

Case IPR2023-00973
U.S. Patent No. 8,468,244

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INTERNATIONAL BUSINESS MACHINES CORPORATION
Petitioner

v.

DIGITAL DOORS, INC.
Patent Owner

IPR2023-00973
U.S. Patent No. 8,468,244
PETITION FOR *INTER PARTES* REVIEW
UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104

TABLE OF CONTENTS

	<u>Page</u>
I. Introduction.....	1
II. Grounds For Standing.....	3
III. Summary Of The '244 Patent.....	3
A. Overview Of The '244 Patent	3
B. Prosecution History Of The '244 Patent	4
C. Priority Date Of The '244 Patent	8
IV. Level Of Ordinary Skill In The Art.....	9
V. Claim Construction.....	9
A. Means-Plus-Function Limitations	11
1. “means for identifying plurality of select content data stores for respective ones of a plurality of security designated data in said server cloud”.....	11
2. “an extractor for extracting and storing said security designated data in respective select content data stores of said server cloud”.....	12
3. “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”	12
4. “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”	14
VI. Relief Requested And The Reasons For The Requested Relief.....	15
A. Challenged Claim And Statutory Grounds For Challenge.....	15

1.	Redlich	15
2.	Ozzie	28
B.	Grounds 1-2: Redlich Renders Obvious Alone (Ground 1) And In Combination With Ozzie (Ground 2) Claim 1.....	30
1.	Independent Claim 1	30
VII.	Discretionary Denial Would Be Inappropriate.....	71
A.	Discretionary Denial Under The <i>Fintiv</i> Factors Is Not Appropriate.....	71
1.	No evidence regarding a stay	71
2.	Parallel proceeding trial date	72
3.	Investment in the parallel proceeding.....	73
4.	Overlapping issues with the parallel proceeding	74
5.	Identity of parties	74
6.	Other circumstances.....	74
B.	Discretionary Denial Under 35 U.S.C. § 325(d) Is Not Appropriate.....	75
VIII.	Conclusion	75
IX.	Mandatory Notices.....	77
A.	Real Party-in-Interest	77
B.	Related Matters.....	77
C.	Lead and Back-up Counsel and Service Information	77

TABLE OF AUTHORITIES

	<u>Pages(s)</u>
<u>Cases</u>	
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020)	71
<i>Automation, Inc. v. Olati LLC</i> , IPR2021-00146, Paper 11 (PTAB May 18, 2021)	10
<i>Continental Intermodal Group – Trucking LLC</i> , IPR2019-01393, Paper 24 (PTAB June 16, 2020)	71
<i>Dish Network L.L.C. v. Broadband iTV, Inc.</i> , IPR2020-01359, Paper 15 (Feb. 12, 2021)	71
<i>Intel Corp. v. PACT XPP Schweiz AG</i> , 61 F.4th 1373 (Fed. Cir. 2023)	67
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007)	65, 68, 69
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013 (Fed. Cir. 2017)	9
<i>PEAG LLC v. Varta Microbattery GmbH</i> , IPR2020-01214, Paper 8 (PTAB Jan. 6, 2021)	73
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	9
<i>Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC</i> , IPR2019-01393, Paper 24 (PTAB June 16, 2020)	74
<u>Statutes</u>	
35 U.S.C. § 102(b)	16
35 U.S.C. § 102(e)	28

35 U.S.C. § 103	15
35 U.S.C. § 112	10
35 U.S.C. § 311	1
35 U.S.C. § 314(a)	1, 15
35 U.S.C. § 325(d)	75

Rules

37 C.F.R. § 42.100	1
37 C.F.R. § 42.100(b)	9
37 C.F.R. § 42.104(a).....	3

EXHIBIT LIST

Exhibit No.	DESCRIPTION
1001	U.S. Patent No. 8,468,244 to Redlich et al.
1002	Prosecution History of U.S. Patent No. 8,468,244
1003	Declaration of Dr. Erez Zadok
1004	<i>Curriculum Vitae</i> of Dr. Erez Zadok
1005	U.S. Patent Publication No. 2003/018,2435 to Redlich et al.
1006	U.S. Patent No. 8,601,598 to Ozzie et al.
1007	Amended Docket Control Order, <i>DigitalDoors, Inc. v. Int’l Bus. Machs. Corp.</i> , Civil Action No. 2:22-cv-00457-JRG-RSP (E.D. Tex. Apr. 5, 2023).
1008	Scheduling Order, <i>DigitalDoors, Inc. v. Int’l Bus. Machs. Corp.</i> , Civil Action No. 2:22-cv-00457-JRG-RSP (E.D. Tex. Feb. 7, 2023).
1009	Federal Case Management Statistics for the Eastern District of Texas, as of June 30, 2022
1010	Plaintiff DigitalDoors, Inc.’s Disclosure of Asserted Claims and Initial Infringement Contentions, <i>DigitalDoors, Inc. v. Int’l Bus. Machs. Corp.</i> , Civil Action No. 2:22-cv-00457-JRG-RSP (E.D. Tex. Feb. 28, 2023).
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. 2007/0087756 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
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

Exhibit No.	DESCRIPTION
1020	Director's June 21, 2022 Memorandum on Discretionary Denials

IBM citations to specific pages of exhibits follow the pagination added to those exhibits per 37 C.F.R. § 42.63(d)(2)(i).

All emphasis has been added unless noted otherwise.

All annotations in Figures have been added unless noted otherwise.

I. Introduction

Pursuant to 35 U.S.C. §§ 311, 314(a), and 37 C.F.R. § 42.100, International Business Machines Corporation (“IBM” or “Petitioner”) respectfully requests that the Board cancel as unpatentable claim 1 (the “Challenged Claim”) of U.S. Patent No. 8,468,244 (“’244 Patent,” EX1001).

The Challenged Claim covers a method for organizing and processing data by separating and securely storing security designated portions of the data in a server cloud environment and then controlling access to the data based on access controls. Digital Doors Inc. (“Digital Doors” or “Patent Owner”) obtained the Challenged Claim by arguing during prosecution that the prior art did not include storing security designated data in data stores with corresponding security access controls and storing of parsed non-secure data in separate data stores.

But the features that Patent Owner highlighted to obtain the Challenged Claim were not new or inventive. This Petition demonstrates that separating and storing security designated data in data stores with corresponding security access controls in a server cloud environment was known. *See, e.g.*, EX1005 (“Redlich”), ¶34 (“The method for securing data ... 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.”); ¶38 (“The method

extracts the security sensitive words, characters or icons from said e-mail data to obtain extracted data and remainder data therefrom. The extracted data is stored in the extract store.... The addresse[e] is permitted to retrieve the extracted data from said extract store only in the presence of a predetermined security clearance...."); EX1006 ("Ozzie"), 4:53-55 ("[R]ather 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."). EX1003, ¶¶52-79.

This Petition also demonstrates that storing of parsed non-secure data in separate data stores was known. *See, e.g.*, EX1005, ¶238 ("The process involves parsing the documents or content into granular data groups ... dispersing the granular data groups into different storage locations...."), ¶37 ("The 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.... For example, financial data maintained by an institute in its original state, and a copy thereof can be parsed with an algorithm, the parsed segments dispersed off-site....").

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

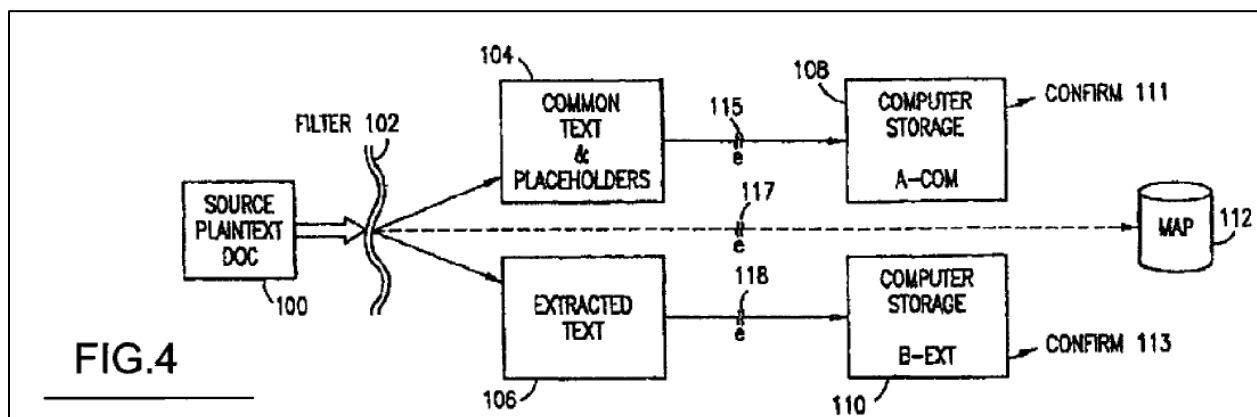
II. Grounds For Standing

Petitioner certifies that the '244 Patent is eligible for IPR and that Petitioner is not barred or estopped from requesting IPR challenging the patent claims. 37 C.F.R. § 42.104(a).

III. Summary Of The '244 Patent

A. Overview Of The '244 Patent

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, 1:15-19. EX1003, ¶80. Figure 4, reproduced below, illustrates the disclosed information management system:



EX1001, Figure 4. As shown, source document 100, which contains data, is passed through filter 102. EX1001, 435:17-19. “Filter 102... separates out common text or remainder data 104 from uncommon text, words, characters, icons or data

objects.” EX1001, 435:40-42. The common data objects are then placed into remainder document or common datafile 104, and the uncommon words (or security sensitive words) are placed into a separate extracted text or extracted data file 106. EX1001, 435:49-56. The remainder and extracted data are then stored separately, with the remainder data stored in common storage memory 108, and the extracted data file 106 stored in a different memory computer storage 110. EX1001, 443:2-3; 443:17-18. EX1003, ¶¶80-85.

B. Prosecution History Of The '244 Patent

The '244 Patent was filed on April 29, 2009. EX1001, 1. The Examiner rejected claims as being unpatentable over U.S. Patent No. 5,960,080 (“Fahlman”) and U.S. Patent Publication No. 2007/0087756 (“Hoffberg”). EX1002, 2230; EX1013; EX1014. 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, 2232. The Examiner noted that Hoffberg “teaches ... cloud based computing.” EX1002, 2233. “It 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, 2233. EX1003, ¶¶87-92.

In response, 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,” as 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 scarcity 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 scarcity 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 ~~scarcity designated~~ remainder data. ~~in said server cloud.~~

EX1002, 2253. EX1003, ¶93.

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, 2259. 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, 2260. 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, 2260. 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, 2260. Applicant also argued that there was no motivation to combine Fahlman with Hoffberg. EX1002, 2261. The Examiner allowed the claims after the amendment and remarks. EX1002, 2390. EX1003, ¶¶94-100.

This Petition illustrates that storing sensitive data in extract stores based on the data security level, storage of parsed remainder data in granular data stores, and allowing reconstruction based on a respective security clearance was known in the art. For example, Redlich—a prior art reference from the same inventors that was not considered by the Examiner—discloses storing sensitive data in extract stores

based on different security levels (e.g., storing security sensitive items of different security levels in different computer storage locations (EX1005, ¶172)), storing parsed remainder data in granular data stores (e.g., storing granular data groups into different storage locations (EX1005, ¶238), and allowing reconstruction based on a respective security clearance (e.g., different security clearances allow full or partial reconstruction (EX1005, Figure 1B, ¶122)).

C. Priority Date Of The '244 Patent

The earliest claimed priority date of the Challenged Claim is January 5, 2007, the filing date of a provisional application (EX1012) which the '244 Patent claims priority to. *See* EX1001, 1. Petitioner does not concede that the Challenged Claim is entitled to a priority date of January 5, 2007. In fact, during prosecution, the Examiner found that the provisional application that the '244 Patent claims priority to “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, 2221. This finding was not challenged by Applicant. However, because the prior art references discussed in this Petition qualify as prior art under the earliest claimed priority date of the '244 Patent, Petitioner does not challenge the priority date in this Petition but reserves the right to do so in other proceedings.

IV. Level Of Ordinary Skill In The Art

A Person Of Ordinary Skill In The Art (“POSITA”) would have had a bachelor’s degree in computer science, computer engineering, electrical engineering, or equivalent, and approximately two years of experience working in the field of data storage systems and data security as of January 5, 2007. Less professional experience can be substituted by additional education, and vice versa. EX1003, ¶¶135-136.

V. Claim Construction

Claim terms in IPRs are construed according to their “ordinary and customary meaning” to those of skill in the art. 37 C.F.R. § 42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (*en banc*). Petitioner submits that, for the purposes of this proceeding and the grounds presented herein, only the terms expressly construed below require express construction.¹ *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

¹ Nothing in this Petition should be construed as an admission that the claims, read in light of the specification and the prosecution history, inform a POSITA with reasonable certainty about the scope of the invention. While Petitioner proposes these constructions for purposes of this proceeding, Petitioner reserves its right to revise or amend these constructions in any other action or forum. *Western Digital*

Corp. v. Spex Techs., Inc., IPR2018-00084, Paper 14 at 11 (PTAB April 25, 2018) (“37 C.F.R. § 104(b)(3) does not require [a p]etitioner to express its subjective agreement regarding correctness of its proffered claim constructions or to take ownership of those constructions”). Petitioner also reserves the right to challenge the validity of the challenged claims under 35 U.S.C. § 112 in another other action or forum. *See Target Corp. v. Proxicom Wireless, LLC*, IPR2020-00904, Paper 11 at 12-13 (PTAB Nov. 10, 2020) (instituting IPR despite indefiniteness arguments in parallel lawsuit, explaining that this kind of “alternative pleading before a district court is common practice, especially where it concerns issues outside the scope of *inter partes* review”). The Board may reach obviousness of means-plus-functions claims—which is particularly the case here where many of the relevant disclosures in the challenged patent and the prior art are identical—even if the claims are indefinite. *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 801, 813-14 (Fed. Cir. 2021) (obviousness determination of indefinite means-plus-function claims possible, as indefiniteness precludes a patentability finding “only when the indefiniteness renders it logically impossible” to assess obviousness); *Haas Automation, Inc. v. Olati LLC*, IPR2021-00146, Paper 11 at 11–13 (PTAB May 18, 2021) (instituting IPR notwithstanding Petitioner’s position that claim term is subject to § 112, ¶ 6 and indefinite).

A. Means-Plus-Function Limitations

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

The function is “identifying plurality of select content data stores for respective ones of a plurality of security designated data in said server cloud.” To the extent a corresponding structure is disclosed, the 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, 436:34-46, and structural equivalents thereof. *See* EX1001, 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.”), 522:15 (“ASP application service provider - server on a network”), Figure 6. EX1003, ¶¶139-142.

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

The function is “extracting and storing said security designated data in respective select content data stores of said server cloud.” To the extent a corresponding structure is disclosed, the structure 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, 437:1-5, and structural equivalents thereof. *See* EX1001, 412:11-13 (“SC filter 45 may be one or more of a content-based filter, contextual filter or a taxonomic classification filter.”), 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.”), Figure 3, Figure 9. EX1003, ¶¶143-146.

