

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Unified Patents Inc.

Petitioner

v.

PanTaurus, LLC.

Patent Owner

IPR2014- _____

Patent 6,272,533

PETITION FOR *INTER PARTES* REVIEW

Mail Stop PATENT BOARD, PTAB

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

TABLE OF CONTENTS

I. INTRODUCTION1

II. MANDATORY NOTICES2

 A. Real Party in Interest2

 B. Related Matters.....4

 C. Identification of Lead and Back-Up Counsel.....5

 D. Service Information5

III. PAYMENT OF FEES6

IV. REQUIREMENTS FOR *INTER PARTES* REVIEW6

 A. Grounds for Standing6

 B. Statement of Precise Relief Requested (37 C.F.R. § 42.22(a))
 and Identification of Challenges (37 C.F.R. § 42.104(b))6

 C. How the Construed Claims are Unpatentable under the
 Statutory Grounds identified in 37 C.F.R. § 42.104(b)(2) and
 Supporting Evidence Relied upon to Support the Challenge.....7

 D. Threshold Showing of Reasonable Likelihood That Petitioner
 Would Prevail With Respect To At Least One Challenged
 Claim (35 U.S.C. § 314(a)) Has Been Met8

V. FACTUAL BACKGROUND.....8

 A. Declaration Evidence8

 B. The State of the Art as of 19999

 C. The Challenged ‘533 Patent12

 D. Prosecution History13

VI. CLAIM CONSTRUCTION (37 C.F.R. § 42.104(B)(3)).....13

A.	Support for Claim Construction	14
B.	Said First Memories of Claim 43 Cannot be Construed	18
VII.	THE GROUNDS SHOWING THAT PETITIONER HAS A REASONABLE LIKELIHOOD OF PREVAILING	19
A.	Holtey II and Holtey I Disclose Each Limitation of Claims 29, 31-34, 38, 39, 42, and 43	19
1.	The Combination of Holtey II and Holtey I	19
2.	Reasons to Combine Holtey II and Holtey I	23
3.	The Storage Device of Holtey II and Holtey I	24
4.	Claim 42 – First and Second Processors Include First and Second Memories	24
B.	Holtey II, Holtey I, and Shafe Disclose Each Limitation of Claims 35 and 36	27
1.	The Combination of Holtey II, Holtey I, and Shafe	27
2.	Reasons to Combine Holtey II and Holtey I with Shafe	32
C.	Claim Chart Demonstrating How Holtey II and Holtey I Render Claims 29, 31-34, 38, 39, 42, and 43 Obvious	33
D.	Claim Chart Demonstrating How Holtey II, Holtey I, and Shafe Render Claims 35 and 36 Obvious	55
VIII.	CONCLUSION	57

I. INTRODUCTION

Pursuant to the provisions of 35 U.S.C. §§ 311-319, Unified Patents Inc., (“Unified” or “Petitioner”) hereby petitions the Patent Trial and Appeal Board to institute *inter partes* review of claims 29, 31-36, 38, 39, 42, and 43 of U.S. Patent No. 6,272,533 to Browne (“the ‘533 Patent,” Ex. 1001).

In short, the ‘533 Patent describes a computer architecture that selectively disables the alteration of data residing on a storage device for security purposes. The architecture utilizes two buses with corresponding processors and a switch that is used to disable writing to the storage device to maintain data integrity on the device. This architecture, however, was well known as of the ‘533 Patent’s earliest priority date as demonstrated by two related patents: U.S. Pat. No. 5,491,827 to Thomas O. Holtey (“Holtey II”) and U.S. Pat. No. 5,442,704 to Thomas O. Holtey (“Holtey I”).

The Petitioner relies upon Holtey II and Holtey I to demonstrate that all but two of the challenged claims are unpatentable as being obvious. For the remaining two claims, the Petitioner relies upon Holtey II and I in combination with U.S. Pat. No. 6,035,429 to Shafe (“Shafe”) to demonstrate that those claims are unpatentable as being obvious. Holtey II, Holtey I, and Shafe were never considered by the Office and teach the exact architecture covered by the challenged claims. As such,

the Petitioner respectfully requests institution of an *inter partes* review of the challenged claims.

II. MANDATORY NOTICES

Pursuant to 37 C.F.R. § 42.8(a)(1), Unified Patents provides the following mandatory disclosures.

A. Real Party in Interest

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner certifies that Unified Patents is the real party-in-interest, and further certifies that no other party exercised control or could exercise control over Unified Patents' participation in this proceeding, the filing of this petition, or the conduct of any ensuing trial.

Unified Patents was founded by intellectual property professionals over concerns with the increasing risk of non-practicing entities (NPEs) asserting poor quality patents against strategic technologies and industries. The founders thus created a first-of-its-kind company whose sole purpose is to deter NPE litigation by protecting technology sectors, like cloud storage, the technology against which the '533 Patent is being asserted. Companies in a technology sector subscribe to Unified's technology specific deterrence, and in turn, Unified performs many NPE-deterrent activities, such as analyzing the technology sector, monitoring patent activity (including patent ownership and sales, NPE demand letters and litigation, and industry companies), conducting prior art research and invalidity

analysis, providing a range of NPE advisory services to its subscribers, sometimes acquiring patents, and sometimes challenging patents at the United States Patent and Trademark Office (USPTO). Since its founding, Unified is 100% owned by its employees; subscribers have absolutely no ownership interest.

Unified has sole and absolute discretion over its decision to contest patents through the USPTO's post-grant proceedings. Should Unified decide to challenge a patent in a post-grant proceeding, it controls every aspect of such a challenge, including controlling which patent and claims to challenge, which prior art to apply and the grounds raised in the challenge, and when to bring any challenge.

Subscribers receive no prior notice of Unified's patent challenges. After filing a post-grant proceeding, Unified retains sole and absolute discretion and control over all strategy decisions (including any decision to continue or terminate Unified's participation). Unified is also solely responsible for paying for the preparation, filing, and prosecution of any post-grant proceeding, including any expenses associated with the proceeding.

In the instant proceeding, Unified exercised its sole discretion and control in deciding to file this petition against the '533 Patent, including paying for all fees and expenses. Unified shall exercise sole and absolute control and discretion of the continued prosecution of this proceeding (including any decision to terminate

Unified's participation) and shall bear all subsequent costs related to this proceeding. Unified is therefore the sole real-party-in-interest in this proceeding.

B. Related Matters

PanTaurus LLC ("PanTaurus") has asserted the '533 Patent against thirty companies in the Eastern District of Texas. The following cases were all filed on April 23, 2014. An "*" indicates that the case has terminated.

- PanTaurus LLC v. Samsung Electronics America, Inc., 1-14-cv-00237
- PanTaurus LLC v. Fuhu, Inc., 1-14-cv-00231
- PanTaurus LLC v. Toshiba America, Inc., 1-14-cv-00240
- PanTaurus LLC v. Symantec Corporation, 1-14-cv-00239*
- PanTaurus LLC v. Code42 Software, Inc., 1-14-cv-00229
- PanTaurus LLC v. Salesforce.com, Inc., 1-14-cv-00236
- PanTaurus LLC v. Carbonite, Inc., 1-14-cv-00228*
- PanTaurus LLC v. Best Buy Purchasing, LLC, 1-14-cv-00234*
- PanTaurus LLC v. Brightpearl, Inc., 1-14-cv-00227
- PanTaurus LLC v. Seagate Technology LLC., 1-14-cv-00238
- PanTaurus LLC v. Dropbox, Inc., 1-14-cv-00230
- PanTaurus LLC v. Microsoft Corporation, 1-14-cv-00235
- PanTaurus LLC v. Hisense USA Corporation, 1-14-cv-00233
- PanTaurus LLC v. Google Inc., 1-14-cv-00232
- PanTaurus LLC v. Amazon.com, Inc., 1-14-cv-00226

The following cases were all filed on September 3, 2013 and all have terminated.

- PanTaurus LLC v. Apricorn, Inc., 1-13-cv-00540
- PanTaurus LLC v. Hewlett-Packard Company, 1-13-cv-00546
- PanTaurus LLC v. Verbatim Americas LLC, 1-13-cv-00552
- PanTaurus LLC v. Sony Electronics Inc., 1-13-cv-00551
- PanTaurus LLC v. Imation Corp., 1-13-cv-00547
- PanTaurus LLC v. Fujitsu America, Inc., 1-13-cv-00545
- PanTaurus LLC v. Data Locker Inc., 1-13-cv-00544
- PanTaurus LLC v. Global Silicon Electronics, Inc., 1-13-cv-00543
- PanTaurus LLC v. ASUS Computer International, 1-13-cv-00541
- PanTaurus LLC v. Acer America Corp., 1-13-cv-00538
- PanTaurus LLC v. Lenovo (United States) Inc., 1-13-cv-00548
- PanTaurus LLC v. Lexar Media, Inc., 1-13-cv-00549
- PanTaurus LLC v. Apple, Inc., 1-13-cv-00539
- PanTaurus LLC v. BlackBerry Corporation, 1-13-cv-00542
- PanTaurus LLC v. Sandisk Corporation, 1-13-cv-00550

C. Identification of Lead and Back-Up Counsel

Pursuant to 37 C.F.R. § 42.8(b)(3), Petitioner provides the following designation of counsel: Lead counsel is Michael L. Kiklis (Reg. No. 38,939) and back-up counsel is Scott A. McKeown (Reg. No. 42,866).

D. Service Information

Pursuant to 37 C.F.R. § 42.8(b)(4), papers concerning this matter should be served on the following:

Address: Michael L. Kiklis
Oblon Spivak
1940 Duke Street
Alexandria, VA 22314
Email: cpdocketkiklis@oblon.com
Telephone: (703) 413-2707/(703)413-3000 (main)
Fax: (703) 413-2220

III. PAYMENT OF FEES

The undersigned authorizes the Office to charge the required fees as well as any additional fees that might be due to Deposit Account No. 15-0030.

IV. REQUIREMENTS FOR *INTER PARTES* REVIEW

As set forth below and pursuant to 37 C.F.R. § 42.104, each requirement for *inter partes* review of the '533 Patent is satisfied.

A. Grounds for Standing

Petitioner certifies pursuant to 37 C.F.R. § 42.104(a) that the '533 Patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting *inter partes* review challenging the patent claims on the grounds identified herein.

