of access to security sensitive information. For example, while Redlich discloses versatile and granular security methods, Ozzie enables placing that secure data on (public) clouds that can be conveniently accessed from anywhere on the Internet.

293. Ozzie discloses storing data within a cloud that is partitioned by user identities, thereby securely and efficiently managing data storage across multiple devices and services. EX1006 (Ozzie), 2:6-9 (“The innovation disclosed and claimed herein, in one aspect thereof, comprises a system that can enable a cloud-based data repository to function as a secure ‘drop-box’ for data that corresponds to a user.”), 5:13-21 (“Because storage occurs within the ‘cloud’, it can be useful to partition or segment the cloud in order to enhance organization and ease of locating

resources. Thus, the partition component 102 can be employed to segment, or virtually segment, the cloud storage (e.g., data repositories 106) as desired. For example, the cloud can be partitioned in accordance with an identity of a user. Thus, all data that corresponds to a particular identity of a user can be located within the same segment of the cloud.”).

294. This storage method of partitioning of a cloud-based repository based on user identity would have been a motivation known to a POSITA in the field of information storage and improves the efficiency of the technology, by enabling the storage of data in a cloud-based data repository by user identities, thus leading to better organization and access of data. A POSITA would have known that conventional computer systems already provide data and file security by users, yet the placement of such data on (public) clouds makes it conveniently accessible from anywhere on the Internet. *See also* Section V.D above.

295. **Third**, a POSITA would have been motivated to use Ozzie’s method of storing data within a cloud because it would improve Redlich’s system for storing security sensitive information in a plurality of extract stores corresponding to the security level of the security sensitive information. Using Ozzie’s technique to improve Redlich’s system would allow for better organization and easier identification and access of a particular user’s data. EX1006 (Ozzie), 5:13-21 (“Because storage occurs within the ‘cloud,’ it can be useful to partition or segment

the cloud in order to *enhance organization and ease of locating resources*. Thus, the partition component 102 can be employed to segment, or virtually segment, the cloud storage (e.g., data repositories 106) as desired. For example, the cloud can be partitioned in accordance with an identity of a user. Thus, all data that corresponds to a particular identity of a user can be located within the same segment of the cloud.”). That is, the combination would merely be a use of a known technique (e.g., storing information in a cloud partitioned based on user identities) to improve similar methods (e.g., storing security sensitive information in data stores corresponding to the security level of the information, and to store all user’s data logically closer together thus improving network latency when a user accesses multiple data items) in the same way (e.g., by storing the information in a plurality of data stores based upon particular criteria).

296. As discussed in Section VI.B.1.ii, Redlich discloses extracting security sensitive content in terms of the data’s level of security or accessibility. Adding Ozzie’s teachings of storing security sensitive information in a cloud partitioned based on user identities would be an improvement to the access control afforded to users of Redlich’s system, because it would allow the storage of data of each user to be performed in a more organized and accessible manner, thus minimizing delay and improving “the overall integrity of the architecture.” EX1006 (Ozzie), 5:8-21. For example, implementing Ozzie’s technique in Redlich’s system could reduce latency

for a user to access their data because the data would be organized within the same or nearby partitions of the cloud. *See* EX1006 (Ozzie), 5:8-21.

297. A POSITA would have understood that Ozzie's teachings of storing security sensitive information in a cloud partitioned based on user identities would enable better secure storage than Redlich alone because the storage of data could be controlled in a more targeted manner. For example, a user's data could be stored in a partition on the cloud specific to the user, thus enabling that data to be more easily locatable and access to that data to be easier to limit. A user could store data in the user's specific data store that is limited only to that user. Alternatively, a user could globally set restrictions for the user's data at all data stores partitioned for that specific user.

298. ***Fourth***, a POSITA would have been motivated to combine Redlich with Ozzie, because the combination would involve applying a known technique (*e.g.*, using Ozzie's storage of content within a cloud) to a known device (*e.g.*, Redlich's network arrangement with a plurality of servers storing security sensitive and non-security sensitive content), which was ready for improvement to yield predictable results.

299. For example, it would be a trivial change to implement Ozzie's method of storing security sensitive information in a cloud partitioned based on user identities to Redlich's system, which already includes a cloud comprising of a

plurality of servers and data stores at which user data could be stored. *See* EX1005 (Redlich) ¶124:

FIG. 2 diagrammatically illustrates a personal computer or PC computer system 140, a second PC or computer 142, and a third PC-3. PCs 140, 142, and PC-3 are connected together via a network 145 (LAN or WAN) and are also connected to an input/output device 146 that may be generally described as a router or a server to an outside communications system. The input/output device 146 is connected to *a telecommunications system 148 which leads to Internet 150*. The Internet is a global computer network. *Internet 150 is coupled to a plurality of servers*, one of which is *server 152*. Server 152 may be designated as an application service processor ASP. *Internet 150 also includes various computer memory storage devices* such as *computer storage I-com 154, computer storage I-ext 156* and computer storage map 158.