3. “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”

The 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.” To the extent a corresponding structure is disclosed, the structure 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, 506:63-

507:8 and 442:55-67, and structural equivalents thereof. *See* EX1005, 412:11-13 (“SC filter 45 may be one or more of a content-based filter, contextual filter or a taxonomic classification filter.”), 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.”), 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.”), 435:17-19 (“A source document 100 containing data, sometimes referred to as a ‘plaintext,’ is passed through a filter 102.”), Figure 3, Figure 41. EX1003, ¶¶147-150.

4. “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”

The 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.” To the extent a corresponding structure is disclosed, the structure 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. *See* EX1001, 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.”), 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.”), Figure 6, Figure 10. EX1003, ¶¶151-154.

VI. Relief Requested And The Reasons For The Requested Relief

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

A. Challenged Claim And Statutory Grounds For Challenge

Petitioner requests cancellation of the Challenged Claim under 35 U.S.C. §103. This Petition, supported by the Declaration of Dr. Erez Zadok (EX1003), demonstrates that there is a reasonable likelihood that Petitioner will prevail with respect to the Challenged Claim. *See* 35 U.S.C. §314(a).

Grounds	Claim	Basis
#1	1	(§103) Redlich
#2	1	(§103) Redlich In View Of Ozzie

1. Redlich

U.S. Patent Publication No. US2003/0182435 (EX1005, “Redlich”), was filed on March 19, 2003, and was published on September 25, 2003. The two inventors (Ron Redlich and Martin Nemzow) are the inventors of the '244 Patent. *Compare* EX1005, 1 *with* EX1001, 1. Redlich was published more than one year before the

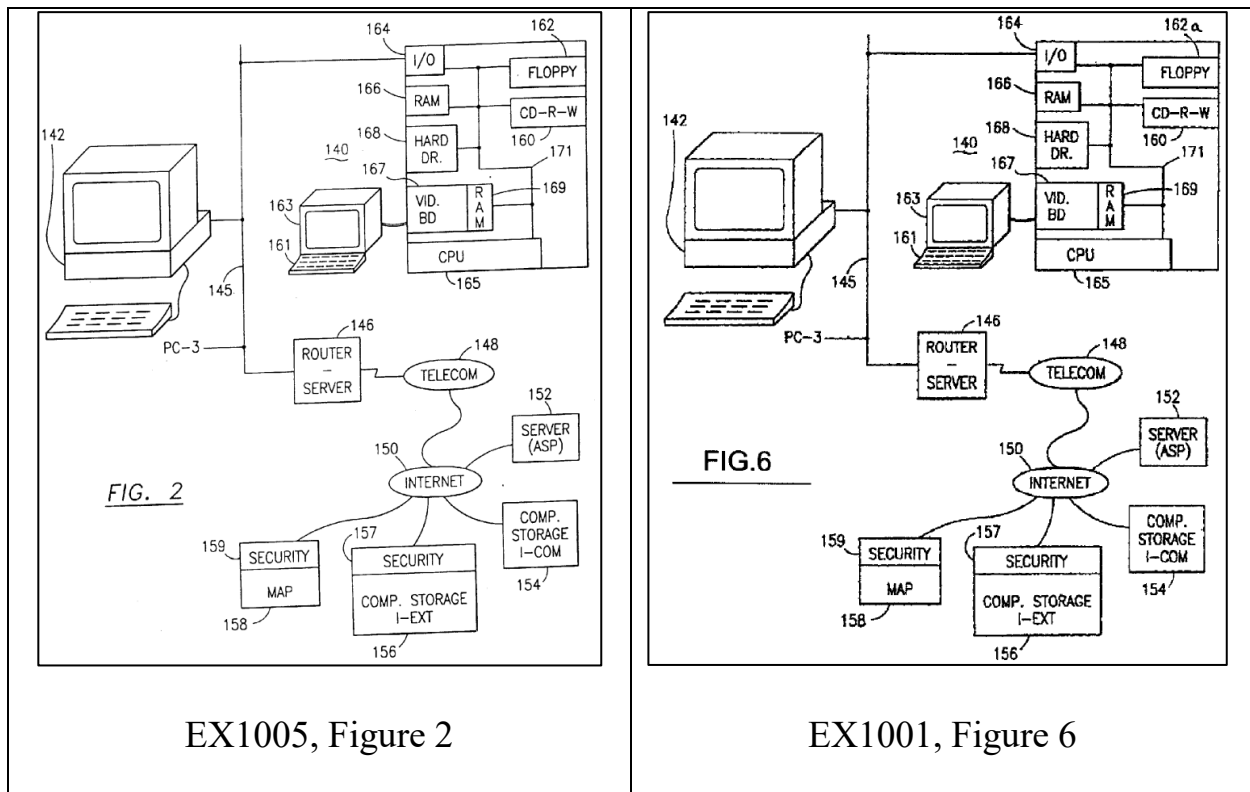
earliest claimed priority date of the '244 Patent and therefore is prior art under at least 35 U.S.C. §102(b). EX1003, ¶¶102-103.

Redlich describes “a data security system and method and, more specifically, to a process, program and system which operates to secure files and data objects...” EX1005, ¶2. In particular, Redlich describes a method for “securing data in a computer system” that includes the steps of “establishing a group of security sensitive words, characters, icons, data streams or data objects,” “extracting the security sensitive data” such that “[t]he extracted data is separated from the remainder data and is separately stored.” EX1005, ¶34. Redlich further describes the “[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....” EX1005, ¶35. EX1003, ¶104.

Redlich discloses that “[t]he system, or method,... may be arranged in a distributed computer system, interconnected by any suitable means” EX1005, ¶99. Redlich describes various examples of computer systems that can be used to implement this method. For example, Redlich discloses a “network implementation,” where “the extracted data” is “stored in one computer and the remainder data” is “stored in another computer.” EX1005, ¶34. Redlich also discloses “a client-server implementation” where “the server” “direct[s] storage of the extracted data to a different location than the remainder data, either on the server

or on a further memory system (computer) interconnected to the server....” EX1005, ¶34. EX1003, ¶105.

The example computer systems disclosed by Redlich are the same as those in the '244 Patent. Figure 2 of Redlich, reproduced below side-by-side with Figure 6 of the '244 Patent, shows a computer system that includes a plurality of computers and a plurality of servers:



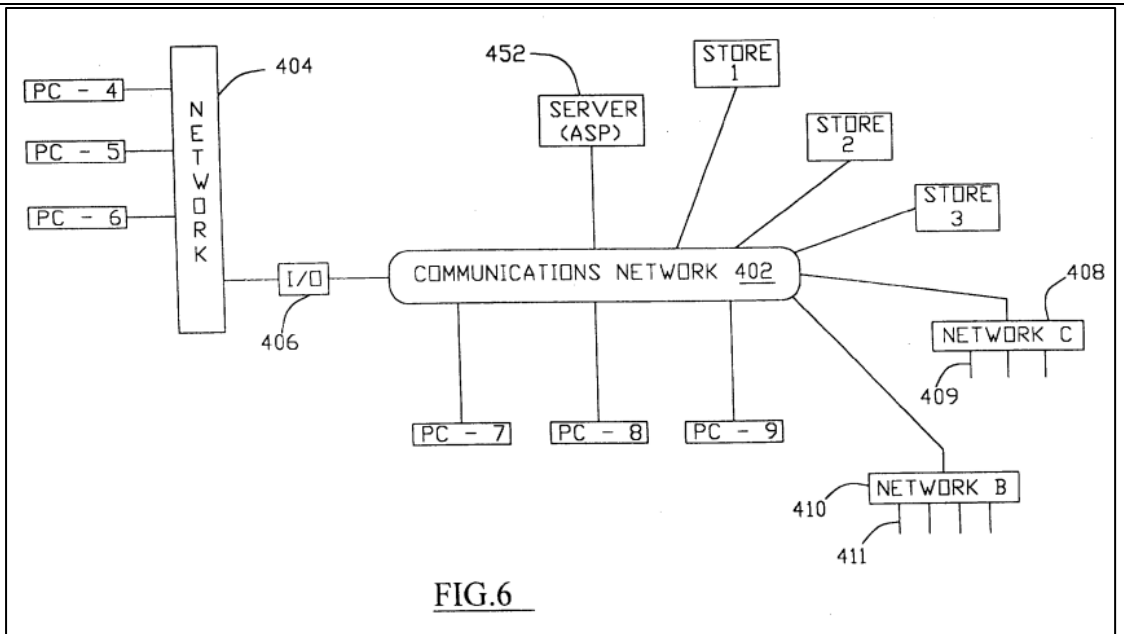
Compare EX1005, Figure 2 with EX1001, Figure 6 (same figure in the '244 Patent). Similar to Figure 6 of the '244 Patent, Figure 2 of Redlich discloses a computer system including a plurality of computers (i.e., PCs 140, 142, and PC-3) that are connected to a network of servers (i.e., Internet 150, Server 152) and a plurality of

extract data stores (i.e., Server 152, computer storage I-com 154, computer storage I-ext 156 and computer storage map 158), via a telecommunications system.

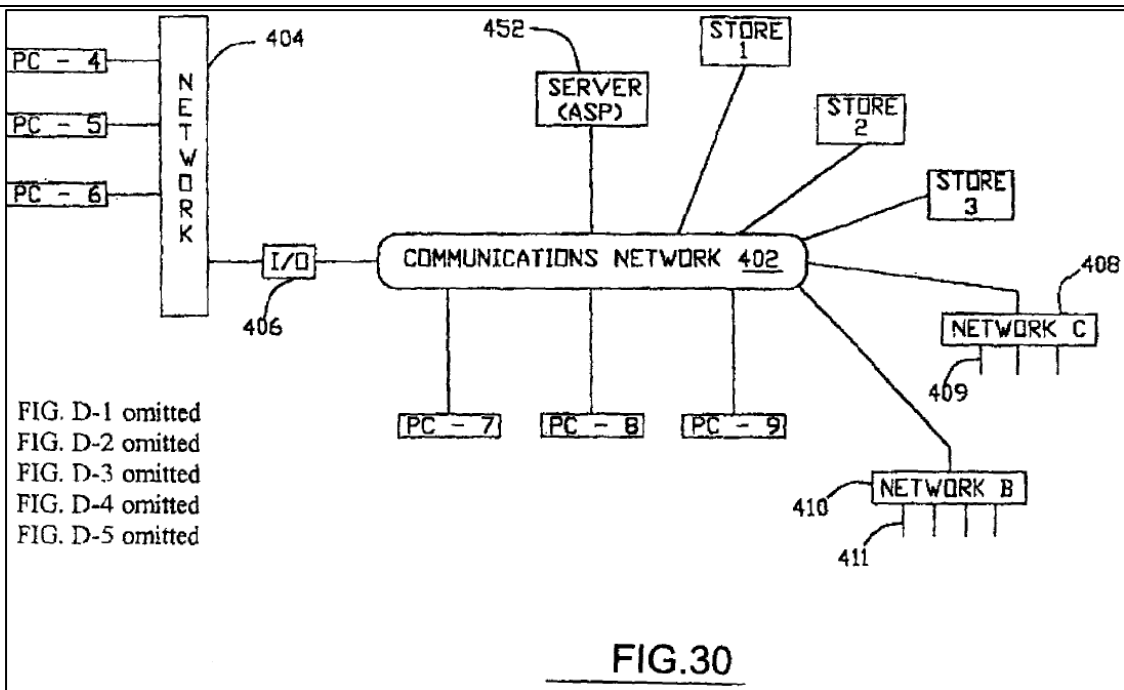
PCs 140, 142, and PC-3 are connected together via a network 145 (LAN or WAN) and are also connected to an input/output device 146 that may be generally described as a router or a server to an outside communications system. The input/output device 146 is connected to a telecommunications system 148 which 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, ¶124; *see also* EX1001, 439:4-15 (same disclosure in the '244 Patent).
EX1003, ¶¶106-107.

Figure 6 of Redlich, reproduced below on top of Figure 30 of the '244 Patent, shows another example of a computer network system that includes a plurality of computers and a plurality of data stores:



EX1005, Figure 6



EX1001, Figure 30

Compare EX1005, Figure 6 *with* EX1001, Figure 30 (same figure in the '244 Patent). Similar to Figure 30 of the '244 Patent, Figure 6 of Redlich discloses a network on which its alleged invention can be implemented comprising a plurality of computers (i.e., PC-4 – PC-9), networks, and data stores interconnected by telecommunications network 402.

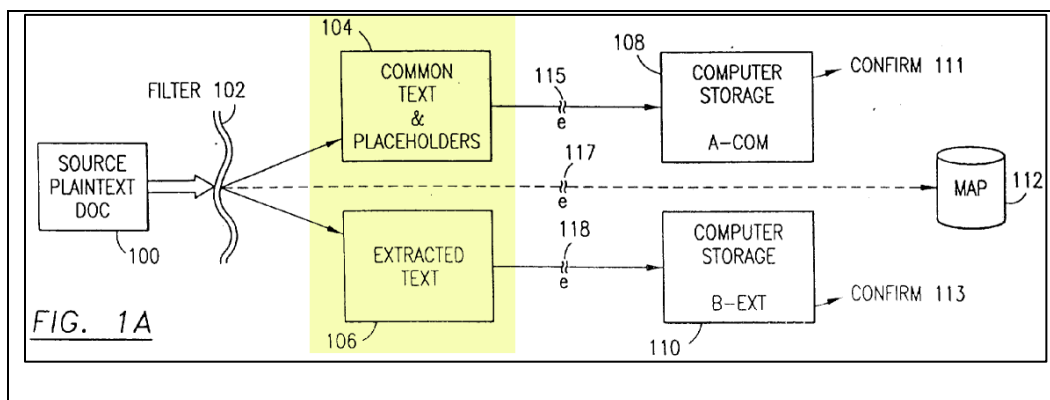
Fig. 6 is an exemplary computer network diagram showing various user communities. The telecommunications network 402 is connected to the server application server provider ASP 452 and *to various networks and personal computers* ... Network A [404] is coupled to various PCs identified in FIG. 6 as PC-4, 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.

