Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 01/31/2018. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	
Filing Date	
First Named Inventor	Joshua Johnson
Title	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR
Art Unit	
Examiner Name	
Attorney Docket Number	980.0023

SIGNATURE of Applicant or Patent Practitioner

Signature	/David H. Schaumann/	Date (Optional)	11/06/2017
Name	David H. Schaumann	Registration Number	50858
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

DocuSign Envelope ID: 9C8B46F9-DF9D-48BD-8796-CD3B7540D8AF

Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 76444

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

Gaea LLC

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature	Curtis H. Bruner	Date (Optional)	2/4/2017
Name	Curtis H. Bruner		
Title	Member, Gaea LLC		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal	
Application Number:	
Filing Date:	
Title of Invention:	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR
First Named Inventor/Applicant Name:	Joshua Johnson
Filer:	David H. Schaumann/Krista Bowen
Attorney Docket Number:	980.0023
Filed as Small Entity	

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
UTILITY FILING FEE (ELECTRONIC FILING)	4011	1	70	70
UTILITY SEARCH FEE	2111	1	300	300
UTILITY EXAMINATION FEE	2311	1	360	360
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	2202	16	40	640
INDEPENDENT CLAIMS IN EXCESS OF 3	2201	3	210	630
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
LATE FILING FEE FOR OATH OR DECLARATION	2051	1	70	70
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**2070**

Electronic Acknowledgement Receipt	
EFS ID:	30868364
Application Number:	15804772
International Application Number:	
Confirmation Number:	2463
Title of Invention:	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR
First Named Inventor/Applicant Name:	Joshua Johnson
Customer Number:	76444
Filer:	David H. Schaumann/Krista Bowen
Filer Authorized By:	David H. Schaumann
Attorney Docket Number:	980.0023
Receipt Date:	06-NOV-2017
Filing Date:	
Time Stamp:	17:27:57
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$2070
RAM confirmation Number	110717INTEFSW17283701
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Application.pdf	244172 946f0d9c35389dc8fe5c35525526c11854a528d1	yes	53
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Abstract		53	53	
	Claims		48	52	
	Specification		1	47	
Warnings:					
Information:					
2	Drawings-only black and white line drawings	Drawings.pdf	161411 c96f75a69aef0230a4a3be536cc4d3382d0f58f7	no	32
Warnings:					
Information:					
3	Application Data Sheet	ADS.pdf	1823559 93238fefa717bc4f917385f78ee3de1f539c18b0	no	11
Warnings:					
Information:					
4	Power of Attorney	POA.pdf	258282 bbb5322511d7b448435fb1c6d5fd1a90bffa7de5	no	2
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	40279 3c3e1c8066a3619174070339 4f2ca14700314368	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	2527703

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

ABSTRACT

In an embodiment, a storage device is provided. A device controller with a memory is coupled with the storage device. The memory stores an application with instructions that direct the controller to receive a storage device policy. The instructions further direct the controller to store content from a storage request in accordance with the storage device policy, and record storage information, including at least a content identifier, to the memory. Subsequent to storing the content, the instructions further direct the controller to retrieve the content according to the storage information received in a storage request. According to an implementation, the instructions further provide instruction to refuse a delete request in accordance to the storage information. According to an implementation, the instructions provide direction to store the storage information at a remote location.

CLAIMS

What is claimed is:

1. An apparatus comprising:

a storage device;

a device controller operatively coupled with the storage device, comprising a memory;

an application stored on the memory and comprising instructions that, when executed, direct the device controller to at least:

receive a storage device policy;

receive a storage request, comprising content;

store the content on the storage device according to the storage device policy;

record storage information for the content on the memory, comprising at least a content identifier for the content;

subsequent to storing the content, receive a content request for the content, comprising at least the content identifier for the content;

in response to the content request, retrieve storage information for the content;

recover the content, at least in part according to the storage information; and

respond to the content request at least by returning the content.

2. The apparatus of claim 1, wherein the storage device policy comprises a data storage areal density.

3. The apparatus of claim 1, wherein the storage device policy comprises a head/media interface strength.

4. The apparatus of claim 1, wherein the storage device policy comprises instructions related to media defect treatment on the storage device.

5. The apparatus of claim 1, wherein the storage device comprises a magnetic disk.

6. The apparatus of claim 1, wherein the storage device comprises a solid-state memory device.

7. The apparatus of claim 1, wherein the content identifier is assigned by the device controller and is returned in a response to the storage request.

8. The apparatus of claim 1, wherein the instructions, when executed, direct the device controller to further:

reply to the storage request with a request for a storage device policy update;

receive a storage device policy update; and

update the storage device policy in accordance with the storage device policy update.

9. An apparatus comprising:

a storage device;

a device controller operatively coupled with the storage device, comprising a memory;

an application stored on the memory and comprising instructions that, when executed, direct the device controller to at least:

receive a storage device policy;

store content on the storage device;

record storage information for the content on the memory, comprising at least a content identifier for the content;

subsequent to storing the content, receive a content request for the content, comprising at least the content identifier for the content;

in response to the content request, retrieve storage information for the content;

recover the content, according to the storage information and according to the storage device policy; and

respond to the content request at least by returning the content.

10. The apparatus of claim 9, wherein the storage device policy comprises a command timeout.

11. The apparatus of claim 9, wherein the storage device policy comprises a read retry count.

12. The apparatus of claim 9, wherein the storage device policy comprises instructions related to background task controls.

13. The apparatus of claim 9, wherein the storage device comprises a magnetic disk.

14. The apparatus of claim 9, wherein the storage device comprises a solid-state memory device.

15. The apparatus of claim 9, wherein the content identifier is assigned by the device controller and is returned in a response to the storage request.

16. An apparatus comprising:

a storage device;

a device controller operatively coupled with the storage device, comprising a memory;

an application stored on the memory and comprising instructions that, when executed, direct the device controller to at least:

receive a storage policy, comprising a write-protection policy;

receive a storage request, comprising content;

store the content on the storage device according to the storage policy;

record storage information for the content on the memory, comprising at least a content identifier for the content;

subsequent to storing the content, receive a delete request for the content, comprising at least the content identifier for the content;

in response to the delete request, retrieve storage information for the content; and

respond to the delete request, indicating that the content was not deleted in accordance with the write-protection policy.

17. The apparatus of claim 16, wherein the storage policy and the delete request are received from the same source.

18. The apparatus of claim 16, wherein the storage policy and the delete request are received from different sources.

19. The apparatus of claim 16, wherein the delete request is a modification request.

20. The apparatus of claim 16, wherein the delete request is an overwrite request.

21. An apparatus comprising:

a storage device;

a device controller operatively coupled with the storage device, comprising a memory;

an application stored on the memory and comprising instructions that, when executed direct the device controller to at least:

receive a storage policy;

receive a storage request, comprising content;

store the content on the storage device according to the storage policy;

send storage information for the content storage to a remote location;

storing lookup information comprising at least a content identifier for the content and an information pointer for the storage information;

subsequent to storing the content, receive a lookup request for the content, comprising at least the content identifier for the content;

in response to the lookup request, retrieve storage information for the content from the remote location, based at least in part on the information pointer; and

retrieve the content.

22. The apparatus of claim 21, wherein the information pointer is a network address.

23. The apparatus of claim 21, wherein the step of retrieving storage information further comprises sending an authentication to the remote location.

24. The apparatus of claim 21, wherein the information pointer is stored in a header attached to the content.

25. The apparatus of claim 21, wherein the information pointer is stored in a memory separate from to the content.

26. An apparatus comprising:

a storage device;

a device controller operatively coupled with the storage device, comprising a memory, the device controller configured to receive content to be stored on the storage device;

a programmable processor, communicatively coupled with the device controller such that the content received by the device controller to be stored on the storage device must pass though the programmable processor; and

an application stored on the memory and comprising instructions that, when executed, direct the device controller to at least store the content on the storage device after the content has been processed by the programmable processor.

27. The apparatus of claim 26, wherein the programmable processor is unprogrammed when the apparatus is manufactured.

28. The apparatus of claim 26, wherein the programmable processor is configured to encrypt content.

29. The apparatus of claim 26, wherein the programmable processor is configured to identify a pattern in the content.

30. The apparatus of claim 29, wherein the pattern is a symbol or string.

31. The apparatus of claim 29, wherein the pattern is an image.

32. An apparatus comprising:

a storage device;

a device controller operatively coupled with the storage device, comprising a memory;

an application stored on the memory and comprising instructions that, when executed, direct the device controller to at least:

receive a storage device policy;

store a first content on the storage device at a first density in accordance with the storage device policy;

store a second content on the storage device at a second density and in accordance with the storage device policy; and

wherein the first density and the second density differ.

33. The apparatus of claim 32, wherein the first density and the second density are dictated by a slope at which the first content and the second content are stored on the storage device.

34. The apparatus of claim 32, wherein the first content and the second content are both stored on the storage device.

35. The apparatus of claim 32, wherein the first content is an image, and the second content is not an image.

36. The apparatus of claim 32, wherein the first and second content are of different types.

DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR

RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application Nos. 62/418,510, 62/418,561, 62/418,687, 62/418,693, 62/418,696, 62/418,717, 62/418,724, 62/418,730, 62/418,742, 62/418,759, 62/418,764, 62/418,768, 62/418,773, 62/418,775, 62/418,780, 62/418,785, all filed on November 7, 2016, and to U.S. Provisional Patent Application 62/448,826, filed January 20, 2017, and which are all hereby incorporated by reference in their entirety.

TECHNICAL FIELD

[0002] Aspects of the disclosure are related to data storage devices and in particular to data storage devices with configurable policy-based read and write behavior.

TECHNICAL BACKGROUND

[0003] Data storage devices come in a wide variety of technologies and configurations such as solid-state drives, hard disk drives, floppy disk drives, and the like. Each of these data storage devices is based around some type of storage medium. For example, solid-state drives are based around integrated circuit memory devices, typically NOR Flash or NAND devices. Hard disk drives and floppy disk drives are typically based around one or more magnetically coated disks. Each of these devices (DRAM, NAND, magnetic disks) has imperfections. In order to deal with these imperfections, and still have a functional and performant device, all of these devices have trade-off decisions made that affect storage space, reliability, speed, etc.

[0004] These trade-off decisions have largely been made by the manufacturer at the time of design and/or manufacture to improve consistency of their product. Consequently, end users have very little to no influence over what trade-offs are made.

OVERVIEW

In an embodiment, a storage device is provided. A device controller with a memory is coupled with the storage device. The memory stores an application with instructions that direct

the controller to receive a storage device policy. The instructions further direct the controller to store content from a storage request in accordance with the storage device policy, and record storage information, including at least a content identifier, to the memory. Subsequent to storing the content, the instructions further direct the controller to retrieve the content according to the storage information received in a storage request. According to an implementation, the instructions further provide instruction to refuse a delete request in accordance to the storage information. According to an implementation, the instructions provide direction to store the storage information at a remote location.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] Many aspects of the disclosure can be better understood with reference to the following drawings. While several implementations are described in connection with these drawings, the disclosure is not limited to the implementations disclosed herein. On the contrary, the intent is to cover all alternatives, modifications, and equivalents.

[0006] Figure 1A illustrates a hard disk drive.

[0007] Figure 1B illustrates solid state drive.

[0008] Figure 2A illustrates a disk mapping from a hard disk drive.

[0009] Figure 2B illustrates multiple recording patterns on a hard disk.

[0010] Figure 3 illustrates a storage array according to an implementation.

[0011] Figure 4A illustrates a data storage arrangement according to an implementation.

[0012] Figure 4B illustrates a data storage arrangement according to an implementation.

[0013] Figure 4C illustrates a data storage arrangement according to an implementation.

[0014] Figure 4D illustrates a data storage arrangement according to an implementation.

[0015] Figure 4E illustrates a data storage arrangement according to an implementation.

[0016] Figure 5 illustrates a storage array according to an implementation.

[0017] Figure 6 illustrates a hard disk drive according to an implementation.

[0018] Figure 7A illustrates a collection of libraries according to an implementation.

[0019] Figure 7B illustrates a collection of libraries according to an implementation.

[0020] Figure 8A illustrates a write process employed by a storage device in an implementation.

[0021] Figure 8B illustrates a write process employed by a storage device in an implementation.

[0022] Figure 8C illustrates an operational sequence in an implementation of a policy-based write.

[0023] Figure 8D illustrates a read process employed by a storage device in an implementation.

[0024] Figure 8E illustrates an operational sequence in an implementation of a policy-based read.

[0025] Figure 9A illustrates a write process employed by a storage device in an implementation.

[0026] Figure 9B illustrates an operational sequence in an implementation of a policy-based write.

[0027] Figure 9C illustrates a read process employed by a storage device in an implementation.

[0028] Figure 9D illustrates an operational sequence in an implementation of a policy-based read.

[0029] Figure 10A illustrates a write process employed by a storage device in an implementation.

[0030] Figure 10B illustrates an operational sequence in an implementation of a policy-based write.

[0031] Figure 10C illustrates a read process employed by a storage device in an implementation.

[0032] Figure 10D illustrates an operational sequence in an implementation of a policy-based read.

[0033] Figure 11A illustrates a write process employed by a storage device in an implementation.

[0034] Figure 11B illustrates an operational sequence in an implementation of a policy-based write.

[0035] Figure 11C illustrates a read process employed by a storage device in an implementation.

[0036] Figure 11D illustrates an operational sequence in an implementation of a policy-based read.

[0037] Figure 12 illustrates a computing system suitable for implementing the policy based storage disclosed herein, including any of the architectures, processes, operational scenarios, and operational sequences illustrated in the Figures and discussed below in the Technical Disclosure.

DETAILED DESCRIPTION

[0038] In the examples below, storage devices are discussed which allow customization of a storage device policy, thus directing how the storage device operates. This storage device policy may cover many or all aspects of operation, for example, controlling margin of error, allowing the user to make trade-offs between reliability of storage and volume of storage. Additionally, the storage device policy may cover details of the write or read processes, allowing a user to customize the operation of the storage device. Further, the storage device policy may control where content is stored within the storage device (layout), granting the user further control over the read/write process.

[0039] User, as used herein, refers to more than just a human user. Rather, user refers to any type of entity that can interact with the devices described herein. User could include, but is not limited to, a human user, a network machine, or an artificial intelligence-based machine, for example.

[0040] From a technical perspective, currently available solutions for data storage allow only extremely minimal configuration of read/write policies within a storage device. Nor do they allow users to direct the read/write process within the storage device.

[0041] In a first example, Fig. 1A illustrates drive 100, which is illustrated here as a hard disk drive including a storage media 110 having a magnetic surface. In this example, drive 100 includes case 105, which physically supports the storage media 110, the device controller 130, a memory 135, interface connectors 125, and connector 120.

[0042] In an implementation, drive 100 includes storage media 110 having a magnetic surface including a plurality of zones or recording locations, a read/write transducer associated with the magnetic surface for reading and writing data in tracks in the plurality of zones, a

actuator arm configured to support and position read/write transducer at a plurality of locations above the magnetic surface, and device controller 130 coupled to a memory 135.

[0043] In an implementation, device controller 130 is significantly more than a traditional hard disk controller. A traditional hard disk controller is a device that must be attached to a host controller and is only capable of responding to host controller commands. Device controller 130 includes all the functionality of a traditional hard disk controller, with additional functionality allowing it to run additional code and/or applications. This additional functionality may exist due to additional processing hardware in the hard disk controller. Device controller 130 may be in the form of a hard disk controller linked with a separate processor chip. Alternatively, device controller 130 could be in the form of a computing system, such as that described in Fig. 12. When device controller is represented by the computing system described in Fig. 12, it should be noted that the storage system 1203 may be represented by memory 135. In other words, while there may be a storage system 1203 within device controller 130 and an additional memory 135, this is not necessary – the memory 135 may already be represented within Fig. 12 as storage system 1203. In an implementation, device controller 130 may be in the form of a computing system as described in Fig. 12 with a learning algorithm or artificial intelligence (AI) loaded thereon. In either case, device controller is configured at least to handle the operations that a traditional hard disk controller handles, i.e. it is configured to control the actuator arm and read/write transducer (or other hardware as needed) to read and write data on storage media 110.

[0044] Device controller 130 is connected to interface connector 125 such that Device controller can communicate in any manner a storage device and/or storage server may communicate including, for example via login (telnet, ssh, etc.), via file sharing service (NFS, SAMBA, FTP, etc.), via an Object Storage API (S3, SWIFT, etc.) or via any other protocol or service that can be run over the interface. The interface connector 125, could be for example, an Ethernet connector configured to communicate over an Ethernet network. In an implementation, the connector and network could work with Ethernet, Infiniband, Fibre Channel, Omni-Path, or any other network technology. Further, device controller 130 may be loaded with any selection of firmware or software. In an implementation, an operating system, and/or virtual machine hosting layer, such as Linux, Windows, etc., is loaded on the device controller 130, allowing a user to load any software of their choosing on the device controller 130.

[0045] In addition to interface connector 125, drive 100 also includes a connector 120 which may include power connectors to power drive 100 or other communication connectors. While this is shown as a separate connector from interface connector 125, it should be understood that the functionality of interface connector 125 and connector 120 can be combined in one physical connector or separated into a plurality of connectors.

[0046] Turning to Fig. 1B, drive 100 utilizes solid-state storage media according to an implementation. It should be noted that, while some of the hardware presented in Figs. 1A and 1B differs, the applicability to the concepts presented herein remains consistent across the drives shown. Consequently, drive 100 is shown in both Fig. 1A and Fig. 1B. Drive 100 is relevant to the discussion herein regardless of whether the storage media 110 is magnetic disk as shown in Fig. 1A, or solid-state memory 145-148 as shown in Fig. 1B, or some other type of storage media 110 not explicitly shown herein.

[0047] In an implementation, drive 100 optionally includes a case 105, which physically supports printed-circuit board 140, interface connector 125 and connector 120. Solid-state memory 145-148, as well as the device controller 130 and memory 135, are mounted on the printed-circuit board 140. In Fig. 1B, solid-state memory 145-149 are shown as four memory elements. This disclosure is not limited to four elements and could be any number of physical elements in any arrangement (i.e. busses, hierarchical, etc.).

[0048] Printed-circuit board 140 is also connected to interface connector 125 and connector 120. Interface connector 125 is structured to allow drive 100 to connect to a network fabric, such as through a cable and/or backplane. In an implementation, the interface connector may be in the form of an RJ45, QSFP, or CXP connector, to which copper wiring or optical fiber optic cable can connect, for example. It should be understood that any form of physical connector can be used that allows drive 100 to connect to a network. The interface connector may comprise a wireless module, such as a Wifi, Zigbee, etc. module through which the device controller 130 can connect to a network. In this way, the interface connector can connect to a network. The interface connector 125 is electrically and communicatively connected to the device controller 130, which is connected to memory 135. As in Fig. 1A, the device controller can be in the form of a computing system, such as that presented in Fig. 12. As the computing system presented in Fig. 12 already includes a storage system 1203, this can represent the same element as memory 135.

[0049] In addition to interface connector 125, drive 100 also includes a connector 120 which may include power connectors to power drive 100 or other communication connectors. As in Fig. 1A, while this is shown as a separate connector from interface connector 125, it should be understood that the functionality of interface connector 125 and connector 120 can be combined in one physical connector or separated into a plurality of connectors.

[0050] Figure 2A illustrates magnetic storage media 110 within drive 100 of figure 1A. In this example implementation, storage media 110 includes a physical disk upon which a magnetic surface resides. Content is written to, and read from storage media 110. The disk (storage media 110) spins. At the same time, an actuator moves the read/write head between the inner and outer edges of the disk. Content can be read and recorded in any pattern around the disk (i.e. circumferential, spiral, sinusoidal, etc.).

[0051] While Fig. 2A was drawn to show the general function of storage media 110, in an implementation in which storage media 110 is a magnetic disk, it should be understood that storage media 110 can be implemented in any form of media, such as the solid-state media shown in Fig. 2A and the result of the present disclosure would be the same. Whatever media may be used for storage media 110 allows content to be stored on storage media 110 in such a way that it can be retrieved at a later time.

[0052] Fig. 2B shows an expanded view of storage media 110 in the form of a magnetic disk. Recording patterns 255, 260 and 265 show partial samples of recorded tracks of content on storage media 110. All of the recording patterns 255, 260 and 265 are shown in a roughly spiral or circular pattern around the storage media 110. Recording pattern 255 is recorded in a tight spiral around the storage media 110. The recording pattern could scribe circles around storage media 110 rather than spirals. According to an implementation, the content could be recorded in any pattern.

[0053] The recording pattern 255 is shown with recording path that records very close the other recording paths. Recording pattern 260 shows paths that are significantly farther apart. Storage media 110 utilizes a magnetic surface for recording content. Depending on the size of the recording head, that content will take some amount of physical space. If two recording paths are recorded too close together, then the paths may interfere with each other, causing the content in one or both of the recording paths to become corrupted. Recording pattern 260, for example, will have a much lower likelihood of the recording paths interfering with each other to

compromise the content on either of the paths. Recording pattern 255 creates a much higher likelihood of compromised content due to the recording paths being too close together. However, recording pattern 255 can store more content than will recording pattern 260 in a similar area. The amount of content stored corresponds directly to the density of recording paths utilized (Assuming the same read/write methodology, etc.) Thus, the path scribed by recording pattern 255 allows significantly more content to be stored. This creates a trade-off decision when deciding how to store content on storage media 110. One can choose to keep recording paths very tight in order to accommodate more content at the risk that the content will be compromised, or one could alternately choose to decrease the amount of content to be stored while also decreasing the chance of corruption of the content.

[0054] In an implementation, instead of varying the density of recording paths, the frequency of recorded bits along the paths may be varied. Similar to the concepts discussed above, if the frequency of the recording (i.e. bits per physical length, such as bits per inch) may be varied. By increasing the number of bits per inch that are recorded, storage capacity in increased, but data integrity may be be degraded. In a further implementation, both of these variables may be adjusted to increase or decrease recording density. Regardless of the recording method chosen, the device controller 130 can utilize the storage device policy to make these trade-offs.

[0055] Historically, this trade-off decision has been made by drive manufacturers based on their own set of priorities. Priorities differ among different users, though. For example, a home user, such as an individual using a hard drive on a personal computer may have only one copy of content stored on the hard drive. For such a user, content integrity is very valuable, so the user would likely prefer that the possibility of content corruption be limited as much as possible. On the other hand, as an example, the owner of a large bank of hard drives that support cloud storage, may be much less concerned about the integrity of the content, and much more concerned with the amount of content able to be stored. This may be due to redundancies in the cloud storage system that allow the user to compensate for compromised content more easily. The space available to store data is of high concern to such a user, though, due to the large amount of data storage needed.

[0056] In addition to the possibility of recording paths interfering with each other, storage space competes with the possibility of imperfections in storage media 110. Imperfections in the

magnetic coating, or other imperfections in storage media 110 can make it impossible to store content on certain areas of storage media 110. This may mean that a sectoris entirely unusable, and the sector can just be eliminated from the mapping of storage media 110. Alternatively, there could be areas of storage media 110 that have minor imperfections that may be dealt with differently. Recording pattern 265 shows an implementation that allows for imperfections in storage media 110. By scanning storage media 110, device controller 130 can identify areas of storage media 110 with imperfections. In an implementation, device controller 130 can then select recording paths such as recording pattern 265 that avoid imperfections in storage media 110. It should be noted that device controller 130 requires more detailed mapping records or storage information than may be required for a simple path of storage, such as recording pattern 255 or recording pattern 260. Nevertheless, device controller 130 can improve storage capacity and reduce content corruption by having the flexibility to avoid areas of imperfection.

[0057] In an implementation, device controller 130 can choose to record content less densely (such as in recording pattern 260) in areas with potential imperfections, while recording content more densely (such as in recording pattern 255) in areas without imperfections. These trade-off decisions can all be made by device controller 130, which can be customized by an end user prior to data being stored, or at the time the data is stored. Furthermore, it may perform different or alternate procedures even on the same storage media surface.

[0058] While the recording process differs for different types of storage media, the concept applies to all types of storage media. For example, if the solid-state memory from Fig. 1B is utilized, the recording paths discussed may be inapplicable. The idea of imperfections within the storage media still applies, though. In solid-state memory devices, such as solid-state memory 145-148 in Fig. 1B, certain blocks of memory, or certain cells may be imperfect. Historically, solid state drives had to set aside a significant amount of over-provisioned storage blocks to use in place of imperfect cells or blocks. In an implementation these over-provisioned storage blocks can be customized and adjusted prior to, or at the time the data is stored to more accurately reflect a user's trade-off choices.

[0059] As another example of a trade-off decision, Error-Correcting Code (ECC) requirements can be changed. ECC requirements can be heightened for important content, and cna be softened for less important content.

[0060] It should be understood that any type of storage media 110 may have its own trade-off choices depending on the particular storage media 110. Regardless of the particular trade-off choices available to be made, the discussion herein facilitates handling these trade-off choices.

[0061] Fig. 3 shows a storage array 300. In an implementation, multiple storage drives, such as drives 310-321 are connected together in an array to create a large amount of available storage. Such an array may be used for cloud storage support, for example. While each of the drives 310-321 in Fig. 3 is shown as a disk drive such as drive 100 shown in Fig. 1A, these drives could be any combination of drives, such as hard disk drives, solid-state drives, etc. Similarly, while 12 drives 310-321 are shown, the storage array 300 could include any number of drives. The drives 310-321 are connected to a user device 305. User device 305 could be any type of network device with a network connection. Historically an array such as the storage array shown in Fig. 3 would require a storage controller in the place of user device 305. Since historically the device controller 130 only worked with a compatible storage controller, a storage controller was required to manage read/write data for the drives 310-321. In this disclosure, the device controller 130 includes capabilities beyond the historical abilities of physically managing the disk read/write process to include the ability to execute code and perform operations that were formerly the purview of the host and host controller. Therefore, each of the drives 310-321 can function independently of user device 305. Thus, each of drives 310-321 can independently connect to a network or networks, and operate as an independent network device.

[0062] Additionally, since each of drives 310-321 includes interface connectors and is configured to communicate directly through a communications capable link, the connection between user device 305 and each of drives 310-321 (and between each of drives 310-321) is a communications connection, not an interface limited to a storage only protocol. This allows for standard network communication to occur between all devices. The device controller 130 can be configured to interact with any network and interact with one or many devices over one or many protocols.

[0063] By having the device controller 130 function independently, storage array 300 gains many operational advantages. In an implementation, by enabling the device controller to function independently and communicate over a network, the need for a storage controller is

eliminated. Further, drives 310-321 are enabled to have independent storage policies that can maximize efficiency of each node as is required/desired for the aggregate array.

[0064] For example, if one drive, such as drive 310 is configured to store medical records, the device controller in drive 310 can be configured to optimize reliability for medical record storage. This might include recording content less densely, in order to reduce content corruption. It might also include storage information identifying the drive as non-rewriteable, so the data will not be overwritten and erased in the future. Similarly, the device controller might require password authorization in order to retrieve the content from the drive, or the drive could encode all content stored on the drive to protect privacy.

[0065] In another implementation, a drive, such as drive 311, could be configured as a drive to store on-line temporal video data. In this case, the drive may be configured to store data very densely, as there may be little concern over content corruption. Similarly, the drive 311 may be configured with little to no security for short-lived, redundant or cached data. The device controller could further be configured to differentiate between short-lived, redundant or cached data, and online shopping financial content, such as credit card data, etc. In this case, the online cached images or video data may be recorded with little to no security, while the online shopping financial data may be recorded with a high level of security. Again, this functionality can be customized to fit the needs and values of the user, and can be applied prior to or on-demand as the data is read from or written to the device. These different data types may be separated by drive, such as drives 311, 312, 313, etc., or the data may be interspersed within the same drive. In either case, the storage device policy can cause the content to be stored according to the correct trade-off choices.

[0066] Each of the drives 310-321 may additionally have differing recording properties. For example, if drive 313 is older than drive 314, it may have an older recording head, which doesn't allow data to be stored as densely as drive 314. The storage device policy can manage these varying properties.

[0067] Figs. 4A and 4B illustrate data storage arrangements. Historically, when a user device 305 writes data to a drive, the user device 305 provides the drive the LBA (Logical Block Address) of where to write the content. The drive then maps the LBA to a PBA (Physical Block Address). The device controller 130, according to an implementation, is capable of managing significantly more storage information. This storage information may contain, for example, an

object identifier, the size of the content stored, a location in which the content was stored, encoding information (including an encryption key, etc.), among many other elements. As discussed above, the location where the object is stored may include a simple start location, or it may be more complex, such as a starting point together with angle information, or even a complete mapping of the path of the content storage.

[0068] Fig. 4B illustrates that in an implementation, the storage information is stored in the device controller. As in Fig. 4A, the storage information may include a number of elements, particularly when, as disclosed herein, the device controller is customizable to allow the user to make trade-off decisions about the storage of content.

[0069] Fig. 4C illustrates the storage information stored within the device controller including an entry for overwrite protection. This selection could be made for the entire drive 100, for individual tracks or sectors or regions, or individually by object or read/write request for example.

[0070] Fig. 4D illustrates that in an implementation, the storage information stored in device controller 130 may also include a pointer to a location storing full storage information for content stored within storage media 110. This pointer information may be consistent for the entire drive 100, or may be made by sector, track, region, or object. In an implementation, the remaining storage information (other than object identifier and pointer) may not be stored in the device controller 130. The pointer may additionally be in any form, for example a network address that will not function when a hard drive is removed from a particular context (i.e. the network, an internet address, etc.).

[0071] Fig. 4E illustrates that any of the storage information may be stored as a header on the content stored within the storage media 110. It should be understood that any of the descriptions herein that describe storing storage information in the memory 135 or the device controller 130 are interchangeable – i.e. any of these descriptions applies equally well if the storage information is stored in memory within the device controller 130, memory 135 external to the device controller 130, or on the media with the data within the storage media 110. While Fig. 4E shows the storage information stored as a header on the content, the storage information can be stored in any location on the media with the content.

[0072] Fig. 5 illustrates a storage array 500. In an implementation, multiple storage drives, such as drives 310-321 are connected together in an array to create a large pool of

available storage. Such an array may be used for cloud storage support, for example. While each of the drives 310-321 in Fig. 3 is shown as a disk drive such as drive 100 shown in Fig. 1A, these drives could be any combination of drives, such as hard disk drives, solid-state drives, etc. Similarly, while 12 drives 310-321 are shown, the storage array 300 could include any number of drives. The drives 310-321 are connected to a user device 305 and a key device 505. User device 305 and key device 505 could each be any type of network device or virtual node with a network connection. Historically an array such as the storage array shown in Fig. 3 would require a storage controller in the place of user device 305 or key device 505. Since historically the device controller 130 worked externally as a response-only device, a storage controller was required to manage the reading/writing of data for the drives 310-321. In this disclosure, the device controller 130 includes capabilities beyond the historical abilities of physically managing the disk read/write process to include the ability to operate autonomously and/or interactively with other devices on the network. Therefore, each of the drives 310-321 can function independently of user device 305 or key device 505. Thus, each of drives 310-321 can independently log in to a network, or operate as any other independent network device.

[0073] Additionally, since each of drives 310-321 can be configured to communicate directly through a communications link, the connection between user device 305 and key device 505 and each of drives 310-321 (and between each of drives 310-321) is a network connection. This allows for network communication to occur between and among the devices. The device controller 130 can be configured to interact with any network.

[0074] Storage array 500 provides many benefits due to the fact that each of drives 310-321 can independently operate and interact, as outlined with reference to Fig. 3. Additionally, key device 505 provides a location to store storage information (i.e. meta-data) in a remote location, optionally a secured location, from the device controller 130, which provides many advantages.

[0075] Historically, a storage controller, such as user device 305 managed the operation of drive 310. User device 305 directed the hard disk controller in drive 310 to write content to an LBA, and drive 310 wrote the content to the PBA that mapped to the LBA identified.

[0076] On a hard drive with a magnetic disk such as storage media 110, there are many reasons that this is done. For example, the translation on the drive may be to obfuscate the

defects on the device and/or various recording technologies (e.g. Shingled Magnetic Recording), or to write the content quickly.

[0077] On a hard drive with solid-state media, such as solid-state memory 145-148, this is done to prevent overuse of a particular address (wear-leveling), avoid bad blocks (media defects), and/or enable faster writing, for example.

[0078] The hard drive then keeps track of various mappings to enable reading of the correct PBA when a specific LBA is requested by the host computer system.

[0079] In an embodiment, the device controller 130 simplifies both the need for the host computer system to keep track of the physical defects, etc. and the list of block addresses for each file or object. Additionally, the device controller 130 enables the storage device to maximize the storage capacity and/or performance of the storage device based on policy.