B. Statement of Precise Relief Requested (37 C.F.R. § 42.22(a)) and Identification of Challenges (37 C.F.R. § 42.104(b))

Petitioner requests *inter partes* review and cancellation of claims 29, 31-36, 38, 39, 42, and 43 of the '533 Patent as being obvious under 35 U.S.C. § 103 in

view of the following U.S. Patents, each of which is prior art pursuant to 35 U.S.C. §§ 102(b) and/or 102(e):

1. U.S. Pat. No. 5,491,827, issued Feb. 13, 1996 (“Holtey II”) (Ex. 1002);
2. U.S. Pat. No. 5,442,704, issued Aug. 15, 1995 (“Holtey I”) (Ex. 1003); and
3. U.S. Pat. No. 6,035,429, priority date of Dec. 23, 1994 (“Shafe”) (Ex. 1004).

Specific Challenges

- 1) Claims 29, 31-34, 38, 39, 42, and 43 are challenged as being obvious under 35 U.S.C. § 103 in view of Holtey II and Holtey I; and
- 2) Claims 35 and 36 are challenged as being obvious under 35 U.S.C. § 103 in view of Holtey II, Holtey I, and Shafe.

C. How the Construed Claims are Unpatentable under the Statutory Grounds identified in 37 C.F.R. § 42.104(b)(2) and Supporting Evidence Relied upon to Support the Challenge

The challenged claims are to be construed as indicated in Section VI, below. Pursuant to 37 C.F.R. § 42.104(b)(4), an explanation of how the challenged claims are unpatentable under the statutory ground identified above, including the identification of where each element of the claim is found in the prior art, is provided in Section VII, below, in the form of two claim charts. Pursuant to 37 C.F.R. § 42.104(b)(5), the appendix numbers of the supporting evidence relied

upon to support the challenges and the relevance of the evidence to the challenges raised, including identifying specific portions of the evidence that support the challenges, are provided in Section VII, below, in the form of two claim charts.

D. Threshold Showing of Reasonable Likelihood That Petitioner Would Prevail With Respect To At Least One Challenged Claim (35 U.S.C. § 314(a)) Has Been Met

The information and evidence presented in this Petition, including unpatentability grounds detailed in Section VII, below, establishes a reasonable likelihood that Petitioner will prevail with respect to at least one of the challenged claims. *See* 35 U.S.C. § 314(a). Indeed, that section, supported by the Kaeli declaration (Ex. 1005) demonstrates that the challenged claims are obvious in view of the relied upon prior art.

V. FACTUAL BACKGROUND

A. Declaration Evidence

This Petition is supported by the declaration of Professor David R. Kaeli, Ph.D. from Northeastern University (attached as Ex. 1005). Dr. Kaeli offers his opinion with respect to the skill level of one of ordinary skill in the art (Ex. 1005, ¶¶ 21 and 22), the content and state of the prior art (Ex. 1005, ¶¶ 23-30), the teachings and suggestions that one of ordinary skill would understand based on Exs. 1002-1004 (Ex. 1005, pps. 15-55), how one of ordinary skill in the art would understand various claim terms (Ex. 1005, at ¶¶ 12-17), the reasons for combining

the teachings from Exs. 1002-1004 (Ex. 1005, ¶¶ 33-41), and the manner in which one of ordinary skill would combine those teachings (Ex. 1005, pps. 19-55). Dr. Kaeli is Distinguished Professor of Electrical and Computer Engineering at Northeastern University in Boston, Massachusetts and is Director of the Northeastern University Computer Architecture Laboratory. He has over twenty years of experience in computer architecture. *See* Ex. 1005.

B. The State of the Art as of 1999

Multi-bus and multi-processor systems were common prior to 1999. Specifically, IBM and other mainframe manufacturers were producing multiprocessor systems. For example, in 1978, IBM introduced the IBM System/370 model 3033 that included a dual-processor with independent buses to a shared disk drive subsystem. Ex. 1005, at ¶ 23.

The ability to enable/disable access to hard drives was also well known prior to 1999. For example, U.S. Patent 6,052,781 (Ex. 1006) discloses:

Access by one system user to another system user's hard disk drive and attendant files is absolutely denied thereby preventing corruption of one user's hard disk drive files by another user's carelessness or malicious intent, or through unique setup adaptation of one user's program files which may otherwise interact with and impose unwanted changes on another's program file's operational performance. Ex. 1005, at ¶ 24; Ex. 1006, at Abstract.

The ability to utilize a switch to disable reading or writing to disk was well known to those of ordinary skill in 1999. For example, U.S. Patent 5,268,960 (Ex. 1007) discloses:

A hard disk protection device comprising a decoding circuit which receives signals from the address and data buses of a personal computer to decode the signals associated with hard disk write actions and generating a signal to suppress the signal of IOW line so as to disable the write function of the hard disk. A switch is provided for a user to disconnect the decoding circuit from the hard disk so as to allow the hard disk to be operated as a conventional hard disk. Ex. 1005, at ¶ 25; Ex. 1007, at Abstract.

Further, U.S. Patent 4,912,633 (Ex. 1009) by NCR Corporation discloses master/slave bus configurations, with the ability of processors to have “mastery” over their own buses:

A modular and hierarchical multiple bus computer architecture in which the master bus and slave bus are substantially identical, and communicate through a combination of an interface controller and a shared dual port RAM responsive to a shared RAM controller. Processor engine modules including a bus, a processor, an interface controller, a shared dual port RAM, and a shared RAM controller are horizontally and/or vertically integrated at multiple levels without major restructuring of the composite system control operations by having each slave processor engine module interface as a peripheral upon the bus of its master. The modularity of the architecture allows

the use of standard peripherals and platform processor engines to expand memory or increase functionality without burdening the master bus processor engine. Each slave bus processor engine is fully functional as an independent processor with mastery over its own bus. Ex. 1005, at ¶ 27; Ex. 1009, at Abstract.

Ex. 1005, at ¶ 27.

Finally, although the challenged claims purport to claim as new “a switch operable to selectively enable and disable at least one of said operating modes, said switch controllable by means distinct and separate from at least one of said processors whereby said one processor is inhibited from controlling said operation of said switch,” this same switching mechanism—and indeed the rest of the limitations of the challenged claims—is disclosed by a pair of related patents: Holtey II and Holtey I. These patents disclose the same switching mechanism used for the same purpose as the ‘533 Patent: protecting a storage device from corruption from malicious software. Ex. 1005, at ¶ 28.

Holtey I describes the design of a secure memory card that plugs into a host. The security mechanism described uses a non-volatile random access memory for storing a security key value. Each block of protected memory includes a lock bit. The key and the lock bit are used together to protect storage elements on the card. The microprocessor associated with the memory card utilizes a set of special instructions to validate the key value and the lock bits. If the validation procedure

is successful, access is granted to the data on the memory card. Holtey I can selectively grant either read or write access to the storage elements on the card. Ex. 1005, at ¶ 29.

Holtey II, related to Holtey I, describes the design of a secure application card or Smart Card that also plugs into a host. One purpose of Holtey II is to protect application memory. The security mechanism described in Holtey II uses multiple microprocessors and multiple buses to control access to non-volatile memory chips, the claimed “storage device.” Access to the non-volatile memory is under control of one of the two microprocessors. The secure application card also contains an access discrimination logic circuit that considers the access type that can be made by each microprocessor for the purpose of protecting stored information in the non-volatile memory. Holtey II’s Fig. 1 shows the exact architecture of the contested claims, as discussed below. Ex. 1002, at Fig. 1; Ex.1005, at ¶ 30.

C. The Challenged ‘533 Patent

Although the ‘533 Patent discloses both a single-bus architecture and a dual-bus architecture, the challenged claims cover only the dual-bus architecture. Each bus is connected to a processor and each bus is connected to a storage device that selectively operates in a plurality of “operating modes,” such as read or write access. Lastly, the challenged claims include a switch “operable to selectively

enable and disable at least one of said operating modes, said switch controllable by means distinct and separate from at least one of said processors whereby said one processor is inhibited from controlling said operation of said switch.” Ex. 1001, at claim 29. As Dr. Kaeli testifies, all the features of the contested claims were well known to one of ordinary skill in the art as of the earliest priority date of the ‘533 Patent. Ex. 1005, at ¶¶ 10-11.

D. Prosecution History

During prosecution, the applicant was unable to obtain claims directed to the single-bus embodiment. Instead, the claims had to be amended to require a dual-bus architecture to gain allowance. See Ex. 1010, at 18-32. Nevertheless, this dual-bus architecture is exactly what is disclosed by Holtey II and Holtey I.

VI. CLAIM CONSTRUCTION (37 C.F.R. § 42.104(B)(3))

Pursuant to 37 C.F.R. § 42.204(b)(3), the claims subject to *inter partes* review shall receive the “broadest reasonable construction in light of the specification of the patent in which [they] appear[.]” See 42 C.F.R. § 100(b). For the purposes of this petition, the Petitioner adopts the plain meaning for all claims terms. The Petitioner proposes a specific construction for several terms below:

Claim Term	Proposed construction
Data storage device (claims 29, 32, 35, 36, and 38)	“any device that retains information”
Operating modes (claims 29, 31, 33, and 34)	“any state of operation of a device”

Switch (claims 29 and 31)	“a control mechanism”
---------------------------	-----------------------

A. Support for Claim Construction

Data storage device (claims 29, 32, 35, 36, and 38) – One of ordinary skill in the art would understand this term to mean “any device that retains information.” The ‘533 Patent states the following about the storage device, using the term broadly, thus supporting this claim construction:

According to another feature of the invention, the storage device may include a magnetic media and comprise a disk drive or a magnetic tape. The storage device may alternatively include a non-volatile electronic memory device, such as an EEPROM. Ex. 1001, at 40-44.

According to still a further feature, the storage device may include an optical storage device such as a CD-ROM or an electro-optical source device such as CD-RW. Ex. 1001, at 45-47.

In this configuration, the two processors are isolated from each other . . . the other providing remote access to the mass storage devices including hard disk drives. Ex. 1001, at 8-12.

The doctrine of claim differentiation also supports this construction.

Specifically, claims 35-42 depend indirectly from claim 29 and further define the “storage device” to be a magnetic media, a disk drive, a magnetic tape, a non-volatile electronic memory device, an EEPROM, an optical storage device, and an

electro-optical storage device, respectively. Ex. 1005, at ¶ 14. Thus, the term “data storage device” must be construed broadly.

Operating modes (claims 29, 31, 33, and 34) – One of ordinary skill in the art would understand this term to mean “any state of operation of a device.” Although the ‘533 Patent refers to a non-secure and secure mode of operation, this refers to whether writing to the storage device is disabled, which is different than the broader notion of “operating modes.” *See* Ex. 1001, at Abstract. Claims 32-34, which depend from claim 29, clarify that “operating modes” include at least a “read-only” mode and a “write-only” mode. With respect to “operating modes,” the ‘533 Patent states:

The storage device is responsive to the processor for selectively operating in a plurality of operating modes including a read mode of operation for retrieving previously stored data and a write mode of operation for storing data. Ex. 1001, at 6:19-22.