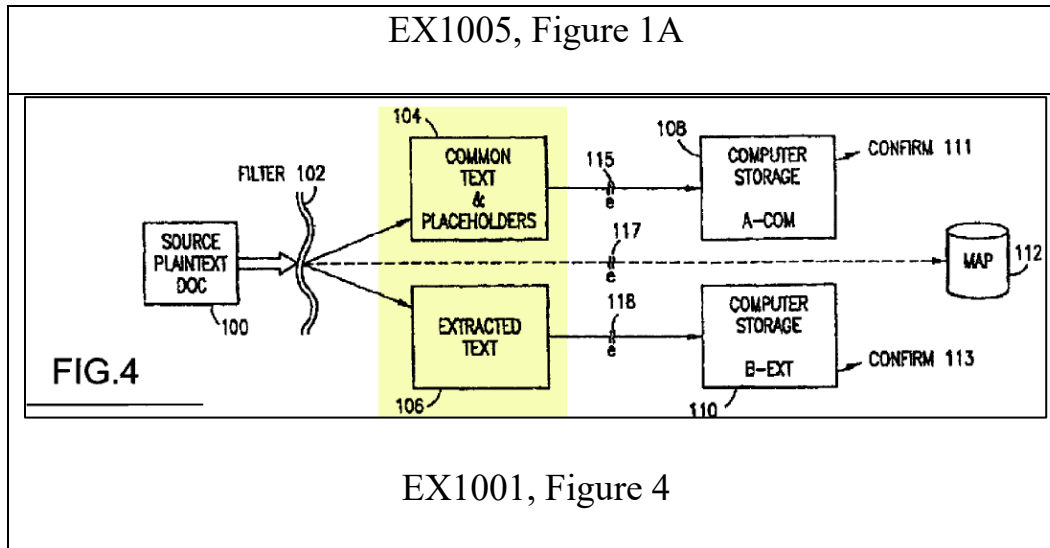
EX1005, ¶177; *see also* EX1001, 490:25-58 (same disclosure in the '244 Patent). EX1003, ¶¶108-109.

Similar to the '244 Patent, Redlich describes extracting the security sensitive data to result in extracted data and remainder data. *Compare* EX1005, ¶¶34 (“The

method for securing data ... includes ... *extracting the security sensitive data*. The extracted data is separated from the remainder data...."); 35 ("The method... 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.") with EX1001, 4:22-25 ("[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."), 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."). EX1003, ¶¶110-111.

Figure 1A of Redlich, reproduced below on top of Figure 4 of the '244 Patent, discloses a diagram showing extracting security sensitive data to result in extracted data (106) and also separating the non-security sensitive data into remainder data (104):





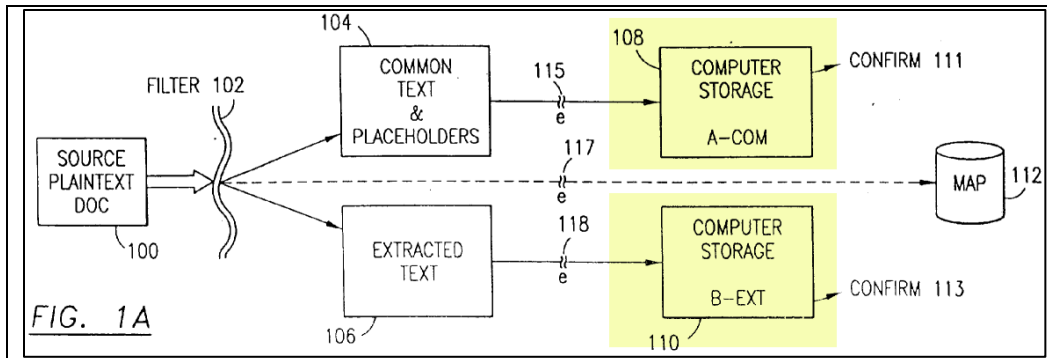
Compare EX1005, Figure 1A (disclosing a diagram illustrating the extraction of security sensitive data to result in extracted data (i.e., Extracted Text 106) and separating the non-security sensitive data into remainder data (i.e., Common Text 104)) with EX1001, Figure 4 (same figure in the '244 Patent).

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.

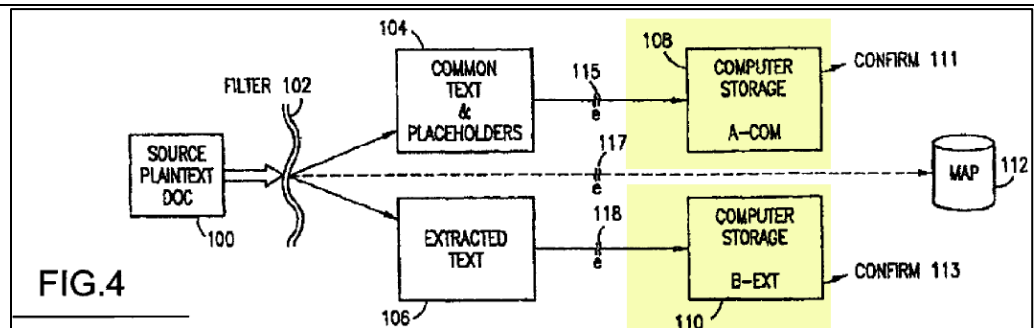
EX1005, ¶104; *see also* EX1001, 435:40-61 (same disclosure in the '244 Patent).
EX1003, ¶¶112-113.

Similar to the '244 Patent, Redlich further describes storing extracted data in different data stores based on the data's security level and separately storing the remainder data. *Compare* EX1005, ¶¶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.*”), 245 (“[T]he extract store may comprise *a plurality of extract stores operative in conjunction with a plurality of security clearance levels.*”), 34 (“The extracted data is separated from the remainder data and is separately stored.”) *with* EX1001, 513:13-15 (same disclosure as EX1005, ¶245), 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.”), 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.”). EX1003, ¶¶114-117.

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



EX1005, Figure 1A



EX1001, Figure 4

Compare EX1005, Figure 1A (illustrating storing extracted data in extract stores (i.e., Computer Storage B-ext 110) and remainder data in a separate store (i.e., Computer Storage A-com 108)) with EX1001, Figure 4 (same figure in the '244 Patent).

[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).

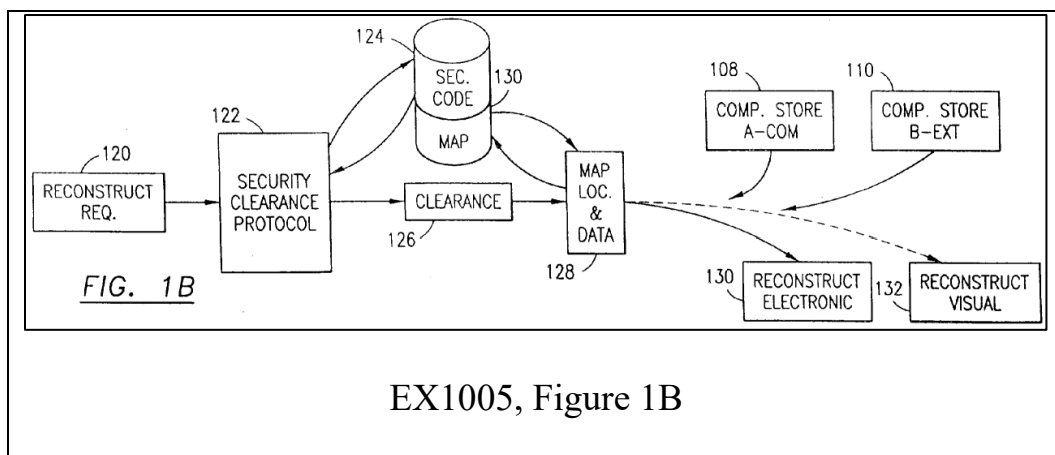
EX1005, ¶107; *see also* EX1001, 443:2-3, 17-20 (same disclosure in the '244 Patent). EX1003, ¶¶118-119.

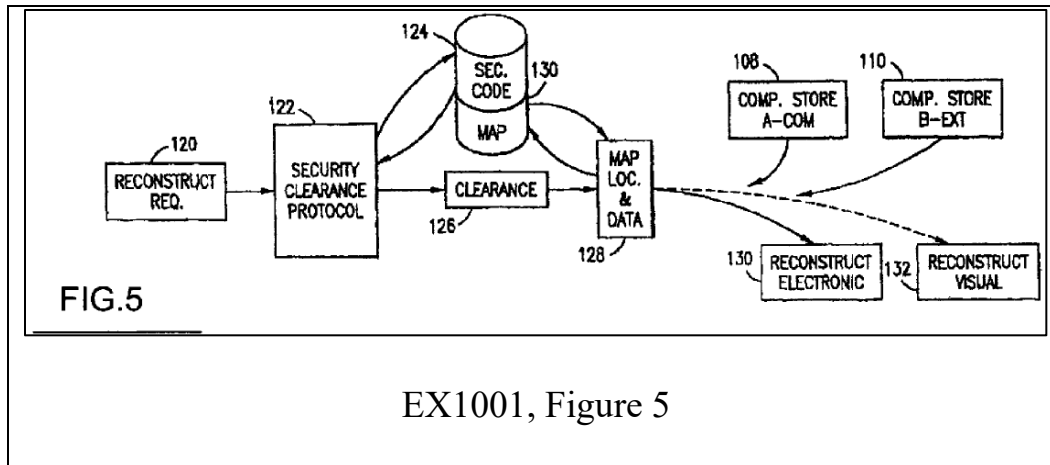
Similar to the '244 Patent, Redlich further describes parsing data into data segments. *Compare* EX1005, ¶¶231 (“The parsing algorithm, as stated earlier, targets the plaintext document or data object 100 and *splits, cuts and segments (that is, parses) the document by bit count, word, word count, page, line count, paragraph count, any identifiable document or icon characteristic, or other identifiable feature such as capital letters, italics, underline*, etc. Hence, the parsed document 100 constitutes at least remainder data and data which is extracted or parsed or segmented out.”), 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”) *with* EX1001, 506:65-507:5 (same disclosure as EX1005, ¶231), 508:34-37 (same disclosure as EX1005, ¶238). EX1003, ¶¶120-121.

Similar to the '244 Patent, Redlich further discloses controlling access to part or all of the security sensitive data based on a user's security clearance. *Compare* EX1005, ¶¶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.”), 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.”) *with* EX1001, 490:11-19 (“A low level security clearance results in only partial reconstruction of the plain text or source document ... [E]ach 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.”), 496:5-13 (same disclosure as EX1005, ¶¶200). EX1003, ¶¶122-123.

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





Compare EX1005, Figure 1B (illustrating permitting full or partial reconstruction of data from the remainder data store (108) and the extract data store (110) after determining that a user has a predetermined security clearance (122 and 126)) *with* EX1001, Figure 5 (same figure in the '244 Patent).

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.

EX1005, ¶122; *see also* EX1001, 447:3-12 (same disclosure in the '244 Patent).

EX1003, ¶¶124-125.

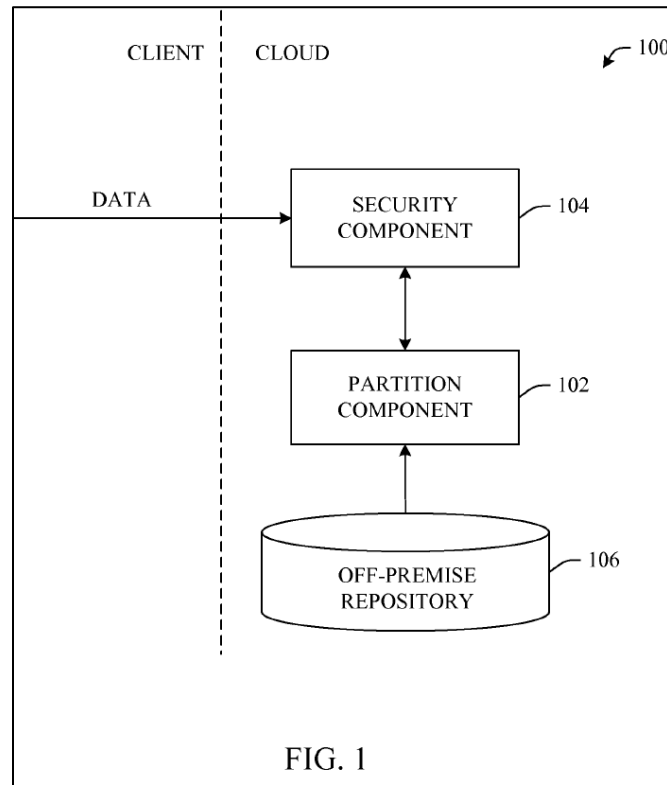
2. Ozzie

U.S. Patent No. 8,601,598 (EX1006, “Ozzie”) was filed on September 29, 2006. Ozzie was published on April 3, 2008, as U.S. Publication No. 2008/0083036 and was issued on April 22, 2014, and is prior art under at least 35 U.S.C. §102(e). EX1003, ¶126.

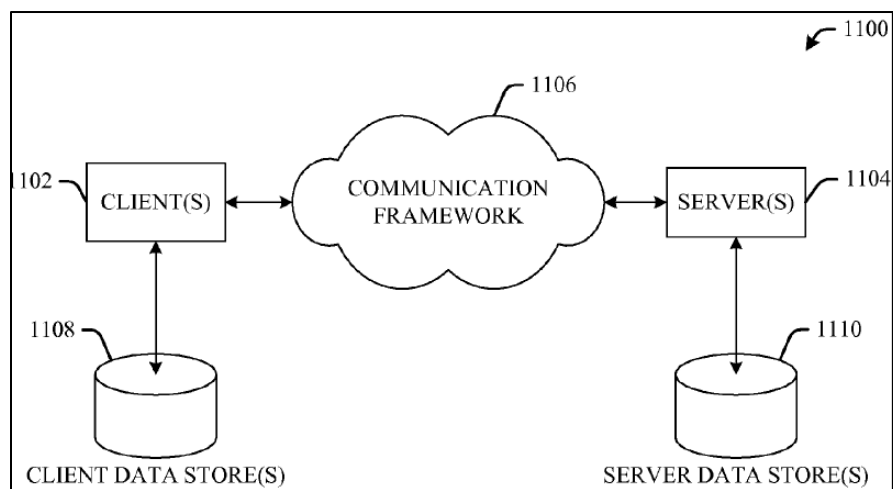
Ozzie describes “a system that can enable *a cloud-based data repository* to function as a secure ‘drop-box’ for data that corresponds to a user.” EX1006, 2:6-9. Specifically, Ozzie describes a system in which data is “stored in partitions within the cloud while preventing unwanted or unintended disclosure of the information.” EX1006, 4:33-36. EX1003, ¶127.

Ozzie discloses a system that “leverages the user-centric architecture of emerging ‘cloud based’ systems. 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, 4:51-57. Ozzie further discloses a system that “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.” EX1006, 4:64-5:1. These partitions are described in Ozzie as “drop-boxes,” which are for storing “data maintained within

the ‘cloud.’” EX1006, 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, 5:3-5; *see also* Fig. 1, Fig. 11. EX1003, ¶¶128-129.



EX1006, Figure 1.



EX1006, Figure 11; EX1006, 13:64 (“The system 1100 also includes one or more server(s) 1104.”), 14:6-9 (“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.”), 14:16-18 (“[T]he server(s) 1104 are operatively connected to one or more server data store(s) 1100 that can be employed to store information local to the servers 1104.”). EX1003, ¶¶130-134.

B. Grounds 1-2: Redlich Renders Obvious Alone (Ground 1) And In Combination With Ozzie (Ground 2) Claim 1

1. Independent Claim 1

i. Claim 1 Preamble

To the extent the preamble is limiting, Redlich discloses and/or renders obvious alone and in combination with Ozzie (for Ground 2) the preamble of independent claim 1, as explained below.