[0080] This is implemented by providing the host computer system with alternate methodologies to maintain location information about files/objects:

[0081] When a host computer system wishes write a file/object to a storage device, the user device 305 provides the data to the drive 100. The device controller 130 stores the data where it deems best, based on the application of one or more polices. This decision may be based on (but not limited to) size of the data, existing state of the storage media, the location of the actuator arm on the media (in the case of hard disk drives), what locations have already been written, the recording technology implemented (e.g. Shingled Magnetic Recording, 3D NAND, etc.), wear leveling, alternate write activity on adjacent blocks, desired reliability level, etc.

[0082] After selecting the location the storage device may write the data to the media and subsequently or coincidentally store the location information, and/or return the location information to the requestor of the operation. This location data could additionally or alternately be written to a key device 505. If, for example, this location information is stored only in a key device 505, additional security for the data can be achieved. The location data may be represented in any number of ways (e.g. polar coordinates, cartesian coordinates, PBA, cylinder/track/sector, etc.). It may or may not include the size/length, reliability requirements, slope, and/or any additional information such as encryption key and/or encoding scheme.

[0083] It should be understood that the data recorded to the user device 305 or the key device 505 need not be limited to only the location of the data stored. The data could also include size of the content, encoding or encryption details of the content, etc.

[0084] The user device 305 or key device 505 then stores the location associated with the data that was written for future use (e.g. reading the data at a later time.)

[0085] Figure 6 illustrates a drive 600 according to an implementation, which is illustrated here as a drive 600 including a storage media 110 having a magnetic surface. In this example, drive 600 includes case 105, which physically supports a storage media 110, a device controller 130, a programmable logic device 605, a memory 135, interface connectors 125, and connector 120.

[0086] In an implementation, drive 600 includes storage media 110 having a magnetic surface including a plurality of zones or recording locations, a read/write transducer associated with the magnetic surface for reading and writing data in tracks in the plurality of zones, an actuator arm configured to support and position read/write transducer at a plurality of locations above the magnetic surface, and device controller 130 coupled a memory 135.

[0087] In an implementation, device controller 130 is significantly more than a traditional hard disk controller. A traditional hard disk controller is merely device that must be attached to a host controller and is only capable of responding to commands. Device controller 130 includes all the functionality of a traditional hard disk controller, with the additional ability to run code and/or applications. Device controller 130 may be in the form of a hard disk controller linked with processor chip. In an implementation, device controller 130 could be in the form of a computing system, such as that described in Fig. 12. When device controller is represented by the computing system described in Fig. 12, it should be noted that the storage system 1203 may be represented by memory 135. In other words, while there may be a storage system 1203 within device controller 130 and an additional memory 135, this is not necessary – the memory 135 may already be represented within Fig. 12 as storage system 1203. In either case, device controller is configured at least to handle the operations that a traditional hard disk controller handles, i.e. it is configured to control the actuator arm and read/write transducer to read and write data on storage media 110.

[0088] Programmable logic device 605 is inserted directly into the data and/or control path of drive 600. The programmable logic device 605 can be programmed by a user of the drive 600 for any operational need that is desired. In an embodiment, this could be used for custom encryption through hardware. Alternatively, this could be used as a regular expression engine to search for words, phrases, pictures etc. that meet certain criteria. The programmable

logic device 605 could be used broadly for the entire drive 600, or could be used on a per-request basis, such that different requests to read or write content could use different programmable logic configurations. For example, a write of a text file may use programmable logic for compression, while a write of a picture may use programmable logic for facial recognition. In an implementation, the programmable logic device 605 may include a learning algorithm or artificial intelligence that can act of the signals passing through drive 100. The programmable logic device 605 may be incorporated into drive 600 as a programmable chip built into the drive 600, or as a socket assembled into the drive 600 which can later accept a programmable chip (after manufacture) for example.

[0089] While programmable logic device 605 is shown connected between interface connector 125 and device controller 130, programmable logic device 605 could also be located (and electrically and/or communicatively connected) elsewhere within the drive 600 to have the same effect. For example, programmable logic device 605 may be connected to device controller 130, and the hardware and/or software in device controller 130 will automatically route some or all of the signals through programmable logic device 605. In an implementation, programmable logic device 605 could be connected to a pre-amplifier (not shown) that is in turn connected to device controller 130.

[0090] Device controller 130 is connected to interface connector 125 (through programmable logic device 605 according to an implementation) such that device controller 130 can communicate in any manner that a network server device can communicate, for example via login (telnet, ssh, etc.), via file sharing service (NFS, SAMBA, FTP, etc.), via an Object Storage API (S3, SWIFT, etc.) or via any other protocol or service that can be run over a network. Further, device controller 130 may be loaded with any selection of firmware or software. In an implementation, an operating system hosting layer or an operating system, such as Linux, Windows, etc., is loaded on the device controller 130, allowing a user to load any software of their choosing on the device controller 130.

[0091] Fig. 7A illustrates a storage device policy according to an implementation. The device controller 130 as discussed herein allows multiple opportunities for the device firmware to adopt and implement flexible operational parameters. Historically, hard drives, both hard disk drives and solid-state drives, have included a single, immutable binary file of device firmware. This firmware, as discussed above, allowed only minimal customization by the user, and

therefore was inefficient, or mis-matched to the operational environment for many users. With device controller 130 as discussed herein, this inflexibility is removed. The device controller 130 can allow selection of parameters that modify device operation, such as command timeout, read retry count, device format block size, background task controls, cache control parameters, etc. The device controller 130 allows a collection of cooperating libraries or execution elements running on one or more processors with varying capabilities.

[0092] The storage device policy can be stored (and modified or updated) on the device controller 130. Alternatively (or additionally) the storage device policy can be stored at a remote location to the device controller 130 and queried by the device controller 130 as needed to implement the storage device policy.

[0093] Collection of libraries 700 shows an example of the cooperating libraries that may be included within device controller 130. Layout library 705 can instruct the device controller 130 how to determine what layout to use for content storage. For example, layout library 705 may include algorithms that take into account the type of content to be written to the storage media 110 to determine how densely to record content onto the storage media 110. Defect avoidance library 710 can include algorithms to determine how to deal with defects within the storage media 110. As discussed above with reference to Fig. 4, this could include recording content on custom paths, or altering density of recorded content based on quality of the storage media 110 in certain tracks or sectors. Read/write control library 715 can contain instructions or algorithms directing device controller 130 on how to track write protection for recorded content, for example. Read/write control library can also contain instructions around encoding of content, including where to hold encryption keys, etc. Servo library 720 can contain entries to control the operation of the physical drive elements. Device supplied library 725 may include other elements of firmware or control relevant to the drive itself, which may be unique to a certain manufacturer or drive. The examples above are mere examples, and each of these libraries may contain any variety of static values, single functions or algorithms or collections of functions or algorithms as well as the ability to obtain parameters prior to, or at, run-time from a source on the network. Similarly, the device controller may access more than just the libraries shown in Fig. 7A, or might not access all of the displayed libraries.

[0094] In this collection of libraries, calls to and from one layer of the software made to a function in another layer of the software can be linked at the time the layer is loaded in the

system. This method of linking at a late time allows for customized code or library entries to be deployed in the device controller 130. This collection of libraries 700 subsumes much of what has traditionally been device firmware on a hard disk controller.

[0095] Fig. 7B illustrates an updated collection of libraries 750 in which the defect avoidance library 710 has been completely replaced by replacement defect avoidance library 760, and a new user supplied library 780 has been added. The approach described herein allows operational characteristics of the device controller 130, i.e. the firmware, to be defined to allow for wholesale replacement of an entire layer or layers of the cooperating libraries by the user of the device. It should be noted, that layers here can refer to anything from a static value, to a single function or algorithm, to a collection of algorithms. The user supplied libraries do not even need to be written in a source language that matches the device-supplied collection of libraries 700 – they only need to satisfy the calling convention requirements of the interface software on the device controller 130.

[0096] In many cases, a user will not want to replace libraries in their entirety. In such cases, the device controller 130 can accept source code or partially compiled code that can be further compiled or interpreted by the device controller 130 and incorporated into the existing collection of libraries 700.

[0097] For example, in traditional firmware, the Read retry features of the device may be a collection of algorithmic options, in different permutations, with a different set of parameters, with some of those parameters being supplied by the user of the device.

Retry Profile	Phase1	Phase2	Phase 3	Phase 4	...
Fast	1_Rev_Retry()	Y_Val_Avg () w/ 2 Rev	Avg_Val() w/ 10 Rev	N/A	N/A
Heroic	1_Rev_Retry()	Avg_Val() w/ 50 Rev	Avg_Val() w/ 100 Rev	Y_Val_Avg. w/ 100 Rev.	"Super" recover algorithm

[0098] In the collection of libraries 700, the same algorithms may be present in a callable form, but the user of the device can write a code snippet or script that would define the ordering of the functions tried, and the associated parameters passed to those functions, e.g.

```
Define: read_retry(timeout, max_rev) is
 call 1_Rev_Retry
   if %ret == good_read then goto done
   call Y_Val_Avg(10_rev)
   if %ret == good_read then goto done
   call Y_Val_Avg(max_rev - 10_rev)
   if %ret == good_read then goto done
   call Avg_Val (max_rev)
   If %ret == good_read then goto done
   call Super_Recover(timeout)
   If %ret == good_read then goto done
   Set global ERR_CODE = cant_read;
  :done
end read_retry;
```

[0099] Historically, the user of the device would be to select one of the choices in the table above, for example the user could choose “Fast” or “Heroic” as a MODE PAGE setting through a MODE SELECT COMMAND, a SET FEATURES setting, or equivalent. The user historically is severely restricted in the number of options available.

[00100] Utilizing the collection of libraries 700 enables the user almost unlimited control of how the device performs the “read_retry” operation. The user can make an algorithmic specification of the desired behavior. The device controller 130 allows, at the user's discretion, the ability to supply an algorithm, or collection of algorithms that extend and control the operation of the device. Another way of thinking of this as that the device controller 130 supplies a “toolkit” and it is up to the user to construct the product behavior they are after by “programming” or “scripting” the behavior themselves. The user can choose to intercept calls between the software layers and make algorithmic transformations, or they may simply replace or extend any function call with one supplied by the user to modify default behavior.

[00101] Additionally, the user supplied algorithm, "script", "byte-code", or "binary" does not necessarily need to be transferred to the device to be utilized. In an implementation, the device controller 130 would allow for the user to insert a "callback" into the collection of libraries 700 wherein the collection of libraries 700 has the ability to make a call to an algorithm or function in another location to obtain the user specified behavior or needed information. The "callback" inserted into the collection of libraries 700 could take many forms; for example, it could be as simple as a pointer to a function in memory, or as complex as a URL that is itself a function call that executes on a remote system. Further, the "callback" does not need to be written in the same language, have a similar CPU instruction set, or be on the device itself. In an implementation, a user selects some of the supplied algorithms within the collection of libraries 700, and provides an entirely new library of defect avoidance algorithms and rules.

[00102] Fig. 8A illustrates a method of writing content 801 according to an implementation. A user sends a request to store content in step 815. As discussed above, a user herein is not limited to a human user, but can rather include any user or network device capable of sending a request to the device controller 130. At a minimum, this request comprises content to be stored. In an implementation, the user may include information such as an identification code, encoding information, or data protection information, for example.

[00103] In step 820, the device controller 130 uses a storage device policy, such as that described in Figs. 7A and 7B, to determine where to store the content. This determination can relate partially to the content being stored, and partially to the storage media 110. For example, if the content contains an indication of priority level, such as information indicating that certain content is highly critical, the device controller 130, based on the storage device policy, may determine that the content should be stored on the storage media 110 at a low density, so the likelihood of data corruption will be minimal. Similarly, the storage device policy may also have an algorithm to determine how to avoid defects, and the storage device policy may instruct the device controller 130 to avoid storing highly critical content in sectors that have defects. Depending on what libraries exist in the device controller 130, and what the libraries control, many factors could be considered when deciding where and how to store the content.

[00104] In step 840, the device controller can write the content to the storage media 110 as determined in step 820. In addition to writing the actual content, in step 845 the device controller can also store a record of the write (the storage information) in memory 135 or to

some non-volatile memory, such as storage media 110. In an implementation, this information can include a unique identifier for the content. This may be an object identifier supplied by the user, or created by the device controller 130, for example. The storage information may also include information relating to encoding, write protection, location, size, etc. Some or all of this information may also, or alternatively, be returned to the user when the write is complete, again based on policy in force at the time of the request.

[00105] Fig. 8B illustrates a method of writing content 801 according to an implementation. In step 805, the device controller receives a storage device policy. Receiving a storage device policy here can mean receiving an update to a storage device policy already in place. The storage device policy can be part of an overall collection of libraries 700 that create the framework for device controller 130 to operate.

[00106] In step 810, these newly selected and newly supplied algorithms and rules are used to update the storage device policy on the device controller 130. In an embodiment, calls to and from one layer of the storage device policy made to a function in another layer of the storage device policy can be linked at the time the layer is loaded in the system. This method of linking at a late time allows for customized code or library entries to be deployed in the device controller 130.

[00107] A user sends a request to store content in step 815. At a minimum, this request comprises content to be stored. In an implementation, the user may include information such as an identification code, encoding information, or data protection information, for example.

[00108] In step 820, the device controller 130 uses the storage device policy to determine where to store the content. This determination can relate partially to the content being stored, and partially to the storage media 110. For example, if the content contains an indication of priority level, such as information indicating that certain content is highly critical, the device controller 130, based on the storage device policy, may determine that the content should be stored on the storage media 110 at a low density, so the likelihood of data corruption will be minimal. Similarly, the storage device policy may also have an algorithm to determine how to avoid defects, and the storage device policy may instruct the device controller 130 to avoid storing highly critical content in sectors that have defects. Depending on what libraries exist in the device controller 130, and what the libraries control, many factors could be considered when deciding where and how to store the content.

[00109] In an implementation, in step 825, the device controller 130 will not have enough information in the storage device policy, and the device controller may reach back out to a network machine, or to a policy server, to request further information. For instance, the collection of libraries 700 may include a rule or algorithm that controls how to store certain content, but the user may not have selected that rule or algorithm or a replacement rule or algorithm. The device controller 130 may send a request to the user prompting the selection of a rule or algorithm or to set values for the generic rule or algorithm.

[00110] When the user supplies the needed information, the device controller 130 can update the storage device policy in step 830, as above in step 810, or can use the information temporally to complete the operation. When the storage device has the needed information, the device controller 130 can also update the determination of where and how to store the content in step 835

[00111] In step 840, the device controller can write the content to the storage media 110 as determined in step 820 and/or step 835. In addition to writing the actual content, in step 845 the device controller can also store a record of the write (the storage information) in memory 135 or to some non-volatile memory, such as storage media 110. In an implementation, this information can include a unique identifier for the content. This may be an object identifier supplied by the user, or created by the device controller 130. The record may also include information relating to encoding, write protection, location, size, etc. Some or all of this information may also be returned to the user when the write is complete, again based on policy in force at the time of the request.

[00112] Fig. 8C illustrates an operational sequence of a policy-based write according to an implementation. The device controller receives a storage device policy from a user device 305. Receiving a storage device policy here can mean receiving an update to a storage device policy already in place. The storage device policy can be part of an overall collection of libraries 700 that create the framework for device controller 130 to operate. In an implementation, a user device 305 provides values for some of the supplied algorithms within the collection of libraries 700, and provides some entirely new rules.

[00113] These algorithms and rules are used to update the storage device policy on the device controller 130. In an embodiment, calls to and from one layer of the storage device policy made to a function in another layer of the storage device policy can be linked at the time

the layer is loaded in the system and can remain in force permanently or temporally. This method of linking at a late time allows for customized code or library entries to be deployed in the device controller 130.

[00114] A second user device 855 then sends a request to the device controller 130 to store content. At a minimum, this request comprises content to be stored. In an implementation, the device controller 130 needs little information beyond the content itself, but the user may still include information such as an identification code, encoding information, of data protection information, for example. This request can come from the second user device 855 for many reasons. For example, both user device 305 and second user device 855 may be part of the same network, and both user devices may have access to the device controller 130 through the network connection. Alternatively, user device 305 may have been disconnected from the network and replaced by the second user device 855 at some point in time after the storage device policy update and before the storage request. In another implementation, the drive 100 may have been disconnected from the network at some point after the storage device policy was updated. Drive 100 may have been connected to a new network that does not include user device 305. Since the customized storage device policy resides on the device controller 130, the storage device policy can move with the drive 100 to the new location.

[00115] The device controller 130 uses the storage device policy to determine where and how to store the content from the second user device 855. This determination can relate partially to the content being stored, and partially to the storage media 110. For example, if the content contains an indication of priority level, such as information indicating that certain content is highly critical, the device controller 130, based on the storage device policy, may determine that the content should be stored on the storage media 110 at a low density, so the likelihood of data corruption will be minimal. Similarly, the storage device policy may also have an algorithm to determine how to avoid defects, and the storage device policy may instruct the device controller 130 to avoid storing highly critical content in sectors that have defects. Depending on what libraries exist in the device controller 130, and what the libraries control, many factors could be considered when deciding where and how to store the content.

[00116] In an implementation, the device controller 130 may not have enough information in the storage device policy, and the device controller may reach back out to the requesting network machine or another network resource to request further information. For instance, the

collection of libraries 700 may include a rule or algorithm that controls how to store certain content, but the user may not have selected that rule or algorithm or a replacement rule or algorithm. The device controller 130 may send a request to the user prompting the selection of a rule or algorithm or to set values for the generic rule or algorithm.

[00117] When the requested information is supplied, the device controller 130 can update the storage device policy. In an implementation, some of the storage device policy defined by the user device 305 may have write protections, such that the second user device 855 does not have authority to change the storage device policy. After the storage device policy is updated, the device controller 130 can also update the determination of where and how to store the content.

[00118] The device controller 130 can write the content to the storage media as determined above. In addition to writing the actual content, the device controller 130 can also store a record of the write (the storage information) in memory 135. In an implementation, this information can include a unique identifier for the content. This may be an object identifier supplied by the second user device 855, or created by the device controller 130. The record may also include information relating to encoding, write protection, location, size, etc. Some or all of this information may also be returned to the second user device 855 when the write is complete.

[00119] Fig. 8D illustrates a method of reading content 850 according to an implementation. In step 860, the device controller receives a storage device policy. Receiving a storage device policy here can mean receiving an update to a storage device policy already in place. The storage device policy can be part of an overall collection of libraries 700 that create the framework for device controller 130 to operate. In an implementation, a user selects some of the supplied algorithms within the collection of libraries 700, and provides an entirely new library of defect avoidance algorithms and rules.

[00120] In step 865, these newly selected and newly supplied algorithms and rules are used to update the storage device policy on the device controller 130. In an embodiment, calls to and from one layer of the storage device policy made to a function in another layer of the storage device policy can be linked at the time the layer is loaded in the system. This method of linking at a late time allows for customized code or library entries to be deployed in the device controller 130.

[00121] A user sends a request to store content in step 870. At a minimum, this request comprises content to be stored. In an implementation, the user may include information such as an identification code, encoding information, of data protection information, or other storage information, for example. The device controller 130 uses the storage device policy to determine where and how to store the content. This determination can relate partially to the content being stored, and partially to the storage media 110. For example, if the content contains an indication of priority level, such as information indicating that certain content is highly critical, the device controller 130, based on the storage device policy, may determine that the content should be stored on the storage media 110 at a low density, so the likelihood of data corruption will be minimal. Similarly, the storage device policy may also have an algorithm to determine how to avoid defects, and the storage device policy may instruct the device controller 130 to avoid storing highly critical content in sectors that have defects. Depending on what libraries exist in the device controller 130, and what the libraries control, many factors could be considered when deciding where and how to store the content.

[00122] In step 875, the device controller can write the content to the storage media as determined. In addition to writing the actual content the device controller 130 can also store a record of the write (the storage information) in memory 135. In an implementation, this information can include a unique identifier for the content. This may be an object identifier supplied by the user, or created by the device controller 130. The record may also include information relating to encoding, write protection, location, size, etc. Some or all of this information may also be returned to the user when the write is complete. In an implementation, some or all of the storage information is provided by the user as part of the request to store content in step 870.

[00123] In step 880, the device controller 130 receives a content request. This request includes at least a content or object identifier to identify the requested content. This request may further include some or all of the information provided to the user after the write of the content was completed in step 875.

[00124] In an implementation, in step 885, the device controller 130 will not have enough information in the storage device policy to complete the content retrieval, and the device controller may reach back out to the requesting network machine to request further information. For instance, the collection of libraries 700 may include a rule or algorithm that controls how to

protect certain content, but the user may not have selected that rule or algorithm or a replacement rule or algorithm. The device controller 130 may send a request to the user prompting the user to select a rule or algorithm or to set values for the generic rule or algorithm.

[00125] When the user supplies the requested information, the device controller 130 can update the storage device policy in step 890, as above in step 865.

[00126] In step 893, the device controller 130 retrieves the requested content according to the storage device policy that has been defined. In step 895, the device controller 130 sends the content back to the user.

[00127] Fig. 8E illustrates an operational sequence of a policy-based write according to an implementation. The device controller receives a storage device policy from a user device 305. Receiving a storage device policy here can mean receiving an update to a storage device policy already in place. The storage device policy can be part of an overall collection of libraries 700 that create the framework for device controller 130 to operate. In an implementation, a user device 305 provides values for some of the supplied algorithms within the collection of libraries 700, and provides some entirely new rules.

[00128] These algorithms and rules are used to update the storage device policy on the device controller 130. In an embodiment, calls to and from one layer of the storage device policy made to a function in another layer of the storage device policy can be linked at the time the layer is loaded in the system. This method of linking at a late time allows for customized code or library entries to be deployed in the device controller 130.

[00129] The user device 305 then sends a request to the device controller 130 to store content. At a minimum, this request comprises content to be stored. In an implementation, the device controller 130 needs little information beyond the content itself, but the user may still include information such as an identification code, encoding information, of data protection information, for example.

[00130] The device controller 130 uses the storage device policy to determine where and how to store the content from the second user device 855. This determination can relate partially to the content being stored, and partially to the storage media 110. For example, if the content contains an indication of priority level, such as information indicating that certain content is highly critical, the device controller 130, based on the storage device policy, may determine that the content should be stored on the storage media 110 at a low density, so the likelihood of data

corruption will be minimal. Similarly, the storage device policy may also have an algorithm to determine how to avoid defects, and the storage device policy may instruct the device controller 130 to avoid storing highly critical content in sectors that have defects. Depending on what libraries exist in the device controller 130, and what the libraries control, many factors could be considered when deciding where to store the content.

[00131] The device controller 130 writes the content to the storage media as determined above. In addition to writing the actual content, the device controller 130 can also store a record of the write (the storage information) in memory 135. In an implementation, this information can include a unique identifier for the content. This may be an object identifier supplied by the second user device 855, or created by the device controller 130. The record may also include information relating to encoding, write protection, location, size, etc. Some or all of this information may also be returned to the second user device 855 when the write is complete.

[00132] At some point, a second user device 855 sends a content request to device controller 130. This request includes at least a content or object identifier to identify the requested content. This request may further include some or all of the information provided to the user device 305 after the write of the content was completed.

[00133] This request can come from the second user device 855 for many reasons. For example, both user device 305 and second user device 855 may be part of the same network, and both user devices may have access to the device controller 130 through the network connection. Alternatively, user device 305 may have been disconnected from the network and replaced by the second user device 855 at some point in time after the storage device policy update and before the storage request. In another implementation, the drive 100 may have been disconnected from the network at some point after the storage device policy was updated. Drive 100 may have been connected to a new network that does not include user device 305. Since the customized storage device policy resides on the device controller 130, the storage device policy can move with the drive 100 to the new location.

[00134] In an implementation, the device controller 130 will not have enough information in the storage device policy, and the device controller may reach back out to the requesting network machine to request further information. For instance, the collection of libraries 700 may include a rule or algorithm that controls how to store certain content, but the user may not have selected that rule or algorithm or a replacement rule or algorithm. The device controller 130 may

send a request to the second user device 855 prompting the second user device 855 to select a rule or algorithm or to set values for the generic rule or algorithm. The storage device policy set by the user device 305 may include protections that restrict later updates to the storage device policy. The second user device 855 may therefore have limited or no option to change the storage device policy.

[00135] When the second user device 855 supplies the requested information, the device controller 130 can update the storage device policy. The device controller 130 retrieves the requested content according to the storage device policy that has been defined. The device controller 130 then sends the content back to the second user device 855.

[00136] Fig. 9A illustrates a method of writing content 900 according to an implementation. In step 905, the device controller receives a storage device policy. Receiving a storage device policy here can mean receiving an update to a storage device policy already in place. The storage device policy can be part of an overall collection of libraries 700 that create the framework for device controller 130 to operate. In an implementation, a user selects some of the supplied algorithms within the collection of libraries 700.

[00137] In step 910, these newly selected and newly supplied algorithms and rules are used to update the storage device policy on the device controller 130. In an embodiment, calls to and from one layer of the storage device policy made to a function in another layer of the storage device policy can be linked at the time the layer is loaded in the system. This method of linking at a late time allows for customized code or library entries to be deployed in the device controller 130.

[00138] A user sends a request to store content in step 915. At a minimum, this request comprises content to be stored. In an implementation, the user may include information such as an identification code, encoding information, of data protection information, for example.

[00139] In step 920, the device controller 130 uses the storage device policy to determine where and how to store the content. This determination can relate partially to the content being stored, and partially to the storage media 110. For example, if the content contains an indication of priority level, such as information indicating that certain content is highly critical, the device controller 130, based on the storage device policy, may determine that the content should be stored on the storage media 110 at a low density, so the likelihood of data corruption will be minimal. Similarly, the storage device policy may also have an algorithm to determine how to

avoid defects, and the storage device policy may instruct the device controller 130 to avoid storing highly critical content in sectors that have defects. Depending on what libraries exist in the device controller 130, and what the libraries control, many factors could be considered when deciding where and how to store the content.

[00140] In an implementation, in step 925, the device controller 130 will determine that the location identified by the device controller 130 to write to content already has content that is write protected. Note that this information (write protection) is stored within the drive 100, and consequently will not lose write protection status is drive 100 is removed from connection with user device 305, for example.

[00141] In step 930, the device controller 130 does not complete the write operation, and in step 935, an error is returned to user device 305. In an embodiment, rather than return an error, the device controller 130 could identify another location that is not write protected, and complete the write operation.

[00142] According to an implementation, drive 100 may be configured so that all data stored thereon is write protected, in which case the device controller 130 may simply write content sequentially through the drive, maintaining a pointer to the next location to write content. In this case, when the pointer reaches the end of the available space on the storage media 110, any additional requests to write will be returned as errors. Alternatively, this behavior may be limited to a portion of the storage media 110, or may be decided on a per-block or per object basis, for example.

[00143] Fig. 9B illustrates an operational sequence of a policy-based write according to an implementation. The device controller receives a storage device policy from a user device 305. Receiving a storage device policy here can mean receiving an update to a storage device policy already in place. The storage device policy can be part of an overall collection of libraries 700 that create the framework for device controller 130 to operate. In an implementation, a user device 305 provides values for some of the supplied algorithms within the collection of libraries 700, and provides some entirely new rules.

[00144] These algorithms and rules are used to update the storage device policy on the device controller 130. In an embodiment, calls to and from one layer of the storage device policy made to a function in another layer of the storage device policy can be linked at the time

the layer is loaded in the system. This method of linking at a late time allows for customized code or library entries to be deployed in the device controller 130.

[00145] A second user device 855 then sends a request to the device controller 130 to store content. At a minimum, this request comprises content to be stored. In an implementation, the device controller 130 needs little information beyond the content itself, but the user may still include information such as an identification code, encoding information, or data protection information, for example. This request can come from the second user device 855 for many reasons. For example, both user device 305 and second user device 855 may be part of the same network, and both user devices may have access to the device controller 130 through the network connection. Alternatively, user device 305 may have been disconnected from the network and replaced by the second user device 855 at some point in time after the storage device policy update and before the storage request. In another implementation, the drive 100 may have been disconnected from the network at some point after the storage device policy was updated. Drive 100 may have been connected to a new network that does not include user device 305. Since the customized storage device policy resides on the device controller 130, the storage device policy can move with the drive 100 to the new location.

[00146] The device controller 130 uses the storage device policy to identify where and how to store the content from the second user device 855. This determination can relate partially to the content being stored, and partially to the storage media 110. For example, if the content contains an indication of priority level, such as information indicating that certain content is highly critical, the device controller 130, based on the storage device policy, may determine that the content should be stored on the storage media 110 at a low density, so the likelihood of data corruption will be minimal. Similarly, the storage device policy may also have an algorithm to determine how to avoid defects, and the storage device policy may instruct the device controller 130 to avoid storing highly critical content in sectors that have defects. Depending on what libraries exist in the device controller 130, and what the libraries control, many factors could be considered when deciding where and how to store the content.

[00147] In an implementation, the device controller 130 will determine that the location identified by the device controller 130 already contains content that is write protected. Consequently, the device controller 130 will not store that content. A notification of an error will then be returned to the second user device 855. According to an implementation, drive 100

may be configured so that all data stored thereon is write protected, in which case the device controller 130 may simply write content sequentially through the drive, maintaining a pointer to the next location to write content. In this case, when the pointer reaches the end of the available space on the storage media 110, any additional requests to write will be returned as errors. Alternatively, this behavior may be limited to a portion of the storage media 110, or may be decided on a per-block or per object basis, for example.

[00148] Fig. 9C illustrates a method of reading content 950 according to an implementation. In step 955, the device controller receives a storage device policy. Receiving a storage device policy here can mean receiving an update to a storage device policy already in place. The storage device policy can be part of an overall collection of libraries 700 that create the framework for device controller 130 to operate. In an implementation, a user selects some of the supplied algorithms within the collection of libraries 700, and provides an entirely new library of defect avoidance algorithms and rules.

[00149] In step 960, these newly selected and newly supplied algorithms and rules are used to update the storage device policy on the device controller 130. In an embodiment, calls to and from one layer of the storage device policy made to a function in another layer of the storage device policy can be linked at the time the layer is loaded in the system. This method of linking at a late time allows for customized code or library entries to be deployed in the device controller 130.

[00150] A user sends a request to store content in step 965. At a minimum, this request comprises content to be stored. In an implementation, the user may include information such as an identification code, encoding information, of data protection information, for example. The device controller 130 uses the storage device policy to determine where and how to store the content. In an implementation, this determination includes a determination that the content should be stored as write-protected (or write-once) such that is will not be deleted later or overwritten. This determination could be based on an entire drive 100 being designated as a write-protected drive, or as certain sectors or tracks or regions being pre-designated as write protected. Alternatively, an individual object may be designated as write-protected as it is stored.

[00151] Any determination of where or how to store the content can relate partially to the content being stored, and partially to the storage media 110. For example, if the content contains

an indication of priority level, such as information indicating that certain content is highly critical, the device controller 130, based on the storage device policy, may determine that the content should be stored on the storage media 110 at a low density, so the likelihood of data corruption will be minimal. Similarly, the storage device policy may also have an algorithm to determine how to avoid defects, and the storage device policy may instruct the device controller 130 to avoid storing highly critical content in sectors that have defects. Depending on what libraries exist in the device controller 130, and what the libraries control, many factors could be considered when deciding where and how to store the content.

[00152] In step 970, the device controller can write the content to the storage media as determined, including an indication of write protection. In addition to writing the actual content the device controller 130 can also store a record of the write (the storage information) in memory 135 or to some non-volatile media, such as storage media 110. In an implementation, this information can include a unique identifier for the content. This may be an object identifier supplied by the user, or created by the device controller 130. The record may also include information relating to encoding, write protection, location, size, etc. Some or all of this information may also be returned to the user when the write is complete.

[00153] In step 975, the device controller 130 receives a content request. This request includes at least a content or object identifier to identify the requested content. This request may further include some or all of the information provided to the user after the write of the content was completed in step 970.

[00154] In step 980, the device controller 130 retrieves the requested content according to the storage device policy that has been defined. In step 985, the device controller 130 sends the content back to the user.

[00155] Fig. 9D illustrates an operational sequence of a policy-based write according to an implementation. The device controller receives a storage device policy from a user device 305. Receiving a storage device policy here can mean receiving an update to a storage device policy already in place. The storage device policy can be part of an overall collection of libraries 700 that create the framework for device controller 130 to operate. In an implementation, a user device 305 provides values for some of the supplied algorithms within the collection of libraries 700, and provides some entirely new rules.

[00156] These algorithms and rules are used to update the storage device policy on the device controller 130. In an embodiment, calls to and from one layer of the storage device policy made to a function in another layer of the storage device policy can be linked at the time the layer is loaded in the system. This method of linking at a late time allows for customized code or library entries to be deployed in the device controller 130.