At least one of the operating modes may be a read mode of operation and, alternatively, may be a write mode of operation. Ex. 1001, at 6:34-36.

For example, the mode limiting switch is applicable to other storage devices and media and to other devices where selection and control of operating modes must be restricted. For example, a restricted user may be limited by the switch to monitoring the output of a device such as a video camera, while a local user may additionally control

the camera. Similarly, the switch may be used in-line with a printer to allow limited printing capabilities for certain users while providing full capabilities to local users of the system. Ex. 1001, at 12:18-28.

In the quote reproduced immediately above at 12:18-28, the '533 Patent attempts to expand the term "operating mode" to cover other concepts beyond merely read and write access, such as printing capabilities. One of ordinary skill in the art would thus understand the term "operating mode" to mean any state of operation of a device. Therefore, in the context of a storage device, an operating mode can include not only read-only access and write-only access, but can also include read/write access and other modes, such as execute access. Ex. 1005, at ¶ 15.

Switch (claims 29 and 31) – One of ordinary skill in the art would understand this term to mean "a control mechanism," and within the context of claim 29, it means a control mechanism "operable to selectively enable and disable one of said operating modes." One of ordinary skill in the art would understand this control mechanism to include either a manual or an automatic switch. Since claim 30 specifically restricts the switch to a manually operated switch, the doctrine of claim differentiation dictates that claim 29 should be construed broader, including not only a manual switch but also an automatic switch. Furthermore, the switch could

be implemented using hardware and/or software. This analysis is supported by the '533 Patent:

A system and method according to the invention limit access to computer system storage media by providing a locally operable switch which selectively prevents alteration to the local storage media. The switch may be a manually operable mechanical device or may be electronic, so long as its operation is isolated from the system being protected, and may be entirely self contained. Ex. 1001, at 3:59-66.

The switch is operable to selectively enable and disable at least one of the operating modes, the switch being controllable by means distinct and separate from the processor so that the processor is inhibited from controlling the operation of the switch. According to a feature of the invention, the switch may be manually operated to selectively make and break an electrical conducting path connecting the processor with the storage device. Ex. 1001, at 6:23-29.

FIG. 2 is a block diagram of a computer system according to the invention including a switch for inhibiting a hard disk drive from operating in a write mode of operation and segmented main memory. Ex. 1001, at 7:9-12.

FIG. 5 is a flow diagram for a software implemented switch for restricting operation of designated peripheral devices to programmed modes of operation. Ex. 1001, at 7:19-21.

Alternatively, switch 202 may include appropriate hardware and software to monitor signals transmitted by controller 108 to hard disk drive 110. Write (or other inhibited actions such as read, erase, etc.) commands to one or more designated devices would be recognized and intercepted, switch 202 generating an appropriate error message back to controller 108. Permissible operations would be transmitted through to disk drive 110 without impediment. In this software implementation of switch 202, predetermined portions of disk drive 202 may be designated as secure so that write commands are selectively inhibited only to designated tracks, sectors, clusters, etc. Ex. 1001, at 8:43-54.

Further, by placing hard disk drive 110b in a “Write only” mode of operation using switch 202b, data uploaded to the drive by remote users of the system cannot be accessed by other remote users thereby enhancing system security. Ex. 1001, at 10:37-40.

For example, the mode limiting switch is applicable to other storage devices and media and to other devices where selection and control of operating modes must be restricted. Ex. 1001, at 12:18-22.

Ex. 1005, at ¶ 15; *see also*, Ex. 1001, at 4:34-44; 4:61-64; 7:60-65; 6:4-10; 10:59-63; 8:62-9:2.

B. Said First Memories of Claim 43 Cannot be Construed

Claim 43’s “said first memories” is not defined in any of the claims from which it depends, rendering it impossible for one of ordinary skill to understand

the meaning of this term. Ex. 1005, at ¶ 17. If the PTAB decides not to institute trial on this claim, the Petitioner respectfully requests this Board state in its Institution Order that this term cannot be construed. Otherwise, for the purposes of this Petition, the Petitioner and Dr. Kaeli will assume that claim 43 depends from claim 42 and demonstrate below that it is obvious.

VII. THE GROUNDS SHOWING THAT PETITIONER HAS A REASONABLE LIKELIHOOD OF PREVAILING

A. Holtey II and Holtey I Disclose Each Limitation of Claims 29, 31-34, 38, 39, 42, and 43

1. The Combination of Holtey II and Holtey I

Holtey II teaches all elements of claims 29, 31-34, 38, 39, 42, and 43.

Nevertheless, Petitioner relies upon both Holtey II and Holtey I to further bolster the analysis regarding operating modes. *See* Ex. 1005, at ¶ 31.

Holtey II discloses the architecture of the '533 Patent. It teaches dual buses, each connected to a processor, and a shared storage device and switch that operate in the same way as the '533 Patent, as annotated Fig. 1 of Holtey II demonstrates:

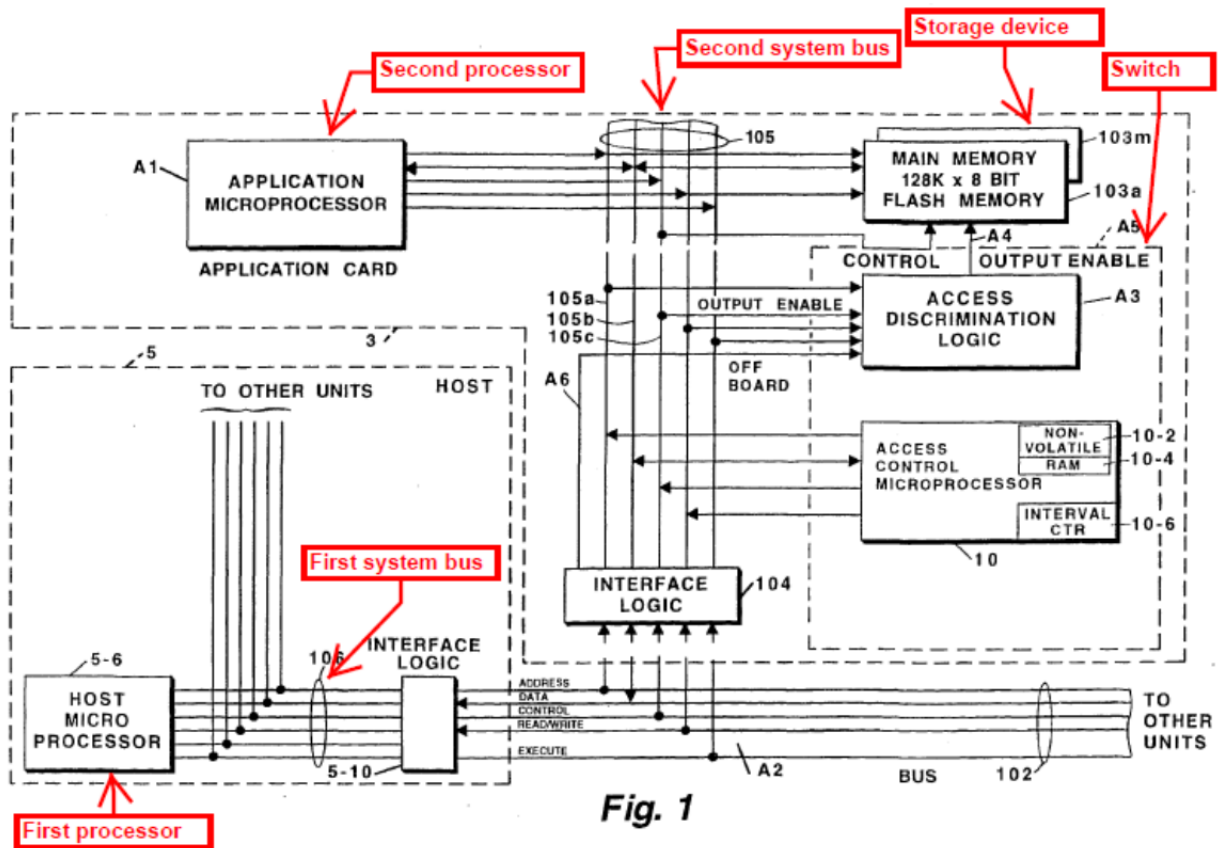


Fig. 1

Ex. 1002, at Fig. 1; Ex. 1005, at ¶ 30. This architecture is the same as the '533

Patent's:

Claim 29 Claim Term	Holtey II
First system bus	Bus 106
First processor connected to first system bus	Host micro processor
Second system bus	Bus 105
Second processor connected to the second system bus	Application microprocessor
Data storage device	Flash memory 103a through 103n
Switch	Discrimination logic unit/access

	control microprocessor
--	------------------------

In the combination of Holtey II and Holtey I, Dr. Kaeli relies upon the flash memory for the claimed “data storage device.” Ex. 1005, at ¶ 30. Holtey II describes using Intel 28F001BX flash memory chips as an example embodiment. Ex. 1002, at 5:19-25. Holtey II describes a plurality of operating modes, including “Execute, read and write control signals generated by any one of the microprocessors.” Ex. 1002, at 5:34-36. Holtey II does not provide too much explicit details of the flash memory because “such circuits can be considered conventional in design” and consequently are only “described to the extent necessary.” Ex. 1002, at 6:50-52. Thus, Holtey II does not provide too much express disclosure of the write-only operating mode. Nevertheless, one of ordinary skill in the art would recognize that the write-only mode is inherently disclosed, if not explicitly disclosed, and that Holtey II’s storage device could be used for providing write-only access. One of ordinary skill would use a write-only capability with Holtey II for the appropriate application, such as for various administrative functions like statistic gathering, monetary receipt collection, or compiling financial data, which is explicitly disclosed in Holtey II at 13:40-60. Ex. 1005, at ¶ 31.

Moreover, Holtey I explicitly discloses write-only access:

As shown in FIG. 3, the flash memory circuits receive a plurality of input address signals A0-A16, data signals D00-D07 and control signals consisting of chip enable, write enable, output enable, power down and erase/program power supply signals CE, WE, OE, PWD, and VPP respectively. The functions performed by these signals are described in Appendix I. Ex. 1003, at 7:39-45.

OE OUTPUT ENABLE: Gates the device's outputs through the data buffers during a read cycle.

OE is active low.

WE WRITE ENABLE: Controls writes to the command register and array blocks. WE is active low. Addresses and data are latched on the rising edge of the WE pulse.