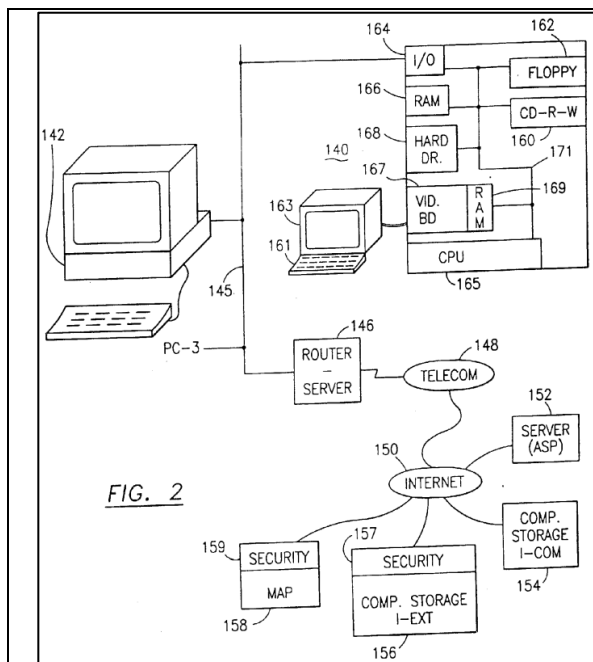
a. [1pre-i] A distributed computer system for organizing and processing data, the data to be processed having select content represented by one or more predetermined words, characters, images, data elements or data objects,

Redlich discloses this limitation.

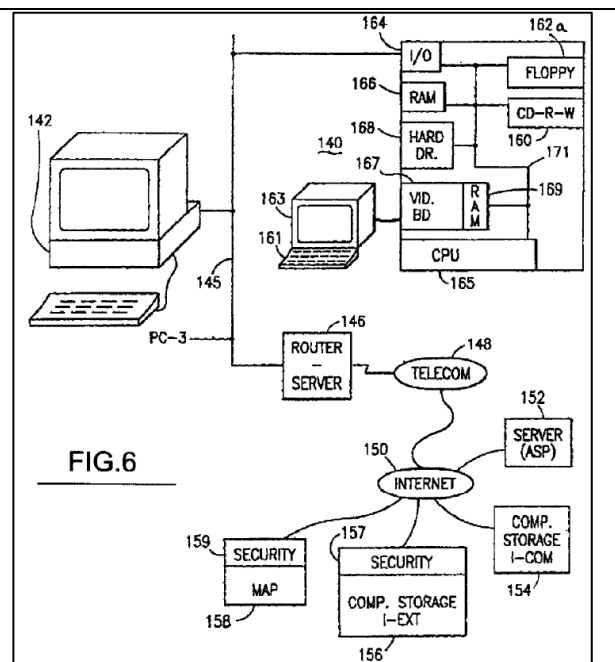
First, Redlich discloses a distributed computer system. Redlich specifically discloses “*a distributed computer system*, interconnected by any suitable means.” EX1005, ¶99; *see also* EX1005, ¶¶231 (“[T]he dispersement 560 largely spreads out

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.”). EX1003, ¶158.

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



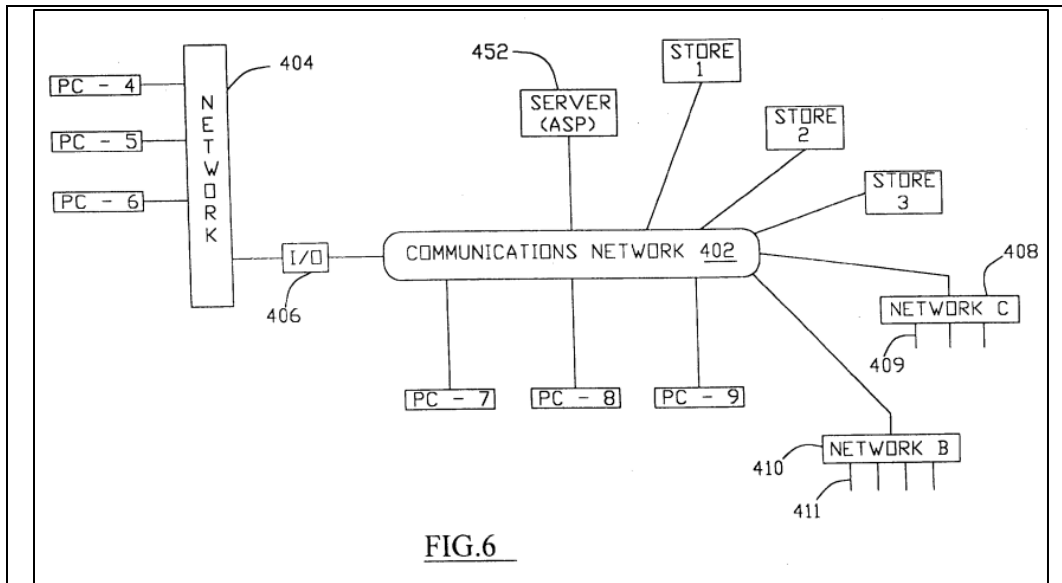
EX1005, Figure 2



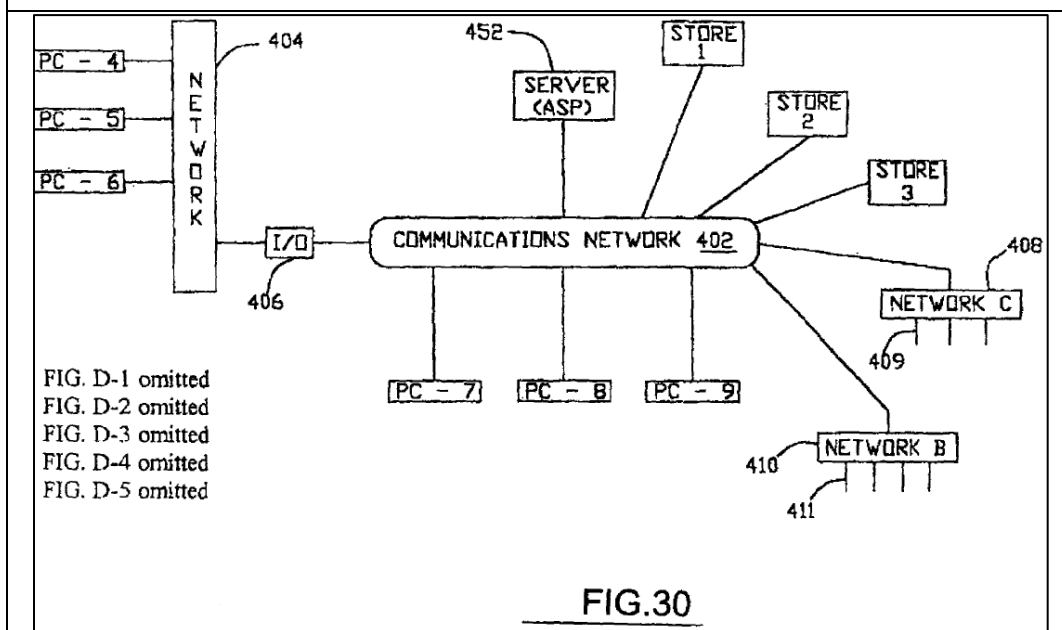
EX1001, Figure 6

Compare EX1005, Figure 2 *with* EX1001, Figure 6 (same figure in the '244 Patent); *see* Section VI.A.1. Similar to '244 Patent Figure 6, Figure 2 shows computers “PCs 140, 142, and PC-3 ... connected together via a network.” *Compare* EX1005, ¶124 *with* EX1001, 439:4-5 (same disclosure in the '244 Patent). The network is further connected to Internet 150, which is connected to “a plurality of servers,” such as server 152, and “various computer memory storage devices such as computer storage I-com 154, computer storage I-ext 156....”. *Compare* EX1005, ¶124 *with* EX1001, 439:7-15 (same disclosure in the '244 Patent). EX1003, ¶¶159-160.

As another example, Figure 6 of Redlich, reproduced below on top of Figure 30 of the '244 Patent, illustrates another distributed computer system comprising a plurality of computers (PC-4 to 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):



EX1005, Figure 6



EX1001, Figure 30

Compare EX1005, Figure 6 with EX1001, Figure 30 (same figure in the '244 Patent); see Section VI.A.1. Similar to '244 Patent Figure 30, Figure 6 discloses a

telecommunications network 402 that connects “various networks and personal computers” such as 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.” EX1005, ¶177; *see also* EX1001, 490:25-58 (same disclosure in the ’244 Patent). EX1003, ¶¶161-163.

Second, Redlich’s distributed computer system is a system for organizing and processing **data**. Specifically, Redlich discloses a method for “securing **data** in a computer system” that includes “extracting the security sensitive data” such that “[t]he extracted data is separated from the remainder data and is separately stored.” EX1005, ¶34. Redlich further discloses 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” EX1005, ¶35. EX1003, ¶¶164-165.

Third, Redlich discloses organizing and processing **data** having select content represented by one or more predetermined words, characters, images, data elements or data objects. For example, Redlich discloses a method for “securing **data** in a computer system” that includes “establishing a group of security sensitive words, characters, icons, data streams or data objects.” EX1005, ¶34; *see also* EX1005, ¶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”). EX1003, ¶166.

Redlich further discloses processing **data** by categorizing security sensitive content into pre-set categories. EX1005, ¶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.”). EX1003, ¶167.

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**,

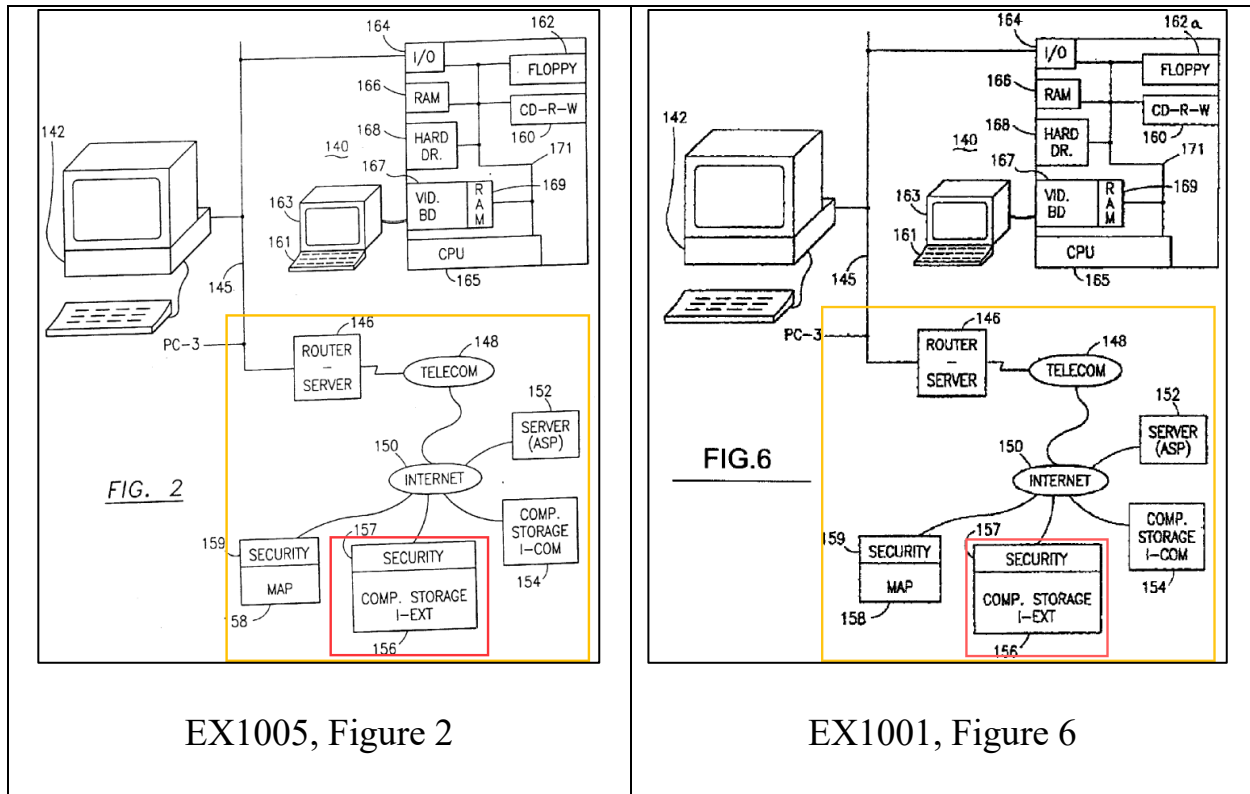
Redlich discloses and/or renders obvious alone (and in combination with Ozzie for Ground 2) this limitation.

First, Redlich's distributed computing system has **a plurality of select content data stores** for respective ones of a **plurality of security designated data**. In particular, Redlich discloses **extract stores** for storing **security sensitive content** extracted from the **data**. EX1005, ¶¶35 (“The method ... includes ... 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)**”). EX1003, ¶171.

Redlich further discloses **a plurality of extract stores**, with each of the **extract stores** storing **security sensitive data** at different security levels. EX1005, ¶245 (“[T]he **extract store** may comprise **a plurality of extract stores** operative in conjunction with a plurality of security clearance levels.”), ¶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.**”). EX1003, ¶172.

Second, Redlich further discloses a **plurality of select content stores** in a **server cloud**. The '244 Patent discloses 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. Similarly, Redlich discloses a distributed computer system comprising many servers and **extracted data** dispersed all over in **extract stores** to achieve high level security. For example, Figure 2 of Redlich, reproduced below side-by-side Figure 6 of the '244 Patent, illustrates a distributed computer system comprising a “plurality of servers” and “various memory storage devices such as computer storage I-com 154, [and] **computer storage I-ext 156.**” EX1005, ¶124; *see also* EX1001, 439:4-15 (same disclosure in the '244 Patent).



Compare EX1005, Figure 2 with EX1001, Figure 6 (same figure in the '244 Patent); see also Section VI.A.1. Redlich further discloses that “the extracted data ... may be stored on computer storage I-ext memory unit 156 via Internet 150, telecommunications system 148 and router/server 146.” EX1005, ¶127; see also EX1001, 439:61-63 (same disclosure in the '244 Patent). EX1003, ¶¶173-175.