[00157] The user device 305 then sends a request to the device controller 130 to store content. At a minimum, this request comprises content to be stored. In an implementation, the device controller 130 needs little information beyond the content itself, but the user may still include information such as an identification code, encoding information, of data protection information, for example. In an implementation, the content is sent with a specific instruction that the content be written and write protected so that the content cannot be overwritten in the future.

[00158] The device controller 130 uses the storage device policy to determine where and how to store the content from the user device 305. In an implementation, this determination includes a determination that the content will be written and write protected. This determination may be due to the specific instruction of write protection for the content delivered, or due to an overarching policy that all content (or some portion of content) stored on drive 100 should be written and write protected.

[00159] The device controller 130 writes the content to the storage media as determined above. In addition to writing the actual content, the device controller 130 can also store a record of the write (the storage information) in memory 135, including an indication of write protection. In an implementation, this information can include a unique identifier for the content. This may be an object identifier supplied by the user device 305, or created by the device controller 130. The record may also include information relating to encoding, write protection, location, size, etc. Some or all of this information may also be returned to the second user device 855 when the write is complete.

[00160] At some point, a second user device 855 sends a content request to device controller 130. This request includes at least a content or object identifier to identify the requested content. This request may further include some or all of the information provided to the user device 305 after the write of the content was completed.

[00161] This request can come from the second user device 855 for many reasons. For example, both user device 305 and second user device 855 may be part of the same network, and both user devices may have access to the device controller 130 through the network connection. Alternatively, user device 305 may have been disconnected from the network and replaced by the second user device 855 at some point in time after the storage device policy update and before the storage request. In another implementation, the drive 100 may have been disconnected from the network at some point after the storage device policy was updated. Drive 100 may have been connected to a new network that does not include user device 305. Since the customized storage device policy resides on the device controller 130, the storage device policy can move with the drive 100 to the new location.

[00162] The device controller 130 retrieves the requested content according to the storage device policy that has been defined. The device controller 130 then sends the content back to the second user device 855.

[00163] Fig. 10A illustrates a method of writing content 1000 according to an implementation. In step 1005, the device controller receives a storage device policy. Receiving a storage device policy here can mean receiving an update to a storage device policy already in place. The storage device policy can be part of an overall collection of libraries 700 that create the framework for device controller 130 to operate. In an implementation, a user selects some of the supplied algorithms within the collection of libraries 700.

[00164] In step 1010, these newly selected and newly supplied algorithms and rules are used to update the storage device policy on the device controller 130. In an embodiment, calls to and from one layer of the storage device policy made to a function in another layer of the storage device policy can be linked at the time the layer is loaded in the system. This method of linking at a late time allows for customized code or library entries to be deployed in the device controller 130.

[00165] A user sends a request to store content in step 1015. At a minimum, this request comprises content to be stored. In an implementation, the user may include information such as an identification code, encoding information, of data protection information, for example.

[00166] In step 1020, the device controller 130 uses the storage device policy to determine where and how to store the content. This determination can relate partially to the content being stored, and partially to the storage media 110. For example, if the content contains an indication

of priority level, such as information indicating that certain content is highly critical, the device controller 130, based on the storage device policy, may determine that the content should be stored on the storage media 110 at a low density, so the likelihood of data corruption will be minimal. Similarly, the storage device policy may also have an algorithm to determine how to avoid defects, and the storage device policy may instruct the device controller 130 to avoid storing highly critical content in sectors that have defects. Depending on what libraries exist in the device controller 130, and what the libraries control, many factors could be considered when deciding where and how to store the content.

[00167] In an implementation, this determination will include a determination of where storage information will be stored. For example, the storage information may be stored on the memory 135 on drive 100. Alternately, the storage information may be returned to the user device 305 that requested the content storage. The storage information could also be sent to a separate device, such as key device 505 for storage. In an implementation, when the storage information is sent to key device 505, the device controller 130 may determine not to store the information on memory 135. In step 1025, an indication of the location of the storage information is stored in memory 135, or inserted into a header 625 stored with the content on storage media 110.

[00168] In step 1030, the device controller 130 completes the write operation, and in step 1035, storage information for the content is written to memory 135. The storage information written to memory may not include all of the storage information. For example, the storage information written to memory 135 may include only an object identifier and a pointer to the storage location of the rest of the storage information. In this way, if the drive 100 is physically removed from its initial location, or for some reason key device 505 is removed, the content stored on storage media 110 can remain secure.

[00169] According to an implementation, drive 100 may be configured so that all data stored thereon has storage information stored in key device 505, thus requiring drive 100 to communicate with the key device 505 prior to retrieving any content. According to an implementation, content objects within drive 100 may be treated individually, such that certain objects have associated storage information stored on a key device 505, while others may not.

[00170] Fig. 10B illustrates an operational sequence of a policy-based write according to an implementation. The device controller receives a storage device policy from a user device

305. Receiving a storage device policy here can mean receiving an update to a storage device policy already in place. The storage device policy can be part of an overall collection of libraries 700 that create the framework for device controller 130 to operate. In an implementation, a user device 305 provides values for some of the supplied algorithms within the collection of libraries 700, and provides some entirely new rules.

[00171] These algorithms and rules are used to update the storage device policy on the device controller 130. In an embodiment, calls to and from one layer of the storage device policy made to a function in another layer of the storage device policy can be linked at the time the layer is loaded in the system. This method of linking at a late time allows for customized code or library entries to be deployed in the device controller 130.

[00172] A user device 305 then sends a request to the device controller 130 to store content. At a minimum, this request comprises content to be stored. In an implementation, the device controller 130 needs little information beyond the content itself, but the user may still include information such as an identification code, encoding information, of data protection information, for example.

[00173] The device controller 130 uses the storage device policy to identify where and how to store the content from the user device 305. This determination may include a determination on where to store storage information. This may be due to an overarching policy that all content stored on the drive 100 should store storage information on key device 505, for example. In an implementation, prior to recording the content to the storage media 110, the device controller reaches out to the key device 505 to request a location pointer for the storage information for the content to be stored (i.e. some indication of where the storage information will be stored). This pointer is returned to the device controller, which inserts the pointer into a header 625 that is inserted into the content to be stored. The content, with the header 625 is then recorded on storage media 110. In an implementation, the location pointer for indicating the location of the storage information (which in turn indicates how to read the stored content) can be provided by the device controller 130 to the key device 505. The key device 505 can then store the storage information at the location indicated by the location pointer.

[00174] Fig. 10C illustrates a method of reading content 1050 according to an implementation. In step 1045, the device controller receives a storage device policy. Receiving a storage device policy here can mean receiving an update to a storage device policy already in

place. The storage device policy can be part of an overall collection of libraries 700 that create the framework for device controller 130 to operate. In an implementation, a user selects some of the supplied algorithms within the collection of libraries 700.

[00175] In step 1055, these newly selected and newly supplied algorithms and rules are used to update the storage device policy on the device controller 130. In an embodiment, calls to and from one layer of the storage device policy made to a function in another layer of the storage device policy can be linked at the time the layer is loaded in the system. This method of linking at a late time allows for customized code or library entries to be deployed in the device controller 130.

[00176] A user sends a request to store content in step 1060. At a minimum, this request comprises content to be stored. In an implementation, the user may include information such as an identification code, encoding information, of data protection information, for example. The device controller 130 uses the storage device policy to determine where and how to store the content. In an implementation, this determination includes a determination that the storage information for the content should be stored as externally to the drive 100 such that is may have additional security. This determination could be based on an entire drive 100 being designated to do so, or as certain sectors or tracks or regions being pre-designated as such. Alternatively, an individual object may be designated to be so treated. According to an implementation, this designation can be flexible, and change over time.

[00177] Any determination of where or how to store the content can relate partially to the content being stored, and partially to the storage media 110. For example, if the content contains an indication of priority level, such as information indicating that certain content is highly critical, the device controller 130, based on the storage device policy, may determine that the content should be stored on the storage media 110 at a low density, so the likelihood of data corruption will be minimal. Similarly, the storage device policy may also have an algorithm to determine how to avoid defects, and the storage device policy may instruct the device controller 130 to avoid storing highly critical content in sectors that have defects. Depending on what libraries exist in the device controller 130, and what the libraries control, many factors could be considered when deciding where and how to store the content.

[00178] In step 1065, The device controller 130 can insert an indication of where the storage information will be stored for the content to be stored.

[00179] In step 1070, the device controller can write the content to the storage media as determined, including an indication of a location of storage information. In addition to writing the actual content the device controller 130 can also store a record of the write (the storage information) in memory 135. In an implementation, the storage information stored on memory 135 is only a subset of the storage memory, for instance only including an object identifier, and a location of the full storage information.

[00180] In step 1075, the device controller 130 receives a content request. This request includes at least a content or object identifier to identify the requested content. This request may further include some or all of the information provided to the user after the write of the content was completed in step 1070.

[00181] In step 1080, the device controller 130 reaches out to the location identified by the pointer (for example the key device 505) for the storage information to determine the storage information. This storage information may include track, sector, or region information indicating where the content is stored on storage media 110. In an implementation, the storage information may include detailed location information, such as polar or cartesian coordinates, slope, derivative or other information identifying the specific location of the content storage. In an implementation, the content could be irretrievable without this specific storage information. In step 1085, the device controller 130 receives the storage information from the key device 505.

[00182] In step 1090, the device controller 130 uses the storage information received from key device 505, together with the storage device policy to retrieve the requested information. In step 1095, the device controller 130 returns the content to the requester.

[00183] Fig. 10D illustrates an operational sequence of a policy-based write according to an implementation. The device controller receives a storage device policy from a user device 305. Receiving a storage device policy here can mean receiving an update to a storage device policy already in place. The storage device policy can be part of an overall collection of libraries 700 that create the framework for device controller 130 to operate. In an implementation, a user device 305 provides values for some of the supplied algorithms within the collection of libraries 700, and provides some entirely new rules.

[00184] These algorithms and rules are used to update the storage device policy on the device controller 130. In an embodiment, calls to and from one layer of the storage device policy made to a function in another layer of the storage device policy can be linked at the time

the layer is loaded in the system. This method of linking at a late time allows for customized code or library entries to be deployed in the device controller 130.

[00185] A user device 305 then sends a request to the device controller 130 to store content. At a minimum, this request comprises content to be stored. In an implementation, the device controller 130 needs little information beyond the content itself, but the user may still include information such as an identification code, encoding information, of data protection information, for example.

[00186] The device controller 130 uses the storage device policy to identify where and how to store the content from the user device 305. This determination may include a determination on where to store storage information. This may be due to an overarching policy that all content stored on the drive 100 should store storage information on key device 505, for example. In an implementation, prior to recording the content to the storage media 110, the device controller 130 determines that storage device information will be stored on a key device 505. This location is inserted into a header 625 that is inserted into the content to be stored. The content, with the header 625 is then recorded on storage media 110.

[00187] At some point, user device 305 sends a content request to device controller 130. This request includes at least a content or object identifier to identify the requested content. This request may further include some or all of the information provided to the user device 305 after the write of the content was completed.

[00188] The device controller reaches out to the key device 505 to retrieve the storage information. It should be understood that the key device 505 may include security protections to ensure that only authorized users can retrieve the storage information. The key device 505 sends the storage information back to the device controller 130, and the device controller uses the storage information, together with the storage device policy, to retrieve the requested content. The device controller 130 then sends the content back to the second user device 855.

[00189] Fig. 11A illustrates a method of writing content 1100 according to an implementation. In step 1105, the device controller receives a storage device policy. Receiving a storage device policy here can mean receiving an update to a storage device policy already in place. The storage device policy can be part of an overall collection of libraries 700 that create the framework for device controller 130 to operate. In an implementation, a user selects some of

the supplied algorithms within the collection of libraries 700, and provides an entirely new library of defect avoidance algorithms and rules.

[00190] In step 1110, these newly selected and newly supplied algorithms and rules are used to update the storage device policy on the device controller 130. In an embodiment, calls to and from one layer of the storage device policy made to a function in another layer of the storage device policy can be linked at the time the layer is loaded in the system. This method of linking at a late time allows for customized code or library entries to be deployed in the device controller 130. The storage device policy may be defined such that each object that is stored on storage media 110 may be handled independently, i.e. with its own distinct storage policy. In this way, one object can be stored with user preferences for increased data security, while another may be stored utilizing preferences for increased storage space, and still another may emphasize redundancy.

[00191] A user sends a request to store content in step 1115. At a minimum, this request comprises content to be stored. In an implementation, the user may include information such as an identification code, encoding information, of data protection information, for example.

[00192] In step 1120, the device controller 130 uses the storage device policy to determine where and how to store the content. This determination can relate partially to the content being stored, and partially to the storage media 110. For example, if the content contains an indication of priority level, such as information indicating that certain content is highly critical, the device controller 130, based on the storage device policy, may determine that the content should be stored on the storage media 110 at a low density, so the likelihood of data corruption will be minimal. Similarly, the storage device policy may also have an algorithm to determine how to avoid defects, and the storage device policy may instruct the device controller 130 to avoid storing highly critical content in sectors that have defects. Depending on what libraries exist in the device controller 130, and what the libraries control, many factors could be considered when deciding where and how to store the content.

[00193] In step 1125, the device controller 130 will store the content how and where determined. The device controller 130 may further store storage information, indicate write-protection, etc.

[00194] In step 1130, the device controller 130 receives a second request to store content, comprising a content to be stored. The device controller, in step 1135 uses the storage device

policy to determine where and how to store the content. In an implementation, the device controller 130 determines to store the content in this second request differently that the device controller 130 stored the first content. In step 1140, the hard drive stores the second content differently than it stored the first content,

[00195] Fig. 11B illustrates an operational sequence of a policy-based write according to an implementation. The device controller receives a storage device policy from a user device 305. Receiving a storage device policy here can mean receiving an update to a storage device policy already in place. The storage device policy can be part of an overall collection of libraries 700 that create the framework for device controller 130 to operate. In an implementation, a user device 305 provides values for some of the supplied algorithms within the collection of libraries 700, and provides some entirely new rules.

[00196] These algorithms and rules are used to update the storage device policy on the device controller 130. In an embodiment, calls to and from one layer of the storage device policy made to a function in another layer of the storage device policy can be linked at the time the layer is loaded in the system. This method of linking at a late time allows for customized code or library entries to be deployed in the device controller 130.

[00197] A second user device 855 then sends a request to the device controller 130 to store content. At a minimum, this request comprises content to be stored. In an implementation, the device controller 130 needs little information beyond the content itself, but the user may still include information such as an identification code, encoding information, of data protection information, for example. This request can come from the second user device 855 for many reasons. For example, both user device 305 and second user device 855 may be part of the same network, and both user devices may have access to the device controller 130 through the network connection. Alternatively, user device 305 may have been disconnected from the network and replaced by the second user device 855 at some point in time after the storage device policy update and before the storage request. In another implementation, the drive 100 may have been disconnected from the network at some point after the storage device policy was updated. Drive 100 may have been connected to a new network that does not include user device 305. Since the customized storage device policy resides on the device controller 130, the storage device policy can move with the drive 100 to the new location.

[00198] The device controller 130 uses the storage device policy to identify where and how to store the content from the second user device 855. This determination can relate partially to the content being stored, and partially to the storage media 110. For example, if the content contains an indication of priority level, such as information indicating that certain content is highly critical, the device controller 130, based on the storage device policy, may determine that the content should be stored on the storage media 110 at a low density, so the likelihood of data corruption will be minimal. Similarly, the storage device policy may also have an algorithm to determine how to avoid defects, and the storage device policy may instruct the device controller 130 to avoid storing highly critical content in sectors that have defects. Depending on what libraries exist in the device controller 130, and what the libraries control, many factors could be considered when deciding where and how to store the content.

[00199] The device controller 130 will store the content in accordance with the determination of where and how to store the content.

[00200] At some point, the device controller 130 receives a second request to store content, comprising at least the content to be stored. This request may come from a device distinct from the second user device 855, such as the user device 305. It should be noted that the second request may also be received from an entirely distinct device that did not participate in defining the storage device policy. As above, the device controller 130 determines where and how to store the second content. According to the storage device policy, this may be distinct from how the first content was stored. The storage device policy may define that certain sectors or regions be stored in certain ways, or may leave flexibility that each individual object can be stored with its own policy determinations. The device controller 130 can then store the content according to the storage device policy.

[00201] Fig. 11C illustrates a method of reading content 1150 according to an implementation. In step 1155, the device controller receives a storage device policy. Receiving a storage device policy here can mean receiving an update to a storage device policy already in place. The storage device policy can be part of an overall collection of libraries 700 that create the framework for device controller 130 to operate. In an implementation, a user selects some of the supplied algorithms within the collection of libraries 700, and provides an entirely new library of defect avoidance algorithms and rules.

[00202] In step 1160, these newly selected and newly supplied algorithms and rules are used to update the storage device policy on the device controller 130. In an embodiment, calls to and from one layer of the storage device policy made to a function in another layer of the storage device policy can be linked at the time the layer is loaded in the system. This method of linking at a late time allows for customized code or library entries to be deployed in the device controller 130.

[00203] A user sends a request to retrieve content in step 1165. At a minimum, this request comprises a content identifier. In step 1170, the device controller can retrieve the requested content in accordance with the storage device policy, and in step 1175, the device controller returns the content to the user.

[00204] In step 1180, the device controller 130 receives a second request for content, comprising at least a second content identifier. In an implementation, this second content may be stored according to different storage device policy rules that was the first content. Consequently, the device controller 130 will use different storage device policy rules to retrieve the second content in step 1185. The device controller 130 can then return the content to the requesting user in step 1190. It is of note that the content stored on storage media 110 can be independently written according to storage device policy at any level – i.e. each individual object may have different value trade-offs within the same drive 100.

[00205] Fig. 11D illustrates an operational sequence of a policy-based write according to an implementation. The device controller receives a storage device policy from a user device 305. Receiving a storage device policy here can mean receiving an update to a storage device policy already in place. The storage device policy can be part of an overall collection of libraries 700 that create the framework for device controller 130 to operate. In an implementation, a user device 305 provides values for some of the supplied algorithms within the collection of libraries 700, and provides some entirely new rules.

[00206] These algorithms and rules are used to update the storage device policy on the device controller 130. In an embodiment, calls to and from one layer of the storage device policy made to a function in another layer of the storage device policy can be linked at the time the layer is loaded in the system. This method of linking at a late time allows for customized code or library entries to be deployed in the device controller 130.

[00207] The user device 305 then sends a request to the device controller 130 to retrieve content. At a minimum, this request comprises a content identifier. In an implementation, the device controller 130 needs little information beyond the content identifier itself, but the user may still include any of the storage information provided by the device controller when the content was stored in storage media 110.

[00208] The device controller 130 uses the storage device policy to retrieve the content from the storage media 110. The device controller then returns that content to the user device 305.

[00209] A second user device 855 then sends a request to the device controller 130 to retrieve content. At a minimum, this request comprises a content identifier. The storage device policy may indicate distinct rules for this content than was used to store the first content. Consequently, the device controller 130 may use different storage device policy rules to retrieve the second requested content than it used to retrieve the first requested content. After retrieving the content, the device controller 130 returns the content to the second user device 855.

[00210] Referring to Figure 12, computing system 1202 may comprise a micro-processor and other circuitry that retrieves and executes software 1205 from storage system 1203. Computing system 1202 may be implemented within a single processing device, but may also be distributed across multiple processing devices or sub-systems that cooperate in executing program instructions. Examples of computing system 1202 include general purpose central processing units, application specific processors, and logic devices, as well as any other type of processing device, combinations, or variations thereof.

[00211] Storage system 1203 may comprise any computer readable storage media readable by computing system 1202 and capable of storing software 1205. Storage system 1203 may include volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information, such as computer readable instructions, data structures, program modules, or other data. Examples of storage media include random access memory, read only memory, magnetic disks, optical disks, flash memory, virtual memory and non-virtual memory, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or other suitable storage media, except for propagated signals. In no case is the computer readable storage media a propagated signal.

[00212] In addition to computer readable storage media, in some implementations storage system 1203 may also include computer readable communication media over which at least some of software 1205 may be communicated internally or externally. Storage system 1203 may be implemented as a single storage device, but may also be implemented across multiple storage devices or sub-systems co-located or distributed relative to each other. Storage system 1203 may comprise additional elements, such as a controller, capable of communicating with computing system 1202 or possibly other systems.

[00213] Software 1205 may be implemented in program instructions and among other functions may, when executed by computing system 1202, direct computing system 1202 to operate as described with respect to the various operational scenarios, sequences, and processes illustrated herein. For example, software 1205 may include program instructions for implementing and updating storage device policies.

[00214] In particular, the program instructions may include various components or modules that cooperate or otherwise interact to carry out the various processes and operational scenarios described herein. The various components or modules may be embodied in compiled or interpreted instructions, or in some other variation or combination of instructions. The various components or modules may be executed in a synchronous or asynchronous manner, serially or in parallel, in a single threaded environment or multi-threaded, or in accordance with any other suitable execution paradigm, variation, or combination thereof. Software 1205 may include additional processes, programs, or components, such as operating system software, virtual machine software, or other application software, in addition to or that include storage process 1206. Software 1205 may also comprise firmware or some other form of machine-readable processing instructions executable by computing system 1202.

[00215] In general, software 1205 may, when loaded into computing system 1202 and executed, transform a suitable apparatus, system, or device (of which computing system 1201 is representative) overall from a general-purpose computing system into a special-purpose computing system enhance calendars of interest. Indeed, encoding software 1205 on storage system 1203 may transform the physical structure of storage system 1203. The specific transformation of the physical structure may depend on various factors in different implementations of this description. Examples of such factors may include, but are not limited to, the technology used to implement the storage media of storage system 1203 and whether the

computer-storage media are characterized as primary or secondary storage, as well as other factors.

[00216] For example, if the computer readable storage media are implemented as semiconductor-based memory, software 1205 may transform the physical state of the semiconductor memory when the program instructions are encoded therein, such as by transforming the state of transistors, capacitors, or other discrete circuit elements constituting the semiconductor memory. A similar transformation may occur with respect to magnetic or optical media. Other transformations of physical media are possible without departing from the scope of the present description, with the foregoing examples provided only to facilitate the present discussion.

[00217] Communication interface system 1207 may include communication connections and devices that allow for communication with other computing systems (not shown) over communication networks (not shown). Examples of connections and devices that together allow for inter-system communication may include network interface cards, antennas, power amplifiers, RF circuitry, transceivers, and other communication circuitry. The connections and devices may communicate over communication media to exchange communications with other computing systems or networks of systems, such as metal, glass, air, or any other suitable communication media. The aforementioned media, connections, and devices are well known and need not be discussed at length here.

[00218] User interface system 1209 is optional and may include a keyboard, a mouse, a voice input device, a touch input device for receiving a touch gesture from a user, a motion input device for detecting non-touch gestures and other motions by a user, and other comparable input devices and associated processing elements capable of receiving user input from a user. Output devices such as a display, speakers, haptic devices, and other types of output devices may also be included in user interface system 1209. In some cases, the input and output devices may be combined in a single device, such as a display capable of displaying images and receiving touch gestures. The aforementioned user input and output devices are well known in the art and need not be discussed at length here.

[00219] Communication between computing system 1201 and other computing systems (not shown), may occur over a communication network or networks and in accordance with various communication protocols, combinations of protocols, or variations thereof. Examples

include intranets, internets, the Internet, local area networks, wide area networks, wireless networks, wired networks, virtual networks, software defined networks, data center buses, computing backplanes, or any other type of network, combination of network, or variation thereof. The aforementioned communication networks and protocols are well known and need not be discussed at length here. However, some communication protocols that may be used include, but are not limited to, the Internet protocol (IP, IPv4, IPv6, etc.), the transfer control protocol (TCP), and the user datagram protocol (UDP), as well as any other suitable communication protocol, variation, or combination thereof.

[00220] The included descriptions and figures depict specific embodiments to teach those skilled in the art how to make and use the best mode. By way of example, many of the implementations discussed described a magnetic hard disk drive. The discussion should also be ready to include other types of storage, such solid-state drives. For the purpose of teaching inventive principles, some conventional aspects have been simplified or omitted. Those skilled in the art will appreciate variations from these embodiments that fall within the scope of the invention. Those skilled in the art will also appreciate that the features described above may be combined in various ways to form multiple embodiments. As a result, the invention is not limited to the specific embodiments described above, but only by the claims and their equivalents.

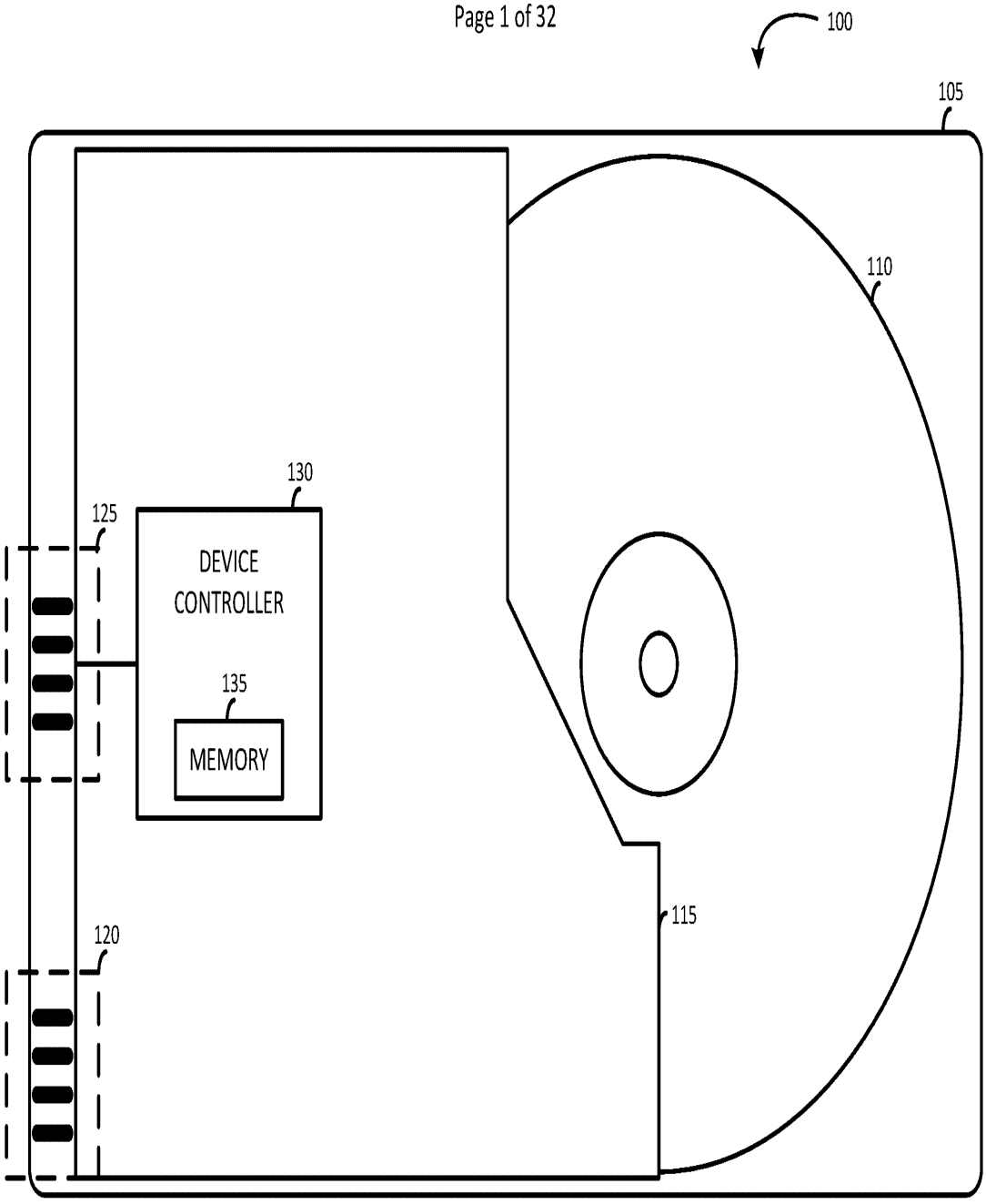


FIG. 1A

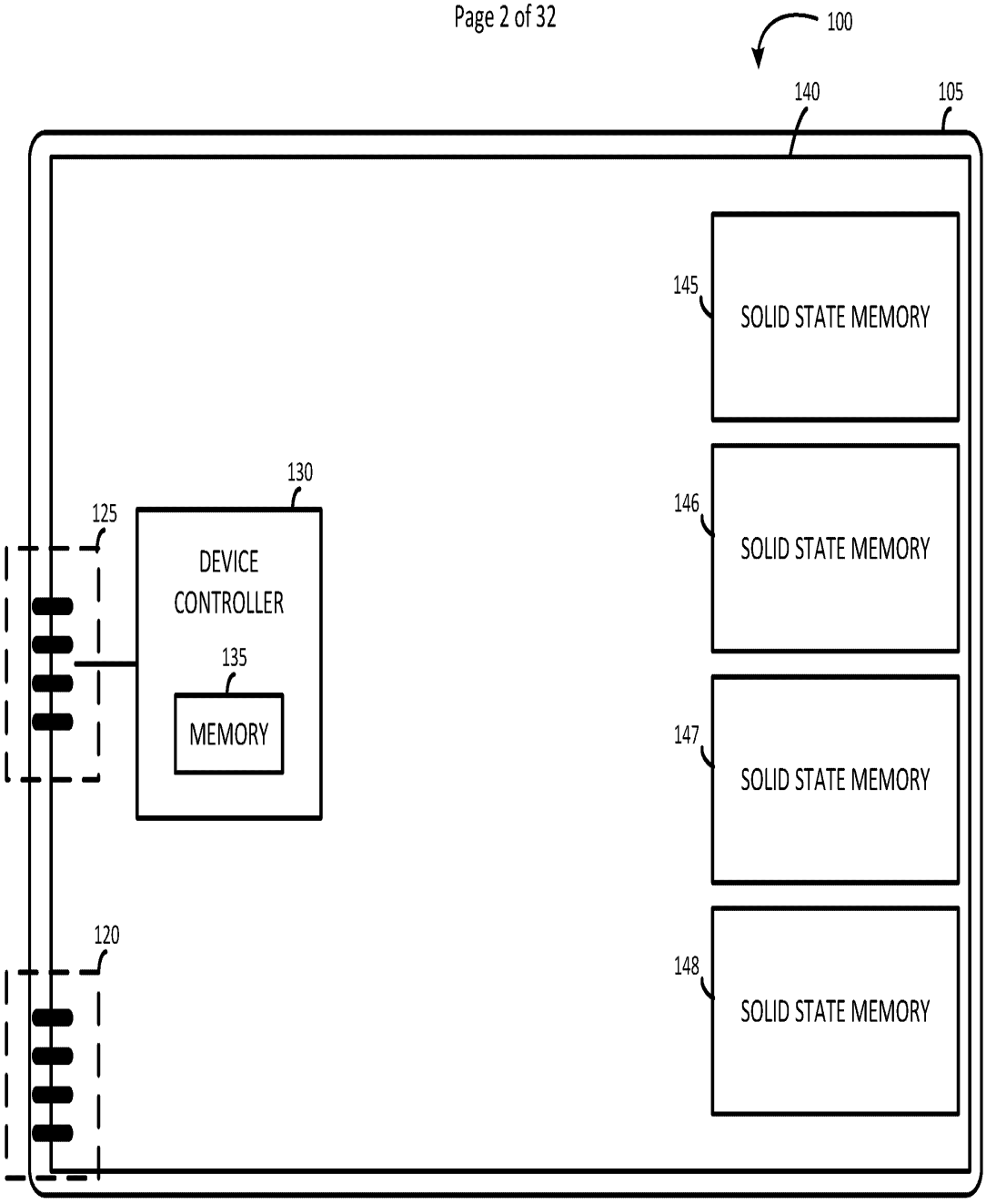

100
140
105
145
SOLID STATE MEMORY
146
SOLID STATE MEMORY
147
SOLID STATE MEMORY
148
SOLID STATE MEMORY
130
125
DEVICE
CONTROLLER
135
MEMORY
120