Vpp ERASE/PROGRAM POWER SUPPLY

for erasing blocks of the array or programming bytes of each block. Note: With $V_{pp} < VPPI \text{ Max}$, memory contents cannot be altered. When Vpp is at a high level, programming can take place; if Vpp is at a low level, the memory array 54 functions as a read only memory. Ex. 1003, at 15:25-37.

Ex. 1005, at ¶ 32.

Holtey I describes using, as an example, the same flash memory as Holtey II, Intel's 28F001BX 1M. Since both Holtey II and I use the same flash memory, the teachings of Holtey I are applicable to and are necessarily present in Holtey II.

Thus, Holtey I's teaching of the write-only operating mode means that the write-only mode is necessarily present in Holtey II. Nevertheless, the combination of Holtey II and I certainly discloses the write-only operating mode, and Petitioner relies upon both Holtey II and Holtey I for claims 29, 31-34, 38, 39, 42, and 43.

2. Reasons to Combine Holtey II and Holtey I

One of ordinary skill in the art would be led to combine Holtey I with Holtey II for many reasons. First, Holtey II specifically identifies Holtey I in the "RELATED APPLICATIONS" section. Ex. 1002, at 1:14-18. In fact, Holtey II expressly indicates that its secure application card should be operated in conjunction with the host system microprocessor of Holtey I:

The above and other objects of the present invention are achieved in the preferred embodiment of a secure application card which is operated in conjunction with one of more host systems such as the host system microprocessor described in the above reference related patent application to Thomas O. Holtey, et al. Ex. 1002, at 2:55-60.

Thus one of ordinary skill when looking at Holtey II would necessarily be led to consider the teachings of Holtey I. Second, both Holtey I and II list the same inventor, Thomas O. Holtey, and were filed on the same day by the same assignee. Third, the Holtey patents are directed to the same problem as the '533 Patent—defending against malicious software attack—as indicated by the field of the

invention and the primary object of the invention of both patents, which are identical:

This invention relates to the field of portable personal computers and more particularly to systems for maintaining data security in a portable digital information environment. Ex. 1002, at 1:21-25; Ex. 1003, at 1:19-24.

Accordingly, it is a primary object of the present invention to provide a portable digital system with a secure memory subsystem.” Ex. 1002, at 2:42-44; Ex. 1003, at 2:42-44.

Lastly, Holtey II and Holtey I appear to be descriptions of the same security device that merely focus on different aspects. This is demonstrated by the dramatic overlap of design details. There are therefore many reasons why one of ordinary skill in the art would be led to combine the teachings of Holtey II and I. Ex. 1005, at ¶ 33; *see also Id.*, at ¶¶ 31-32.

3. The Storage Device of Holtey II and Holtey I

Holtey II and Holtey I describe a flash memory, which Dr. Kaeli uses in his analysis as the storage device of the claims. As Dr. Kaeli testifies, one of ordinary skill in the art recognizes that flash memory is a form of non-volatile memory (claim 38) and is also a form of EEPROM (claim 39). Ex. 1005, at ¶ 34.

4. Claim 42 – First and Second Processors Include First and Second Memories

Claim 42 requires a first and second processor that include “a first memory for storing program instructions and a second memory, separate and distinct from said first memory, storing data.” Holtey II explicitly shows that the host processor (the first processor) has a first memory that stores program instructions in a ROM:

The host microprocessor is a simple device which operates the peripheral devices but has minimum functionality of its own. For example, the microprocessor can be constructed using an Intel 8051 chip. It has its own read only memory (ROM) which contain start up and self test code only. Thus, the host device can be viewed as a “shell” with all of the significant functionality contained within the application card 3. Ex. 1002, at 8:2-9.

As Dr. Kaeli notes, since ROM is read only, this quote satisfies the limitations of claim 43. Ex. 1005, at ¶ 35.

Holtey II also explicitly shows that the application processor (the second processor) includes a first memory storing program instructions:

The application microprocessor A1 is contained in the application card and is programmed to perform all operation functions required for running a given application. In the preferred embodiment, the microprocessor may be constructed using an Intel 80286 microprocessor chip. The application microprocessor A1 also has a random access memory which is uses to perform certain intermediate

calculations in running specific applications. Ex. 1002, at 7:55-62 (emphasis added).

Holtey II does not explicitly disclose that the host processor and the application processor have a separate memory that stores data. However, such is necessarily present in these processors because Holtey II describes the application processor as being an Intel 80286 chip and describes the host processor as being an Intel 8051 chip. Dr. Kaeli is familiar with both architectures, and testifies that these processors store program instructions and data in separate memories. For example, in the Intel 80286 chip, program instructions are stored in a local RAM memory (as the above quote indicates) that is directly accessed by the chip and also has an on-chip, separate memory that stores data (descriptor registers used for addressing memory). *See* Ex. 1011. In the Intel 8051 processor, the program instructions and data are stored in separate memories. *See* Ex. 1012. Moreover, many processor architectures at the time of the '533 Patent stored data in a separate memory from program instructions. The decision of whether to store program instructions and data in a single or separate memories therefore is an obvious matter of design choice well within the skill level of one of ordinary skill in the art. Ex. 1005, at ¶ 36.

B. Holtey II, Holtey I, and Shafe Disclose Each Limitation of Claims 35 and 36

1. The Combination of Holtey II, Holtey I, and Shafe

The combination of Holtey II and Holtey I suggest using a magnetic media (claim 35) and/or a disk drive (claim 36) rather than flash memory, but nevertheless the Petitioner relies upon the combination of Holtey II, Holtey I, and Shafe for claims 35 and 36 for explicit support. Shafe adds a suitable hard disk that is on a PCMCIA compatible card to the Holtey II and Holtey I combination. *See* Ex. 1004; Ex. 1005, at ¶ 37.

One of ordinary skill in the art would recognize that the invention of Holtey II and I is applicable to non-volatile memory generally (*see e.g.*, Ex. 1002, at 13:25-30), and could easily be applied to hard disks. Moreover, one of ordinary skill in the art would recognize that magnetic disks and flash memory are fungible in many respects. Even Holtey II refers to how one of ordinary skill in the art would recognize that flash memory and magnetic disks are fungible. *See* Ex. 1002, at 2:7-12; 2:23-33; Ex. 1005, at ¶ 38.

It would therefore be an obvious matter of design choice to one of ordinary skill in the art to implement the security methodology of Holtey II and I using a hard disk drive (magnetic media) rather than flash memory. One of ordinary skill in the art would recognize the need for such a modification for applications that

utilize more memory than flash memory provided at the time of the '533 Patent's filing date. Examples of such applications may include those mentioned at 13:39-59 of Holtey II. Ex. 1005, at ¶ 38.

Any one of these applications could easily exceed the flash memory limits of that time frame. One of ordinary skill in the art would recognize that the security methodology of Holtey II and I would accommodate hard disks. Such a modification would be readily accommodated by using the standard PCMCIA interface, or another suitable interface, to the host (Ex. 1002, at 3:56-60) as well as the application microprocessor, access discrimination logic and access control microprocessor of Holtey II. *See* Ex. 1002, at Fig. 1; 5:10-17. One of ordinary skill in the art would therefore recognize the desirability and ease with which a hard drive could be used with the invention of Holtey II and Holtey I. Ex. 1005, at ¶ 39.

One such hard disk is provided by Shafe (U.S. Pat. No. 6,035,429). In fact, Shafe's hard disk is embodied in a PCMCIA compatible card, just like Holtey II and Holtey I, providing one of ordinary skill in the art with motivation for the combination:

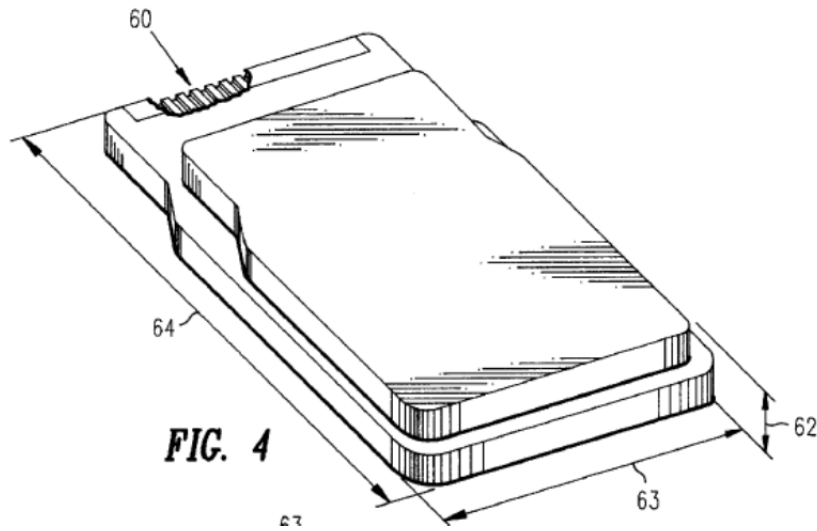


FIG. 4 is representative of a card enclosure for an electronic circuit, adapted to be plugged into a compatible computer slot at connector 64. It may, for example, be a PCMCIA card type I, II or III having a predefined length 64, width 63, and height 62. The card thickness 62 is generally the most critical dimension of a card enclosure. Ex. 1004, at 6:22-27.

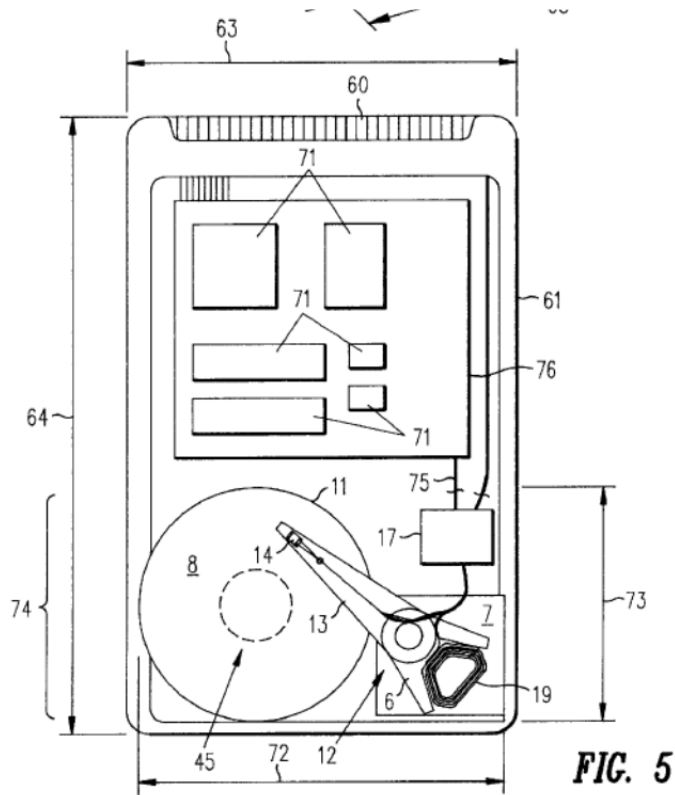


FIG. 5 illustrates generally the preferred embodiment of the electronic circuit apparatus of the present invention. The circuit implements a discrete, component sized disk drive 74 for local storage and resides in a card enclosure such as a PCMCIA type II or type III format, although it will be understood that the circuit apparatus of the present invention may also be enclosed in other card formats, or may comprise the electronic circuit of an electronic device and reside within the device enclosure rather than within a card enclosure (e.g. a camera). Ex. 1004, at 6:28-37.