A POSITA would have understood that Redlich’s group of servers and data stores is a **server cloud** as claimed in Claim 1 of the '244 Patent. Claim 1 requires “a **plurality of select content data stores in a server cloud.**” The '244 Patent further 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, 62:15-

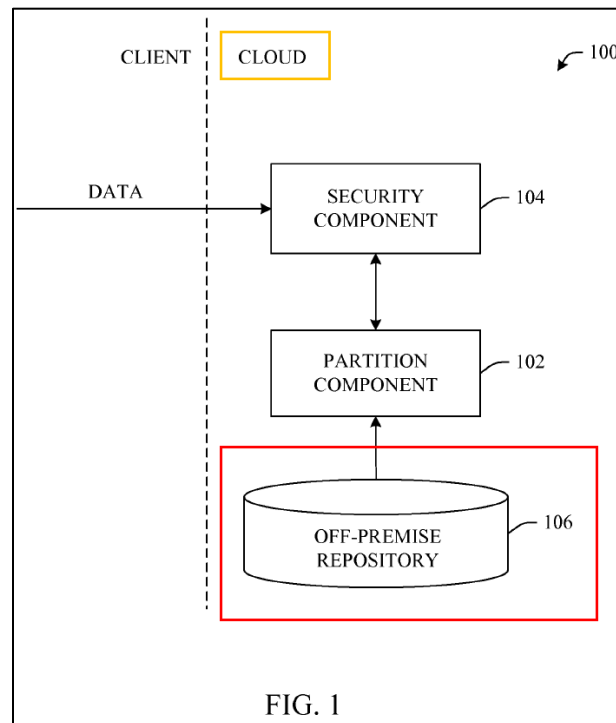
17. Similarly, as explained above, Redlich's group of servers and data stores shown in Figure 2 "consists of many servers" (i.e., a plurality of servers) and "a **plurality of select content data stores**" (i.e., **extract stores**) in which "**sensitive extract** may be dispersed." EX1003, ¶¶176-178.

Second, Redlich's distributed computing system also has a **plurality of granular data stores**. In particular, Redlich discloses **data stores for storing granular data segments**. EX1005, ¶¶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 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*"). EX1003, ¶179.

For Ground 2, 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**. As explained above, the '244 Patent explains that "[t]he 'cloud' consists of many servers." EX1001, 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

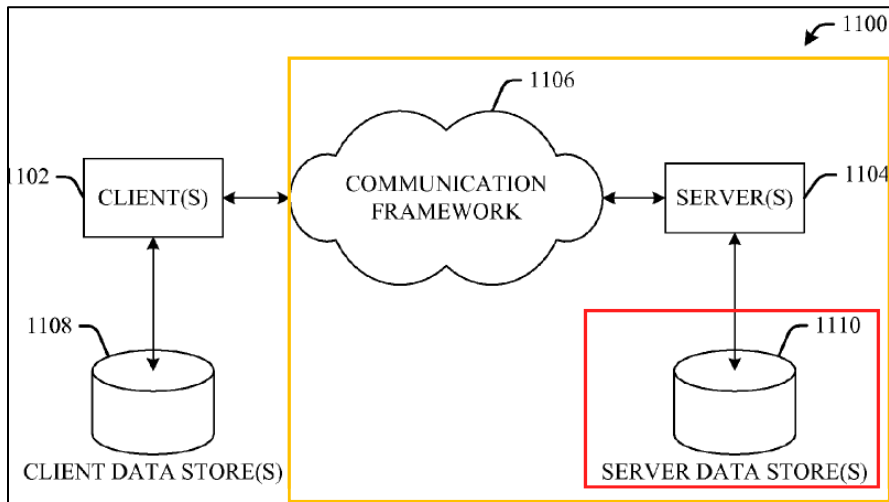
explains that “sensitive extracts may be dispersed all over the cloud.” EX1001, 62:15-17. EX1003, ¶¶252-254.

Similarly, 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, 4:53-55. Figure 1 of Ozzie below illustrates that the “cloud” comprises “cloud-based repositories” (EX1006, 4:64-5:1) that can be used to store data:



EX1006, Figure 1. Ozzie explains that the “*off-site or ‘cloud-based’ repository 106*” can be partitioned into individual segments, which are “viewed as ‘drop-boxes’ for data maintained within the ‘cloud.’” EX1006, 5:1-3. EX1003, ¶¶255-257.

Figure 11 of Ozzie, reproduced below, provides another example of a **server cloud** “consist[ing] of ‘many servers’” and a **plurality of data stores** intended for the storage of data:



EX1006, Figure 11. The system illustrated in Figure 11 similarly comprises “one or more servers(s) 1104” and cloud-based repositories in the form of “one or more **server data store(s) 1100** that can be employed to store information local to the servers 1104.” EX1006, 13:64, 14:16-18. EX1003, ¶¶258-260.

Similar to the '244 Patent, Ozzie further discloses that the **data** can be dispersed throughout the **cloud**. In particular, Ozzie discloses that “**data** can be offloaded to a ‘**cloud**’” comprising the “off-premise servers.” EX1006, 4:53-55. Specifically, 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, 5:3-5. Ozzie, therefore, discloses the **server cloud** as required in Claim 1 of the '244 Patent. EX1003, ¶¶261-262.

As discussed in Section VI.B.1.vii, 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. EX1003, ¶263.

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,

Redlich discloses and/or renders obvious alone (and in combination with Ozzie for Ground 2) this limitation.

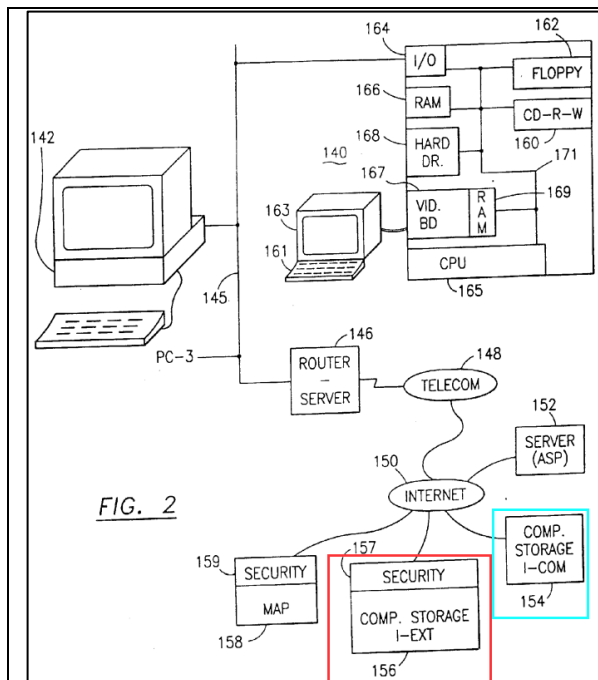
First, Redlich discloses **select content data stores** and **granular data stores** having respective **access controls**. In particular, Redlich discloses that access to both the **select content data stores** and **granular data stores** are dependent upon having appropriate **passwords and security clearances**. EX1005, ¶¶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.”), 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.”). EX1003, ¶¶182-183.

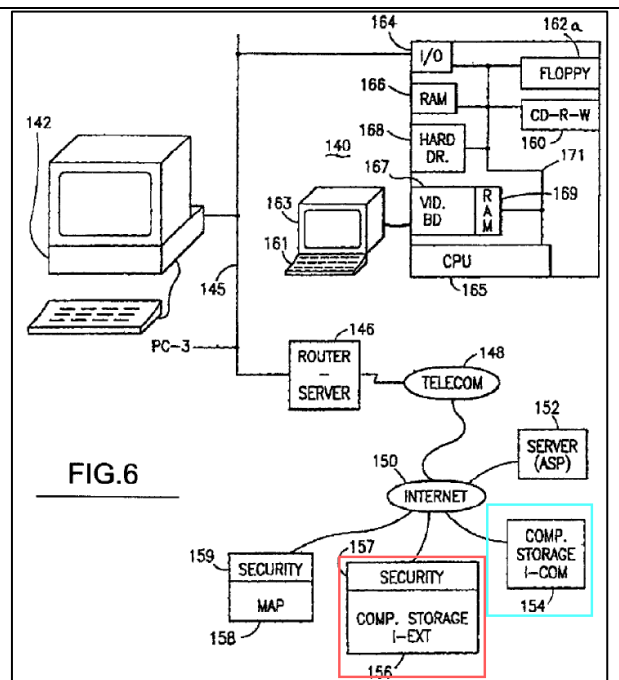
Additionally, Redlich discloses limiting access to **extract data stores** based on the level of a user’s **security clearance**. Users with **high security clearances** are granted access to the **data** comprising of **extracted data** and remainder data, while users with a **security clearance** below the security level of the **extracted data** will be granted access to a sanitized document containing only remainder data. EX1005, ¶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 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.”). EX1003, ¶184.

Second, Figure 2 of Redlich, reproduced below side-by-side Figure 6 of the ’244 Patent, discloses the plurality of data stores (i.e., data stores such as **computer storage I-com 154** and **computer storage I-ext 156**) and said **server cloud** (i.e., the “plurality of servers” and “various memory storage devices”) operatively coupled over a communications network (i.e., telecommunications system 148 and/or Internet 150).



EX1005, Figure 2



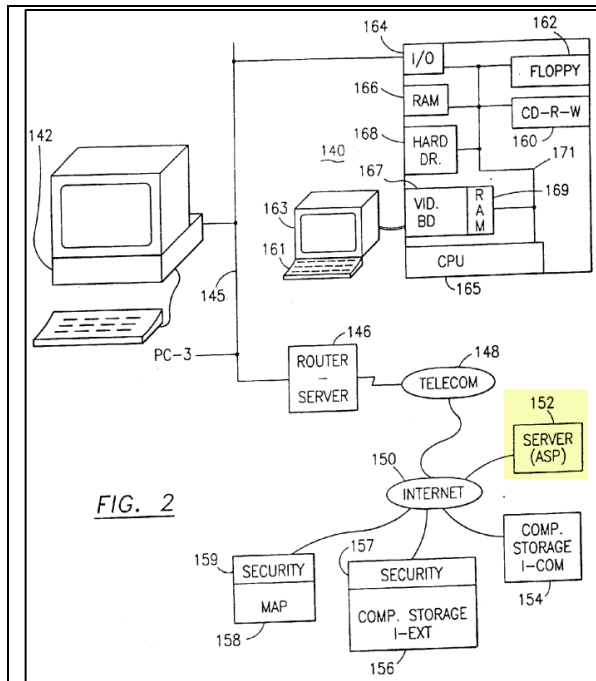
EX1001, Figure 6

Compare EX1005, Figure 2 *with* EX1001, Figure 6 (same figure in the '244 Patent); EX1005, ¶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**[.]”); *see also* EX1001, 439:60-65 (same disclosure in the '244 Patent); Section VI.A.1. EX1003, ¶185.

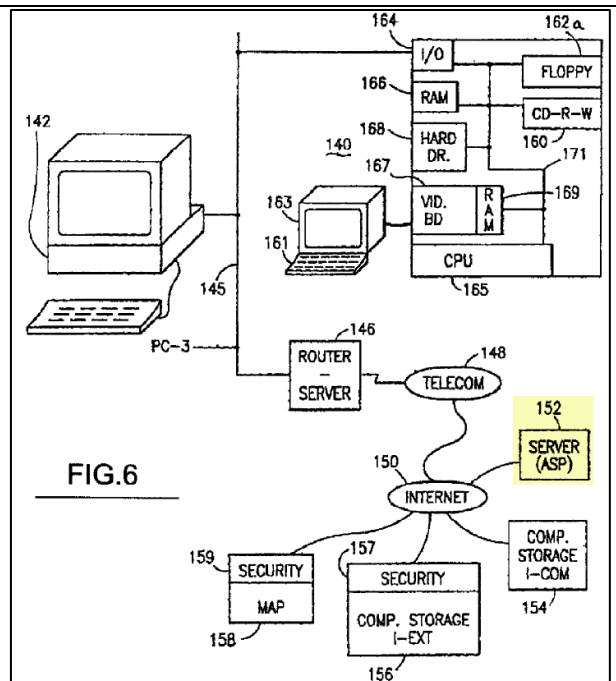
As discussed in Section B.1.i.b, Redlich discloses and/or renders obvious alone (and in combination with Ozzie for Ground 2 renders obvious) a **plurality of select content data stores** in a **server cloud**. EX1003, ¶¶186, 266.

- 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**;

Redlich discloses and/or renders obvious alone (and in combination with Ozzie for Ground 2) this limitation. *First*, Redlich discloses the structure of this limitation. Redlich discloses the same server and algorithm disclosed in the '244 Patent. Figure 2 of Redlich, reproduced below side-by-side Figure 6 of the '244 Patent, discloses the server:



EX1005, Figure 2



EX1001, Figure 6

Compare EX1005, Figure 2 at box 152 with EX1001, Figure 6 at box 152. The algorithm performed by the server is described in EX1005, ¶142, which is the same algorithm disclosed in the '244 Patent. See EX1001, 436:34-46. EX1003, ¶¶188, 190-191.

Second, Redlich discloses the function of the means-plus-function term. Specifically, Redlich discloses identifying a **plurality of select content data stores** for respective ones of a **plurality of security designated data** in said **server cloud**. Both Redlich and the '244 Patent provide the same disclosure for identifying a **plurality of extract stores** for storing **security sensitive extracted data**. Compare EX1005, ¶¶142 (“The sites may be randomly *selected by ASP 152*. The ASP may

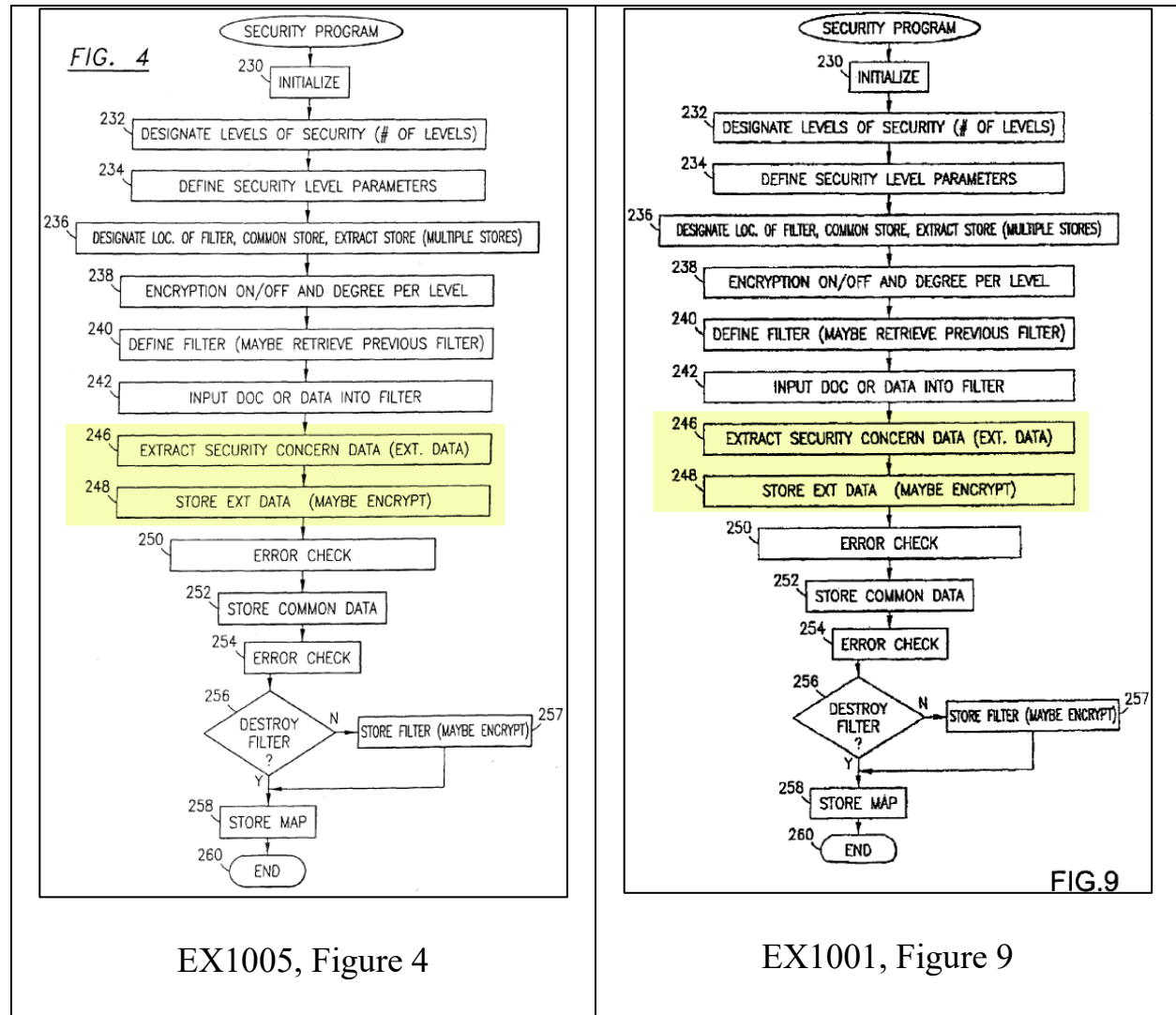
use artificial intelligence AI to **locate secure extract data storage sites**. AI or inference machines can ascertain (a) traffic on communications channels, (b) storage limit issues, (c) transmission failures in the communications links, and (d) the degree of security necessitated by exterior events, i.e., terrorism alerts, virus alerts, war, data security warnings posted by trusted sources, Microsoft, Norton, NASA, DoD, CDC, FBI, etc.”), 245 (“[T]he **extract store** may comprise a **plurality of extract stores** operative in conjunction with a plurality of security clearance levels.”), 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.*”) with EX1001, 436:37-46, 513:13-15, 489:45-48 (identical disclosures in the ’244 Patent); *see also* EX1005, ¶35 (“The **subsets of extracted data** are stored in **one or more computer memories** in the network **identified as extracted stores.**”). EX1003, ¶¶192-193.