FIG. 1B

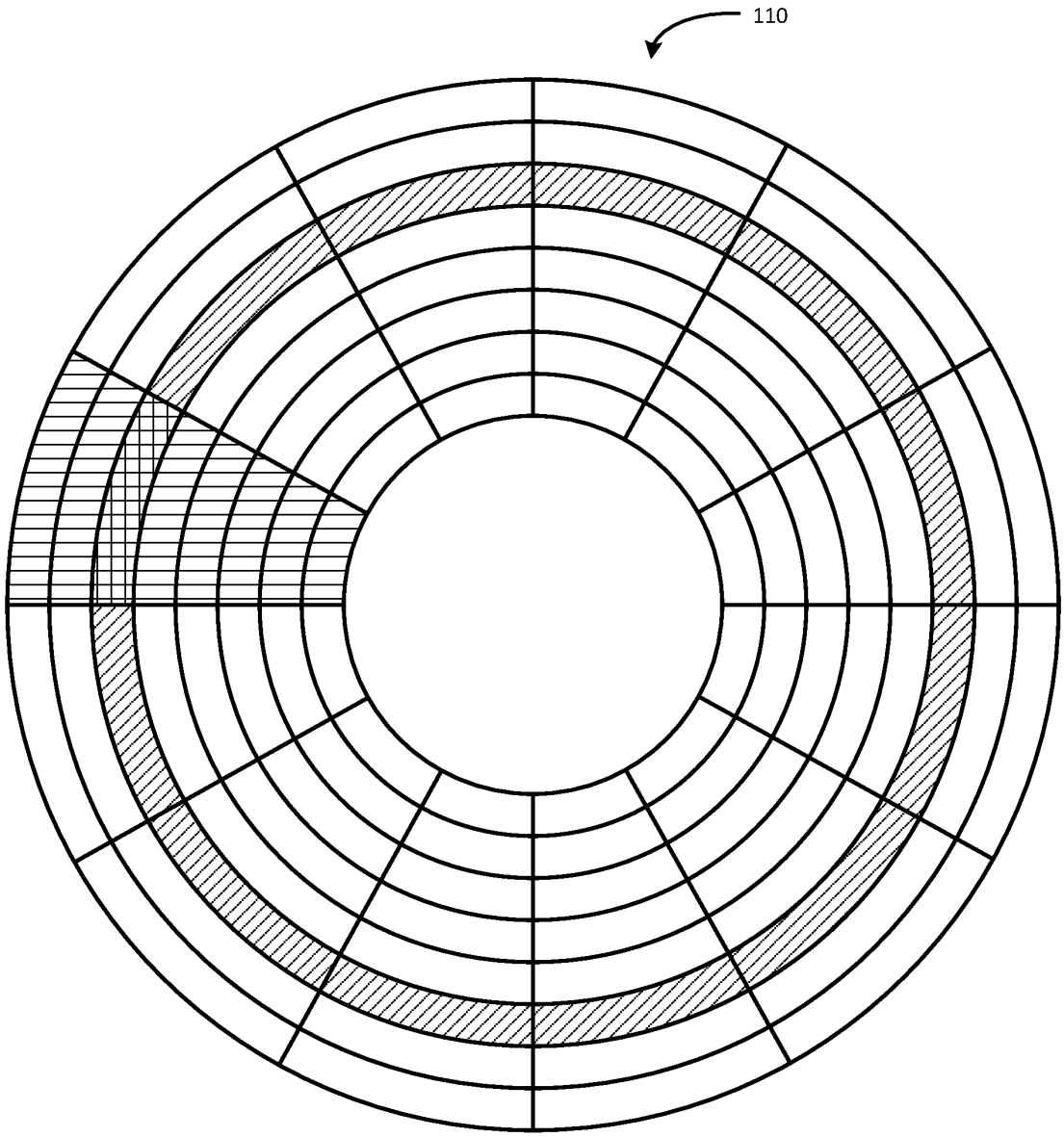


FIG. 2A

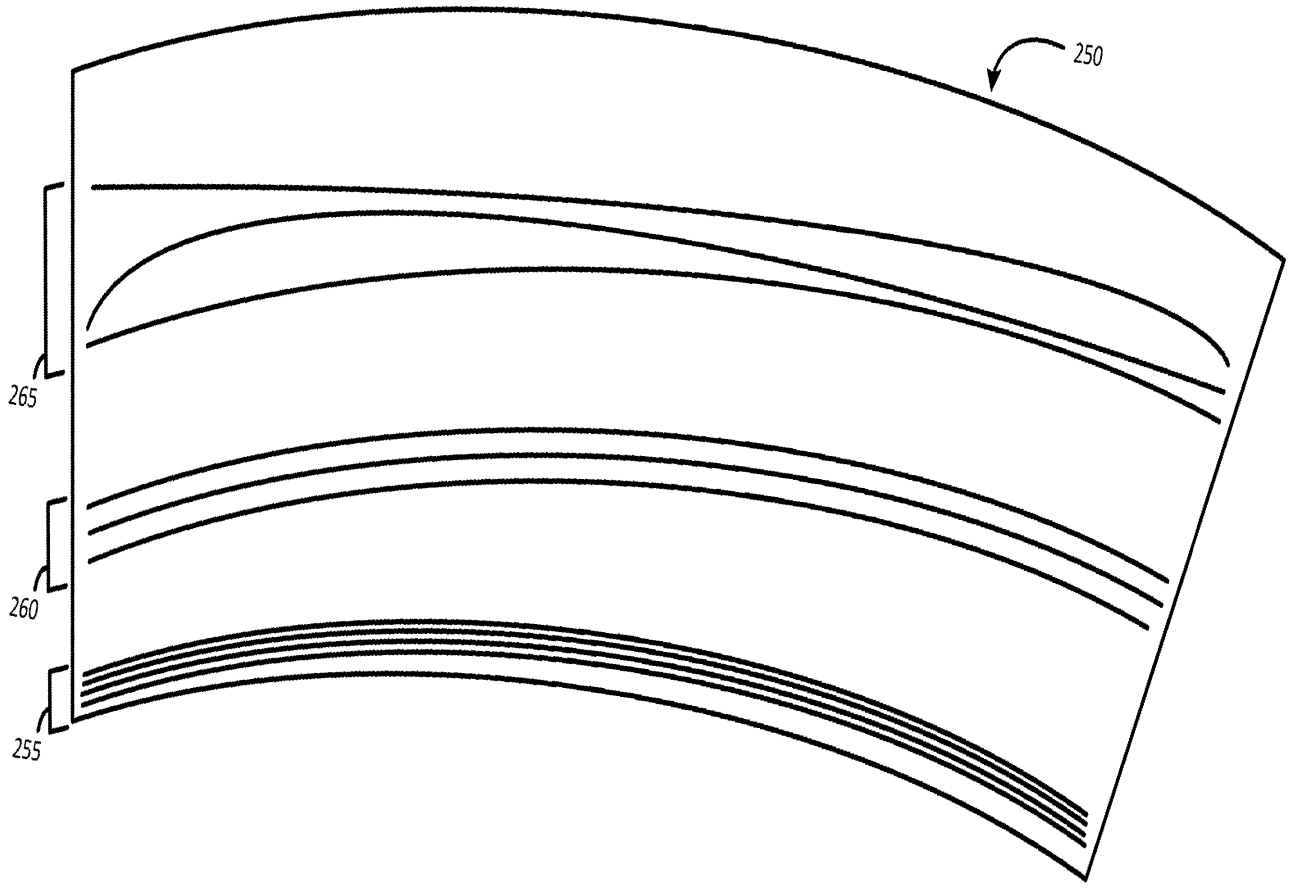


FIG. 2B

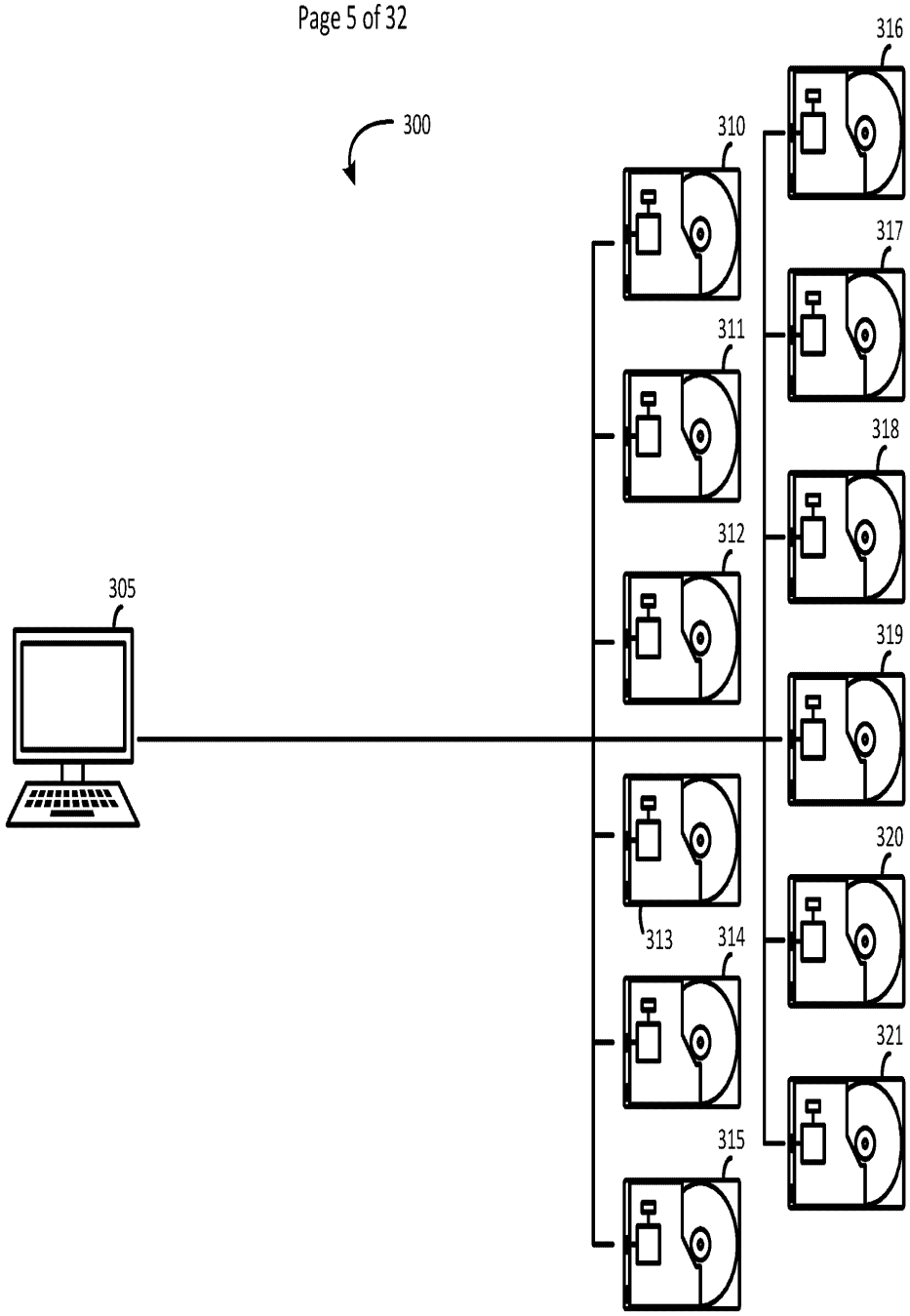


FIG. 3

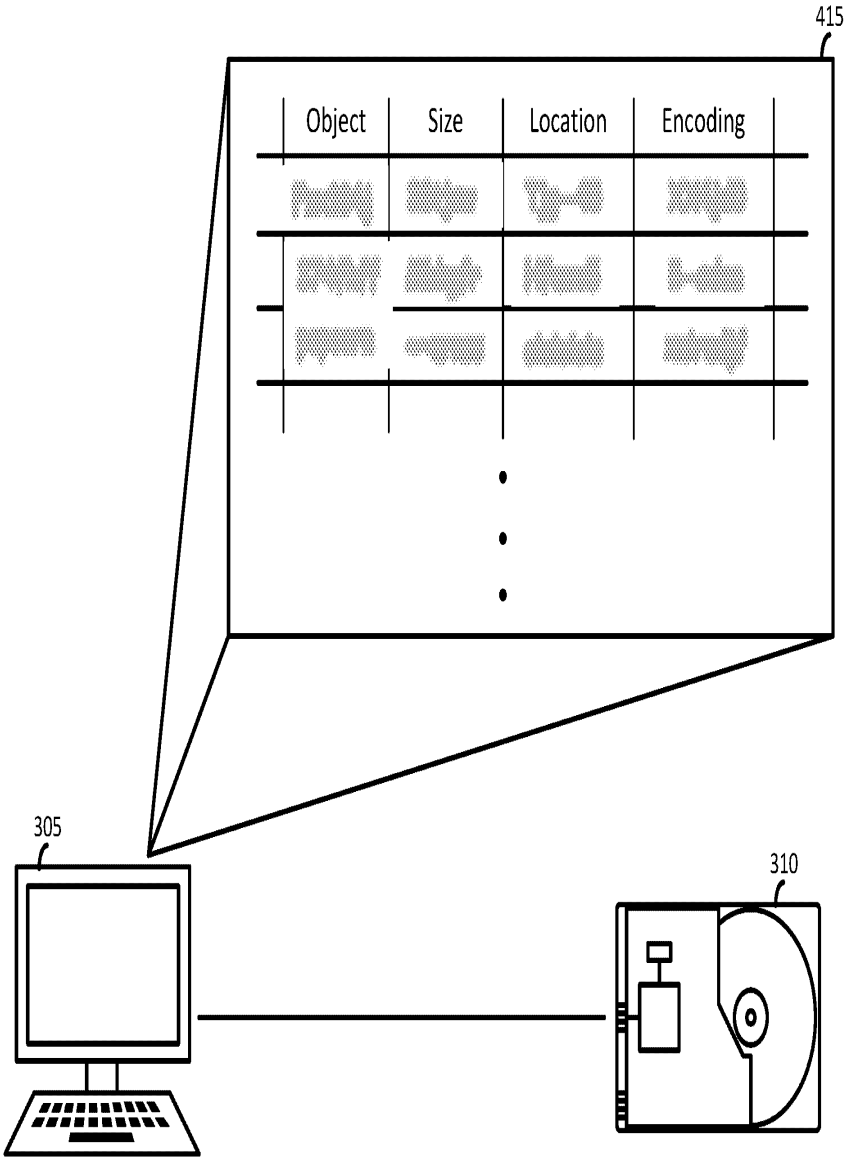


FIG. 4A

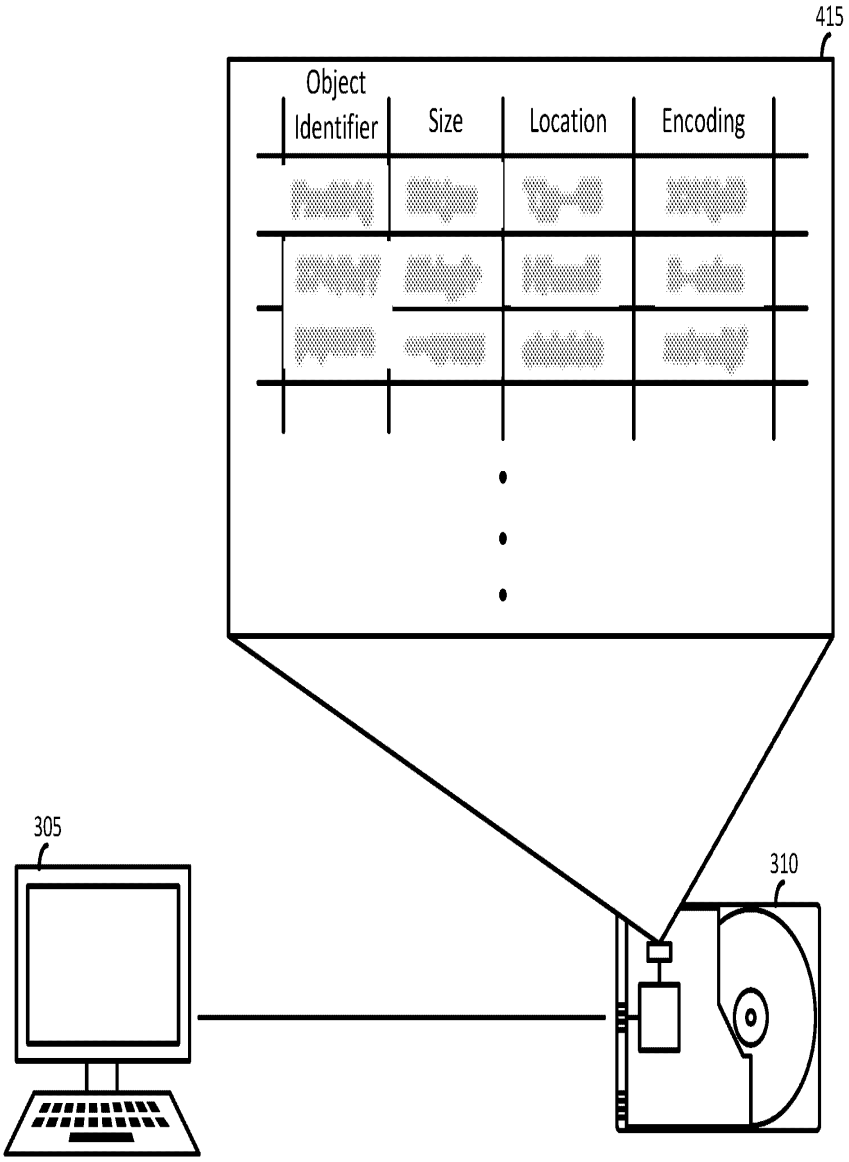


FIG. 4B

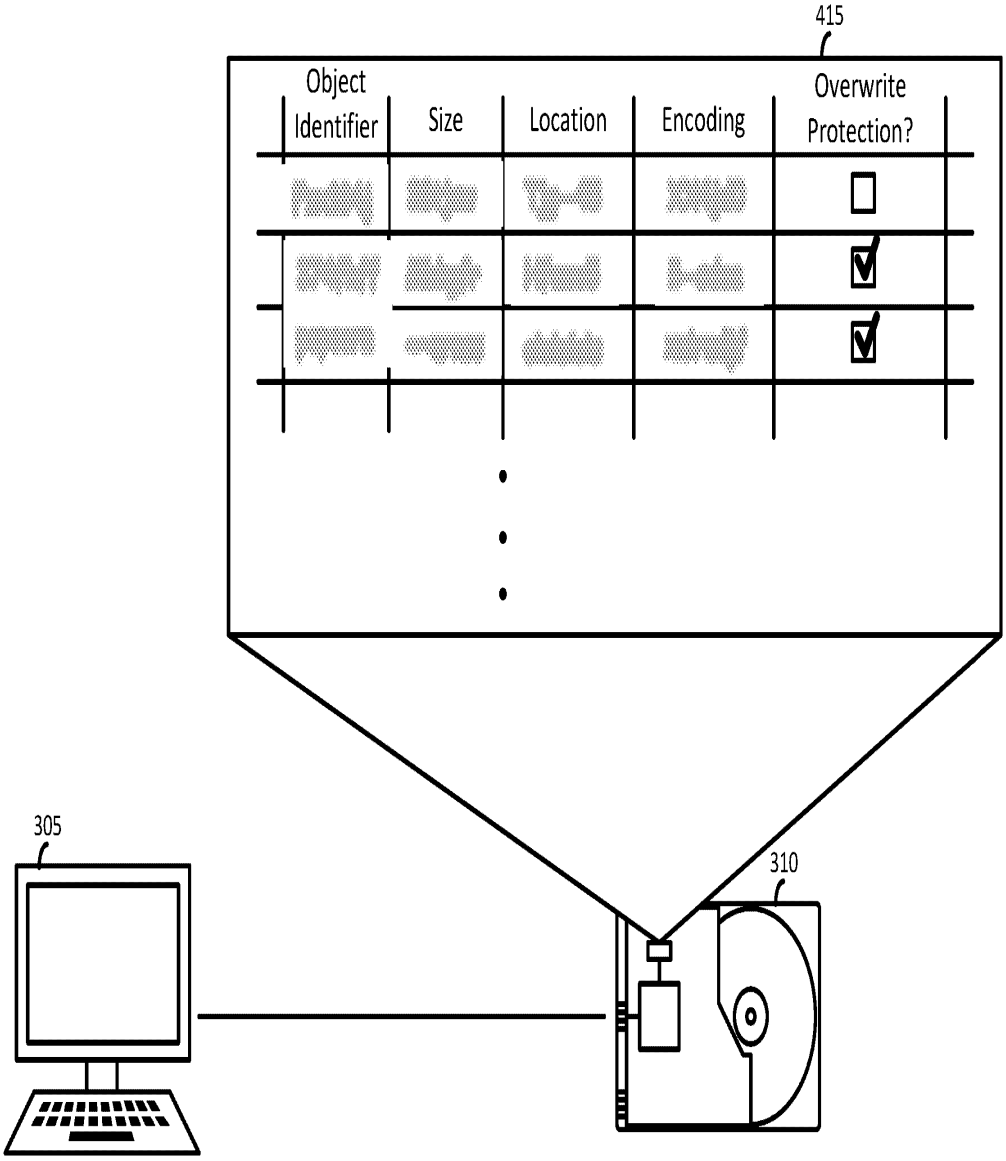

415
Object Identifier
Size
Location
Encoding
Overwrite Protection?
305
310

FIG. 4C

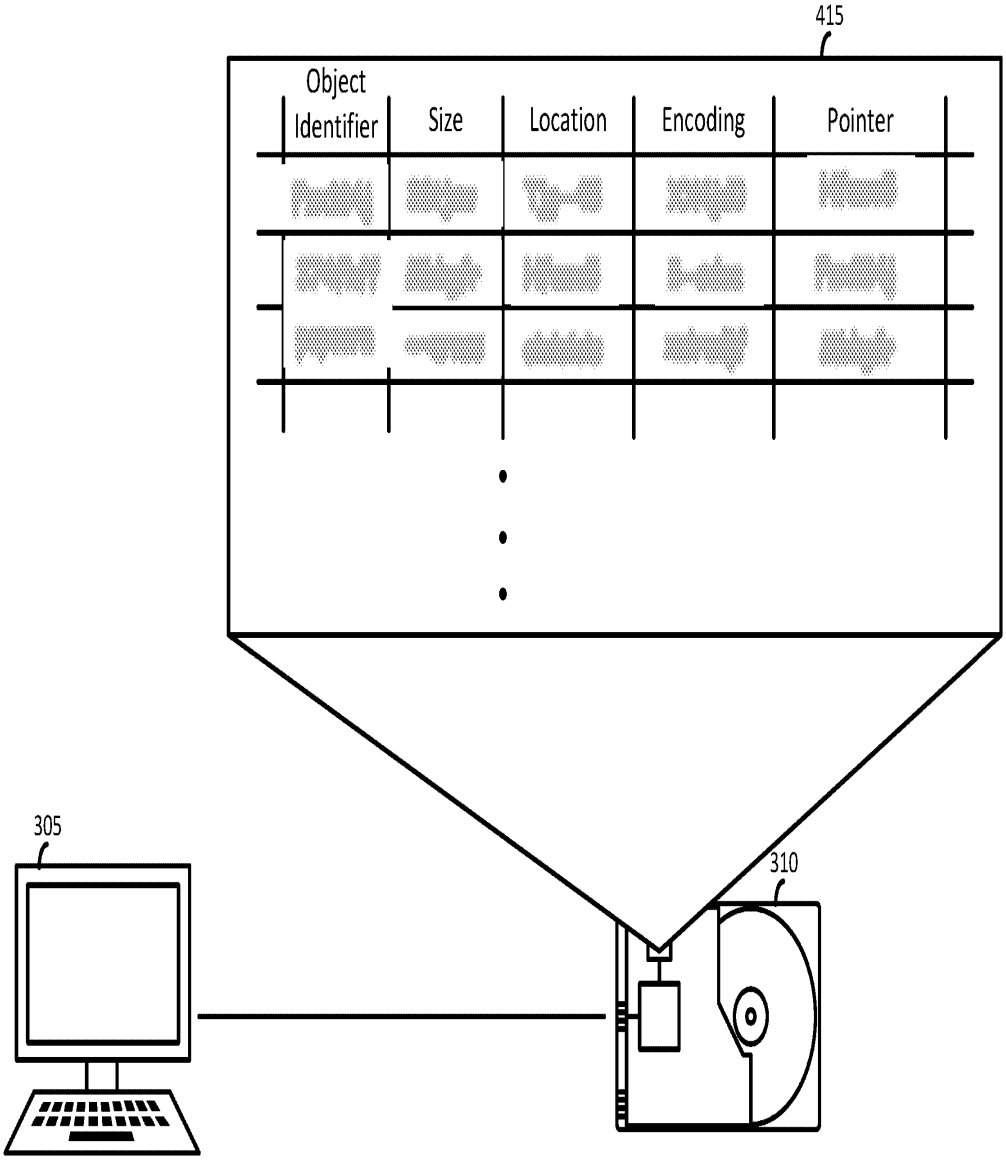

415
Object Identifier
Size
Location
Encoding
Pointer
305
310

FIG. 4D

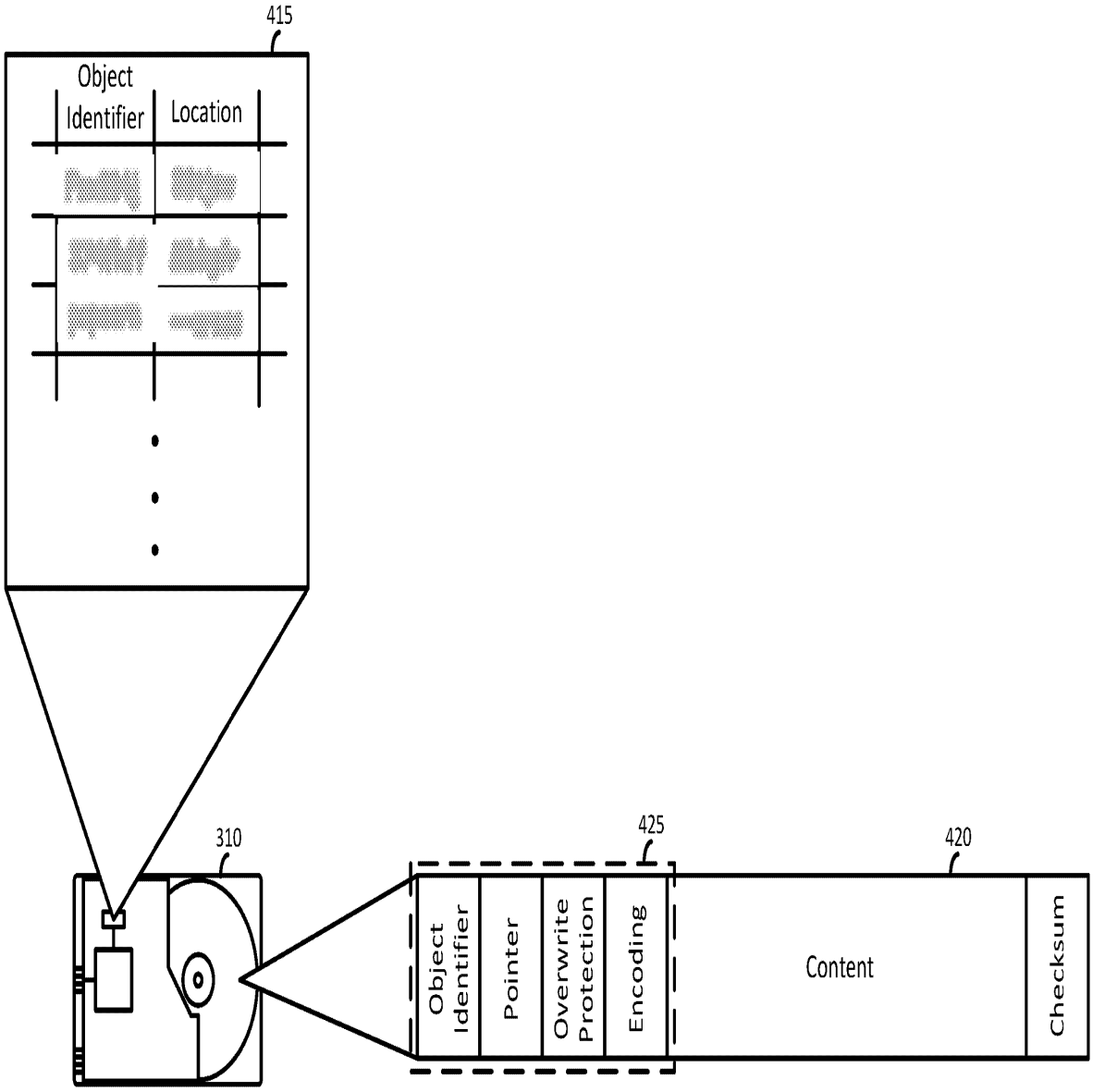

415
Object Identifier
Location
310
425
420
Object Identifier
Pointer
Overwrite Protection
Encoding
Content
Checksum

FIG. 4E

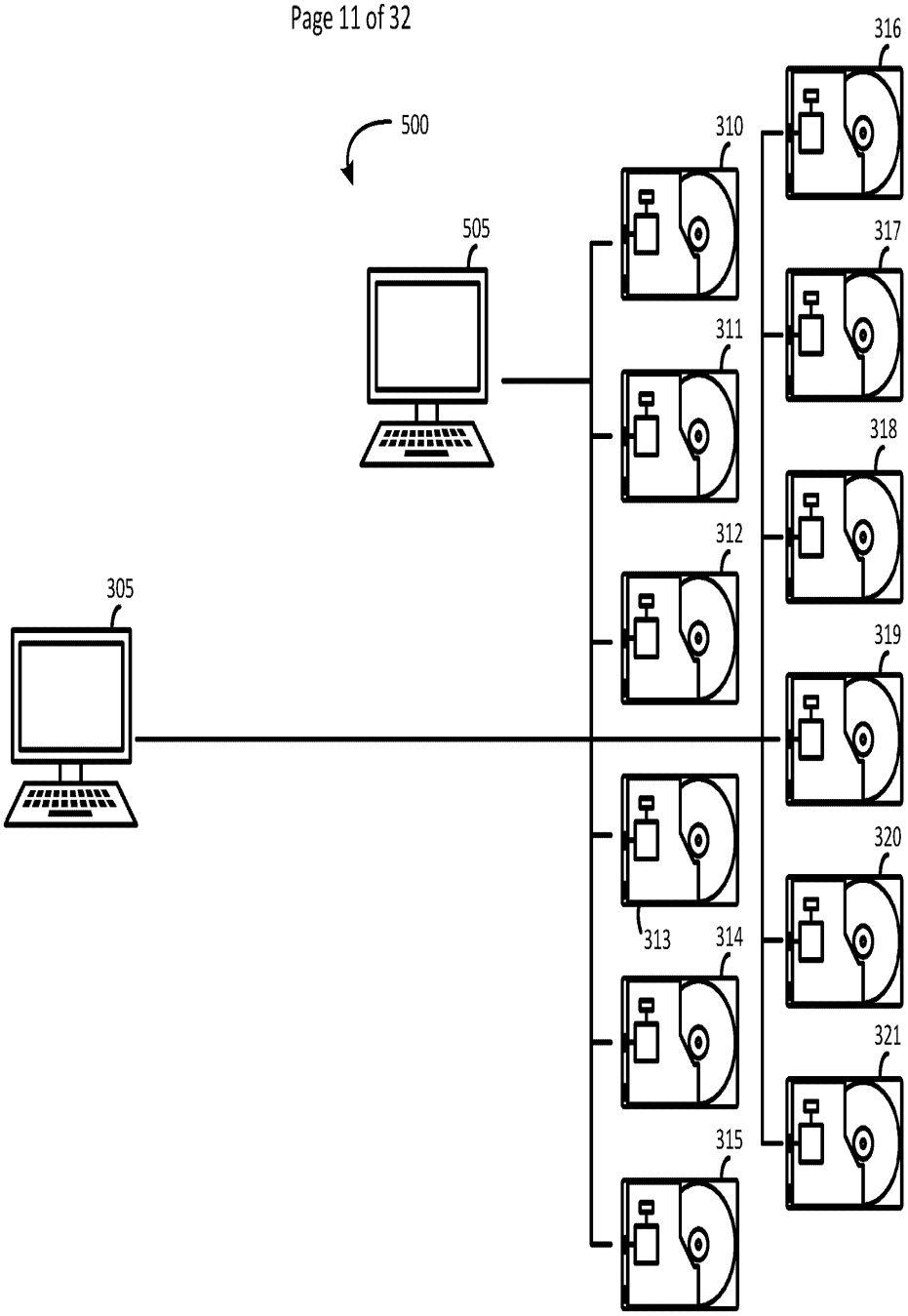


FIG. 5

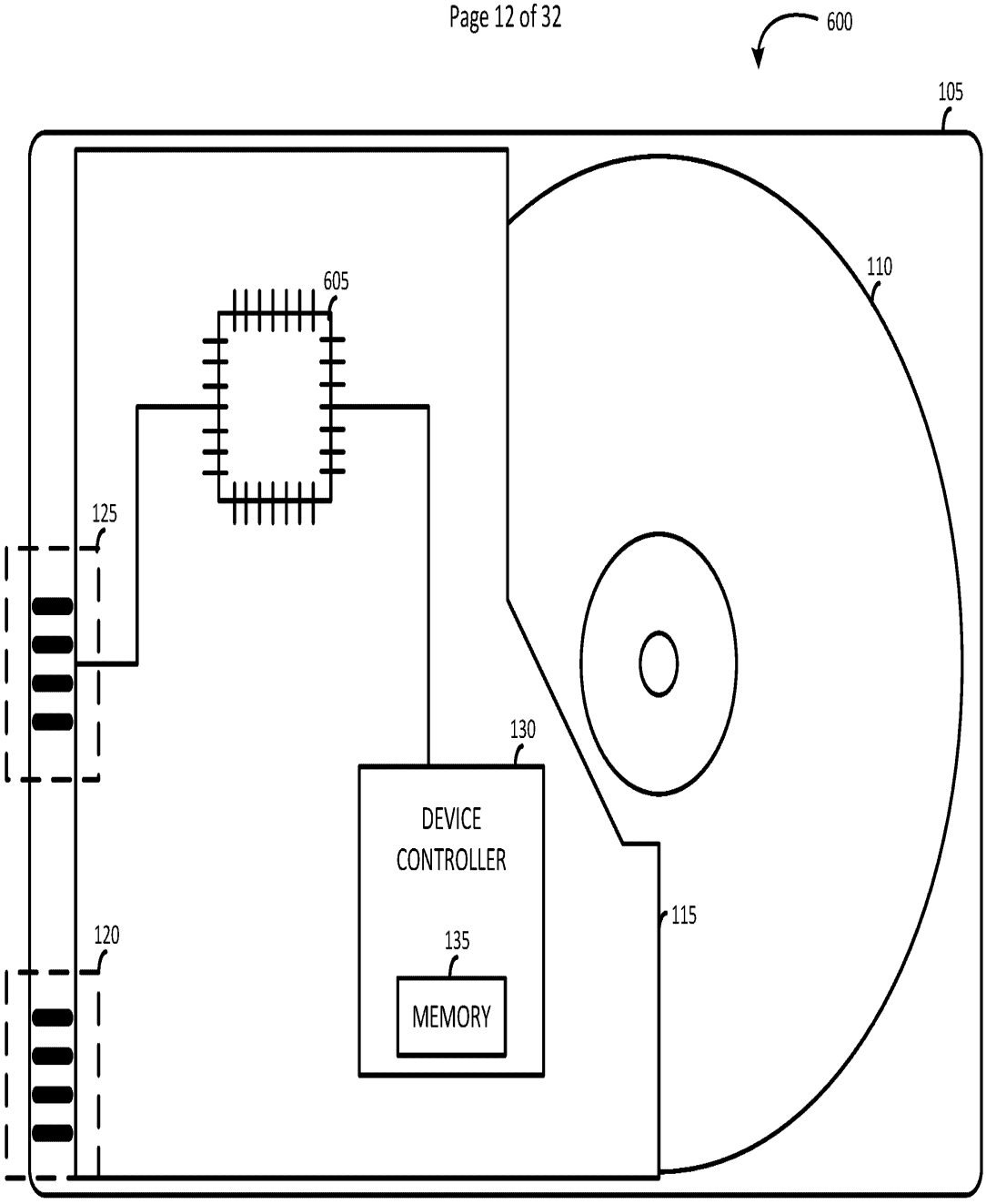


FIG. 6

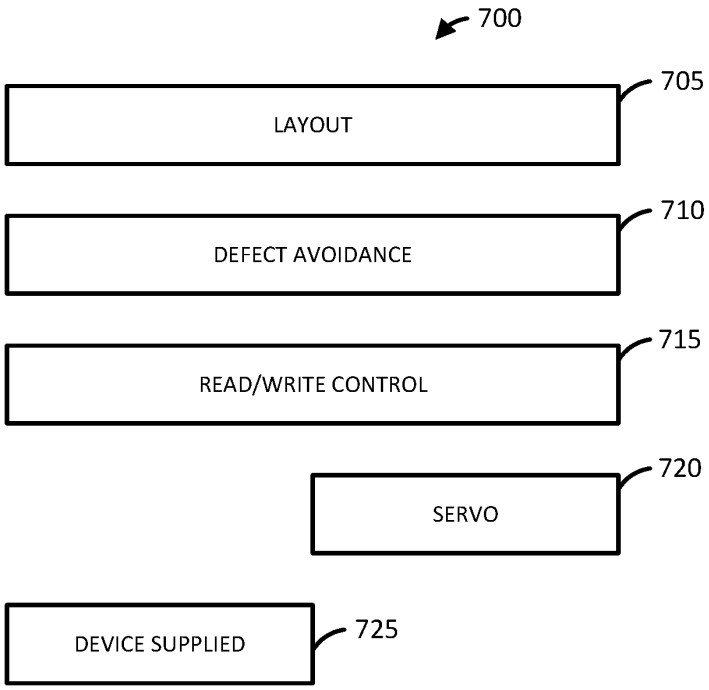

700
705
LAYOUT
710
DEFECT AVOIDANCE
715
READ/WRITE CONTROL
720
SERVO
DEVICE SUPPLIED
725

FIG. 7A

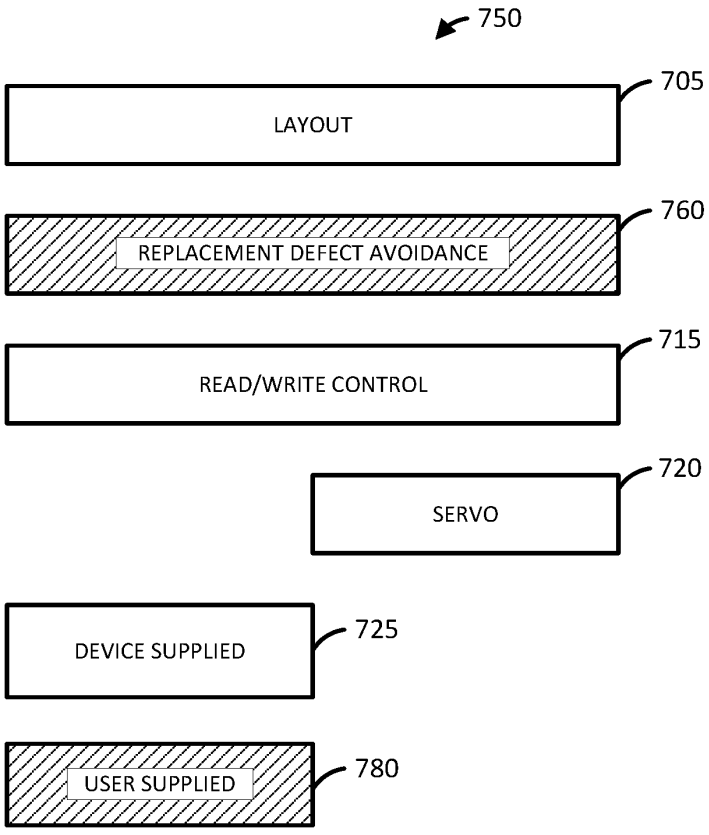

750
705
LAYOUT
760
REPLACEMENT DEFECT AVOIDANCE
715
READ/WRITE CONTROL
720
SERVO
DEVICE SUPPLIED
725
USER SUPPLIED
780

FIG. 7B

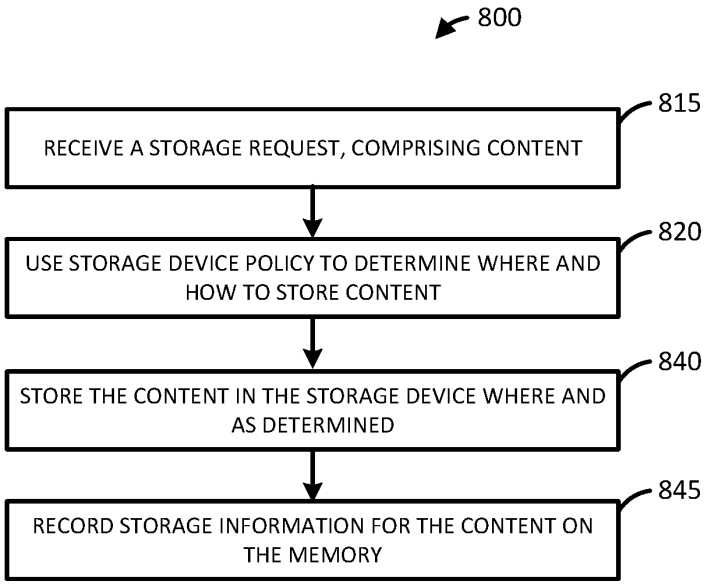

800
RECEIVE A STORAGE REQUEST, COMPRISING CONTENT
815
USE STORAGE DEVICE POLICY TO DETERMINE WHERE AND HOW TO STORE CONTENT
820
STORE THE CONTENT IN THE STORAGE DEVICE WHERE AND AS DETERMINED
840
RECORD STORAGE INFORMATION FOR THE CONTENT ON THE MEMORY
845

FIG. 8A

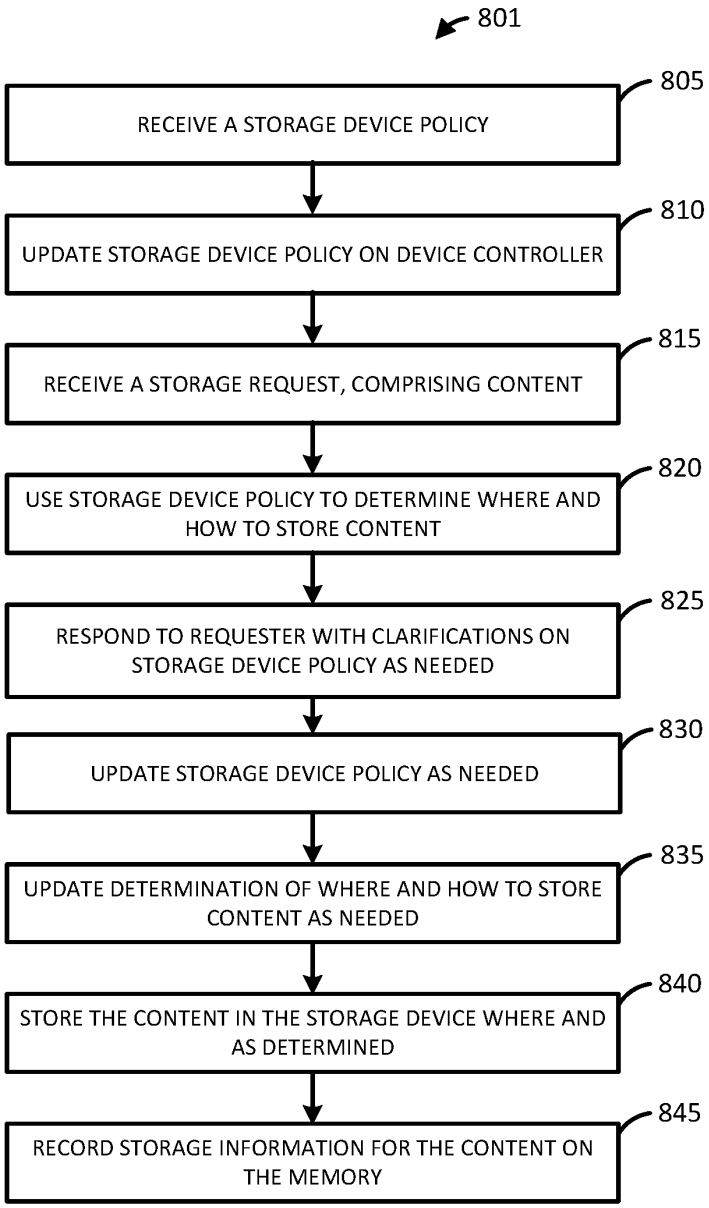

801
805
RECEIVE A STORAGE DEVICE POLICY
810
UPDATE STORAGE DEVICE POLICY ON DEVICE CONTROLLER
815
RECEIVE A STORAGE REQUEST, COMPRISING CONTENT
820
USE STORAGE DEVICE POLICY TO DETERMINE WHERE AND HOW TO STORE CONTENT
825
RESPOND TO REQUESTER WITH CLARIFICATIONS ON STORAGE DEVICE POLICY AS NEEDED
830
UPDATE STORAGE DEVICE POLICY AS NEEDED
835
UPDATE DETERMINATION OF WHERE AND HOW TO STORE CONTENT AS NEEDED
840
STORE THE CONTENT IN THE STORAGE DEVICE WHERE AND AS DETERMINED
845
RECORD STORAGE INFORMATION FOR THE CONTENT ON THE MEMORY

FIG. 8B

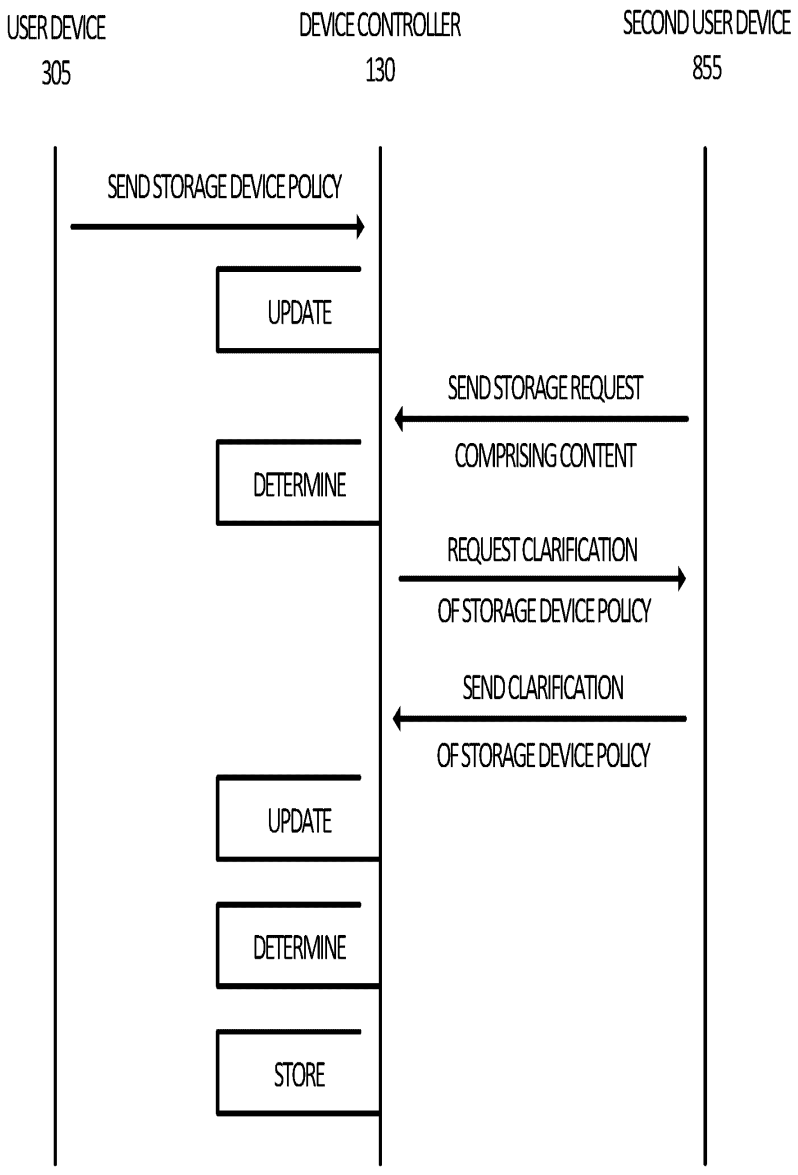

USER DEVICE
305
DEVICE CONTROLLER
130
SECOND USER DEVICE
855
SEND STORAGE DEVICE POLICY
UPDATE
SEND STORAGE REQUEST