300. Ozzie discloses a particular way of storing data in a cloud, by partitioning the cloud based on user identities and storing the data of each user at the user's partition. EX1006 (Ozzie), 5:15-21 ("Thus, the partition component 102 can be employed to segment, or virtually segment, the cloud storage (e.g., data repositories 106) as desired. For example, the *cloud can be partitioned in accordance with an identity of a user*. Thus, *all data that corresponds to a particular identity of a user can be located within the same segment of the cloud.*").

301. *Fifth*, Ozzie provides express motivations that would have led a POSITA to combine Ozzie's and Redlich's teachings. Ozzie acknowledges that "[a]s network connectivity has continued to improve, it has become apparent that a more efficient computing model includes lightweight (e.g., inexpensive) clients that continuously communicate with third-party computing devices to achieve substantially similar end results when compared to the conventional computing paradigm. In accordance with this architecture, the third-party can provide a 'cloud' of data, devices, and services, such that the requests by several clients can simultaneously be serviced within the cloud without the user noticing any degradation in computing performance." EX1006 (Ozzie), 1:20-26.

302. Ozzie then discloses a particular way of storing information in the cloud. For example, Ozzie illustrates an invention wherein information is "stored in partitions within a cloud while preventing unwanted or unintended disclosure of the information." EX1006 (Ozzie), 4:33-36. Specifically, Ozzie discloses that the partitioning of the cloud-based repository could be "based upon any criteria, including but not limited to, user identity, data type, associated service, associated activity, date created/modified, etc." EX1006 (Ozzie), 4:64-5:1.

303. Ozzie thus suggests that its method of storing of information in partitions within a cloud could be implemented in other inventions for which the storing of data across data stores distinguished based on a particular criterion, such

as Redlich's invention of storing security sensitive data in a plurality of extract stores corresponding to a plurality of security levels.

304. Ozzie further recognizes that storing information in partitions in a cloud has some security limitations. In particular, Ozzie acknowledges that "availability of data in this distributed architecture prompts a need for a mechanism by which data can be secured. In other words, because data is pooled within a cloud, it is important to limit access to data within the cloud-based architecture." EX1006 (Ozzie), 4:59-63. Ozzie thus recognizes that security access controls would be required for the storage of data within a cloud, such as the access controls disclosed by Redlich. *See* EX1005 (Redlich), ¶38 ("The addresse[e] is ***permitted to retrieve the extracted data*** from said extract store ***only in the presence of a predetermined security clearance*** and hence, reconstruct the e-mail data with said extracted data and remainder data.").

305. ***Finally***, a POSITA would have found that Redlich and Ozzie were analogous to the '244 Patent. All three pertain to the same field of endeavor, *i.e.*, securing and controlling access to security-sensitive information. *Compare* EX1001 (the '244 Patent), 1:15-19 ("The present invention relates to information management data processing modules and computer software system and method enabling protection of confidential information, identification of such information, identification of select content, classification for the same, and security system for

the same.”) *with* EX1005 (Redlich), ¶2 (“The present invention relates to a data security system and method and, more specifically, to a process, program and system which operates to secure files and data objects in portable computing devices. The invention extracts, disperses, via a controlled release of data segments to storage locations, and permits reconstruction utilizing security protocols to provide a security system for data.”) *and* EX1006 (Ozzie), 2:6-9 (“The innovation disclosed and claimed herein, in one aspect thereof, comprises a system that can enable a cloud-based data repository to function as a secure drop-box for data that corresponds to a user.”).

306. Furthermore, Redlich and the ’244 Patent have the same inventors listed (Ron Redlich and Martin Nemzow). *Compare* EX1005 (Redlich), 1 *with* EX1001 (the ’244 Patent), 1.

307. A POSITA would also have had a reasonable expectation of success in combining Redlich with Ozzie. Combining Redlich with Ozzie would merely involve incorporating a particular way of partitioning the databases in a cloud (*e.g.*, based on user identity) to Redlich’s system, which comprises a cloud comprising of a plurality of servers and databases in which user data could be stored. EX1006 (Ozzie), 2:6-9 (“The innovation disclosed and claimed herein, in one aspect thereof, comprises a system that can enable a cloud-based data repository to function as a secure drop-box for data that corresponds to a user.”), 5:15-21 (“Thus, the partition

component 102 can be employed to segment, or virtually segment, the cloud storage (e.g., data repositories 106) as desired. For example, the cloud can be partitioned in accordance with an identity of a user. Thus, all data that corresponds to a particular identity of a user can be located within the same segment of the cloud.”).

308. Ozzie provides a specific way for partitioning the cloud, which would be doable by a POSITA. *See* EX1006 (Ozzie), 4:64-5:1 (“[S]ystem 100 can include a partition component 104 that can partition an off-site or ‘cloud-based’ repository 106 based upon any criteria including, but not limited to, user identity, data type, associated service, associated activity, date created/modified, etc.”).

XI. Conclusion

309. In my opinion, the challenged claim 1 of the ’244 Patent is unpatentable.

XII. Availability for Cross-Examination

310. 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

311. 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

312. 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 22, 2023

Dr. Erez Zadok