As discussed in Section B.1.i.b, Redlich discloses and/or renders obvious alone (and in combination with Ozzie for Ground 2 renders obvious) a **plurality of select content data stores** in a **server cloud**. EX1003, ¶¶194, 268.

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

Redlich discloses and/or renders obvious alone (and in combination with Ozzie for Ground 2) this limitation. *First*, Redlich discloses the structure of this

limitation. In Redlich, the filter is described in EX1005, ¶135 (“*a data filter* for the data input from the data input computer which extracts the security sensitive words, phrases, icons or data objects.”). Redlich discloses that the filter performs the same algorithm as identified in the ’244 Patent:

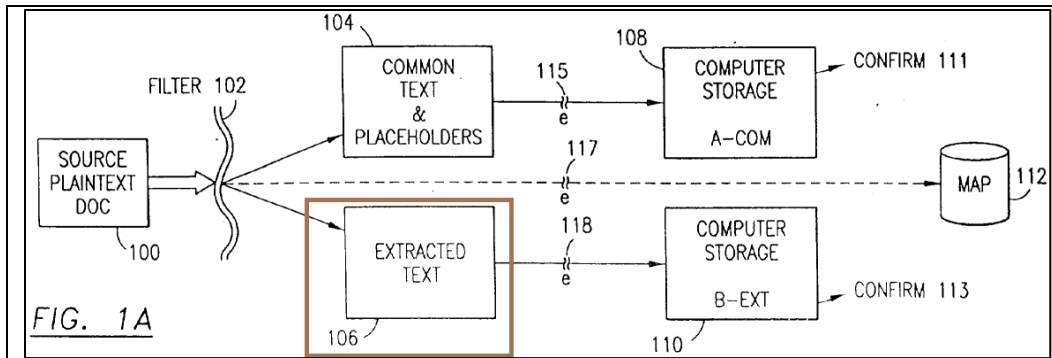


Compare EX1005, Figure 4 at boxes 246 and 248 with EX1001, Figure 9 at boxes 246 and 248. The algorithm performed by the filter is described in EX1005, ¶143,

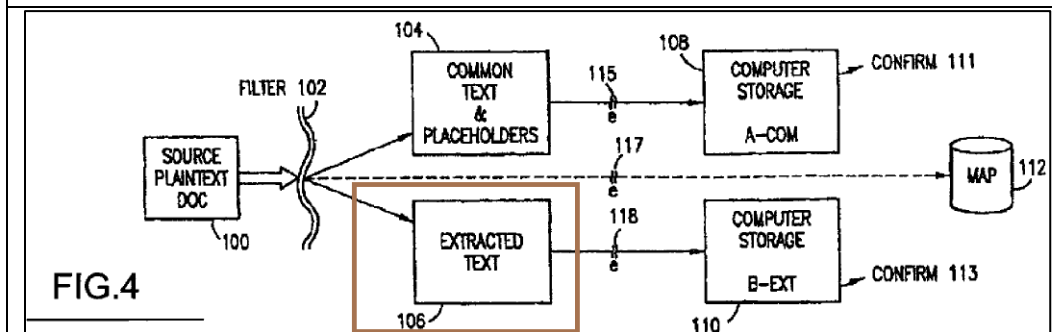
which is the same algorithm disclosed in the '244 Patent. *See* EX1001, 437:1-5. EX1003, ¶¶196, 198-200.

Second, Redlich discloses the function of the means-plus-function term (“extracting and storing said **security designated data** in **respective select content data stores** of said **server cloud**”). Specifically, Redlich discloses extracting the **security sensitive data** from the **data** to separate **extracted data** from remainder data. EX1005, ¶¶34 (“The method for securing data ... includes ... *extracting security sensitive data*. The *extracted data* is *separated from* the remainder data”), 35 (“The method ... 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 (“*[E]xtracting the security sensitive words, characters, icons or data objects* to obtain **extracted data** and remainder data thereat...”), Claim 139 (“[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.”). EX1003, ¶201.

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



EX1005, Figure 1A



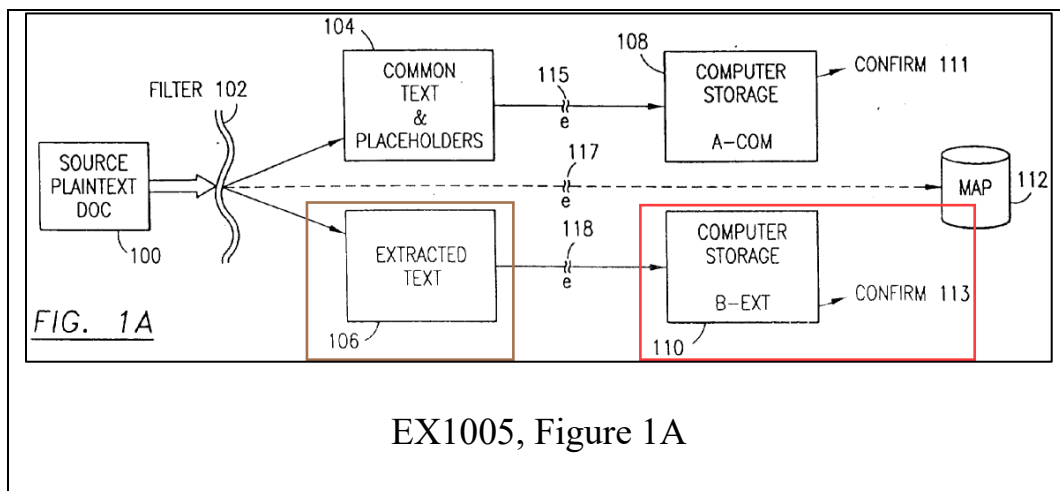
EX1001, Figure 4

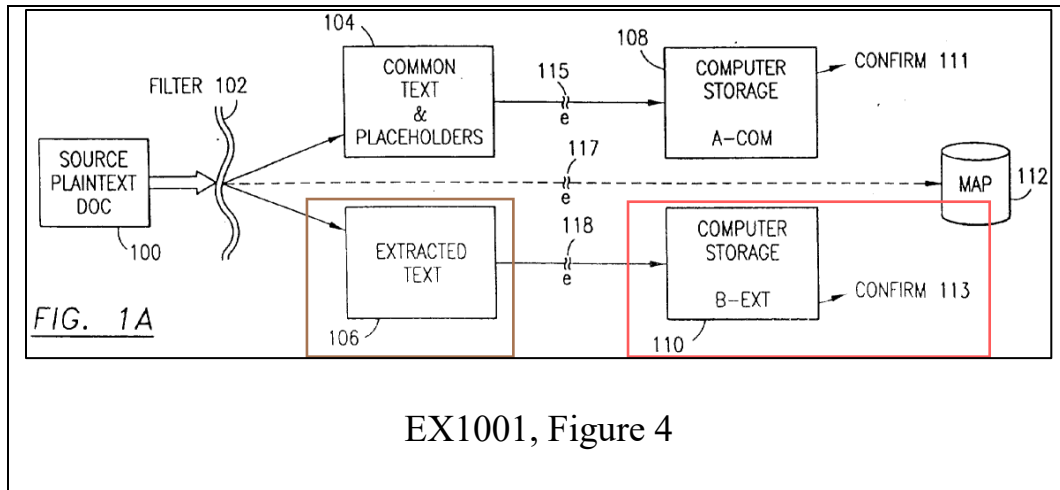
Compare EX1005, Figure 1A and ¶104 (“Filter 102, in a most basic sense, *separates out common text or remainder data 104 from uncommon text, words, characters, icons or data objects*. The *security sensitive words, characters, icons or data objects* are *separated from remainder or common text 104* as *extracted text 106*.”) with EX1001, Figure 4 and 435:40-44 (identical disclosure in the ’244 Patent). EX1003, ¶¶202-203.

Redlich discloses storing the **extracted data** in a **plurality of extract stores** in the same way as disclosed in the ’244 Patent. Compare EX1005, ¶¶172 (“Each

filter could filter out **different levels of security sensitive items** and **group of security sensitive items** (from each distinct filter) could be *stored at different computer storage locations.*”), 245 (“[T]he **extract store** may comprise a **plurality of extract stores** operative in conjunction with a plurality of security clearance levels.”) *with* EX1001, 489:45-48, 513:13-15 (same disclosure in the ’244); *see also* EX1005, ¶35 (“The **subsets of extracted data** are *stored* in **one or more computer memories in the network identified as extracted stores.**”). EX1003, ¶¶204-205.

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





Compare EX1005, Figure 1A and ¶104 (“The **extracted data file 106** is *stored in a different memory computer storage 110.*”) with EX1001, Fig. 4 and 443:17-18 (same disclosure in the ’244 Patent). EX1003, ¶¶206-207.

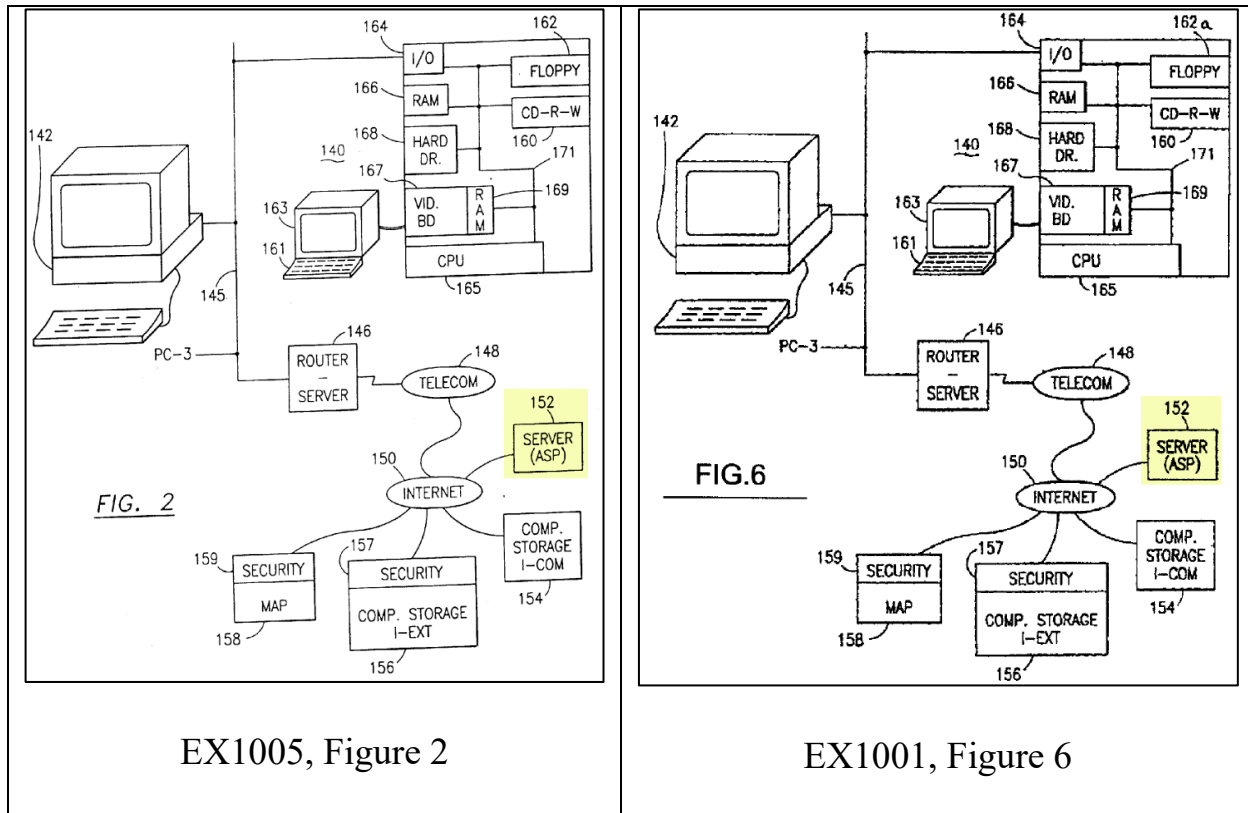
As discussed in Section B.1.i.b, Redlich discloses and/or renders obvious alone (and in combination with Ozzie for Ground 2) a **plurality of select content data stores** in a **server cloud**. EX1003, ¶¶208, 270.

- 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;

Redlich discloses and/or renders obvious alone (and in combination with Ozzie for Ground 2) this limitation.

First, a POSITA would have understood that Redlich discloses a processor in the same manner as in the ’244 Patent. In particular, a POSITA would have

understood that the application service provider (“ASP”) server is a computer that comprises a processor that would carry out the instructions for implementing the server applications/services. Figure 2 of Redlich, reproduced below side-by-side Figure 6 of the ’244 Patent, discloses the ASP server:



Compare EX1005, Figure 2 at box 152 with EX1001, Figure 6 at box 152. The ASP server in Redlich is described in EX1005, ¶103, which is the same description as in the ’244 Patent. Compare EX1005, ¶103 (“ASP – application service provider – server on a network.”) with EX1001, 522:15. EX1003, ¶¶211-213.