COMPRISING CONTENT
DETERMINE
REQUEST CLARIFICATION
OF STORAGE DEVICE POLICY
SEND CLARIFICATION
OF STORAGE DEVICE POLICY
UPDATE
DETERMINE
STORE

FIG. 8C

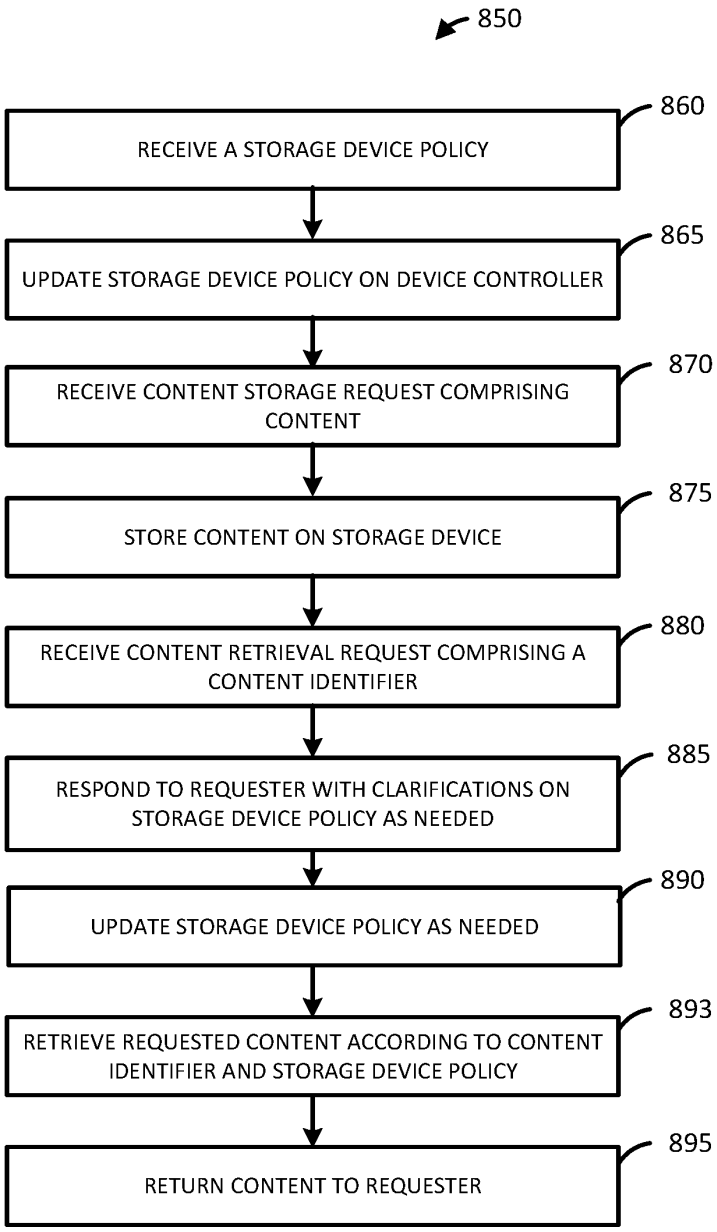

850
RECEIVE A STORAGE DEVICE POLICY
860
UPDATE STORAGE DEVICE POLICY ON DEVICE CONTROLLER
865
RECEIVE CONTENT STORAGE REQUEST COMPRISING CONTENT
870
STORE CONTENT ON STORAGE DEVICE
875
RECEIVE CONTENT RETRIEVAL REQUEST COMPRISING A CONTENT IDENTIFIER
880
RESPOND TO REQUESTER WITH CLARIFICATIONS ON STORAGE DEVICE POLICY AS NEEDED
885
UPDATE STORAGE DEVICE POLICY AS NEEDED
890
RETRIEVE REQUESTED CONTENT ACCORDING TO CONTENT IDENTIFIER AND STORAGE DEVICE POLICY
893
RETURN CONTENT TO REQUESTER
895

FIG. 8D

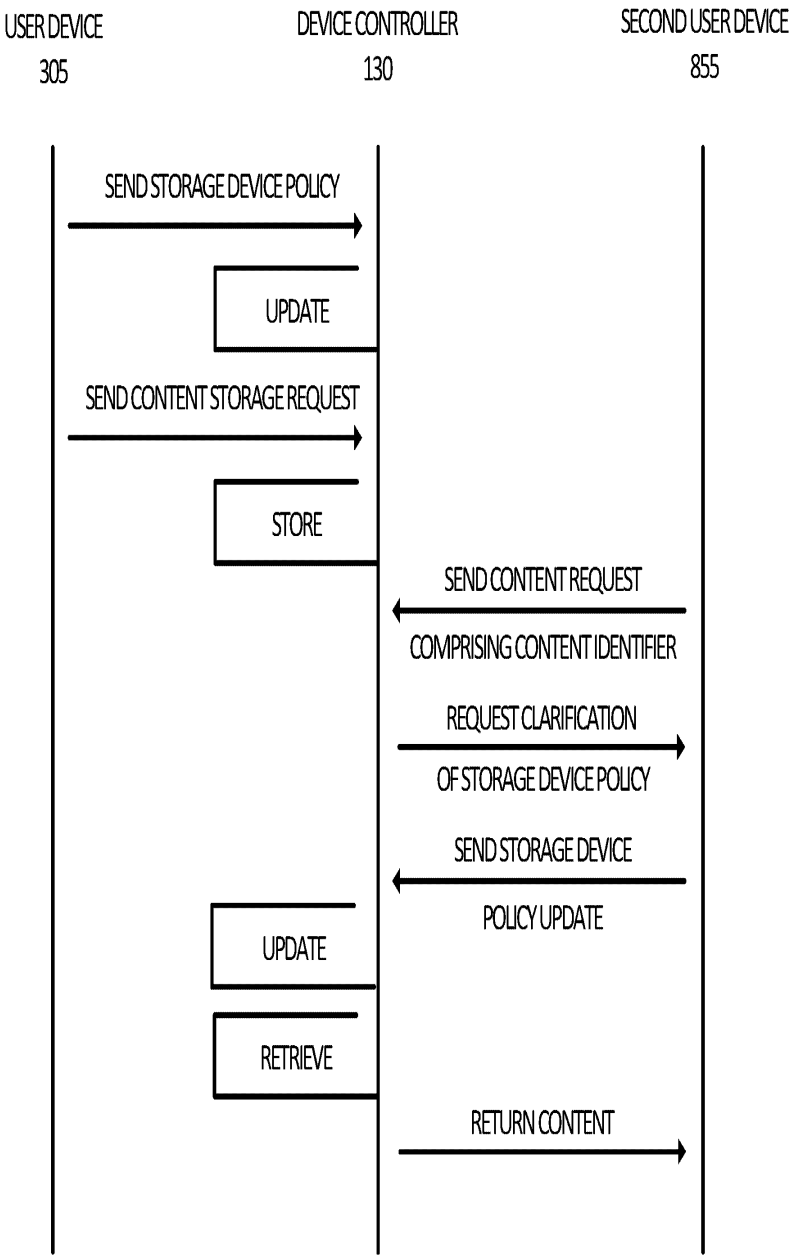

USER DEVICE
305
DEVICE CONTROLLER
130
SECOND USER DEVICE
855
SEND STORAGE DEVICE POLICY
UPDATE
SEND CONTENT STORAGE REQUEST
STORE
SEND CONTENT REQUEST
COMPRISING CONTENT IDENTIFIER
REQUEST CLARIFICATION
OF STORAGE DEVICE POLICY
SEND STORAGE DEVICE
POLICY UPDATE
UPDATE
RETRIEVE
RETURN CONTENT

FIG. 8E

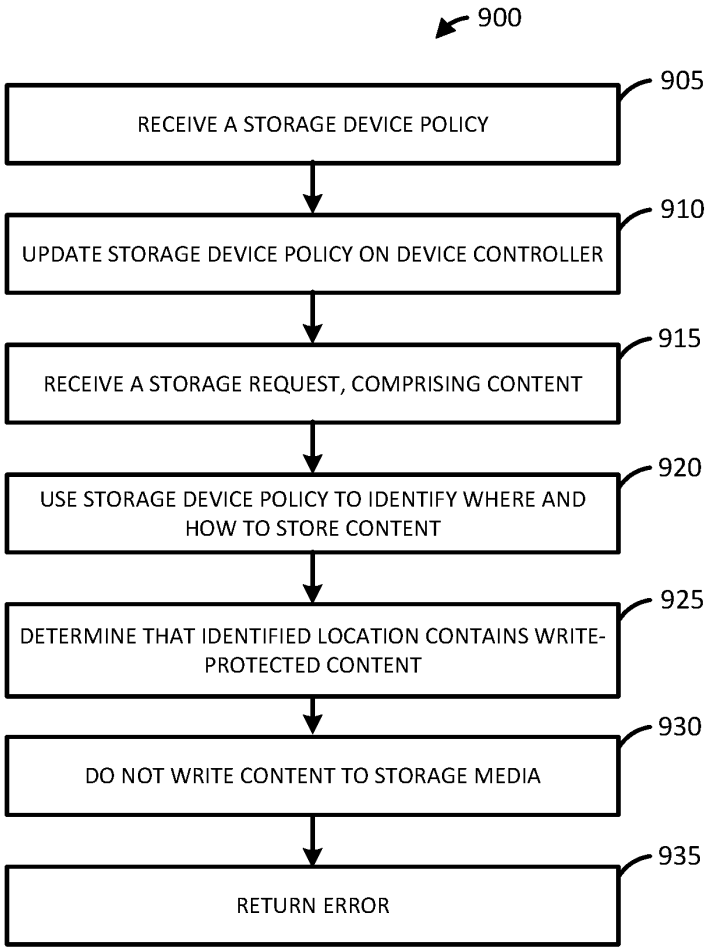

900
905
RECEIVE A STORAGE DEVICE POLICY
910
UPDATE STORAGE DEVICE POLICY ON DEVICE CONTROLLER
915
RECEIVE A STORAGE REQUEST, COMPRISING CONTENT
920
USE STORAGE DEVICE POLICY TO IDENTIFY WHERE AND HOW TO STORE CONTENT
925
DETERMINE THAT IDENTIFIED LOCATION CONTAINS WRITE-PROTECTED CONTENT
930
DO NOT WRITE CONTENT TO STORAGE MEDIA
935
RETURN ERROR

FIG. 9A

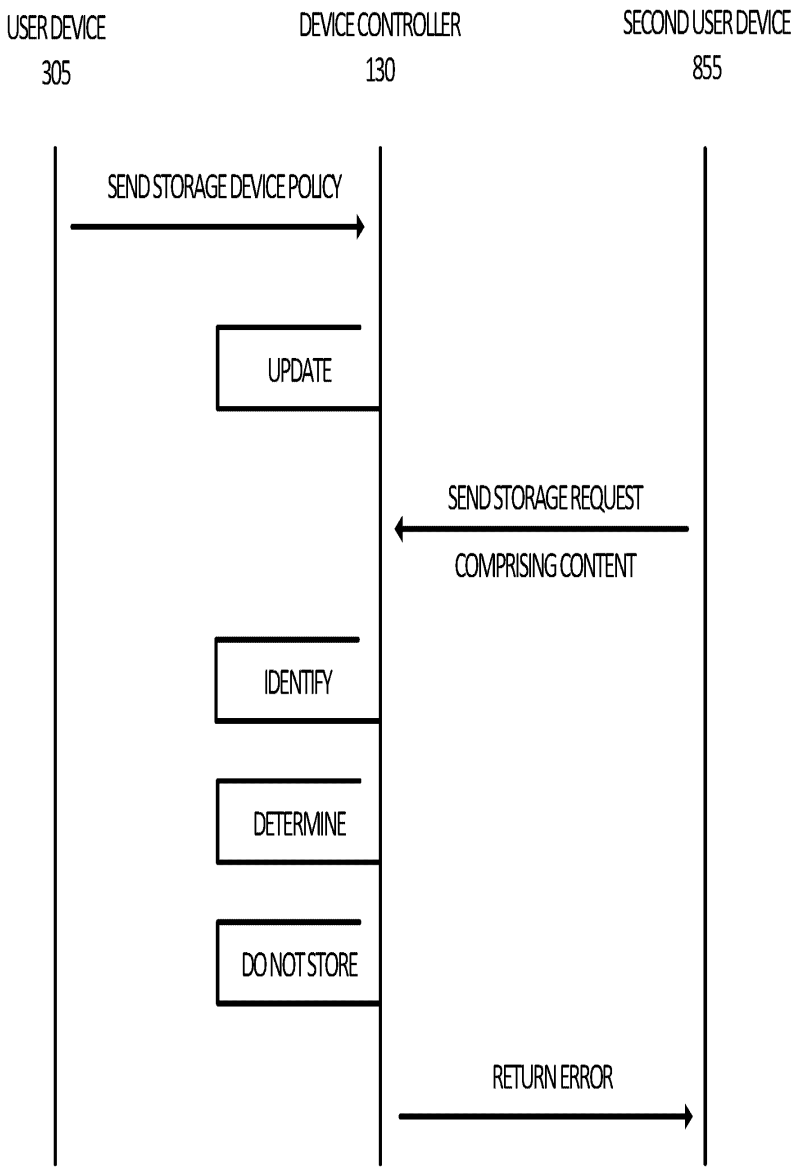

USER DEVICE
305
DEVICE CONTROLLER
130
SECOND USER DEVICE
855
SEND STORAGE DEVICE POLICY
UPDATE
SEND STORAGE REQUEST
COMPRISING CONTENT
IDENTIFY
DETERMINE
DO NOT STORE
RETURN ERROR

FIG. 9B

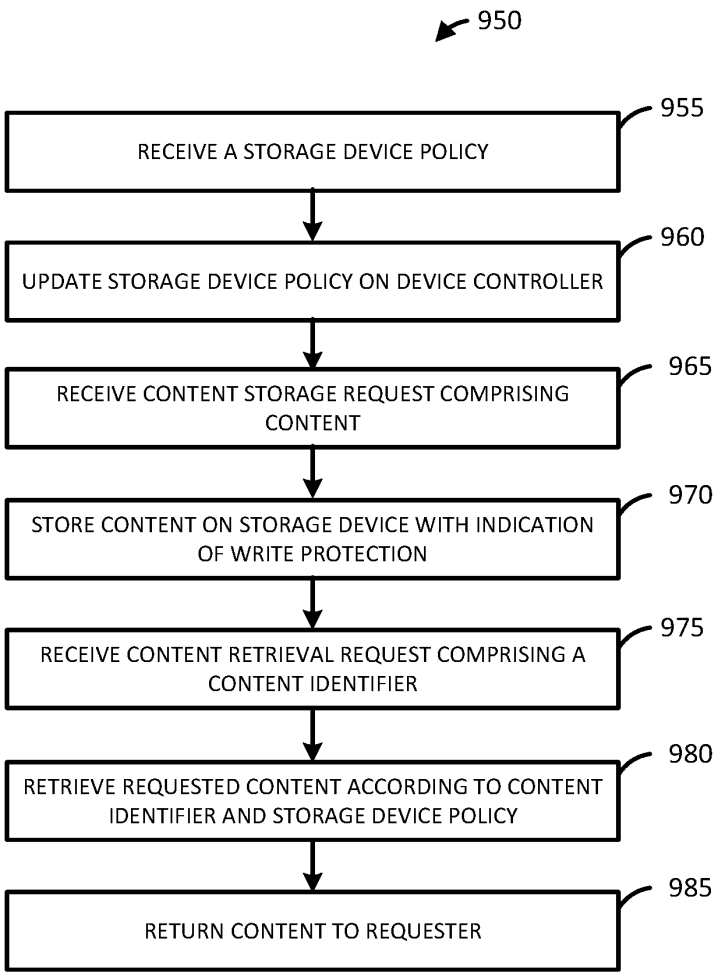

950
955
RECEIVE A STORAGE DEVICE POLICY
960
UPDATE STORAGE DEVICE POLICY ON DEVICE CONTROLLER
965
RECEIVE CONTENT STORAGE REQUEST COMPRISING CONTENT
970
STORE CONTENT ON STORAGE DEVICE WITH INDICATION OF WRITE PROTECTION
975
RECEIVE CONTENT RETRIEVAL REQUEST COMPRISING A CONTENT IDENTIFIER
980
RETRIEVE REQUESTED CONTENT ACCORDING TO CONTENT IDENTIFIER AND STORAGE DEVICE POLICY
985
RETURN CONTENT TO REQUESTER