Shafe recognizes, as does one of ordinary skill in the art, that for applications where more data is required, it is advantageous to use magnetic disk drives rather than solid state memory:

State-of-the art portable message devices that rely on solid state memories are limited in the amount of information they can store, making them impractical for receiving large documents, electronic mail, pictures and video images. This limitation is overcome by replacing the memory with a component disk drive. Ex. 1004, at 8:51-56.

Unfortunately, the cost of solid state memory increases almost linearly with its storage capacity. Moreover, since there are physical limitations to known solid state technologies, an increase in the storage capacity of memory corresponds to an increase in its physical size. These limitations present a foreseeable problem with the growing demand for small, sophisticated, portable, and inexpensive devices with substantial storage requirements.

One area in which the limitations of solid state memory are becoming apparent is card-based electronic circuits. For example, circuits embodying or controlling fax machines, modems, cellular phones, printers, cameras, disk drives, and other devices are presently being housed in credit-card sized formats of predefined dimensions that plug into a compatible socket of a laptop computer, PC, or other electronic device. Three standard formats that have emerged for such credit-

card-type applications are the PCMCIA formats. . . .

In contrast to solid state memories, magnetic disk drives in general are becoming smaller, and their cost per megabyte is decreasing. It is therefore advantageous to provide a magnetic disk drive small enough to replace solid state memory in electronic devices, such as printers, and in card-based electronic circuits, e.g. PCMCIA formats. Furthermore, magnetic disk drives are ideal for many of the applications discussed above because they provide modifiable, high density, nonvolatile storage. Ex. 1004, at 1:32-62.

Shafe also recognizes the prevalence of small disk drives and recognizes the need for security of the data on the disk. Ex. 1004, at 2:8-19; 9:39-41; Ex. 1005, at ¶ 40.

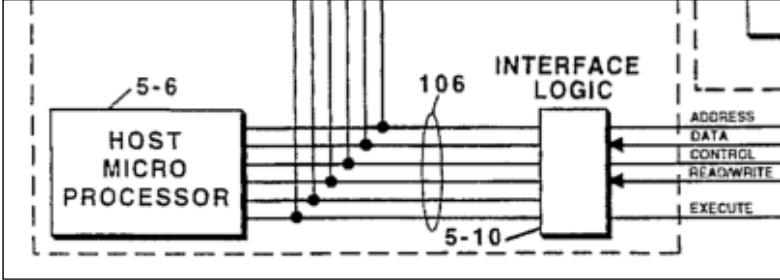
2. Reasons to Combine Holtey II and Holtey I with Shafe

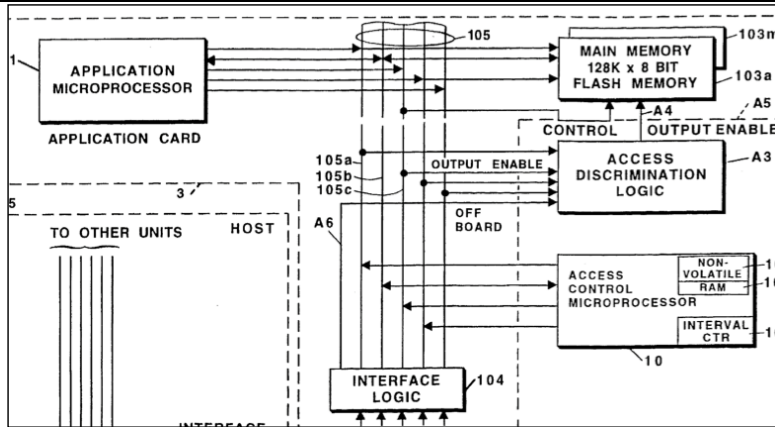
One of ordinary skill in the art would combine Shafe's disk drive with the application card of Holtey II and I for many reasons, some of which are discussed *supra* at VII(A)(1). For example, for applications that require large amounts of data, the cost of solid state memory "increases almost linearly," and the more solid state memory that is required only serves to increase the size of the device. Ex. 1004, at 1:31-39; 9:51-56. Some of these applications are mentioned in Holtey II. Ex. 1002, at 13:39-59. At the time of the invention, hard disks had become prevalent, offering a cheaper, more cost-effective alternative. Ex. 1004, at 2:8-19. Replacing solid state memory with a hard disk was both well-known and well-

motivated by the storage limitations of solid state memory. Ex. 1004, at 8:51-56. Moreover, the well-recognized fungibility of hard disk drives with flash memory at the time of the invention would lead one of ordinary skill in the art to look to hard disk drives depending upon their particular design goals, storage requirements, cost constraints, and application. Ex. 1002, at 2:7-33; Ex. 1004, at 1:32-59. Also, one of ordinary skill in the art would recognize the suitability for Shafe's hard disk on the application card of Holtey II because Shafe's card is PCMCIA compatible and Schafe recognizes the need to secure the data on its storage device. Ex. 1004, at 9:39-41. One of ordinary skill in the art would consider it an obvious matter of design choice to combine Shafe's disk drive with the security application card of Holtey II and I and would be led to form such a combination. Ex. 1005, at ¶ 41.

C. Claim Chart Demonstrating How Holtey II and Holtey I Render Claims 29, 31-34, 38, 39, 42, and 43 Obvious

The following claim chart demonstrates, on a limitation-by-limitation basis, how claims 29, 31-34, 38, 39, 42, and 43 of the '533 Patent are rendered obvious by Holtey II in view of Holtey I. This claim chart is directly supported by Dr. Kaeli's declaration and includes his testimony. Ex. 1005, at pp. 30-51. That is, Dr. Kaeli's declaration provides a claim chart that corresponds directly to the one below, claim-by-claim and element-by-element. *Id.*

	<p>and the interface logic circuits of block 5-10. (Ex. 1002, at 4:55-57)</p>  <p>(Ex. 1002, at Fig. 1)</p> <p>Each of the buses 102, 105, and 106 include a data bus, a control bus and an address bus and provide continuous signal paths through all like buses. (Ex. 1002, at 5:5-7)</p>
<p>a second system bus;</p>	<p>Holtey II teaches the application microprocessor is connected to an internal bus 105 (second system bus) which is a different bus from internal bus 106 (first system bus).</p> <p>As shown, in FIG. 1, the application card 3 of the present invention includes an access control microprocessor (ACP) 10 which couples to bus 105, a plurality of CMOS flash memory chips designated as 103a through 103n which couple to internal bus 105, an application microprocessor A1 which couples to bus 105 and an access discrimination logic unit A3 which couples to bus 105 and to flash memories 103a through 103n as shown. (Ex. 1002, at 5:10-17)</p>



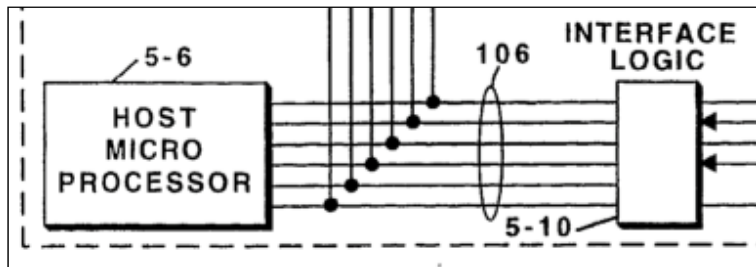
(Ex. 1002, at Fig. 1)

Each of the buses 102, 105, and 106 include a data bus, a control bus and an address bus and provide continuous signal paths through all like buses. For (Ex. 1002, at 5:5-7)

a first processor connected to said first system bus;

Holtey II teaches a host microprocessor (first processor) connected to internal bus 106 (first system bus).

The host processor 5 includes a micro-processor 5-6 which connects to bus 102 via an internal bus 106 and the interface logic circuits of block 5-10. (Ex. 1002, at 4:55-57)



(Ex. 1002, at Fig. 1)

The host microprocessor is a simple device which operates the peripheral devices but has minimum functionality of its own. For example, the microprocessor can be constructed using an Intel 8051 chip. (Ex. 1002, at 8:2-5)

Each of the buses 102, 105, and 106 include a data

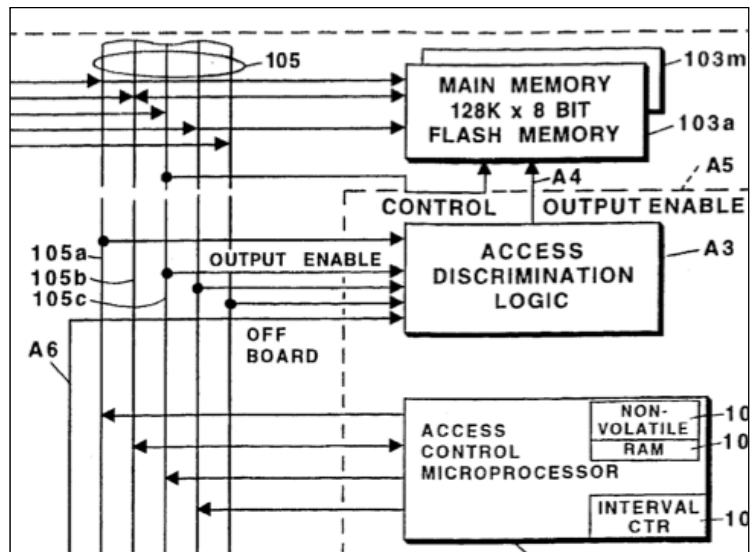
	<p>bus, a control bus and an address bus and provide continuous signal paths through all like buses. (Ex. 1002, at 5:5-7)</p>
<p>a second processor connected to said second system bus;</p>	<p>Holtey II teaches an application microprocessor (second processor) connected to internal bus 105 (second system bus).</p> <p>According to the teachings of the present invention, the secure application card further includes an application microprocessor which also connects to the internal bus. (Ex. 1002, at 3:14-16)</p> <div data-bbox="639 684 1414 888" data-label="Diagram"> <p>The diagram, labeled 'APPLICATION CARD', shows a rectangular box on the left containing the text 'APPLICATION MICROPROCESSOR' and 'A1'. To the right of this box is a vertical bus structure labeled '105'. Multiple horizontal lines with arrows connect the microprocessor to the bus, indicating bidirectional communication. Below the bus structure, there are several vertical lines representing other components connected to the bus.</p> </div> <p>(Ex. 1002, at Fig. 1)</p> <p>As shown, in FIG. 1, the application card 3 of the present invention includes an access control microprocessor (ACP) 10 which couples to bus 105, a plurality of CMOS flash memory chips designated as 103a through 103n which couple to internal bus 105, an application microprocessor A1 which couples to bus 105 and an access discrimination logic unit A3 which couples to bus 105 and to flash memories 103a through 103n as shown. (Ex. 1002, at 5:10-17)</p> <p>The application microprocessor A1 is contained in the application card and is programmed to perform all operation functions required for running a given application. In the preferred embodiment, the microprocessor may be constructed using an Intel 80286 microprocessor chip. (Ex. 1002, at 7:55-59)</p> <p>Each of the buses 102, 105, and 106 include a data bus, a control bus and an address bus and provide continuous signal paths through all like buses.</p>