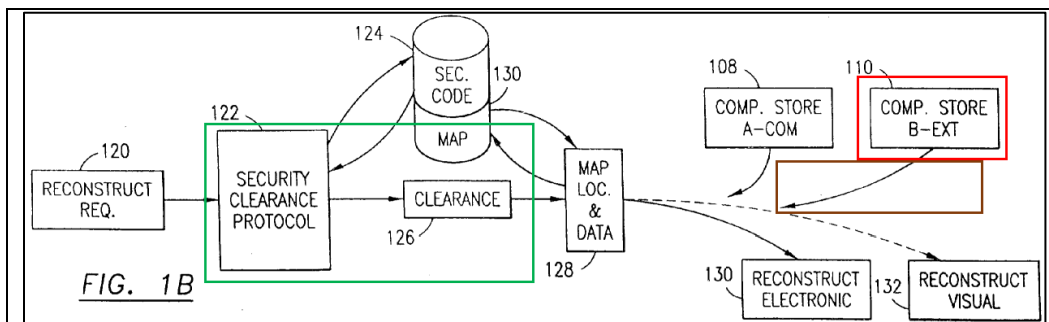
Similar to the ’244 Patent and consistent with the understanding of a POSITA, Redlich discloses that a server is a computer. Compare EX1005, ¶¶177 (“Of course,

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, 490:57-58, 511:39-41. *See also*, EX1015, 403-404. Further, similar to the '244 Patent, Redlich discloses that a computer includes a processor. *Compare* EX1005, ¶125 (“PCs include ... a central processing unit CPU 165 ...”) *with* EX1001, 523:36-37. A POSITA would therefore understand that ASP server 152 would include a processor. EX1003, ¶¶214-217.

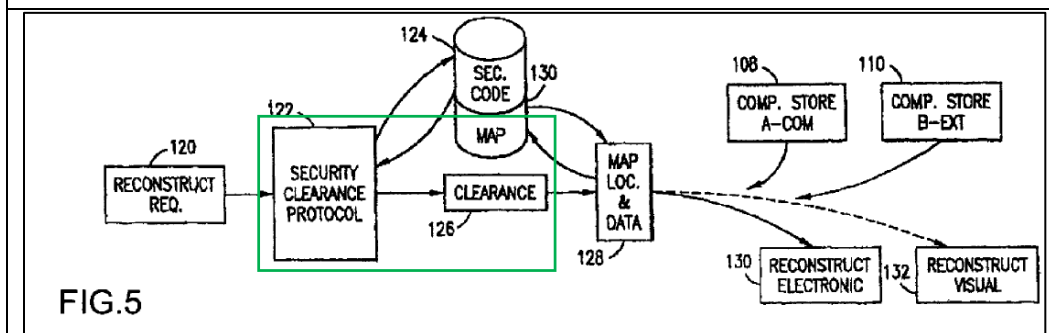
Second, Redlich discloses activating **extract stores** to retrieve **extracted data** from the **extract stores** in the presence of a **predetermined security clearance**, thereby permitting access to **extract stores** and their respective **extracted data**. In particular, Redlich discloses that when the proper **security clearance** and/or **additional access control** is provided by a user, **extracted data** corresponding to that **security clearance** and/or **additional access control** is received from the associated **extract store**. EX1005, ¶¶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**.”). EX1003, ¶218.

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



EX1005, Fig. 1B



EX1001, Fig. 5

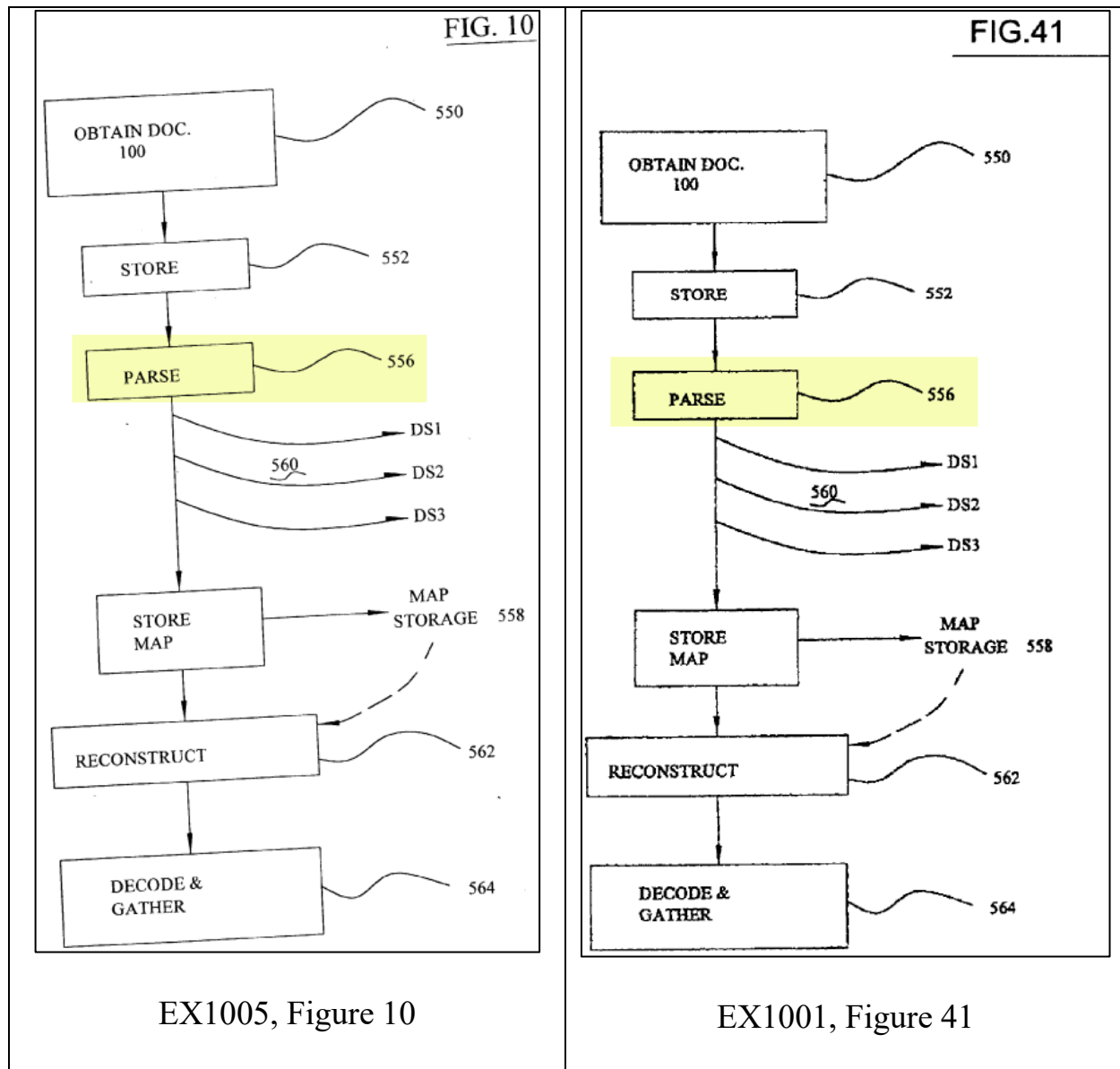
Compare EX1005, Figure 1B and ¶122 (“The system first executes a security clearance protocol routine 122 in order to determine whether the user has the proper security clearance. The **security clearance** may be thought of as a **security clearance control** ... [T]he security clearance protocol determines the level of security clearance and, hence, the full or partial reconstruction of the plaintext. ... Typically, the **extracted** or **security sensitive data** from **B-ext** is downloaded.”) *with* EX1001, Figure 5 and 447:3-12 (same disclosure in the ’244 Patent). EX1003, ¶¶219-221.

A POSITA would have understood that the processor of ASP server 152 would perform the activating step. Redlich discloses that the activating step discussed above is performed by ASP server 152. EX1005, ¶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 involved in ... permitting reconstruction via a separate or combined downloads of the remainder data and the extracted data into computer 140.”). A POSITA would have understood that the processor of ASP server 152 performs such an activating step, because typically processors execute instructions for implementing the various services provided by a server. EX1003, ¶¶221-222.

As discussed in Section B.1.i.b, Redlich discloses and/or renders obvious alone (and in combination with Ozzie for Ground 2 renders obvious) a **plurality of select content data stores** in a **server cloud**. EX1003, ¶¶223, 272.

- 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**;

Redlich discloses and/or renders obvious alone this limitation. *First*, Redlich discloses the structure of this limitation. Specifically, Redlich describes “a ***data filter*** for the data input from the data input computer.” EX1005, ¶35. Redlich’s data filter performs the same algorithm as the algorithm identified in the ’244 Patent, as illustrated below:



Compare EX1005, Figure 10 at box 556 with EX1001, Figure 41 at box 556. The algorithm performed is described in EX1005, ¶¶231, 106, which is the same algorithm described in the '244 Patent. See EX1001, 506:63-507:8 and 442:55-67 (same disclosure in the '244 Patent). In particular, similar to the '244 Patent, Redlich discloses that “[t]he parsing algorithm ... splits, cuts, and segments [] 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.” *Compare* EX1005, ¶106 with EX1001, 506:65-507:3. EX1003, ¶¶225, 227-229.

Second, a POSITA would have understood that Redlich discloses and/or renders obvious parsing the **remainder data** not extracted from the **data** and storing the **parsed data** as data segments in **granular data stores**.

Redlich discloses parsing of **data** granularly into data segments. EX1005, ¶¶37 (“The *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**. ... For example, financial data maintained by an institute in its original state, and 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) ...”), 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.”), 143 (“*Granular extraction of data elements* in a data object may be permitted.”), 238 (“The process involves *parsing the documents or content into granular data groups*”). EX1003, ¶¶230-232.

Redlich further discloses parsing a plain text document at the same granularity as disclosed in the '244 Patent. *Compare* EX1005, ¶106 (“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. Algorithms may be implemented to parse the plain text document.”) *with* EX1001, 442:55-62. EX1003, ¶233.

Moreover, a POSITA would have understood that after the **security sensitive data** is extracted from the data, the **remainder data** would need to be stored in data stores to allow for subsequent retrieval and reconstruction of the **original data**. One way to store the **remainder data** is by further dividing the **remainder data** and dispersing the divided **remainder data** to available **granular data stores**, e.g., with enough capacity. Redlich discloses one 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, ¶106. EX1003, ¶¶234-235.

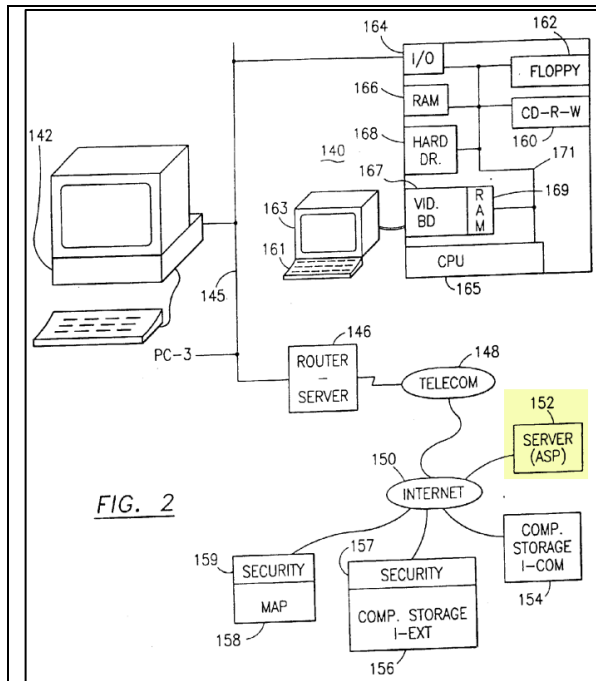
Redlich further discloses storing the parsed data in **granular data stores**. EX1005, ¶¶37 (“[F]inancial data ... can be parsed with an algorithm, the **parsed segments dispersed off-site**, (that is, separated and stored in extract and remainder stores or computer memories)”), 64 (“The present invention, 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*.”). EX1003, ¶¶236-237.

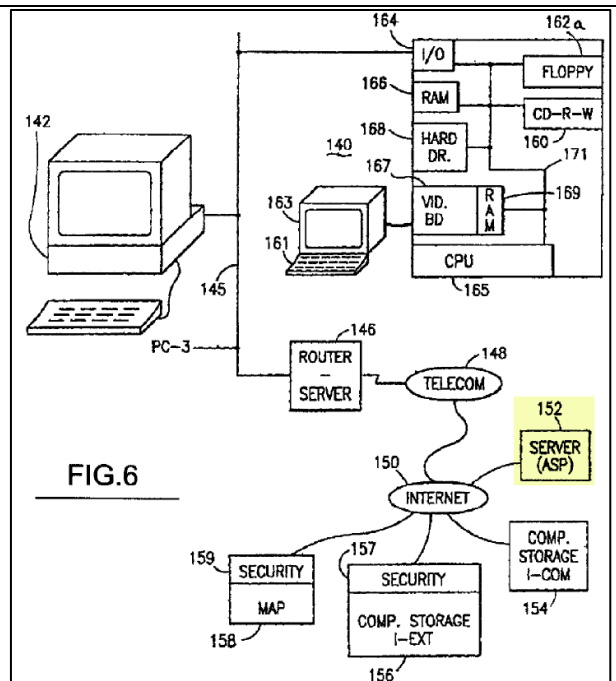
- vi. [1e] said processor having means for applying a reconstruction data process employing said respective *access controls* to combine one or more of said *security designated data* and *remainder data*.

Redlich discloses this limitation. *First*, as discussed in Section VI.B.1.iv, Redlich discloses a processor.