FIG. 9C

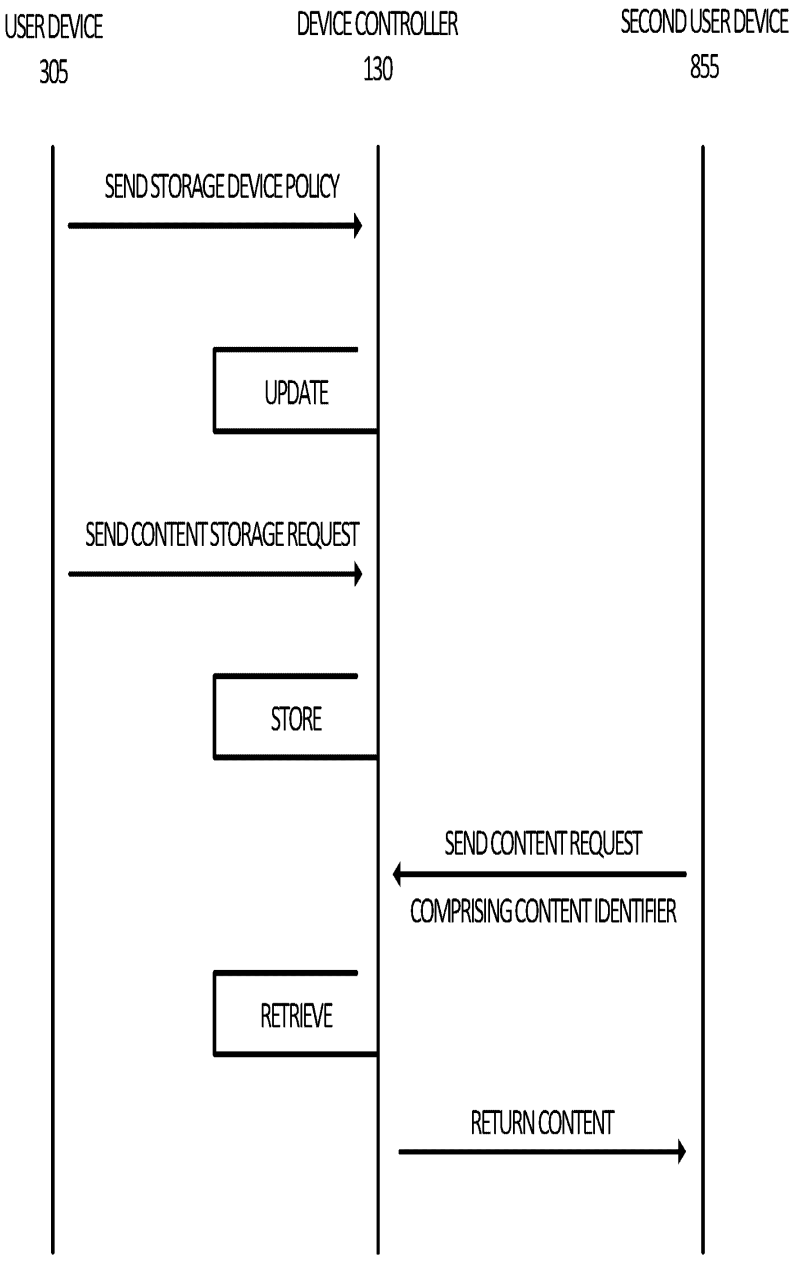

USER DEVICE
305
DEVICE CONTROLLER
130
SECOND USER DEVICE
855
SEND STORAGE DEVICE POLICY
UPDATE
SEND CONTENT STORAGE REQUEST
STORE
SEND CONTENT REQUEST
COMPRISING CONTENT IDENTIFIER
RETRIEVE
RETURN CONTENT

FIG. 9D

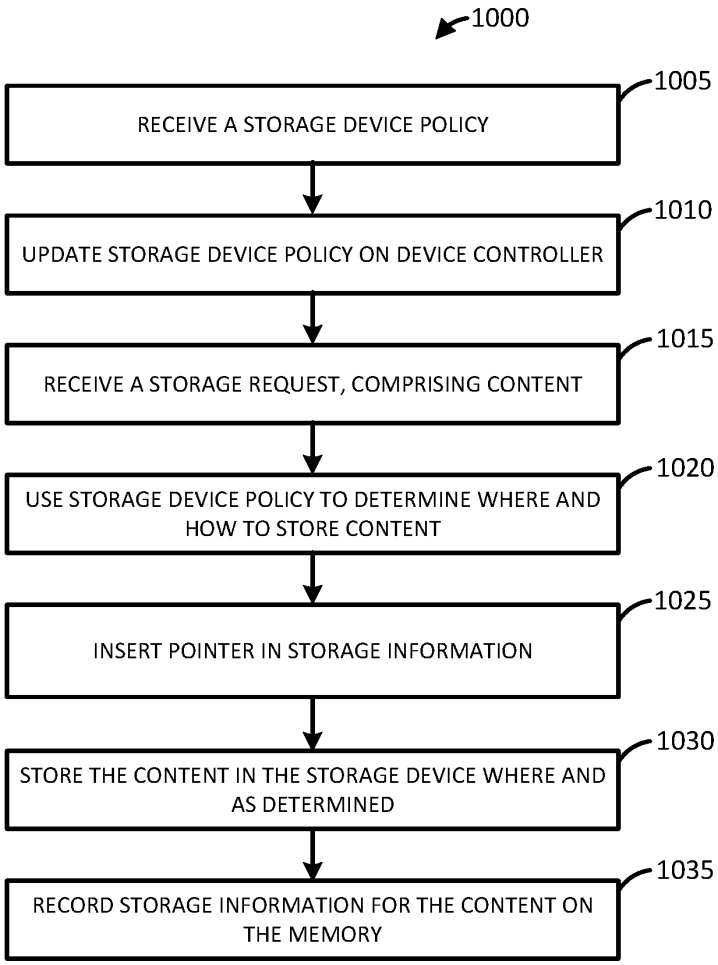

1000
1005
RECEIVE A STORAGE DEVICE POLICY
1010
UPDATE STORAGE DEVICE POLICY ON DEVICE CONTROLLER
1015
RECEIVE A STORAGE REQUEST, COMPRISING CONTENT
1020
USE STORAGE DEVICE POLICY TO DETERMINE WHERE AND HOW TO STORE CONTENT
1025
INSERT POINTER IN STORAGE INFORMATION
1030
STORE THE CONTENT IN THE STORAGE DEVICE WHERE AND AS DETERMINED
1035
RECORD STORAGE INFORMATION FOR THE CONTENT ON THE MEMORY

FIG. 10A

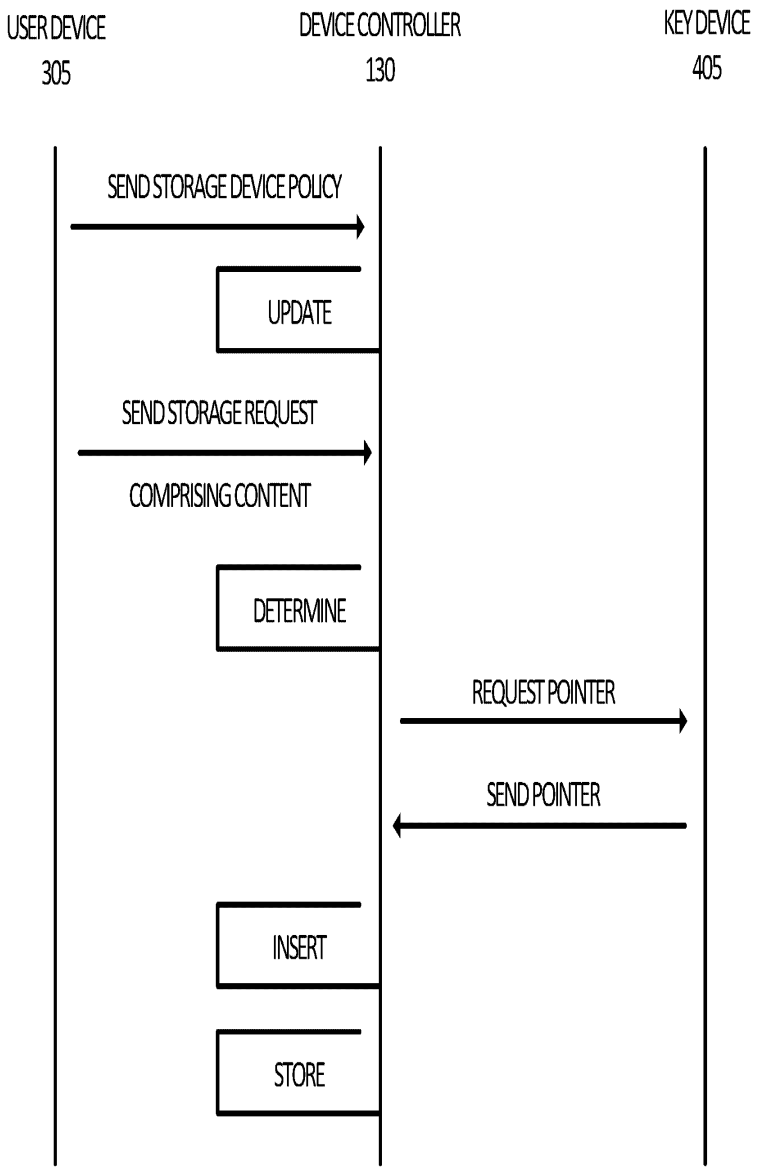

USER DEVICE
305
DEVICE CONTROLLER
130
KEY DEVICE
405
SEND STORAGE DEVICE POLICY
UPDATE
SEND STORAGE REQUEST
COMPRISING CONTENT
DETERMINE
REQUEST POINTER
SEND POINTER
INSERT
STORE

FIG. 10B

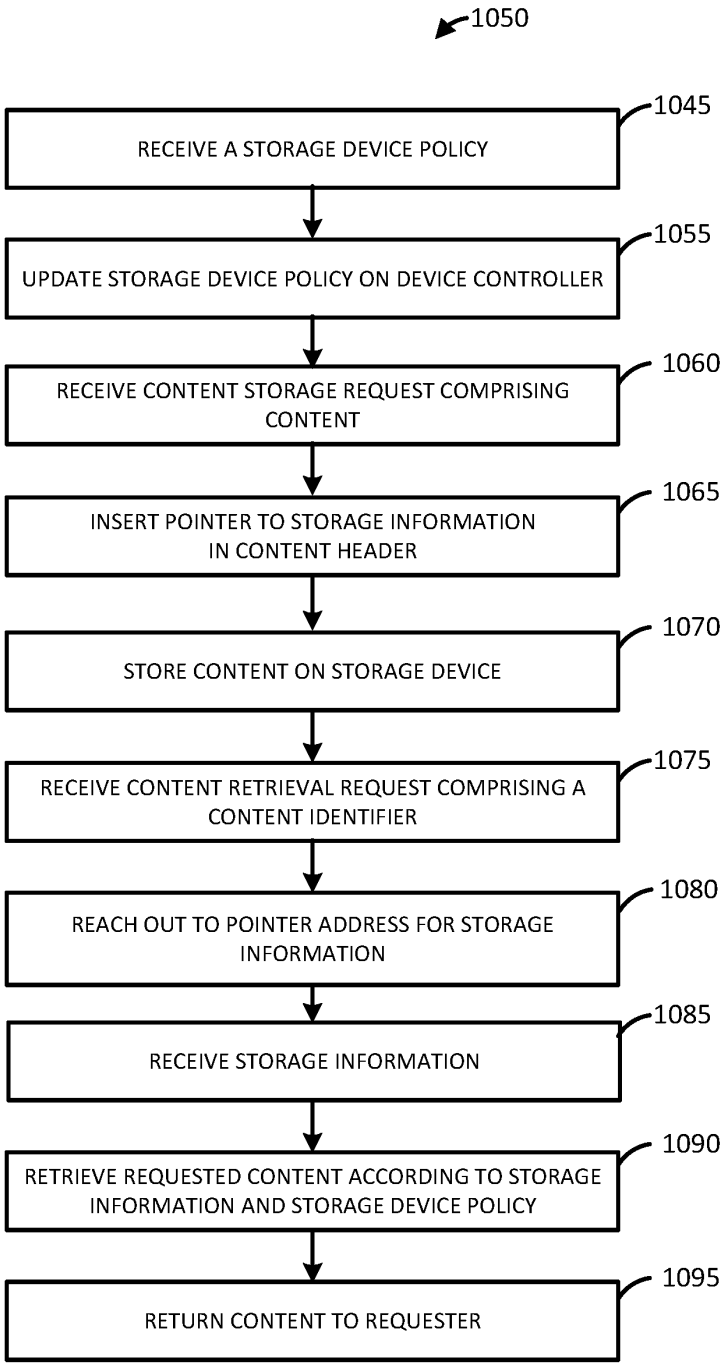

1050
RECEIVE A STORAGE DEVICE POLICY
1045
UPDATE STORAGE DEVICE POLICY ON DEVICE CONTROLLER
1055
RECEIVE CONTENT STORAGE REQUEST COMPRISING CONTENT
1060
INSERT POINTER TO STORAGE INFORMATION IN CONTENT HEADER
1065
STORE CONTENT ON STORAGE DEVICE
1070
RECEIVE CONTENT RETRIEVAL REQUEST COMPRISING A CONTENT IDENTIFIER
1075
REACH OUT TO POINTER ADDRESS FOR STORAGE INFORMATION
1080
RECEIVE STORAGE INFORMATION
1085
RETRIEVE REQUESTED CONTENT ACCORDING TO STORAGE INFORMATION AND STORAGE DEVICE POLICY
1090
RETURN CONTENT TO REQUESTER
1095

FIG. 10C

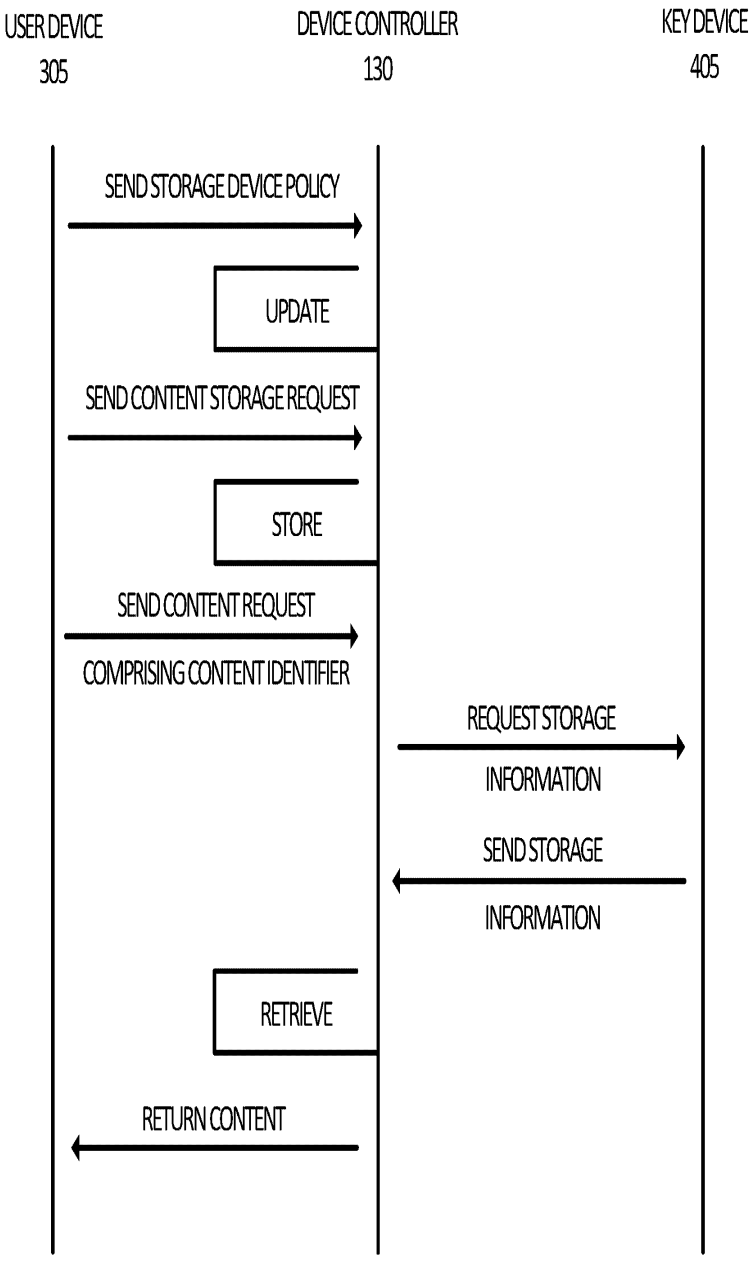

USER DEVICE
305
DEVICE CONTROLLER
130
KEY DEVICE
405
SEND STORAGE DEVICE POLICY
UPDATE
SEND CONTENT STORAGE REQUEST
STORE
SEND CONTENT REQUEST
COMPRISING CONTENT IDENTIFIER
REQUEST STORAGE
INFORMATION
SEND STORAGE
INFORMATION
RETRIEVE
RETURN CONTENT

FIG. 10D

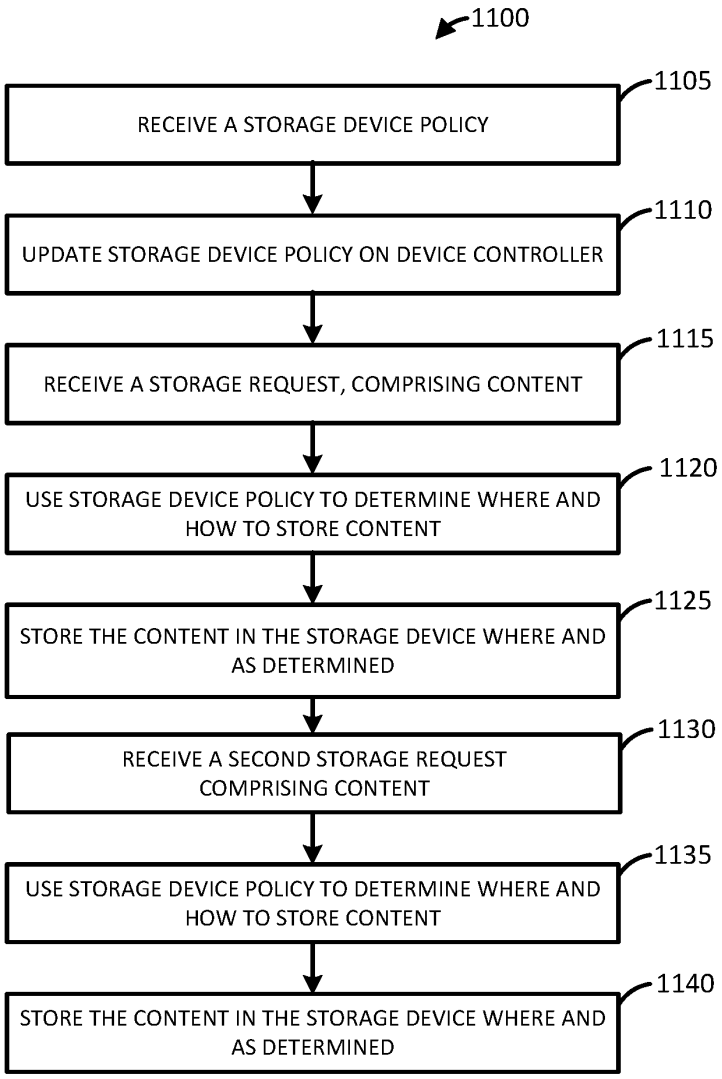

1100
1105
RECEIVE A STORAGE DEVICE POLICY
1110
UPDATE STORAGE DEVICE POLICY ON DEVICE CONTROLLER
1115
RECEIVE A STORAGE REQUEST, COMPRISING CONTENT
1120
USE STORAGE DEVICE POLICY TO DETERMINE WHERE AND HOW TO STORE CONTENT
1125
STORE THE CONTENT IN THE STORAGE DEVICE WHERE AND AS DETERMINED
1130
RECEIVE A SECOND STORAGE REQUEST COMPRISING CONTENT
1135
USE STORAGE DEVICE POLICY TO DETERMINE WHERE AND HOW TO STORE CONTENT
1140
STORE THE CONTENT IN THE STORAGE DEVICE WHERE AND AS DETERMINED

FIG. 11A

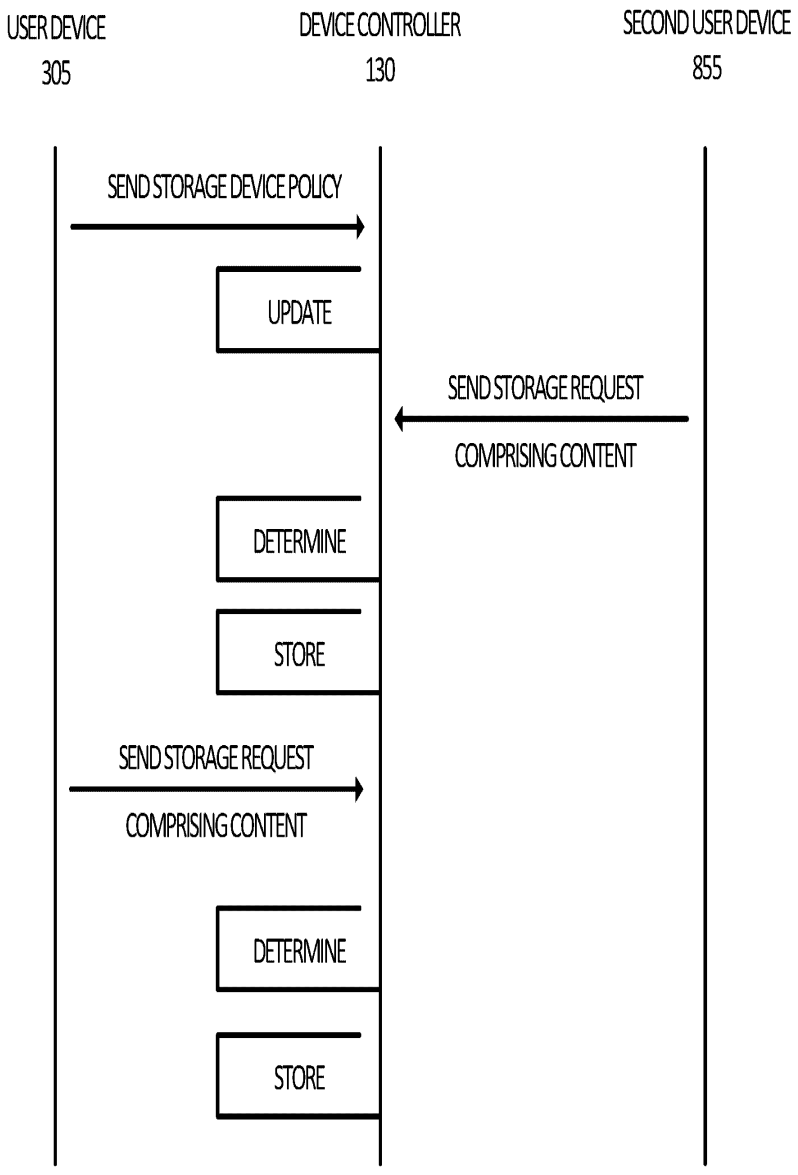

USER DEVICE
305
DEVICE CONTROLLER
130
SECOND USER DEVICE
855
SEND STORAGE DEVICE POLICY
UPDATE
SEND STORAGE REQUEST
COMPRISING CONTENT
DETERMINE
STORE
SEND STORAGE REQUEST
COMPRISING CONTENT
DETERMINE
STORE

FIG. 11B

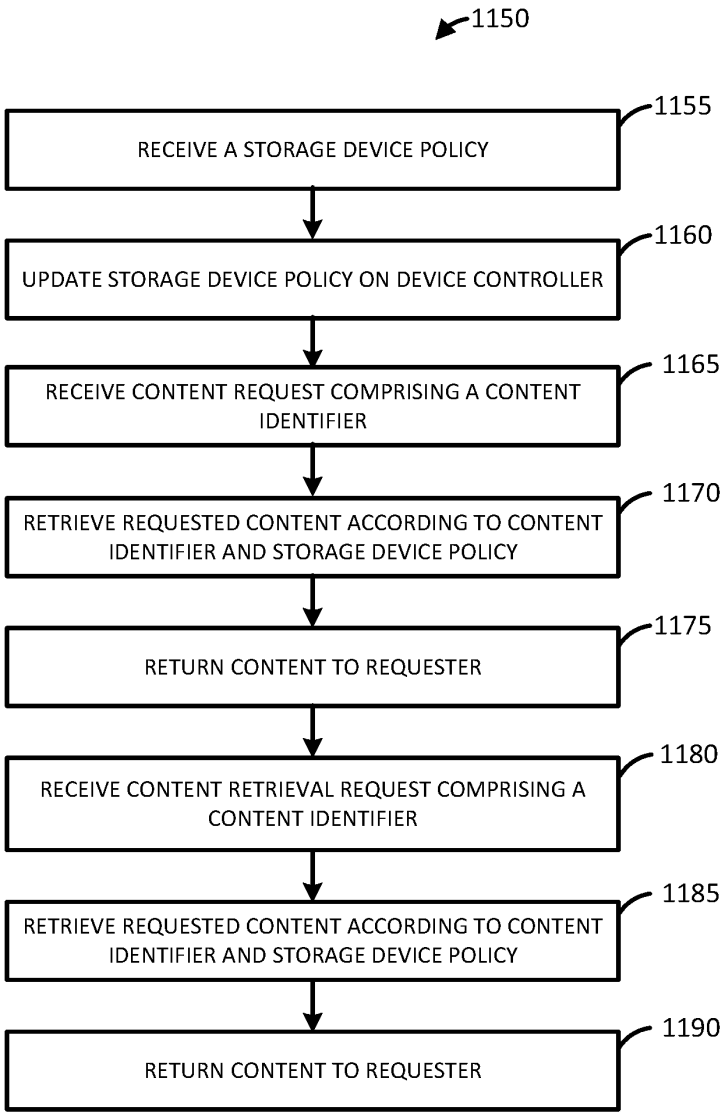

1150
1155
RECEIVE A STORAGE DEVICE POLICY
1160
UPDATE STORAGE DEVICE POLICY ON DEVICE CONTROLLER
1165
RECEIVE CONTENT REQUEST COMPRISING A CONTENT IDENTIFIER
1170
RETRIEVE REQUESTED CONTENT ACCORDING TO CONTENT IDENTIFIER AND STORAGE DEVICE POLICY
1175
RETURN CONTENT TO REQUESTER
1180
RECEIVE CONTENT RETRIEVAL REQUEST COMPRISING A CONTENT IDENTIFIER
1185
RETRIEVE REQUESTED CONTENT ACCORDING TO CONTENT IDENTIFIER AND STORAGE DEVICE POLICY
1190
RETURN CONTENT TO REQUESTER

FIG. 11C

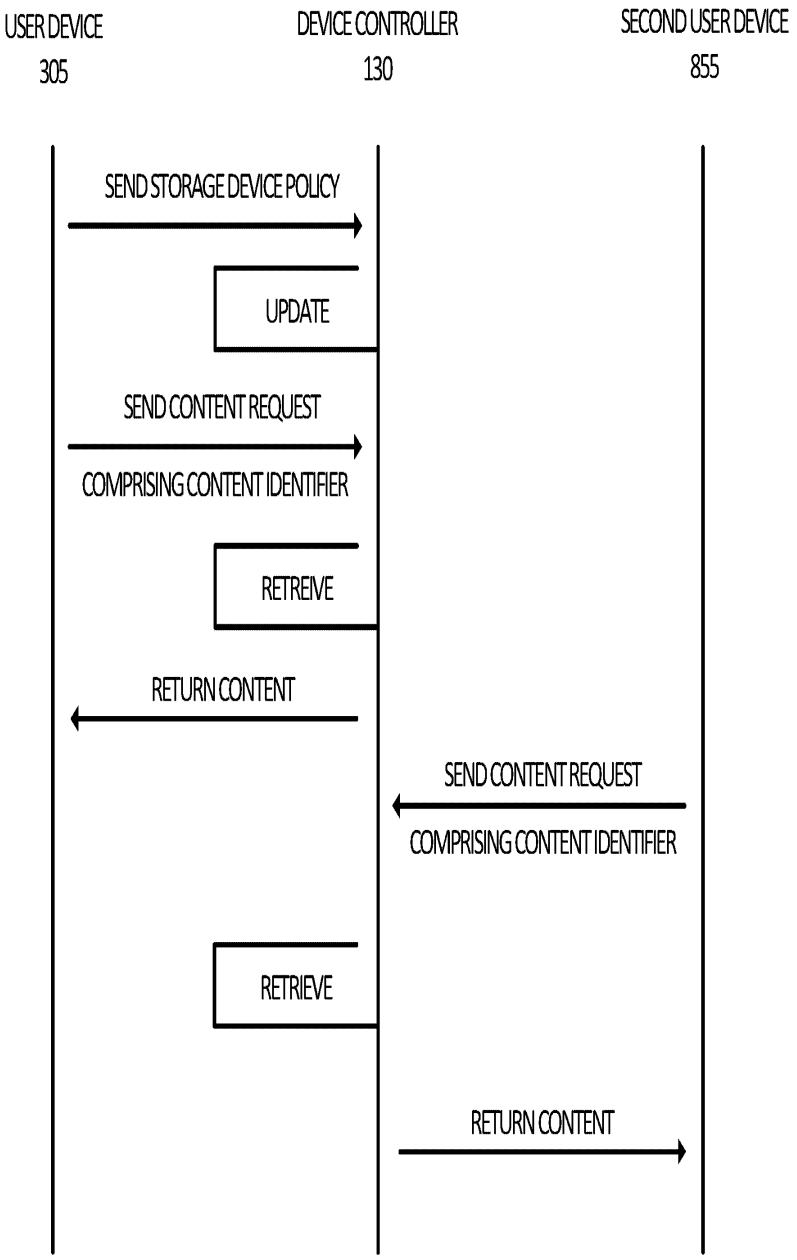

USER DEVICE
305
DEVICE CONTROLLER
130
SECOND USER DEVICE
855
SEND STORAGE DEVICE POLICY
UPDATE
SEND CONTENT REQUEST
COMPRISING CONTENT IDENTIFIER
RETREIVE
RETURN CONTENT
SEND CONTENT REQUEST
COMPRISING CONTENT IDENTIFIER
RETRIEVE
RETURN CONTENT

FIG. 11D

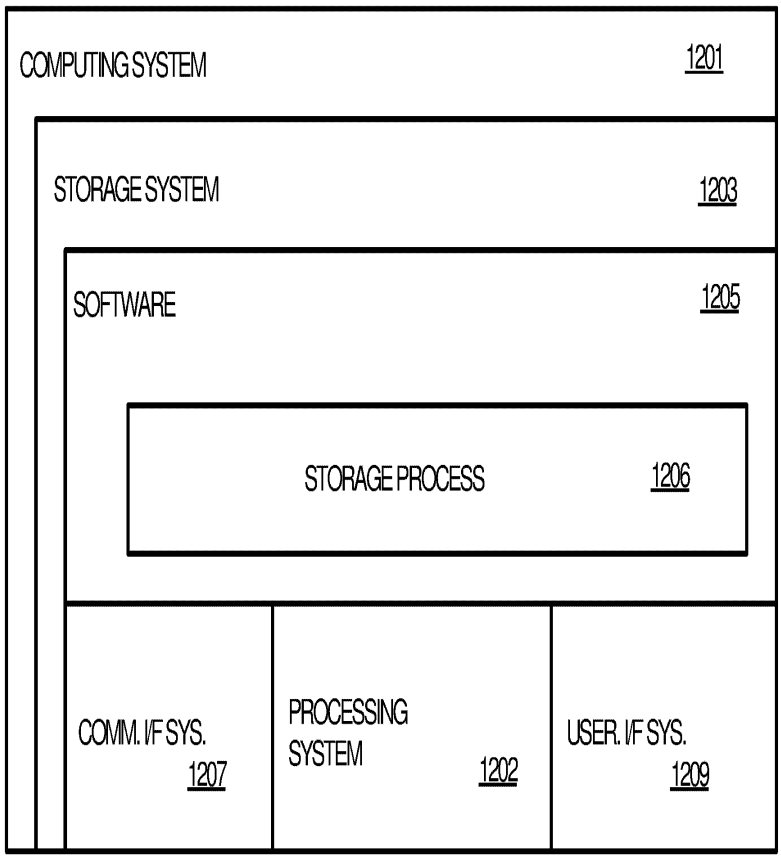

COMPUTING SYSTEM
1201
STORAGE SYSTEM
1203
SOFTWARE
1205
STORAGE PROCESS
1206
COMM. I/F SYS.
1207
PROCESSING SYSTEM
1202
USER. I/F SYS.
1209

FIG. 12

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	980.0023
	Application Number	
Title of Invention	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Joshua		Johnson	

Residence Information (Select One) ● US Residency Non US Residency Active US Military Service

City	State/Province	Country of Residence
Frederick	CO	US

Mailing Address of Inventor:

Address 1	c/o Gaea LLC
Address 2	8374 Greenwood Drive
City	Niwot
State/Province	CO
Postal Code	80503
Country	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Curt		Bruner	

Residence Information (Select One) ◉ US Residency Non US Residency Active US Military Service

City	State/Province	Country of Residence
Niwot	CO	US

Mailing Address of Inventor:

Address 1	c/o Gaea LLC
Address 2	8374 Greenwood Drive
City	Niwot
State/Province	CO
Postal Code	80503
Country	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Jeffrey		Reh	

Residence Information (Select One) ◉ US Residency Non US Residency Active US Military Service

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	980.0023
	Application Number	
Title of Invention	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR	

City	Longmont	State/Province	CO	Country of Residence	US

Mailing Address of Inventor:

Address 1	c/o Gaea LLC
Address 2	8374 Greenwood Drive

City	Niwot	State/Province	CO
Postal Code	80503	Country	US

Inventor 4 — Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Christopher		Squires	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Boulder	State/Province	CO	Country of Residence	US

Mailing Address of Inventor:

Address 1	c/o Gaea LLC
Address 2	8374 Greenwood Drive

City	Niwot	State/Province	CO
Postal Code	80503	Country	US

Inventor 5 — Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Brian		Wilson	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Zumbro Falls	State/Province	MN	Country of Residence	US

Mailing Address of Inventor:

Address 1	c/o Gaea LLC
Address 2	8374 Greenwood Drive

City	Niwot	State/Province	CO
Postal Code	80503	Country	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. — Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	980.0023
	Application Number	
Title of Invention	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR	

Customer Number	76444		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR		
Attorney Docket Number	980.0023	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	32	**Suggested Figure for Publication (if any)**	

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	● Customer Number	US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	76444		

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	980.0023
	Application Number	
Title of Invention	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR	

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62418510	2016-11-07
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62418561	2016-11-07
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62418687	2016-11-07
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62418693	2016-11-07
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62418696	2016-11-07
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62418717	2016-11-07
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62418724	2016-11-07
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62418730	2016-11-07

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	980.0023
	Application Number	
Title of Invention	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR	

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62418742	2016-11-07
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62418759	2016-11-07
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62418764	2016-11-07
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62418768	2016-11-07
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62418773	2016-11-07
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62418775	2016-11-07
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62418780	2016-11-07
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62418785	2016-11-07
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62448826	2017-01-20

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	980.0023
	Application Number	
Title of Invention	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR	

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	980.0023
	Application Number	
Title of Invention	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	980.0023
	Application Number	
Title of Invention	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

● Assignee	Legal Representative under 35 U.S.C. 117	Joint Inventor
Person to whom the inventor is obligated to assign.	Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	Gaea LLC		
Mailing Address Information For Applicant:			
Address 1	8374 Greenwood Drive		
Address 2			
City	Niwot	**State/Province**	CO
Country	US	Postal Code	80503
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	980.0023
	Application Number	
Title of Invention	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR	

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country [i]		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/David H. Schaumann/			Date (YYYY-MM-DD)	2017-11-06
First Name	David	Last Name	Schaumann	Registration Number	50858

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	980.0023
	Application Number	
Title of Invention	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1 The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3 A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent CooperationTreaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

DocCode – SCORE

SCORE Placeholder Sheet for IFW Content

Application Number: 15804772 Document Date: 11/06/2017

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

- Drawing

At the time of document entry (noted above):

- USPTO employees may access SCORE content via eDAN using the Supplemental Content tab, or via the SCORE web page.
- External customers may access SCORE content via PAIR using the Supplemental Content tab.