<p>a data storage device connected to said first and second system buses for selectively operating in a plurality of operating modes so as to access said data storage device; and</p>	<p>(Ex. 1002, at 5:5-7)</p> <p>Holtey II teaches a secure application card containing a plurality of flash memory chips 103a through 103n (data storage device).</p> <p>The secure application card of the preferred embodiment includes an access control microprocessor (ACP) on a single semiconductor chip and one or more non-volatile addressable memory chips which serve as main memory. (Ex. 1002, at 2:62-66)</p> <p>As in the case of the related patent application, the present invention melds the “Smart Card” and “memory card” technologies which is key to allowing the protection of large amounts of data made possible by flash memory technology in the “security harsh” environments created by electronic miniaturization. Also, the present invention also retains the features of the secure card of the related patent application relative to being capable of operating in secure and non-secure modes, eliminating the need for encrypting and decrypting data, and protecting memory contents if the card or its host processor is lost, stolen, powered off or left unattended. In the event of theft, the memory contents is protected from access even if the memory card is opened and probed electronically or the memory chips are removed and placed in another device. (Ex. 1002, at 4:12-26)</p> <p>The CMOS flash memories 103a through 103n may take the form of flash memory chips manufactured by Intel Corporation. For example, they may take the form of the Intel flash memory chips designated as Intel 28F001BX 1M which includes eight 128Kilobyte×8-bit CMOS flash memories. Thus, a 4 Megabyte flash memory card could include 32 such flash memories (i.e. n=32). (Ex. 1002, at 5:19-</p>
--	---

25)

Holtey II teaches the flash memory chips (data storage device) are connected to the first and second system buses. Holtey II teaches the flash memory chips are connected to the internal bus 105 (second system bus).

As shown, in FIG. 1, the application card 3 of the present invention includes an access control microprocessor (ACP) 10 which couples to bus 105, a plurality of CMOS flash memory chips designated as 103a through 103n which couple to internal bus 105, an application microprocessor A1 which couples to bus 105 and an access discrimination logic unit A3 which couples to bus 105 and to flash memories 103a through 103n as shown. (Ex. 1002, at 5:10-17)



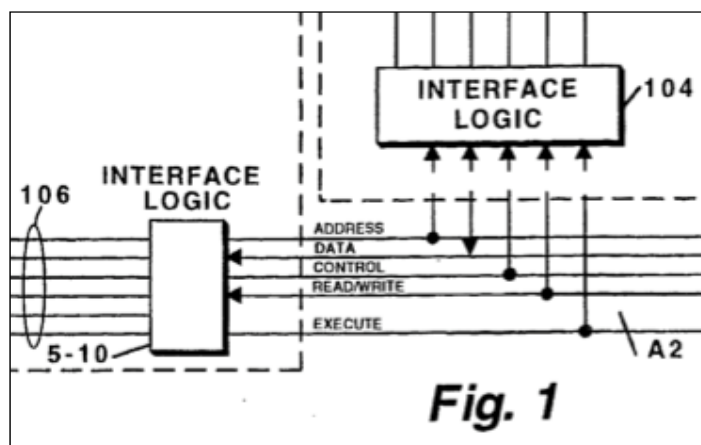
(Ex. 1002, at Fig. 1)

Holtey II teaches the flash memory chips (data storage device) are connected to internal bus 106 (first system bus).

In the preferred embodiment, each host microprocessor couples to the application card

through a standard interface such as one of the interfaces which conforms to the Personal Computer Memory Card International Association (PCMCIA) standards. More specifically, the particular PCMCIA interface selected is one which has the so-called "Execute-in-Place" (XIP) functionality which can be used in conjunction with card processors which provide bus mastering and intercard communications capabilities. (Ex. 1002, at 3:56-64)

The connection between the application card 3 and host microprocessor 5 is established through a standard bus interface. In the preferred embodiment, the bus 102 conforms to the Personal Computer Memory Card International Association (PCMCIA) standard which includes an "Execute-in-Place" (XIP) capability. The interface 102 provides a path for transferring address, control and data information between host processor 5 and the application card system 3 via a standard interface chip 104 and an internal bus 105. Each of the buses 102, 105, and 106 include a data bus, a control bus and an address bus and provide continuous signal paths through all like buses. (Ex. 1002, at 4:63-67 to 5:1-7)



(Ex. 1002, at Fig. 1)

The host processor 5 includes a microprocessor 5-6 which connects to bus 102 via an internal bus 106 and the interface logic circuits of block 5-10. (Ex. 1002, at 4:55-57)

Holtey II teaches a plurality of operating modes to access the data storage device using an access control microprocessor for controlling the “access by type memory” on the application memory card.

According to the present invention, as seen from FIG. 1, the control portion of internal bus 105 as well as external bus 102, contains a plurality of control signal lines which apply Execute, Read and Write control signals generated by any one of the microprocessors 5-6, 10 or A1. More specifically, each of the microprocessors include means for initiating Execute, Read and Write cycles of operation. through the different states of various control lines. (Ex. 1002, at 5:31-39)

The access control microprocessor includes an addressable non-volatile memory for storing configuration information including a number of key values and program instruction information for controlling the transfer of address, data and control information on the internal bus. In the preferred embodiment, a portion of the configuration information serves as the content for the access by type memory which is loaded at power-up. This data is protected by the ACP and can be modified via the host processor only with proper permissions (ala changing passwords). (Ex. 1002, at 3:3-13)

Associated with the application processor is an access discrimination logic unit included on the same chip as the access control microprocessor which controls access to the non-volatile memory

chips. The access discrimination logic unit includes an access by type random access memory (RAM) having a plurality of word locations, each location associated with a different block of the addressable memory chips and having a number of access control bits coded for defining different types of access as a function of the specific application being run.

(Ex. 1002, at 3:23-32)

Holtey I teaches that the storage device operates in a plurality of operating modes:

As shown in FIG. 3, the flash memory circuits receive a plurality of input address signals A0-A16, data signals D00-D07 and control signals consisting of chip enable, write enable, output enable, power down and erase/program power supply signals CE, WE, OE, PWD, and VPP respectively. The functions performed by these signals are described in Appendix I. (Ex. 1003, at 7:39-45)

OE OUTPUT ENABLE: Gates the device's outputs through the data buffers during a read cycle.

OE is active low.

WE WRITE ENABLE: Controls writes to the command register and array blocks. WE is active low. Addresses and data are latched on the rising edge of the WE pulse.

Vpp ERASE/PROGRAM POWER SUPPLY for erasing blocks of the array or programming bytes of each block. Note: With $V_{pp} < V_{PPI\ Max}$, memory contents cannot be altered. When Vpp is at a high level, programming can take place; if Vpp is at a low level, the memory array 54 functions as a read only memory.

(Ex. 1003, at 15:25-37)

	<p>Holtey II teaches that the type of access required by the processors such as data read access or execute access is a type of memory access and that the access discrimination logic and access control microprocessor selectively operate in a plurality of operating modes to control access to the data storage device.</p> <p>In the preferred embodiment, the states of the “Execute” and “Off Board” signal lines define several different types of memory access. These are: Data Read Access from the host microprocessor, Data Read access from the application card’s microprocessor, Execute Access from the host microprocessor, and Execute Access from the application card’s microprocessor. (Ex. 1002, at 3:42-49)</p> <p>In accordance with the present invention, these signals define four different types of memory access, These are: Data Read Access from Host Microprocessor 5-6, Data Read Access from the Application Microprocessor A1, Execute Access from the Host Microprocessor 5-6, and Execute Access from the Application Microprocessor A1. (Ex. 1002, at 5:55-60)</p> <p><i>See also</i> the analysis for claim 32 below.</p>
<p>a switch operable to selectively enable and disable at least one of said operating modes, said switch controllable by means distinct and separate from at least one of said</p>	<p>Holtey II teaches access discrimination logic unit and access control microprocessor (switch) operable to selectively enable and disable at least one of said operating modes. Holtey II teaches memory blocks may have read, write, or execute permissions applied.</p> <p>Associated with the application processor is an access discrimination logic unit included on the same chip as the access control microprocessor which controls access to the non-volatile memory</p>

processors whereby said one processor is inhibited from controlling said operation of said switch.

chips. The access discrimination logic unit includes an access by type random access memory (RAM) having a plurality of word locations, each location associated with a different block of the addressable memory chips and having a number of access control bits coded for defining different types of access as a function of the specific application being run.
(Ex. 1002, at 3:16-32)

The access discrimination logic unit A3 as discussed in greater detail in connection with FIG. 3 includes an Access by Type Random Access Memory (RAM) array containing a plurality of word locations, one location for each block of the memory chips 103a through 103n and input selector circuits connected to the "Execute" and "Off Board" control signal lines indicating the nature and source of the memory access. In accordance with the present invention, these signals define four different types of memory access, These are: Data Read Access from Host Microprocessor 5-6, Data Read Access from the Application Microprocessor A1, Execute Access from the Host Microprocessor 5-6, and Execute Access from the Application Microprocessor A1. The Access Discrimination Logic Unit A3 performs the task of applying the output enable control to the memory chips 103a through 103n. That is, it determines which type of enable control signal is to be applied to the memory chips 103a through 103n as a function of the state of the selected prestored access control bits of the location associated with the block being addressed.
(Ex. 1002, at 5:48-67)

For example, in the application card of the preferred embodiment, as discussed above, there are four different types of accesses. These accesses are designated by bit positions 0 through 3 of each

word. As indicated, bit positions 0 and 1 are used to control application microprocessor access to data and programs respectively. Bit positions 2 and 3 of each word are used to control host microprocessor access to data and programs respectively. When, any bit position is preset to a binary ONE state, this indicates that access is permitted. When a bit position is preset to a binary ZERO state, this indicates that access is not allowed. (Ex. 1002, at 8:20-31)

In the preferred embodiment, the discrimination logic A3 and access control microprocessor are contained microprocessor are contained on a single chip A5. (Ex. 1002, at 8:47-50)

Holtey II teaches that the switch is controllable by means distinct and separate from at least one of said processors whereby said one processor is inhibited from controlling said operation of said switch.