Second, Redlich discloses the structure of the claimed “means.” Redlich discloses the same processor and algorithm disclosed in the ’244 Patent. Figure 2 of Redlich discloses the ASP server, which a POSITA would have understood comprises a processor. *See also* Section B.1.iv. Figure 2 of Redlich, reproduced below side-by-side Figure 6 of the ’244 Patent, shows the same ASP server:



EX1005, Figure 2



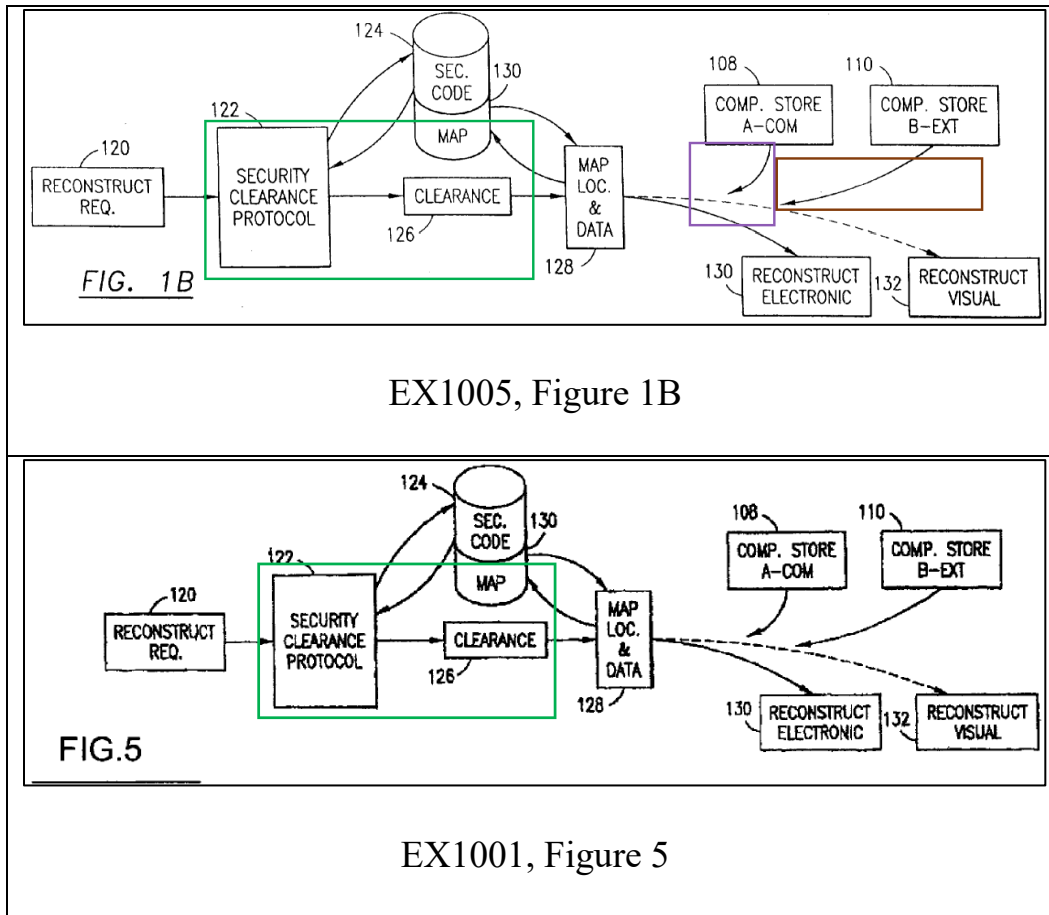
EX1001, Figure 6

Compare EX1005, Figure 2 at box 152 with EX1001, Figure 6 at box 152. The algorithm performed is described in EX1005, ¶¶131, 146, which is the same algorithm described in the '244 Patent. See EX1001, 438:9-15, 441:16-30. In particular, similar to the '244 Patent, Redlich discloses that “[t]o reconstruct the document, the user ...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** [and] **I-ext 156** ... The system compiles the entirety of the **plaintext document** by gathering the dispersed components thereof

or compiles partial reconstructions for different levels of security.”). *Compare* EX1005, ¶131 with EX1001, 441:16-25. EX1003, ¶¶239, 241-242.

Third, Redlich discloses the function of the claimed “means.” Specifically, Redlich discloses 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, ¶¶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**.”), 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.”), 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**.”); *see also* EX1005, ¶¶131, 200. EX1003, ¶¶243-245.

Figure 1B of Redlich, reproduced below on top of Figure 5 of the ’244 Patent, 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**:



Compare EX1005, Figure 1B with EX1001, Figure 5. Figure 1B shows a reconstruction process of a **plaintext document**. After determining that a user has “the **proper security clearance**,” the system provides a “full or partial reconstruction of the **plaintext**” by “gather[ing] the **extracted data** and **remainder data** into a **single plaintext document**.” EX1005, ¶122; see also EX1001, 447:5-31 (same disclosure in the ’244 Patent). EX1003, ¶¶246-247.

vii. Reasons To Combine Redlich With Ozzie

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 them separately from the remainder data, for several reasons.

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. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). Redlich and Ozzie relate to the same field of storing information and address the same problem of maintaining security and efficient storage of the information. The Redlich and Ozzie combination would merely involve using Ozzie's method of storing data in a cloud partitioned based on user identity in 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. EX1005, ¶¶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."); EX1006, 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.”); *see also*, EX1005, ¶¶64, 124, 177, Figure 2, Figure 6, Claim 139; EX1006, 1:16-26, 4:33-36, 4:59-5:12-11, 13:56-59, 13:64-66, 14:6-9, 14:16-18, Figure 1, Figure 11. EX1003, ¶¶276-289.

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). “Nothing more is required to show a motivation to combine under *KSR*....” See *Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373, 1381 (Fed. Cir. 2023) (holding that it was “enough for [Petitioner] to show that there was a known problem” in the art and that the referenced prior art helped address that issue). Ozzie’s disclosure of storing data within a cloud that is partitioned by user identities, thereby securely and efficiently managing data storage across multiple devices and services, is a “universal motivation” known 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. “‘Universal’ motivations known in a particular field to improve technology provide ‘a motivation to combine prior art references even absent any hint of suggestion in the references themselves.’” *Intel Corp.*, 61 F.4th at 1380. EX1003, ¶¶290-294.

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. Redlich’s system would improve by using Ozzie’s technique because incorporating Ozzie’s technique of storing data in a cloud partitioned based on user identities would allow for better organization and easier identification and access of a particular user’s data. EX1006, 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.”); *see also* EX1002, 2233 (during prosecution of the ’244 Patent, Examiner explained that “[b]y allowing the computing environment to be a cloud, the devices contained within the environment can communicate without the need for additional security clearances/credentials.”). 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) in the same way (e.g., by storing the information in a plurality of data stores based upon particular criteria). *KSR*, 550 U.S. at 417. EX1003, ¶295.

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, 5:8-21; EX1002, 2233. 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, 5:8-21. EX1003, ¶¶296-297.

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. *KSR*, 550 U.S. at 401. EX1003, ¶¶298-300.

Fifth, Ozzie provides express motivations that would have led a POSITA to combine Ozzie’s and Redlich’s teachings. Indeed, Ozzie explains 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, 1:16-26. Ozzie then illustrates an invention wherein information is “stored in partitions within a cloud while preventing unwanted or unintended disclosure of the information.” EX1006, 4:33-36. Ozzie then 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, 4:66-5:1. 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 is distinguished based on a particular criteria, such as Redlich’s invention of storing security sensitive data in a plurality of extract stores corresponding to a plurality of security levels. EX1003, ¶¶301-303.

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, 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. EX1003, ¶304.

A POSITA would also have had a reasonable expectation of success in combining Redlich with Ozzie. Combining Redlich with Ozzie would merely involve using partitions within a cloud as the extract stores disclosed in Redlich's system while incorporating the access controls in Redlich's system to limit the access to those partitions. As mentioned above, a POSITA would appreciate the teachings from Ozzie that such partitions could be based upon any criteria, such as the criteria of a plurality of security levels. *See* EX1006, 4:64-5:1. EX1003, ¶¶305-308.

VII. Discretionary Denial Would Be Inappropriate

A. Discretionary Denial Under The *Fintiv* Factors Is Not Appropriate

The six factors considered for § 314 denial strongly favor institution. *See Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential).

1. No evidence regarding a stay

No motion to stay has been filed, so this factor is neutral. *Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (PTAB June 16, 2020) (informative); *see also Dish Network L.L.C. v. Broadband iTV, Inc.*, IPR2020-01359, Paper 15 (Feb. 12, 2021) (“It would be improper to speculate, at this stage, what the Texas court might do regarding a motion to stay...”).

2. Parallel proceeding trial date

This factor is neutral. The Board’s Final Written Decision is expected in December 2024.² While trial is currently scheduled for August 19, 2024 (EX1008), the Board recognizes “that scheduled trial dates are unreliable and often change.” *See* EX1020 (Director’s June 21, 2022 Memorandum on Discretionary Denials (“EX1020”)), 8. Accordingly, the Board now uses median time-to-trial statistics in the relevant venue to determine a projected trial date for *Fintiv* purposes: “The PTAB will weigh this factor [factor 2] against exercising discretion to deny institution under *Fintiv* if the median time-to-trial is around the same time or after the projected statutory deadline for the PTAB’s final written decision.” EX1020, 9.

The co-pending district court case was filed in the Eastern District of Texas on November 28, 2022. The statistics for the two most recent periods show a median time-to-trial in the Eastern District of Texas between 19 months March 2023) and 24.5 months (March 2022). EX1009, 1. Accordingly, the projected trial date for purposes of *Fintiv* is between June 2024 (which is unlikely since June 2024 is before the scheduled trial date of August 2024) and December 2024—approximately 24 months after November of 2022—and around the Board’s Final Written Decision,

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

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

3. Investment in the parallel proceeding

The co-pending litigation is in its very early stages, and the investment in it has been minimal. *See* EX1007, EX1010. The parties have not exchanged preliminary positions on claim construction, and expert discovery has not begun. *See PEAG LLC v. Varta Microbattery GmbH*, IPR2020-01214, Paper 8, 17 (PTAB Jan. 6, 2021) Further, the Markman hearing is not scheduled until March of 2024. EX1007, 4.

Moreover, Patent Owner served their infringement contentions on Petitioner and confirmed which claims were being asserted only on February 28, 2023. EX1010. Under *Fintiv*, Petitioner’s prompt filing “weigh[s] against exercising the authority to deny institution.” *Fintiv*, Paper 11 at 11 (“If the evidence shows that the petitioner filed the petition expeditiously, such as promptly after becoming aware of the claims being asserted, this fact has weighed against exercising the authority to deny institution under NHK”). This factor favors institution.

4. Overlapping issues with the parallel proceeding

Petitioner stipulates that if the IPR is instituted, Petitioner will not pursue the same grounds in the district court litigation. *Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (June 16, 2020) (informative).

5. Identity of parties

Petitioner is a defendant in the litigation. That is true of most Petitioners in IPR proceedings. Accordingly, this factor should not be a basis for denying institution.

6. Other circumstances

The prior art presented in this Petition renders the Challenged Claim unpatentable as obvious. “[T]he PTAB will not deny institution of an IPR or PGR under *Fintiv* (i) when a petition presents compelling evidence of unpatentability.” EX1020, 2. “Compelling, meritorious challenges are those in which the evidence, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.” EX1020, 4. Here, the Petition plainly shows that the ’244 Patent claims no more than the known concept of storing sensitive data in security-controlled memories. The evidence of unpatentability is compelling, and thus the PTAB should not deny institution under *Fintiv*.

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

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

Discretionary denial under § 325(d) is not warranted because the challenges presented in this petition are neither cumulative nor redundant to the prosecution of the '244 patent. The PTO has not previously considered Redlich or Ozzie in connection with the claims of the '244 Patent. Further, the combination is not redundant to any combination of references considered during prosecution. Additionally, Dr. Zadok is an expert in the relevant art, and his analysis of the prior art has not been presented to the PTO. EX1003, ¶¶46-309. In view of the new information presented in this Petition, the Board has ample discretion to institute an IPR on the grounds presented.

VIII. Conclusion

Accordingly, Petitioner has established a reasonable likelihood that the Challenged Claim is unpatentable.

Case IPR2023-00973
U.S. Patent No. 8,468,244

Dated: June 23, 2023

Respectfully submitted,

/Theodoros Konstantakopoulos/
Theodoros Konstantakopoulos
(Reg. No. 74,155)
tkonstantakopoulos@desmaraisllp.com
DESMARAIS LLP
230 Park Ave
New York, NY 10169
212-808-1060 (telephone)
212-351-3401 (facsimile)

Counsel for Petitioner

IX. Mandatory Notices

A. Real Party-in-Interest

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner certifies that the real party-in-interest is International Business Machines Corporation.

B. Related Matters

Pursuant to 37 C.F.R. § 42.8(b)(2), to the best knowledge of the Petitioner, the '244 patent is or was involved in the following case:

Case Heading	Number	Court	Date
<i>DigitalDoors, Inc.³ v. International Business Machines Corporation</i>	2:22-cv-457	EDTX	Nov. 29, 2022

C. Lead and Back-up Counsel and Service Information

Lead Counsel

Theodoros Konstantakopoulos
Desmarais LLP
230 Park Ave
New York, NY 10023

Phone: (212) 351-3400
tkonstantakopoulos@desmaraisllp.com
USPTO Reg. No. 74,155

³ The '244 Patent cover page (EX1001, 1) and the USPTO assignment database (<https://assignment.uspto.gov/patent/index.html#/patent/search/resultAbstract?id=8468244&type=patNum>) identify “Digital Doors, Inc.” as the assignee of the '244 Patent.

Case IPR2023-00973
U.S. Patent No. 8,468,244

Back-up Counsel

Brian D. Matty
Desmarais LLP
230 Park Ave
New York, NY 10023

Phone: (212) 351-3400
bmatty@desmaraisllp.com
USPTO Reg. No. 70,358

Emily Weber
Desmarais LLP
101 California Street
San Francisco, CA 94111

Phone: (415) 573-1858
eweber@desmaraisllp.com
USPTO Reg. No. 79,973

Please address all correspondence to lead and back-up counsel. Petitioner consents to service in this proceeding by email at the addresses above and at IBMDigitalDoorsIPRService@desmaraisllp.com.

CERTIFICATION UNDER 37 C.F.R. § 42.24(d)

Pursuant to 37 C.F.R. § 42.24(d), Petitioner hereby certifies, in accordance with and in reliance on the word count provided by the word-processing system used to prepare this Petition, that the number of words in this paper is 13,117. Pursuant to 37 C.F.R. § 42.24(d), this word count excludes the table of contents, table of authorities, mandatory notices under § 42.8, certificate of service, certificate of word count, appendix of exhibits, and any claim listing.

Dated: June 23, 2023

Respectfully submitted,

/Theodoros Konstantakopoulos/
Theodoros Konstantakopoulos
(Reg. No. 74,155)
tkonstantakopoulos@desmaraisllp.com
DESMARAIS LLP
230 Park Ave
New York, NY 10169
212-808-1060 (telephone)
212-351-3401 (facsimile)

Counsel for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), the undersigned certifies that a complete copy of the foregoing materials:

- Petition for Inter Partes Review Under 35 U.S.C. § 312 and 37 C.F.R. § 42.104 of U.S. 8,468,244;
- Exhibit List;
- Exhibits 1001-1020;
- Word Count Certification Under 37 CFR § 42.24(d);
- Petitioner's Power of Attorney

was served on counsel of record for Patent Owner by filing this document through P-TACTS on June 23, 2023, and by sending this document via Federal Express Priority Overnight shipping, which is at least as fast and reliable as U.S. Priority Mail Express, to counsel of record for Patent Owner at the correspondence address indicated in Patent Center:

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

Case IPR2023-00973
U.S. Patent No. 8,468,244

Dated: June 23, 2023

Respectfully submitted,

/Theodoros Konstantakopoulos/
Theodoros Konstantakopoulos
(Reg. No. 74,155)
tkonstantakopoulos@desmaraisllp.com
DESMARAIS LLP
230 Park Ave
New York, NY 10169
212-808-1060 (telephone)
212-351-3401 (facsimile)

Counsel for Petitioner