Form Revision Date: August 26, 2013

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
15/804,772	11/06/2017	2827	2070	980.0023	36	6

CONFIRMATION NO. 2463

FILING RECEIPT

76444
Setter Roche LLP
14694 Orchard Parkway
Building A, Suite 200
Westminster, CO 80023



Date Mailed: 11/24/2017

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Joshua Johnson, Frederick, CO;
Curt Bruner, Niwot, CO;
Jeffrey Reh, Longmont, CO;
Christopher Squires, Boulder, CO;
Brian Wilson, Zumbro Falls, MN;

Applicant(s)

Gaea LLC, Niwot, CO;

Power of Attorney: The patent practitioners associated with Customer Number 76444

Domestic Priority data as claimed by applicant

This appln claims benefit of 62/418,510 11/07/2016
and claims benefit of 62/418,561 11/07/2016
and claims benefit of 62/418,687 11/07/2016
and claims benefit of 62/418,693 11/07/2016
and claims benefit of 62/418,696 11/07/2016
and claims benefit of 62/418,717 11/07/2016
and claims benefit of 62/418,724 11/07/2016
and claims benefit of 62/418,730 11/07/2016
and claims benefit of 62/418,742 11/07/2016
and claims benefit of 62/418,759 11/07/2016
and claims benefit of 62/418,764 11/07/2016
and claims benefit of 62/418,768 11/07/2016
and claims benefit of 62/418,773 11/07/2016
and claims benefit of 62/418,775 11/07/2016
and claims benefit of 62/418,780 11/07/2016

and claims benefit of 62/418,785 11/07/2016
and claims benefit of 62/448,826 01/20/2017

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 11/21/2017
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/804,772**
Projected Publication Date: 05/10/2018
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR

Preliminary Class

365

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application

serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 15/804,772

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	36 minus 20 =	* 16	x 40 =	640	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	6 minus 3 =	* 3	x 210 =	630			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	2000		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/804,772	11/06/2017	Joshua Johnson	980.0023

CONFIRMATION NO. 2463

76444
Setter Roche LLP
14694 Orchard Parkway
Building A, Suite 200
Westminster, CO 80023

INFORMAL NOTICE

OC000000095622710

Date Mailed: 11/24/2017

INFORMATIONAL NOTICE TO APPLICANT

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

The item(s) indicated below are also required and should be submitted with any reply to this notice to avoid further processing delays.

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
  Joshua Johnson
  Curt Bruner
  Jeffrey Reh
  Christopher Squires
  Brian Wilson

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/thaile/

DocuSign Envelope ID: 4C9C24EB-0107-4AB0-BD0C-94940AB05917

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR Docket # 980.0023

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 15/804,772 filed on 11/06/2017.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Joshua Johnson Date (Optional): 2/1/2018

Signature: Joshua Johnson

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

DocuSign Envelope ID: 4C9C24EB-0107-4AB0-BD0C-94940AB05917

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR Docket # 980.0023

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 15/804,772 filed on 11/06/2017.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Curt Bruner Date (Optional): 1/31/2018

Signature: Curt Bruner

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

DocuSign Envelope ID: E00AE8C8-AC9D-466C-9399-15F684A41EAD

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR Docket # 980.0023

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 15/804,772 filed on 11/06/2017.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Jeffrey Reh Date (Optional): 4/3/2018

Signature: Jeffrey A. Reh

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

DocuSign Envelope ID: 4C9C24EB-0107-4AB0-BD0C-94940AB05917

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR Docket # 980.0023

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 15/804,772 filed on 11/06/2017.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Christopher Squires Date (Optional): 2/20/2018

Signature: Christopher Squires

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

DocuSign Envelope ID: 4C9C24EB-0107-4AB0-BD0C-94940AB05917

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR Docket # 980.0023

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 15/804,772 filed on 11/06/2017.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Brian Wilson Date (Optional): 2/5/2018

Signature: Brian Wilson

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	32247868
Application Number:	15804772
International Application Number:	
Confirmation Number:	2463
Title of Invention:	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR
First Named Inventor/Applicant Name:	Joshua Johnson
Customer Number:	76444
Filer:	Stephen S. Roche/Jamie Cameron
Filer Authorized By:	Stephen S. Roche
Attorney Docket Number:	980.0023
Receipt Date:	04-APR-2018
Filing Date:	06-NOV-2017
Time Stamp:	16:56:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Oath or Declaration filed	Declaration.pdf	350754 3f123f9d56095d078de1e1181ba6ada3111c0cf2	no	5

Warnings:

Information:	
Total Files Size (in bytes):	350754

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/804,772	11/06/2017	Joshua Johnson	980.0023

CONFIRMATION NO. 2463

76444
Setter Roche LLP
14694 Orchard Parkway
Building A, Suite 200
Westminster, CO 80023

PUBLICATION NOTICE

OC000000099438306

Title:DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR

Publication No.US-2018-0129439-A1
Publication Date:05/10/2018

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently https://portal.uspto.gov/pair/PublicPair. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/804,772	11/06/2017	Joshua Johnson	980.0023	2463

76444 7590 05/03/2019

Setter Roche LLP
14694 Orchard Parkway
Building A, Suite 200
Westminster, CO 80023

EXAMINER	
LANE, JOHN A	

ART UNIT	PAPER NUMBER
2139	

NOTIFICATION DATE	DELIVERY MODE
05/03/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@setterroche.com

PTOL-90A (Rev. 04/07)

Office Action Summary	**Application No.** 15/804,772	**Applicant(s)** Johnson et al.	
	Examiner JOHN A LANE	**Art Unit** 2139	**AIA (FITF) Status** Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 11/06/2017.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-36 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-36 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 11/06/2017 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

1. This Office action is responsive to the application filed 11/06/2017. The Drawings are accepted by the Examiner. Claims 1-36 are presented for examination. Neither a preliminary amendment nor an Information Disclosure Statement (IDS) has been filed in the application If any copies are missing please notify the examiner in response to this action.

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

2. Claim 2 is rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

Regarding claim 2, "areal" is unclear.

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. section 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --
>
> (a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

4. Claims 1-36 are rejected under 35 U.S.C. 102(a)(2) as being anticipated by Olster et al. (2015/0052167).

> 1. An apparatus comprising:
>
> a storage device **(corresponds to "storage media", (see [0022], [0026] and throughout)**;
>
> a device controller operatively coupled with the storage device **(corresponds to "controller…included with the storage media and/or storage node", (see [0026]) and throughout)**, comprising a memory **(corresponds to "volatile memory and non-volatile memory", see [0024] and throughout)**;
>
> an application stored on the memory and comprising instructions **(corresponds to "software", "application**

program", "object code", "machine code", (see [0020] and throughout) that, when executed, direct the device controller to at least:

receive a storage device policy **(corresponds to "storage policy", "policy" or "polices", (see [0030] and throughout)**;

receive a storage request **(corresponds to "request", (see [0046], [0047] and throughout)**, comprising content **(corresponds to "data" or "object" discuss throughout)**;

store the content on the storage device according to the storage device policy **(corresponds to "[t]he object including its constituent data portion may be stored among storage nodes and storage zones according to the storage policy…", (see [0030]; "replication and placement component of a policy defines the replication and placement of data objects in the data storage system", (see [0031]; "[t]he maximum size of the embedded object databases may be a configuration parameter…or parameter of the policy", see (0039])**;

record storage information for the content on the memory, comprising at least a content identifier for the content **(corresponds to "metadata", "object identifier", (see [0039], [0040], [0041] and throughout)**;

subsequent to storing the content, receive a content request for the content, comprising at least the content identifier for the content **(corresponds to "reading", (see [0029]) "request" throughout)**;

in response to the content request, retrieve storage information for the content **(corresponds to reading metadata (see [0039], [0041] and [0049])**;

recover the content, at least in part according to the storage information **(corresponds to reading the file/data/object using metadata, object identifier, etc.)**; and

respond to the content request at least by returning the content.

26. An apparatus comprising:

a storage device **(discussed above)**;

a device controller operatively coupled with the storage device, comprising a memory, the device controller configured to receive content to be stored on the storage device **(discussed above)**;

a programmable processor **(corresponds to "processors such as microprocessors", (see [0020] and throughout)**, communicatively coupled with the device controller such that the content received by the device controller to be stored on

the storage device must pass though the programmable processor; and

an application stored on the memory and comprising instructions that, when executed, direct the device controller to at least store the content on the storage device after the content has been processed by the programmable processor **(discussed above)**.

32. An apparatus comprising:

a storage device **(discussed above)**;

a device controller operatively coupled with the storage device, comprising a memory **(discussed above)**;

an application stored on the memory and comprising instructions that, when executed, direct the device controller to at least **(discussed above)**:

receive a storage device policy **(discussed above)**;

store a first content on the storage device at a first density in accordance with the storage device policy **(corresponds to storing "documents, images, audio, videos" (see [0060]); "[a]dditional fields may also be**

stored as metadata regarding the object such as a code or designator or text name for (a) the kind of data represented by the object, including, for example, image, video, audio, text document, and the like…", (see[0039]); see also above regarding storing data in accordance with metadata and/or policy);

store a second content on the storage device at a second density and in accordance with the storage device policy; and

wherein the first density and the second density differ **(corresponds to storing another type of data in accordance with metadata and/or policy).**

Independent claims 9, 16 and 21 define embodiments similar in scope to that of claim 1 and are rejected accordingly.

The remaining dependent claim features are expressly or inherently found in the applied art.

5. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 2-8, 10-15, 17-20, 22-25, 27-31 and 33-36 are rejected under 35 U.S.C. 103 as being unpatentable over Olster et al. (US 2015/0052167) in view of known prior art (Official notice taken).

Official notice is taken of the prior art teaching any dependent claim feature not specifically discussed above or found in Olster. That is, any prior art (including that of record) teaching the well known claim features found in the dependent claims. The dependent claim features, while part of the invention, appear to be well known and their relevance not essential to the main invention found in the independent claim(s).

Thus, a detailed discussion of the well known claim feature(s) is not warranted at this time.

Any response to this action should be mailed to:

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

or faxed to:

(571) 273-8300, (for Official communications intended for entry)

Or:

(571) 273-4208, (for Non-Official or draft communications, please label "Non-Official" or "DRAFT")

Or:

Via e-mail at Jack.Lane@uspto.gov (for Non-Official or Draft communications, please label “Non-Official or “DRAFT”)

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Jack Lane whose telephone number is 571 272-4208. The examiner can normally be reached on Mon-Fri 7:30AM-6:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Reg Bragdon can be reached on 571 272-4204.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571 272-2100.

/JOHN A LANE/

Primary Examiner, Art Unit 2139

Notice of References Cited	Application/Control No. 15/804,772	Applicant(s)/Patent Under Reexamination Johnson et al.	
	Examiner JOHN A LANE	Art Unit 2139	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20140172930-A1	06-2014	Molaro; Donald J.	G06F11/1076	707/827
*	B	US-20100218177-A1	08-2010	MIURA; Hiroyuki	G06F8/65	717/170
*	C	US-20150052167-A1	02-2015	Olster; Dan	G06F16/2471	707/769
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/804,772	Johnson et al.
	Examiner	Art Unit
	JOHN A LANE	2139

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
EAST text search	04/29/2019	JAL

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
711	ALL	04/29/2019	JAL

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002
Page 131

US-PAT-NO: 10185667

DOCUMENT-IDENTIFIER: US 10185667 B2

TITLE: Storage controller

DATE-ISSUED: January 22, 2019

PRIOR-PUBLICATION-INFORMATION:

DOCUMENT-IDENTIFIER	DOCUMENT-DATE
US 20170357597 A1	December 14, 2017

PATENT-FAMILY-ID: 56178256

Primary Examiner - XP (1):

Lane; John A

Claims Text - CLTX (1):

1. A storage controller, the controller having an array of entries, each entry associated with a partition of one or more partitions, wherein the controller comprises logic configured to identify a partition identifier of an entry and apply a **policy** to the entry based on or in response to the partition identifier.

Claims Text - CLTX (3):

3. The controller according to claim 2, further comprising a partition **policy** unit for each partition, each partition **policy** unit configured to apply a partition specific **policy** to each entry having a corresponding partition identifier to determine a first adjusted weight.

Claims Text - CLTX (4):

4. The controller according to claim 3, wherein the partition **policy** unit is programmable with a particular **policy**.

Claims Text - CLTX (6):

6. The controller according to claim 5, further comprising a global **policy** unit for generating a global weight.

Claims Text – CLTX (7):

7. The controller according to claim 6, comprising an adjustment function for applying the global weight to adjust the first adjusted weight in accordance with an associated **policy** to generate a second adjusted weight.

Claims Text – CLTX (10):

10. The controller according to claim 3, wherein each partition **policy** unit comprises one or more selectable **policy** logic elements, whereby a first **policy** logic element is selectable for determining the first adjusted weight according to a first **policy**.

Claims Text – CLTX (11):

11. The controller according to claim 10, wherein the first **policy** logic element is selectable for determining an insertion weight according to the first **policy**.

Claims Text – CLTX (12):

12. The controller according to claim 3, wherein each partition **policy** unit comprises a programmable control for regulating bypassing of victim tag word determination according to a cache **policy**.

Claims Text – CLTX (13):

13. The controller according to claim 3, wherein each partition **policy** unit further comprises a programmable control for size scaling of replacement weights.

Claims Text – CLTX (14):

14. The controller according to claim 1, wherein each partition **policy** unit is configured to generate an insert type signal and a delete type signal according to a cache **policy** and information in the request.

Claims Text – CLTX (15):

15. The controller according to claim 1, wherein the **policy** comprises a replacement **policy** or an insertion **policy**.

Claims Text – CLTX (17):

17. A method for controlling a partitioned storage array, the partitioned storage array comprising one or more ways, each way having one or more entries, each entry associated with a partition, the method comprising: determining, from a set of entries, the respective partitions with which each entry of the set are associated with; applying to each entry of the set, a respective **policy** corresponding to the partition with which each entry is associated; and selecting a victim from the set based on or in response to the applied respective **policy** for each entry.

US-PAT-NO: 6973556

DOCUMENT-IDENTIFIER: US 6973556 B2

TITLE: Data element including metadata that includes data
management information for managing the data element

DATE-ISSUED: December 6, 2005

PATENT-FAMILY-ID: 25022868

---------- KWIC ---------

Primary Examiner - XP (1):
Lane; Jack

Claims Text - CLTX (1):
1. A method far managing data comprising: providing a data element that includes metadata within said data element; storing data management information in the metadata, said data management information for managing said data element; storing, within said data element, one or more anchor points to begin selected analysis processes; and storing data management **rules** and processing **rules** in the metadata; and wherein the management information comprises one of a pointer to a sequencing **rule,** a pointer to a management **rule,** a pointer to an anchor point for beginning a selected analysis process, or a pointer to a processing **rule**.

Claims Text - CLTX (3):
3. The method of claim 1, wherein the management **rule** comprises one of performance criteria, reliability criteria, availability criteria, and capacity criteria.

Claims Text - CLTX (4):
4. The method of claim 1, wherein the management information comprises a sequencing **rule**.

Claims Text - CLTX (5):
5. The method of claim 4, wherein the sequencing **rule** comprises one of a logical **rule,** a time **rule,** and a structure **rule**.

Claims Text - CLTX (6):
6. The method of claim 1, wherein the management information comprises a management function far accomplishing management **rules**.

Claims Text - CLTX (11):
11. The method of claim 1, wherein processing **rules** define the order of selecting data elements for processing.

Claims Text - CLTX (12):
12. The method of 1, wherein processing **rules** define controls for processing management information for each data element.

Claims Text - CLTX (18):
18. The method of claim 1, wherein management information comprises a pointer to the location where **rules** are stored.

Claims Text - CLTX (19):
19. A self-defining data element for enhanced data management and recovery, comprising: a data portion; and a metadata portion, wherein the metadata includes management information including management **rules** and processing **rules** and one or more anchor points to begin selected analysis processes; and wherein the management information comprises one of a pointer to a sequencing **rule,** a pointer to a management **rule,** a pointer to an anchor point for beginning a selected analysis process, or a pointer to a processing **rule**.

Claims Text - CLTX (21):
21. The self-defining data element of claim 19, wherein the management **rule** comprises one of performance criteria, reliability criteria, availability criteria, and capacity criteria.

Claims Text - CLTX (22):
22. The self-defining data element of claim 19, wherein the management

information comprises a pointer to a management **rule**.

Claims Text - CLTX (23):
23. The self-defining data clement of claim 19, wherein the management
information comprises a sequencing **rule**.

Claims Text - CLTX (24):
24. The self-defining data element of claim 23, wherein the sequencing **rule**
comprises one of a logical **rule,** a time **rule,** and a structure **rule**.

Claims Text - CLTX (25):
25. The self-defining data element of claim 19, wherein the management
information comprises a pointer to a sequencing **rule**.

Claims Text - CLTX (26):
26. The self-defining data element of claim 19, wherein the management
information comprises a management function for accomplishing management **rules**.

DOCUMENT-IDENTIFIER: US 20140172930 A1

TITLE: FAILURE RESILIENT DISTRIBUTED REPLICATED DATA STORAGE SYSTEM

PATENT-FAMILY-ID: 50932227

Claims Text - CLTX (1):

1. A system comprising: a plurality of storage zones, each storage zone comprising a plurality of nodes wherein each node comprises a plurality of storage **devices and a controller, the controller** including a processor and **memory** a first node of a plurality of nodes included in a first zone of the plurality of zones, the first node having instructions which when executed cause a first processor included in a first **controller** in the first node to perform actions including: receiving a storage request from a client of the system to store a data item partitioning the data item into a plurality of data **objects, each object** including a storage **policy identifier** and a data portion creating a plurality of parity **objects** for the data item creating reassembly instructions for the data item storing groups of some of the data **objects** and groups of some of the parity **objects** and the reassembly instructions among the nodes included in the storage zones according to a predetermined set of criteria. wherein each of the data objects are included in at least one of the groups of data objects. wherein each of the parity objects are included in at least one of the groups of parity objects. wherein the predefined set of criteria ensures that the data item can be reconstructed by a accessing a subset of the plurality of data objects and the plurality of the parity objects.

Claims Text - CLTX (16):

16. A system comprising: a plurality of storage zones, each storage zone comprising a plurality of storage nodes wherein each storage node comprises a plurality of storage **devices and a controller, the controller** including a processor and **memory** a first node of a plurality of nodes included in a first zone of the plurality of zones, the first node having instructions which when executed cause a first processor included in a first **controller** in the first node to perform actions including: receiving a storage request from a client of the system to store a data item, the storage

request include (a) the data item or a data item reference and (b) a storage criteria partitioning the data item into a plurality of data **objects, each object** including a storage **policy identifier** and a data portion according to the storage criteria creating a plurality of parity **objects** for the data item according to the storage criteria creating reassembly instructions for the data item according to the storage criteria storing a the data **objects** and the parity **objects** among the nodes among the storage zones according to the storage criteria storing the reassembly instructions among the storage nodes among the storage zones wherein each of the data **objects** are included in at least one of the storage zones wherein each of the parity **objects** are included in at least one of the storage zones wherein the reassembly instructions specify how the data item can be reconstructed from a subset of the plurality of data **objects** and the plurality of parity **objects**.

US-PAT-NO: 8578111

DOCUMENT-IDENTIFIER: US 8578111 B2

TITLE: Backup optimization policy table for controlling buffered/un-buffered input/output

DATE-ISSUED: November 5, 2013

PRIOR-PUBLICATION-INFORMATION:

DOCUMENT-IDENTIFIER	DOCUMENT-DATE
US 20130091333 A1	April 11, 2013

PATENT-FAMILY-ID: 48042877

Primary Examiner - XP (1):

Lane; John

Claims Text - CLTX (1):

1. A method for backup optimization, the method comprising: collecting, by a data collector module of a host device, values for a plurality of device parameters; receiving, by a **policy** module of the host device, values for the plurality of device parameters; updating, by the **policy** module of the host device, a **policy** table with the values for the plurality of device parameters; receiving, by an optimizer module of a host device, the **policy** table; determining, by the optimizer module of the host device, whether to proceed with buffered input/output or un-buffered input/output for a read call based at least in part on the **policy** table; and instructing, by the optimizer module of the host device, a read module of a backup application to proceed with either buffered input/output or un-buffered input/output for the read call.

Claims Text - CLTX (3):

3. The method of claim 1, wherein determining whether to proceed with buffered input/output or un-buffered input/output comprises evaluating the **policy** table in view of a **rule** set.

Claims Text - CLTX (6):

6. The method of claim 1, wherein the optimizer module instructs the reader module to proceed with buffered input/output for the read call if the **policy** table indicates that a file system type is a hierarchical file system.

Claims Text - CLTX (8):

8. A processor-readable storage medium having processor-executable instructions stored thereon that, when executed, cause a processor to: collect values for a plurality of device parameters; update a **policy** table with the values for the plurality of device parameters; determine, based at least in part on the **policy** table, whether to proceed with buffered input/output or un-buffered input/output for a read call; and send an instruction to proceed with either buffered input/output or un-buffered input/output for the read call.

Claims Text - CLTX (10):

10. The processor-readable storage medium of claim 8, wherein determining whether to proceed with buffered input/output or un-buffered input/output comprises evaluating the values in the **policy** table in view of a **rule** set.

Claims Text - CLTX (12):

12. The processor-readable storage medium of claim 8, comprising further processor-executable instructions that, when executed, cause the processor to update the **policy** table with a recommended input/output technique based on the current and prior values in the **policy** table.

Claims Text - CLTX (14):

14. A system comprising: one or more memories; and one or more processors communicatively coupled to the one or more memories, wherein the one or more memories store instructions that when executed by the one or more processors implement operations comprising collecting values for a plurality of device parameters; receiving the values for the plurality of device parameters and updating a **policy** table; determining, based on the **policy** table, whether to proceed with buffered input/output or un-buffered input/output for a read call; and providing instructing to proceed with either buffered input/output or un-buffered input/output for the read call.

Claims Text - CLTX (15):

15. The system of claim 14, wherein the instructions, when executed, determine whether to proceed with buffered input/output or un-buffered input/output for the read call by evaluating the **policy** table in view of a **rule** set.

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	4	"8578111".pn. or "6973556".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 11:14
L2	4041	(programmable with memory with controller).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 11:16
L3	6	(programmable with memory with controller with policy).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 11:17
L4	100	((processor or microprocessor or computer or cpu) with memory adj5 controller with policy).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 11:23
L5	7	"20110075555"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 11:25
L6	4	"20160054922"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 11:26
L7	9	4 AND ((G06F13/1694 OR G06F2009/45583 OR G06F2212/70).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 11:30
L8	349	((processor or microprocessor or computer or cpu) with memory adj5 controller with policy)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 11:33
L9	25	8 AND ((G06F13/1694 OR G06F2009/45583 OR G06F2212/70).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 11:34
L10	1282	((jack or john) and lane).xp.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 11:52
L11	6	10 and ((processor or microprocessor or computer or cpu) with memory adj5 controller with policy)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 11:52
L12	708	(((memory or device) with controller) with object with (id or identif$5)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 12:04

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002
Page 143

L13	0	12 AND ((G06F13/1694 OR G06F2009/45583 OR G06F2212/70).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 12:07
L14	15	(((memory or device) with controller) with object with (Id or identif$5) same (policy or rule)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 12:08
L15	2	"20100218177"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 12:18
L16	5	"20150052167"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 12:26
L17	2	16 and (storage adj5 devices)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 12:26
L18	2	16 and (controller)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 12:28
L19	3	16 and (storage with (media or device))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 12:34
L20	3	16 and (instruct$5 or code or program$5 or application or app)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 12:40
L21	3	16 and (instruct$5 or code or program$5 or application or app or software)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 12:42
L22	2	16 and (policy or rule)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 12:44
L23	3	16 and (request$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 12:47
L24	3	16 and (data or object)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 12:49
L26	2	16 and ((stor$5 or writ$5 or record$5 or sav$5) with (policy or rule))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 12:50
L27	2	16 and (identifier)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 12:55
L28	2	16 and ((read$5 or recover$5 or return$4) with (object or id or identifier))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2019/04/29 12:58

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002
Page 144

			IBM_TDB			
L29	2	16 and ((read$5 or recover$5 or return$4))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 13:00
L30	3	16 and (metadata)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 13:04
L31	2	16 and (metadata with (id or identifier))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 13:09
L32	2	16 and (image or text or picture)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 13:31
L33	2	16 and (image or text or picture or density or compact$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 13:32
L34	0	16 and (density or compact$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/29 13:32

4/29/2019 2:09:51 PM

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002
Page 145

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O.BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

Setter Roche LLP
14694 Orchard Parkway
Building A, Suite 200
Westminster, CO 80023

Courtesy Reminder for
Application Serial No: 15/804,772

Attorney Docket No: 980.0023
Customer Number: 76444
Date of Electronic Notification: 05/03/2019

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:
uspto@setterroche.com

To view your correspondence online or update your email addresses, please visit us anytime at **https://ppair-my.uspto.gov/pair/PrivatePair.**
If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/804,772	Filing Date 11/06/2017	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $40 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $210 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	10/03/2019	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 36	Minus	** 36	= 0		x $50 =	0
	Independent (37 CFR 1.16(h))	* 4	Minus	*** 4	= 0		x $230 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/JESSICA T GAYNOR/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal

Application Number:	15804772
Filing Date:	06-Nov-2017
Title of Invention:	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR
First Named Inventor/Applicant Name:	Joshua Johnson
Filer:	Stephen S. Roche/Jamie Cameron
Attorney Docket Number:	980.0023

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 2 months with $0 paid	2252	1	300	300
Miscellaneous:				
		Total in USD ($)		**300**

Electronic Acknowledgement Receipt	
EFS ID:	37361444
Application Number:	15804772
International Application Number:	
Confirmation Number:	2463
Title of Invention:	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR
First Named Inventor/Applicant Name:	Joshua Johnson
Customer Number:	76444
Filer:	Stephen S. Roche/Jamie Cameron
Filer Authorized By:	Stephen S. Roche
Attorney Docket Number:	980.0023
Receipt Date:	03-OCT-2019
Filing Date:	06-NOV-2017
Time Stamp:	17:02:57
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$300
RAM confirmation Number	E201903H03104804
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Extension of Time	2019-10-03_980-0023_EOT.pdf	147979 2abb4e7f7ee9d0051b0ae37e37057587292 3e83a	no	2
Warnings:					
Information:					
2	Amendment/Req. Reconsideration-After Non-Final Reject	2019-10-03_980-0023_Response_to_NFOA.pdf	72317 883d7cb38369ac09d5828600cacc7c793df d0f65	no	14
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30904 1b31ad6296492b94e4dfd6cd5f1afe88e3e7 ba1f	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	251200		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/AIA/22 (03-13)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) 980.0023
Application Number 15/804,772	Filed 11/06/2017
For DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR	
Art Unit 2139	Examiner John A. Lane

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	Micro Entity Fee	
☐	One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☑	Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$ 300
☐	Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐	Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐	Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☑ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☐ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number _____.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 52176.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Stephen S. Roche/ — Signature

10/03/2019 — Date

Stephen S. Roche — Typed or printed name

(303) 641-1762 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ * Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Practitioner's Docket No. 980.0023 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Joshua Johnson et al. Confirmation No.: 2463

Application No.: 15/804,772 Art Unit: 2139

Filed: 11/06/2017 Examiner: Lane, John A.

For: DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR

Mail Stop: Amendment
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT

In response to the non-final Office action dated 05/03/2019, please enter the present amendment and consider the following remarks.

In the Claims:

CLAIMS

What is claimed is:

1. (Currently Amended) An apparatus comprising:

a storage device;

a device controller operatively coupled with the storage device, comprising a memory;

an application stored on the memory and comprising instructions that, when executed, direct the device controller to at least:

receive ~~a~~ at least one storage device policy, wherein the at least one storage device policy indicates at least a storage density;

receive a storage request[[,]] ~~comprising content~~ to store content;

store the content on the storage device ~~according to the~~ at the storage density specified by the at least one storage device policy;

record storage information for the content on the memory, comprising at least a content identifier for the content;

subsequent to storing the content, receive a content request for the content, comprising at least the content identifier for the content;

in response to the content request, retrieve from the memory the storage information for the content;

recover the content from the storage device, at least in part according to the storage information; and

respond to the content request at least by returning the content.

2. (Currently Amended) The apparatus of claim 1, wherein the storage ~~device policy~~ density indicated by the at least one storage device policy comprises a ~~data storage areal~~ recording path density.

3. (Currently Amended) The apparatus of claim [[1]] 2, wherein the at least one storage device policy further comprises a head/media interface strength.

4. (Currently Amended) The apparatus of claim [[1]] 3, wherein the at least one storage device policy further comprises instructions related to media defect treatment on the storage device.

5. (Currently Amended) The apparatus of claim [[1]] 4, wherein the storage ~~device comprises a magnetic disk~~ density indicated by the at least one storage device policy further comprises a recording frequency.

6. (Currently Amended) The apparatus of claim [[1]] 5, wherein the at least one storage device ~~comprises a solid-state memory device~~ policy further comprises instructions to differentiate content by a content type.

7. (Original) The apparatus of claim 1, wherein the content identifier is assigned by the device controller and is returned in a response to the storage request.