The access control microprocessor includes an addressable non-volatile memory for storing configuration information including a number of key values and program instruction information for controlling the transfer of address, data and control information on the internal bus. In the preferred embodiment, a portion of the configuration information serves as the content for the access by type memory which is loaded at power-up. This data is protected by the ACP and can be modified via the host processor only with proper permissions (ala changing passwords). (Ex. 1002, at 3:3-13)

The access control microprocessor writes the contents of the access by type RAM in a conventional manner during power-up. As indicated, the host or application processor is allowed to modify the contents of this RAM only

	<p>under the control of the ACP thereby maintaining security. (Ex. 1002, at 3:50-55)</p>
<p>31. The digital computer system according to claim 29 wherein said switch comprises a digital controller, an operation of which is independent of said second processor for selectively enabling and disabling said at least one of said operating modes.</p>	<p>Holtey II teaches access discrimination logic unit and access control microprocessor (digital controller) which may be contained on a single chip (switch comprises a digital controller).</p> <p>In the preferred embodiment, the access discrimination logic A3 and access control microprocessor are contained microprocessor are contained on a single chip A5. (Ex. 1002, at 8:47-50)</p> <p>Holtey II teaches the access control microprocessor (digital controller) operates independently of the application processor (second processor).</p> <p>Associated with the application processor is an access discrimination logic unit included on the same chip as the access control microprocessor which controls access to the non-volatile memory chips. The access discrimination logic unit includes an access by type random access memory (RAM) having a plurality of word locations, each location associated with a different block of the addressable memory chips and having a number of access control bits coded for defining different types of access as a function of the specific application being run. (Ex. 1002, at 3:16-32)</p> <p>The access control microprocessor includes an addressable non-volatile memory for storing configuration information including a number of key values and program instruction information for controlling the transfer of address, data and control information on the internal bus. In the preferred embodiment, a portion of the configuration</p>

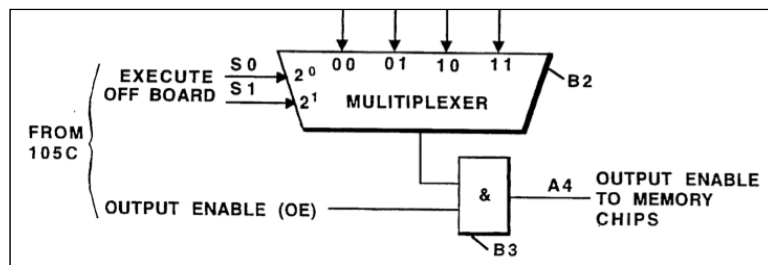
	<p>information serves as the content for the access by type memory which is loaded at power-up. This data is protected by the ACP and can be modified via the host processor only with proper permissions (ala changing passwords). (Ex. 1002, at 3:3-13)</p> <p>The access control microprocessor writes the contents of the access by type RAM in a conventional manner during power-up. As indicated, the host or application processor is allowed to modify the contents of this RAM only under the control of the ACP thereby maintaining security. (Ex. 1002, at 3:50-55)</p>
<p>32. The digital computer system according to claim 29 wherein said data storage device is operable in (i) a read-only mode of operation for retrieving previously stored data and (ii) a write-only mode of operation for storing data.</p>	<p>The combination of Holtey II & I teaches the flash memory chips (data storage device) may operate in a read-only mode.</p> <p>The combination of Holtey II & I teaches a secure system that has memory “access type” controls. The combination teaches permission controls for read, write and execute memory access where “read-only mode” is the “Data Read access” of the preferred embodiment where the write enable control signal does not permit writing to flash memory and/or the Vpp signal is in a state that forces the memory array to function as read only memory.</p> <p>As shown in FIG. 3, the flash memory circuits receive a plurality of input address signals A0-A16, data signals D00-D07 and control signals consisting of chip enable, write enable, output enable, power down and erase/program power supply signals CE, WE, OE, PWD, and VPP respectively. The functions performed by these signals are described in Appendix I. (Ex. 1003, at 7:39-45)</p> <p>OE OUTPUT ENABLE: Gates the device’s outputs through the data buffers during a read cycle. OE is active low.</p>

	<p>WE WRITE ENABLE: Controls writes to the command register and array blocks. WE is active low. Addresses and data are latched on the rising edge of the WE pulse.</p> <p>Vpp ERASE/PROGRAM POWER SUPPLY for erasing blocks of the array or programming bytes of each block. Note: With $V_{pp} < V_{PPI\ Max}$, memory contents cannot be altered. When Vpp is at a high level, programming can take place; if Vpp is at a low level, the memory array 54 functions as a read only memory.</p> <p>(Ex. 1003, at 15:25-37)</p> <p>These are: Data Read Access from the host microprocessor, Data Read access from the application card's microprocessor, Execute Access from the host microprocessor, and Execute Access from the application card's microprocessor. The access control microprocessor writes the contents of the access by type RAM in a conventional manner during power-up. As indicated, the host or application processor is allowed to modify the contents of this RAM only under the control of the ACP thereby maintaining security.</p> <p>(Ex. 1002, at 3:45-54)</p> <p>The combination teaches the flash memory chips (data storage device) may operate in a write-only mode. Holtey II teaches an embodiment for flash memory being the Intel 28F001BX which has both CE (chip enable) and OE (output enable) control signals.</p> <p>The CMOS flash memories 103a through 103n may take the form of flash memory chips manufactured by Intel Corporation. For example, they may take the form of the Intel flash memory chips designated as Intel 28F001BX 1M which includes eight</p>
--	---

128Kilobyte×8-bit CMOS flash memories. Thus, a 4 Megabyte flash memory card could include 32 such flash memories (i.e. n=32). (Ex. 1002, at 5:19-25)

Holtey II teaches the access control memory bits inhibit the output buffer of the flash memory by gating the OE control line.

As seen from FIG. 3, section 103S includes a security access control unit 30 and a volatile access control memory 43 interconnected as shown. The output of the access control memory 43 is applied as an enabling input to output buffer 52 during each memory read cycle when the contents of a byte location of any block of memory array 53 is being read out. That is, a read cycle may occur, however, the data read out is inhibited from passing through output buffer 52 in the absence of the appropriate block's access control memory gating signal. (Ex. 1002, at 7:25-34)



(Ex. 1002, at Fig. 3)

Holtey I teaches that the access control memory bits do not inhibit the CE control signal and therefore both read or execute access may be disabled but not the write access which therefore provides a write-only mode.

As shown in FIG. 3, the flash memory circuits receive a plurality of input address signals A0-A16, data signals D00-D07 and control signals consisting of chip enable, write enable, output enable, power down and erase/program power supply signals CE,

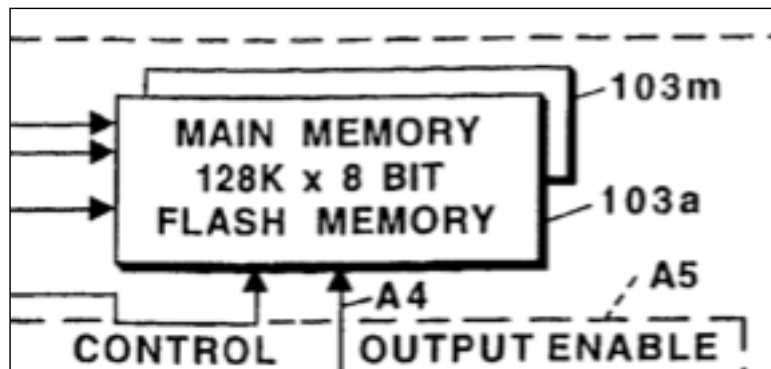
	<p>WE, OE, PWD, and VPP respectively. The functions performed by these signals are described in Appendix I. (‘Ex. 1003, at 7:39-45)</p> <p>OE OUTPUT ENABLE: Gates the device’s outputs through the data buffers during a read cycle. OE is active low.</p> <p>WE WRITE ENABLE: Controls writes to the command register and array blocks. WE is active low. Addresses and data are latched on the rising edge of the WE pulse.</p> <p>Vpp ERASE/PROGRAM POWER SUPPLY for erasing blocks of the array or programming bytes of each block. Note: With $V_{pp} < V_{PPI\ Max}$, memory content cannot be altered. When V_{pp} is at a high level, programming can take place; if V_{pp} is at a low level, the memory array 54 functions as a read only memory.</p> <p>(Ex. 1003, at 1525-37)</p>
<p>33. The digital computer system according to claim 32 wherein said at least one of said operating modes is said read-only mode of operation.</p>	<p>See claim 32 read-only mode.</p>
<p>34. The digital computer system according to claim 32 wherein said at least one of said operating modes is said write-only mode of operation.</p>	<p>See claim 32 write-only mode.</p>
<p>38. The digital computer according to claim 32 wherein</p>	<p>See <i>supra</i> at VII(A)(3); Ex. 1005, at ¶ 34.</p> <p>Holtey II teaches the use of a flash memory that is a non-</p>

said data storage device comprises a non-volatile electronic memory device.

volatile electronic memory.

The CMOS flash memories 103a through 103n may take the form of flash memory chips manufactured by Intel Corporation. For example, they may take the form of the Intel flash memory chips designated as Intel 28F001BX 1M which includes eight 128Kilobyte×8-bit CMOS flash memories. Thus, a 4 Megabyte flash memory card could include 32 such flash memories (i.e. n=32). (Ex. 1002, at 5:19-25)

FLASH MEMORIES 103a through 103n
FIG. 3 shows in block diagram form, flash memory 103a which is identical in construction to the remaining flash memories 103b through 103n. As shown, memory 103a includes two sections, a memory section 103M organized according to the present invention and a security logic section 103S containing the security access control circuits of the present invention. (Ex. 1002, at 6:32-39)



(Ex. 1002, at Fig. 1)

The recent emergence of the flash memory and removable “memory cards” have allowed major reductions in size and power requirements of the portable of the portable computer. The flash memory combines the flexibility of random access memories (RAMs) with the permanence of disks.

	(Ex. 1002, at 2:23-27)
39. The digital computer according to claim 38 wherein said electronic non-volatile electronic memory device comprises an EEPROM.	See claim 38. See <i>supra</i> at VII(A)(3); Ex. 1005, at ¶ 34.
42. The digital computer according to claim 32 wherein each of said first and second processors include a central processing unit, a first memory storing program instructions and a second memory, separate and distinct from said first memory, storing data.	<p>See <i>supra</i> at VII(A)(4); Ex. 1005, at ¶¶ 35-36.</p> <p>Holtey II teaches a first processor (host processor) that includes a central processing unit (microprocessor) and a first memory storing program instructions (ROM which contain start up and self test code).</p> <p>The host microprocessor is a simple device which operates the peripheral devices but has minimum functionality of its own. For example, the microprocessor can be constructed using an Intel 8051 chip. It has its own read only memory (ROM) which contain start up and self test code only. Thus, the host device can be viewed as a “shell” with all of the significant functionality contained within the application card 3. (Ex. 1002, at 8:2-9)</p> <p>Holtey II teaches a second processor (application processor) that includes a central processing unit (microprocessor) and a first memory storing program instructions.</p> <p>The application microprocessor A1 is contained in the application card and is programmed to perform all operation functions required for running a given application. In the preferred embodiment, the microprocessor may be constructed using an Intel 80286 microprocessor chip. The application microprocessor A1 also has a random access memory which is uses to perform certain</p>

	<p>intermediate calculations in running specific applications. (Ex. 1002, at 7:55-62)</p> <p>Holtey II teaches a secure system that controls memory access type permissions that includes “Execute” permissions and therefore teaches the memory for storing program instructions is separate from memory storing data.</p> <p>These accesses are designated by bit positions 0 through 3 of each word. As indicated, bit positions 0 and 1 are used to control application microprocessor access to data and programs respectively. Bit positions 2 and 3 of each word are used to control host microprocessor access to data and programs respectively. When, any bit position is preset to a binary ONE state, this indicates that access is permitted. When a bit position is preset to a binary ZERO state, this indicates that access is not allowed. (Ex. 1002, at 8:22-31)</p> <p>The piece of data which would be not changed, is the program code for the application microprocessor itself. An important part of that code is the algorithms and encryptions that allow messages to be sent over the credit network via the communications link of FIG. 4 which includes the information describing how the hand held device is to access that network. That is, it includes the information which properly identifies the requester used for establishing that the transaction is a legitimate transaction to make a charge against a given account. This is highly secure information that is kept in the application card. (Ex. 1002, at 10:65-11:8)</p> <p>From the above, it is seen how the application card constructed according to the principles of the</p>
--	--

present invention provides a secure environment for both data and programs. It allows sharing of such information stored within a non-volatile memory between a plurality of microprocessors. Further, it enables application software to be packaged with its own application processor making such systems more economical to produce and use. (Ex. 1002, at 13:25-32)

Holtey II teaches storing program instructions stored separately and in distinct memory from data.

For example, the table given below illustrates further examples of memory 103a for sample applications.

APPLICATION PROCESSOR		HOST PROCESSOR	
DATA-"A"	PROGRAM-"B"	DATA-"C"	PROGRAM-"D"
A compilation of Financial Data	Analysis Program to perform specific analysis at a fee per transaction	General Workspace (valuable slots are limited)	Interface Program with Application
Compressed maps (or other images)	Decompression software at a fee per transaction	Specific Map being viewed	Interface Program with Application
—	Any Application (e.g. a program which is not authorized to be copied such as "MS WORD")	Users Workspace	Interface Program with Application

(Ex. 1002, at 37-59)

43. The digital computer according to claim 33 wherein at least one of said first memories is operable in a read-only mode of operation in which

It is assumed that this claim depends from claim 42.

See claim 42 above; See *supra* at VII(A)(4); see Ex. 1005, at ¶¶ 35-36.

said program instructions are protected from alteration and erasure by a corresponding one of said central processing units.	
--	--

D. Claim Chart Demonstrating How Holtey II, Holtey I, and Shafe Render Claims 35 and 36 Obvious

The following claim chart demonstrates, on a limitation-by-limitation basis, how claims 35 and 36 of the ‘533 Patent are rendered obvious by Holtey II, Holtey I and Shafe. This claim chart is directly supported by Dr. Kaeli’s declaration and includes his testimony. Ex. 1005, at pp. 51-54. That is, Dr. Kaeli’s declaration provides a claim chart that corresponds directly to the one below, claim-by-claim and element-by-element. *Id.*

U.S. Patent No. 6,272,533	Holtey II (U.S. Pat. No. 5,491,827), Holtey I (U.S. Pat. No. 5,442,704), and Shafe (U.S. Pat. No. 6,035,429)
35. The digital computer according to claim 32 wherein said data storage device comprises a magnetic media.	<p>See Ex. 1005, at ¶¶ 37-40.</p> <p>Holtey II teaches the use of a memory consisting of a conventional disk that is constructed from a magnetic media.</p> <p>The recent emergence of the flash memory and removable “memory cards” have allowed major reductions in size and power requirements of the portable of the portable computer. The flash memory combines the flexibility of random access memories (RAMs) with the permanence of disks. Today, the combining of these technologies allows up to 20</p>

million bytes of data to be stored without power, in a credit card size removable package. This data can be made to appear to a host system either as if it were stored on a conventional disk drive or if it were stored in an extension of the host system's memory. (Ex. 1002, at 2:23-33)

Holtey II's invention relates to non-volatile memory generally, of which magnetic disk is one:

From the above, it is seen how the application card constructed according to the principles of the present invention provides a secure environment for both data and programs. It allows sharing of such information stored within a non-volatile memory between a plurality of microprocessors. (Ex. 1002, at 13:25-30).

Shafe teaches a PCMCIA card with an on-board magnetic disk (disk drive) as an alternative to costlier solid state memory.

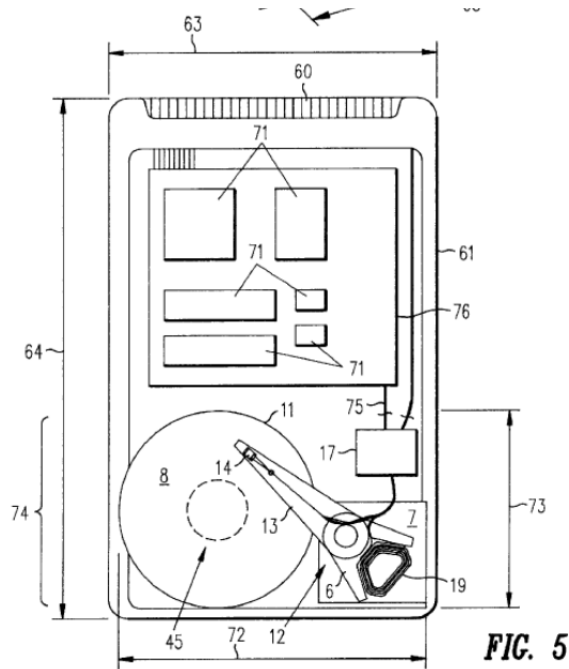


FIG. 5 illustrates generally the preferred embodiment

	<p>of the electronic circuit apparatus of the present invention. The circuit implements a discrete, component sized disk drive 74 for local storage and resides in a card enclosure such as a PCMCIA type II or type III format, although it will be understood that the circuit apparatus of the present invention may also be enclosed in other card formats, or may comprise the electronic circuit of an electronic device and reside within the device enclosure rather than within a card enclosure (e.g. a camera). (Ex. 1004, at 6:28-37)</p> <p>The disk 11 is preferably magnetic and includes one recording surface 42 with a substantially planar region 45 at its center. (Ex. 1004, at 4:51-53)</p> <p>The present invention relates generally to electronic devices implementing local storage, and in particular to an electronic circuit that incorporates a component level disk drive in lieu of costlier solid state memory. (Ex. 1004, at 1:8-11)</p> <p>See also, Ex. 1004, at Abstract; Fig. 4; 1:32-62; 2:8-19; 6:22-27; 8:51-56; 9:39-41.</p>
<p>36. The digital computer according to claim 32 wherein said data storage device comprises a disk drive.</p>	<p>See claim 35. See Ex. 1005, at ¶¶ 37-40.</p>

VIII. CONCLUSION

For the reasons set forth above, Petitioner has established a reasonable likelihood of prevailing with respect to at least one claim of the '533 Patent.

Therefore, Petitioner respectfully requests that the Patent Trial and Appeal Board institute an *inter partes* review and then proceed to cancel claims 29, 31-36, 38, 39, 42, and 43.

Respectfully submitted,

OBLON SPIVAK

Dated: August 29, 2014

/Michael L. Kiklis/

Michael L. Kiklis

Reg. No. 38,939

Customer Number

22850

Tel. (703) 413-3000

Fax. (703) 413-2220

(OSMMN 02/10)

Petitioner's Exhibit List (August 29, 2014)

PETITIONER'S EXHIBIT LIST
August 29, 2014

Exhibit	Description
Ex. 1001	U.S. Patent No. 6,272,533
Ex. 1002	U.S. Patent No. 5,491,827 to Holtey ("Holtey II")
Ex. 1003	U.S. Patent No. 5,442,704 to Holtey ("Holtey I")
Ex. 1004	U.S. Patent No. 6,035,429 to Shafe ("Shafe")
Ex. 1005	Declaration of David R. Kaeli, Ph.D.
Ex. 1006	U.S. Patent No. 6,052,781 to Weber
Ex. 1007	U.S. Patent No. 5,268,960 to Hung, et al.
Ex. 1008	U.S. Patent No. 5,263,139 to Testa, et al.
Ex. 1009	U.S. Patent No. 4,912,633 to Schweizer, et al.
Ex. 1010	Selected pages from the prosecution of U.S. Patent No. 6,272,533
Ex. 1011	Intel 80286 Hardware Reference Manual, 1987
Ex. 1012	Intel MCS 51 Microcontroller Family User's Manual, Feb. 1994

CERTIFICATE OF SERVICE

The undersigned certifies service pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(b) on the Patent Owner by UPS Next Day Air of a copy of this Petition for *Inter Partes* Review and supporting materials at the correspondence address of record for the '533 Patent:

ROBERT J KOCH
FULBRIGHT & JAWORSKI
801 PENNSYLVANIA AVENUE NW
WASHINGTON DC 20004

Dated: Aug. 29, 2014

By: /Michael L. Kiklis/
Michael L. Kiklis
Reg. No. 38,939