8. (Original) The apparatus of claim 1, wherein the instructions, when executed, direct the device controller to further:

reply to the storage request with a request for a storage device policy update;

receive a storage device policy update; and

update the storage device policy in accordance with the storage device policy update.

9. (Currently Amended) An apparatus comprising:

a storage device;

a device controller operatively coupled with the storage device, comprising a memory;

an application stored on the memory and comprising instructions that, when executed, direct the device controller to at least:

receive ~~a~~ at least one storage device policy, wherein the at least one storage device policy indicates at least a storage density;

store content on the storage device at the storage density specified by the at least one storage device policy;

record storage information for the content on the memory, comprising at least a content identifier for the content;

subsequent to storing the content, receive a content request for the content, comprising at least the content identifier for the content;

in response to the content request, retrieve from the memory the storage information for the content;

recover the content from the storage device, according to the storage information and according to the at least one storage device policy; and

respond to the content request at least by returning the content.

10. (Currently Amended) The apparatus of claim 9, wherein the at least one storage device policy comprises a command timeout.

11. (Currently Amended) The apparatus of claim [[9]] 10, wherein the at least one storage device policy further comprises a read retry count.

12. (Currently Amended) The apparatus of claim [[9]] 11, wherein the at least one storage device policy further comprises instructions related to background task controls.

13. (Original) The apparatus of claim 9, wherein the storage device comprises a magnetic disk.

14. (Original) The apparatus of claim 9, wherein the storage device comprises a solid-state memory device.

15. (Original) The apparatus of claim 9, wherein the content identifier is assigned by the device controller and is returned in a response to the storage request.

16. (Currently Amended) An apparatus comprising:

a storage device;

a device controller operatively coupled with the storage device, comprising a memory;

an application stored on the memory and comprising instructions that, when executed, direct the device controller to at least:

receive a storage policy, wherein the storage policy comprises ~~comprising~~ a write-protection policy and a storage density;

receive a storage request[[,]] ~~comprising content~~ to store content;

store the content on the storage device ~~according to the~~ at the storage density specified by the storage policy;

record storage information for the content on the memory, comprising at least a content identifier for the content;

subsequent to storing the content, receive a delete request for the content, comprising at least the content identifier for the content;

in response to the delete request, retrieve from the memory the storage information for the content; and

respond to the delete request, indicating that the content was not deleted in accordance with the write-protection policy.

17. (Original) The apparatus of claim 16, wherein the storage policy and the delete request are received from the same source.

18. (Original) The apparatus of claim 16, wherein the storage policy and the delete request are received from different sources.

19. (Original) The apparatus of claim 16, wherein the delete request is a modification request.

20. (Original) The apparatus of claim 16, wherein the delete request is an overwrite request.

21. (Currently Amended) An apparatus comprising:

a storage device;

a device controller operatively coupled with the storage device, comprising a memory;

an application stored on the memory and comprising instructions that, when executed direct the device controller to at least:

receive a storage policy, wherein the storage policy indicates at least a storage density;

receive a storage request[[,]] ~~comprising content~~ to store content;

store the content on the storage device ~~according to~~ at the storage density specified by the storage policy;

send storage information for the content ~~storage~~ to a remote location;

~~storing~~ store lookup information comprising at least a content identifier for the content and an information pointer for the storage information;

subsequent to storing the content, receive a lookup request for the content, comprising at least the content identifier for the content;

in response to the lookup request, retrieve storage information for the content from the remote location, based at least in part on the information pointer; and

retrieve the content.

22. (Original) The apparatus of claim 21, wherein the information pointer is a network address.

23. (Original) The apparatus of claim 21, wherein the step of retrieving storage information further comprises sending an authentication to the remote location.

24. (Original) The apparatus of claim 21, wherein the information pointer is stored in a header attached to the content.

25. (Original) The apparatus of claim 21, wherein the information pointer is stored in a memory separate from to the content.

26. (Currently Amended) An apparatus comprising:

a storage device;

a device controller operatively coupled with the storage device, comprising a memory, the device controller configured to receive content to be stored on the storage device;

a programmable processor configured to implement a storage device policy wherein the storage device policy indicates at least a storage density, the programmable processor communicatively coupled with the device controller such that the content received by the device controller to be stored on the storage device must pass though the programmable processor; and

an application stored on the memory and comprising instructions that, when executed, direct the device controller to at least store the content on the storage device after the content has been processed by the programmable processor at the storage density specified by the storage device policy.

27. (Original) The apparatus of claim 26, wherein the programmable processor is unprogrammed when the apparatus is manufactured.

28. (Currently Amended) The apparatus of claim 26, wherein the programmable processor is configured to implement the storage device policy wherein the storage device policy further comprises instructions to encrypt content.

29. (Currently Amended) The apparatus of claim 26, wherein the programmable processor is configured to implement the storage device policy wherein the storage device policy further comprises instructions to identify a pattern in the content.

30. (Original) The apparatus of claim 29, wherein the pattern is a symbol or string.

31. (Original) The apparatus of claim 29, wherein the pattern is an image.

32. (Currently Amended) An apparatus comprising:

a storage device;

a device controller operatively coupled with the storage device, comprising a memory;

an application stored on the memory and comprising instructions that, when executed, direct the device controller to at least:

receive a storage device policy, wherein the storage device policy indicates a plurality of storage densities;

differentiate content by a content type;

store a first content on the storage device at a first density in accordance with the storage device policy; and

store a second content on the storage device at a second density ~~and~~ in accordance with the storage device policy[[;]] ~~and~~ wherein the first density and the second density differ.

33. (Original) The apparatus of claim 32, wherein the first density and the second density are dictated by a slope at which the first content and the second content are stored on the storage device.

34. (Original) The apparatus of claim 32, wherein the first content and the second content are both stored on the storage device.

35. (Currently Amended) The apparatus of claim [[32]] 34, wherein the first content is an image, and the second content is not an image.

36. (Currently Amended) The apparatus of claim [[32]] 34, wherein the first content and the second content are ~~of~~ different content types.

Remarks

Claims 1-36 are pending in the application. Claims 1-36 stand rejected. Claims 1-6, 9-12, 16, 21, 26, 28-29, 32, and 35-36 are herein amended. Claims 1, 9, 16, 26, and 32 are the independent claims. The Applicant respectfully requests consideration of the following remarks and allowance of the claims.

35 U.S.C. § 112 Rejection

Claim 2 stands rejected under U.S.C. § 112(b). Specifically, the Office action states that the limitation in claim 2 which states "the storage device policy comprises a data storage areal density" is indefinite and does not point out and distinctly claim any subject matter (Office action p. 2). The Office action places specific emphasis placed on the term "areal" as used in claim 2.

The Applicant has amended claim 2 to overcome the U.S.C. § 112(b) rejection. Claim 2 as amended herein now recites, the apparatus of claim 1, wherein the storage density comprises a recording path density. A recoding path is region on a magnetic surface, such as a magnetic hard disk drive, where information is recorded as described in paragraph [0053] of the specification. A recoding path density describes the distance between one or more adjacent recording paths as shown in Figure 2B.

Therefore, considering the discussion above, the Applicant respectfully requests withdrawal of the U.S.C. § 112(b) rejection of claim 2.

35 U.S.C. § 102 Rejections

Claims 1-36 stand rejected under 35 U.S.C. § 102(a)(2) as being anticipated by U.S. Patent Application Publication No. 2015/0052167 (Olster) referred to hereon as Olster. The Applicant respectfully traverses the rejection for at least the following reasons.

Claim 1 as amended herein now recites, in part, a device controller operatively coupled with the storage device, comprising a memory; an application stored on the memory and comprising instructions that, when executed, direct the device controller to at least: receive at least one storage device policy***, wherein the at least one storage device policy indicates at least a storage density***; receive a storage request to store content; store the content on the storage device

at the ***storage density specified by the at least one storage device policy***. The applicant respectfully asserts that the art of record fails to teach at least these limitations of claim 1.

The Office action asserts that Olster teaches a device controller that receives a storage device policy (Office action, p. 4). In particular, the Office action asserts that Olster teaches these limitations at paragraph [0030], where Olster teaches that [storage] policies have two components: a replication and placement component as well as a searchability component. The replication and placement component of a policy defines the replication and placement of data objects in the data storage system (Olster, paragraph [0031]). Olster further states that the searchability component of a [storage] policy may specify those metadata fields in an object group that are searchable, if any (Olster, paragraph [0032]). However, claim 1 as amended herein requires that the device controller to receive at least one storage device policy, wherein the at least one storage device policy indicates at least a storage density. Contrasting this limitation or claim 1, Olster does not make any mention of a storage policy that indicates a ***storage density*** of any type. Therefore, the storage policies taught by Olster and the storage device policy of the claimed invention are fundamentally distinct, and therefore not anticipated by Olster.

The Office action further asserts that Olster teaches a device controller which stores the content on the storage device according to the storage device policy. In particular, the Office action asserts that Olster teaches these limitations in paragraph [0030] where Olster states that the object and its constituent data portion may be stored among storage nodes and storage zones according to the storage policy. However, claim 1 as amended herein further requires a device controller to store the content on the storage device at the storage density specified by the storage device policy. Olster fails to mention or suggest a device controller that directs a storage device to store content at a ***density specified by a storage device policy.*** In contrast, the replication and placement policy directs a device controller as to how many times content is replicated and where the content is placed in a storage system. Olster provides examples of replication and placement policies which include, full distribution, single copy, single copy to a specific zone, and copy to all zone[s] but a specified zone (Olster, paragraph [0031]). The storage policy examples as provided by Olster do not teach or suggest a storage device policy which directs a device controller to store content on a storage device at a specific storage density.

The Office further claims that Olster teaches storing content on a storage device according to the storage device policy in paragraph [0039] where Olster states the maximum size of the

embedded object databases may be a configuration parameter of the system of it may be a parameter of the policy that the objects are stored under. However, the object database is a storage location for object specific information including certain metadata about the objects (Olster, paragraph [0039]). Although the object database may be a parameter configured by the storage policy, it is not related to storing content at a density specified by a storage device policy and therefore does not anticipate claim 1.

Furthermore, Olster does not teach or suggest anything relating to mechanisms which affect content storage density on a storage device. For example, Olster fails to teach a device controller which alters the storage density on a storage device by changing the spacing between recording pathways on a hard disk drive or a device controller which alters the frequency at which data is recorded on a hard disk drive. The device controller as taught by Olster may handle coordination, management, search queries, and the distribution and promulgation of storage and replication policies (Olster, paragraph [0025]). In contrast, Olster does not disclose a controller which would perform any operation which would affect the density at which data is being recorded. In fact, Olster fails to mention or suggest anything relating to ***density, storage density,*** or storing content at a ***specific density*** anywhere the publication. Consequently, Olster does not disclose a storage device controller which directs a storage device to store information on the storage device at a storage density specified by a storage device policy.

Based on the above comments, Olster does not teach or suggest all of the limitations of independent claim 1 and consequently fails to anticipate every limitation of independent claim 1. Claim 1 is therefore allowable over the art of record and such indication is respectfully requested.

Independent claims 9, 16, 21, 26 and 32 contain limitations similar to those of claim 1 and are therefore allowable over the art of record for at least the same reasons as discussed above for claim 1. Dependent claims 2-8, 10-15, 17-20, 22-25, 27-31, and 33-36, while separately allowable over the art of record, depend from otherwise allowable independent claims. Therefore, the Applicant respectfully contends that claims 2-8, 10-15, 17-20, 22-25, 27-31, and 33-36 are allowable for at least the reasons presented above in support of their respective independent claims, and such indication is respectfully requested. The Applicant refrains from further discussion of the independent claims for the sake of brevity.

35 U.S.C. § 103 Rejections

Claims 2-8, 10-15, 17-20, 22-25, and 33-36 stand rejected under 35 U.S.C. § 103 as being unpatentable over Olster in view of known prior art. The Office action indicates that Official notice is taken of the prior art teaching any dependent claim feature not specifically discussed or found in Olster (Office action p. 8). The Applicant respectfully traverses the rejection of dependent claims 2-8, 10-15, 17-20, 22-25, and 33-36 at least because the Office has failed to establish a prima facie case of obviousness. Additionally, the Applicant respectfully traverses this attempted use of Official Notice as improper, at least because the Office's attempt to take Official Notice is not in compliance with the Office's own procedures as laid out in subchapter 2144.03 of the *Manual of Patent Examining Procedure* (MPEP). Specifically, the Office's attempt to officially notice the level of ordinary skill in the art fails to at least comply with subsections 2144.03(A) and 2144.03(B) of the MPEP. Consequently, a necessary element of a prima facie case is absent. The Office action further asserts that the dependent claim features, while part of the invention, appear to be well known and their relevance not essential to the main invention found in the independent claims (Office action, p. 8).

Firstly, it is to be appreciated that the Office action asserts that the dependent claim features are not essential to the main invention found in the independent claims (Office action, p. 8). However, claim 2 as amended now recites, the apparatus of claim 1, wherein the storage density comprises a recording path density. Additionally, claim 5 as amended now recites, the apparatus of claim 4, wherein the storage density further comprises a recording frequency. Both claims are now essential to defining the "storage density" as recited in claim 1. More specifically, these claims define how the device controller will control the mechanical operation of a magnetic disk hard drive with relation to how densely data is to be stored. For at least these reasons, the Applicant respectfully asserts that the Office action is incorrect in the assertion that the dependent claim features are not essential to the invention in the independent claims. The Applicant refrains from further discussion regarding the relevance of the remaining dependent claims for the sake of brevity.

Secondly, the MPEP states it would not be appropriate for the examiner to take Official Notice of facts without citing a prior art reference where the facts asserted to be well known are not capable of instant and unquestionable demonstration as being well-known (MPEP § 2144.03(A)). The Office action asserts that the dependent claim features, while part of the

invention, appear to be well known (Office action p. 8). However, the MPEP goes on to state that assertions of technical facts in the areas of esoteric technology or specific knowledge of the prior art must always be supported by citation to some reference work recognized as standard in the pertinent art (MPEP § 2144.03(A)). The Office action offers no explanation as to why the technical facts of the claimed technology do not fall under the area of esoteric technology or an area where specific knowledge of the prior art is required. Additionally, the Office action fails produce a citation of any referenced work that would be recognized as standard in the pertinent art. Naked assertions about what is allegedly known in the art, like those made at page 8 of the Office action, cannot satisfy these requirements. Consequently, the Office has failed to properly determine whether it was appropriate to take Official Notice without documentary evidence to support the Examiner's conclusion as required by MPEP § 2144.03(A) nor has the Office provided citation to reference recognized as standard in the pertinent art as further required by MPEP § 2144.03(A).

When Official Notice is taken of a fact and is unsupported by documentary evidence, the technical line of reasoning underlying a decision to take such a notice must be clear and unmistakable. The *Manual of Patent Examining Procedure* (MPEP) states the examiner must provide specific factual findings predicated on sound technical and scientific reasoning to support the conclusion of common knowledge (MPEP § 2144.03(B)). However, the Office action fails to provide any specific factual findings to support the conclusion that the dependent claims are common knowledge within the art. The MPEP goes on to explain that this means the Office should present an Applicant with the explicit basis on which Official Notice is based so that the Applicant is able to challenge the assertion in the next reply after the Office action (MPEP §2144.03(B)). Again, naked assertions about what is allegedly known in the art, like those made at page 8 of the Office action, cannot satisfy these requirements. For at least these reasons, the Applicant respectfully asserts that the Office's attempt to officially notice the level of ordinary skill in the art is improper and consequently has failed to establish a prima facie case of obviousness needed to sustain a rejection under 35 U.S.C. § 103.

Thirdly, the Applicant respectfully asserts once more that dependent claims 2-8, 10-15, 17-20, 22-25, 27-31, and 33-36, while separately allowable over the art of record, depend from otherwise allowable independent claims. Therefore, the Applicant respectfully contends that claims 2-8, 10-15, 17-20, 22-25, 27-31, and 33-36 are allowable for at least the reasons presented

above in support of their respective independent claims, and such indication is respectfully requested.

In summary, the Office's attempts at Official Notice are improper and traversed. Claims 2-8, 10-15, 17-20, 22-25, 27-31, and 33-36, are therefore allowable over the art of record and such indication is respectfully requested.

CONCLUSION

Based on the above remarks, the Applicant submits that the claims in their present form are allowable over the art of record. Additional reasons in support of patentability exist, but such reasons are moot in light of the above remarks and are omitted in the interests of clarity and brevity. No estoppel is intended and no estoppel should apply to assertions in the recent Office action that are not refuted herein. The Applicant respectfully requests allowance of the claims at the Examiner's earliest convenience.

Included herewith is the appropriate fee for a two-month extension of time. The applicant believes no additional fees are due. However, should the Office determine that fees are necessary, the Office is hereby requested to contact the undersigned to arrange for payment of the applicable fees.

Respectfully submitted,

/Stephen S. Roche/
SIGNATURE OF PRACTITIONER
Stephen S. Roche, Reg. No. 52,176
Setter Roche LLP
Telephone: (303) 641-1762
E-mail: steve@setterroche.com

Correspondence address:

CUSTOMER NO. 76444
Setter Roche LLP
14694 Orchard Parkway
Building A, Suite 200
Westminster, CO 80023

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	REQUEST ID
15/804,772		2139	97129

PAIR Correspondence Address/Fee Address Change

The following fields have been changed to Customer Number 70440 on 10/05/2019 via Private PAIR in view of the certification copied below that authorized the change.

- Correspondence Address

The address for Customer Number 70440 is:
70440
SETTER ROCHE LLP
14694 Orchard Parkway
Building A, Suite 200
Westminster, CO 80023

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

An attorney or Agent of Record registered to practice before the Patent and Trademark Office who has been given power of attorney in this application

Signature:	/Kirk A. Cesari/
Name:	Kirk A. Cesari
Registration Number:	47479

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	REQUEST ID
15/804,772		2139	97129

PAIR Correspondence Address/Fee Address Change

The following fields have been changed to Customer Number 70440 on 10/05/2019 via Private PAIR in view of the certification copied below that authorized the change.

- Maintenance Fee Address

The address for Customer Number 70440 is:
70440
SETTER ROCHE LLP
14694 Orchard Parkway
Building A, Suite 200
Westminster, CO 80023

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

An attorney or Agent of Record registered to practice before the Patent and Trademark Office who has been given power of attorney in this application

Signature:	/Kirk A. Cesari/
Name:	Kirk A. Cesari
Registration Number:	47479

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/804,772	11/06/2017	Joshua Johnson	980.0023	2463

70440 7590 10/25/2019

SETTER ROCHE LLP
14694 Orchard Parkway
Building A, Suite 200
Westminster, CO 80023

EXAMINER
LANE, JOHN A

ART UNIT	PAPER NUMBER
2139	

NOTIFICATION DATE	DELIVERY MODE
10/25/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@setterroche.com

PTOL-90A (Rev. 04/07)

Office Action Summary	**Application No.** 15/804,772	**Applicant(s)** Johnson et al.	
	Examiner JOHN A LANE	**Art Unit** 2139	**AIA (FITF) Status** Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 10/03/2019.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☑ This action is **FINAL.** 2b) ☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-36 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-36 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

1. This Office action is responsive to the amendment filed 10/03/2019.

2. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-36 are rejected under 35 U.S.C. 103 as being unpatentable over Olster et al. (US 2015/0052167) in view of Leow et al. (US 2002/0036852).

1. An apparatus comprising:

a storage device (**corresponds to "storage media", see [0022], [0026] and throughout Olster; corresponds to disk drive 100, see Fig. 1 of Leow**);

a device controller operatively coupled with the storage device (**corresponds to "controller…included with the storage media and/or storage node", see [0026] and throughout Olster; corresponds to controller/circuit board 128 and/or circuitry including frequency processor 308, see [0047], [0048] of Leow**) comprising a memory (**corresponds to "volatile memory and non-volatile memory", see [0024] and throughout Olster; corresponds to "BPI setting table may be stored in a controller (not shown)", see [0047] of Leow**); an application stored on the memory and comprising instructions (**corresponds to "software", "application program", "object code", "machine code", see [0020] and throughout Olster; programming of some kind appears to be inherent within the device of Leow**) that, when executed, direct the device controller to at least:

receive at least one storage device policy (**corresponds to "storage policy", "policy" or "polices", see [0030] and throughout Olster; corresponds to "capacity requirements of the disc drive", "error rate requirements", "BPI setting", see [0020], [0023] and throughout Leow**) wherein the at least one storage device policy indicates at least a storage density

(corresponds to "BPI setting", "selected data density", see [0017] and throughout Leow);

receive a storage request **(corresponds to "request", (see [0046], [0047] and throughout Olster; corresponds to signals generated by host computer (not shown), see [0014] of Leow)** to store content **(corresponds to "data" or "object" discussed throughout Olster; corresponds to "data" discussed throughout Leow)**;

store the content on the storage device at the storage density specified by the at least one storage device policy **(corresponds to "[t]he object including its constituent data portion may be stored among storage nodes and storage zones according to the storage policy…", see [0030] of Olster; "replication and placement component of a policy defines the replication and placement of data objects in the data storage system", see [0031] of Olster; "[t]he maximum size of the embedded object databases may be a configuration parameter…or parameter of the policy", see [0039] of Olster; corresponds to "density" discussed throughout Leow)**;

record storage information for the content on the memory, comprising at least a content identifier for the content **(corresponds to "metadata", "object identifier", (see [0039], [0040], [0041] and throughout Olster)**;

subsequent to storing the content, receive a content request for the content, comprising at least the content identifier for the content **(corresponds to "reading", see [0029]) "request" throughout Olster)**;

in response to the content request, retrieve from the memory the storage information for the content **(corresponds to reading metadata (see [0039], [0041] and [0049] of Olster)**;

recover the content from the storage device, at least in part according to the storage information **(corresponds to reading the file/data/object using metadata, object identifier, etc. of Olster)**; and

respond to the content request at least by returning the content.

26. An apparatus comprising:

a storage device **(discussed above)**;

a device controller operatively coupled with the storage device, comprising a memory, the device controller configured to receive content to be stored on the storage device **(discussed above)**;

a programmable processor configured to implement a storage device policy wherein the storage device policy indicated a least a storage density **(corresponds to "processors such as microprocessors", see [0020] and**

throughout Olster, see above with regard to Leow), the programmable processor communicatively coupled with the device controller such that the content received by the device controller to be stored on the storage device must pass though the programmable processor; and

an application stored on the memory and comprising instructions that, when executed, direct the device controller to at least store the content on the storage device after the content has been processed by the programmable processor at the storage density specified by the storage device policy **(discussed above)**.

32. An apparatus comprising:

a storage device **(discussed above)**;

a device controller operatively coupled with the storage device, comprising a memory **(discussed above)**;

an application stored on the memory and comprising instructions that, when executed, direct the device controller to at least **(discussed above)**:

receive a storage device policy, wherein the storage device policy indicates a plurality of storage densities **(discussed above)**;

differential content by content type;

store a first content on the storage device at a first density in accordance with the storage device policy **(corresponds to storing "documents, images, audio, videos", see [0060] of Olster; "[a]dditional fields may also be stored as metadata regarding the object such as a code or designator or text name for (a) the kind of data represented by the object, including, for example, image, video, audio, text document, and the like…", see [0039] of Olster; see also above regarding storing data in accordance with metadata and/or policy)**; and

store a second content on the storage device at a second density and in accordance with the storage device policy; and

wherein the first density and the second density differ (corresponds to storing another type of data in accordance with metadata and/or policy).

Independent claims 9, 16 and 21 define embodiments similar in scope to that of claim 1 and are rejected accordingly.

The remaining dependent claim features are expressly or inherently found in the applied art.

4. Applicant's arguments filed 10/03/2019 have been fully considered but they are not deemed to be persuasive.

Applicant should reconsider the rejection above in section 3 of the Office action with regard to the claimed "density". As stated in the Official notification in the prior Office action, storing or recording data in accordance with densities to manage errors/corruption/error rate on a disk appears to be well known as found in Leow.

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 C.F.R. section 1.136(a).

6. A SHORTENED STATUTORY PERIOD FOR RESPONSE TO THIS FINAL ACTION IS SET TO EXPIRE THREE MONTHS FROM THE DATE OF THIS ACTION. IN THE EVENT A FIRST RESPONSE IS FILED WITHIN TWO MONTHS OF THE MAILING DATE OF THIS FINAL ACTION AND THE ADVISORY ACTION IS NOT MAILED UNTIL AFTER THE END OF THE THREE-MONTH SHORTENED STATUTORY PERIOD, THEN THE SHORTENED STATUTORY PERIOD WILL EXPIRE ON THE DATE THE ADVISORY ACTION IS MAILED, AND ANY EXTENSION FEE PURSUANT TO 37 C.F.R. □ 1.136(a) WILL BE CALCULATED FROM THE MAILING DATE OF THE ADVISORY ACTION. IN NO EVENT WILL THE STATUTORY PERIOD FOR RESPONSE EXPIRE LATER THAN SIX MONTHS FROM THE DATE OF THIS FINAL ACTION.

Any response to this final action should be mailed to:
Box AF

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

or faxed to:

(571) 273-8300, (for Official communications intended for entry)

Or:

(571) 273-4208, (for Non-Official or Draft communications, please label "Non-Official" or "DRAFT")

Or:

Via e-mail at Jack.Lane@uspto.gov (for Non-Official or Draft communications, please label "Non-Official or "DRAFT")

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JOHN A LANE whose telephone number is 571 272-4208. The examiner can normally be reached on M-F 6:30am-6pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Reg Bragdon can be reached on 571 272-4204.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571 272-2100.

/JOHN A LANE/
Primary Examiner, Art Unit 2139

Notice of References Cited	Application/Control No. 15/804,772	Applicant(s)/Patent Under Reexamination Johnson et al.	
	Examiner JOHN A LANE	Art Unit 2139	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-5596458-A	01-1997	Emo; Bruce D.	G11B5/00	360/46
*	B	US-6195218-B1	02-2001	Guttmann; James Edward	G11B5/012	360/48
*	C	US-20020036852-A1	03-2002	Leow, SoonWah	G11B20/1816	360/31
*	D	US-20040174627-A1	09-2004	Kim, Jong-yoon	G11B5/09	360/31
*	E	US-20060061356-A1	03-2006	Makifuchi; Masaki	G11B5/455	324/212
*	F	US-8151077-B1	04-2012	Bauer; Andreas L.	G06F12/0802	711/118
*	G	US-9280987-B1	03-2016	Bao; Haoji	G11B20/1217	1/1
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/804,772	Johnson et al.
	Examiner	Art Unit
	JOHN A LANE	2139

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
EAST text search	04/29/2019	JAL
EAST to date	10/21/2019	JAL
STIC search	10/22/2019	JAL

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
711	ALL	04/29/2019	JAL

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002
Page 182

US-PAT-NO: 8151077

DOCUMENT-IDENTIFIER: US 8151077 B1

TITLE: Application aware cache management

DATE-ISSUED: April 3, 2012

PATENT-FAMILY-ID: 45877479

Series Code and Application Number - APP (1):

12/164336

Brief Summary Text - BSTX (8):

Typically, a memory in a modern digital data processing system such as a data storage system consists of a hierarchy of storage elements, extending from large **-capacity** but relatively slow storage elements and various levels of lower **-capacity** and relatively fast storage devices. The large **-capacity** and relatively slow devices include such types of devices as disk or tape storage devices which store information on a magnetic medium; such devices are relatively inexpensive on a storage cost per unit of storage basis. Intermediate in the hierarchy, both in terms of speed and storage **capacity** are random-access memories, which are somewhat faster than the disk or tape devices, but which are also more expensive on a storage cost per unit of storage basis. At the fastest end of the hierarchy are cache memories, which are also the most expensive and thus generally the smallest.

Brief Summary Text - BSTX (9):

Generally, during processing operations, a processor will enable information to be processed to be copied from the slower devices to the increasingly faster devices for faster retrieval. Generally, transfers between, for example, disk devices and random-access memories are in relatively large blocks, and transfers between the random-access memories and cache memories are in somewhat smaller "cache lines." In both cases, information is copied to the random-access memory and cache memory on an "as needed" basis, that is, when the processor determines that it needs particular information in its processing, it will enable blocks or cache lines which contain information to be copied to the respective next faster information

storage level in the memory hierarchy. Certain prediction methodologies have been developed to attempt to predict the whether a processor will need information for processing before it (that is, the processor) actually needs the information, and to enable the information to be copied to the respective next faster information storage level. However, generally at some point in the processing operations, the processor will determine that information required for processing is not available in the faster information storage level, that is, a "read miss" will occur, and it (that is, the processor) will need to delay its processing operations until the information is available. Generally, the rate at which read misses will occur with storage element(s) at a particular level in the hierarchy will be related to the storage **capacity** of the storage element(s) at the particular level, as well as the pattern with which the processor accesses the information in the respective storage level. In any case, to enhance the processing efficiency of a digital data processing system, it is generally helpful to be able to assess the effect of changing the **capacity** of the memory element(s) at a particular level in the memory hierarchy on the rate of read misses at the particular level. (Similarly, with respect to a write cache, if a write cache is full of data that has not yet been destaged to slower storage elements, a write pends until a portion of the cache is flushed. In another case, write-through may be used when the cache is full. In either case, a similar delay to that experienced for the read miss is endured.)

Description Paragraph - DETX (36):

The generic storage resource requirements 104 may be mapped by the second mapping or translation stage 122 into physical data storage requirements 106. The requirements 106 may vary with the particular type of data storage system (e.g., different data storage system by same or different vendor), customer's configuration and data storage environment (e.g., which data storage system types, number of each, vendor), amount and type of cache, number and type of devices on each data storage system (e.g., disks, disk or other device characteristics such as **capacity,** number of disks), and the like. The requirements 106 identify data storage system resources used in connection with implementing or fulfilling a request to provision storage for use by the application. Such resources may include the one or more physical devices from which storage is allocated for use in storing data and any parity information. In an embodiment in which the data storage system is a multiprocessor architecture, a designated section of cache of the data storage system may be assigned to service I/O requests for one or more portions of the allocated storage. (Note that it is possible to practice the technique by allowing all applications to share the same cache but to prioritize one application's storage over another. Thus, in an alternative preferred embodiment, instead of setting aside a portion of the cache for each application, a priority scheme is used,

such that when there is little competition for resources, all applications may take advantage of the cache.) The processing of stage 122 maps the generic requirements of 104 in accordance with the different data storage specific properties that may be associated with each provision request to the physical resources of the data storage system. As an example, a provision request for an application is mapped to a section of cache in accordance with the data storage best practices codified in 122. With reference to the generic storage requirements 104 that may refer to write-weighted or read-weighted cache configuration, data storage system best practices may determine how-weighted and read-weighted cache configuration are defined for each type of data storage system.

Description Paragraph - DETX (41):

A policy may be defined in an embodiment in accordance with the best practices for applications and data storage systems. A policy may be characterized as an instantiation of the application practices and/or data storage system best practices in an embodiment. A policy including application best practices may specify defaults used in connection with the different user levels for one or more applications. For example, for an email application, the policy may specify a cache configuration strategy and a default amount of mailbox data storage **capacity** and log storage **capacity** for each mailbox or group of mailboxes, may indicate that mailbox data is stored on FAST storage and that log data is stored on CHEAP storage, and may also specify other application independent or application-neutral criteria that may be used in servicing the provisioning request. The other criteria may include whether the data storage for the application should be allowed to share a RAID group with a different application thus affecting I/O performance, whether the storage needs to be expandable for use with the application's future storage needs, an expansion factor or amount indicating a threshold minimum amount of available storage for use with future data storage needs of the application, and the like. A policy including data storage system best practices may define CHEAP and FAST for each type of data storage system. For example, an embodiment may specify a data storage system best practices policy for a first type of data storage system in which FAST is defined as using Fibre Channel drives, a RAID-10 configuration of device pairs, and assigning servicing of I/O requests by a particular data storage system service processor since the first type of data storage system is a multi-processor architecture. For a second type of data storage system, FAST may be defined as using Fibre channel drives, and a RAID-5 (4 data drives+1 parity drive) configuration. The second type of data storage system does not include multiple data storage system service processors for servicing I/O requests thus no data storage service processor assignment is made. If the second type of data storage system does not support use of Fibre channel drives but rather uses a different form of storage or other device having high speed performance

characteristics, then such a device may be specified rather than the Fibre channel devices. Different elements that may be included in a policy are described herein in more detail.

Description Paragraph - DETX (43):

Referring to FIG. 4, shown is an example illustrating use of the techniques herein with the two stage mapping processing as described in connection with FIG. 1. The example 200 includes application provision requirements 202 which are input in connection with a NOVICE user proficiency level for an email application hosting storage on the data storage system. In this example, the requirements of 202 include a server name, such as "SERVER1", and a number of mailboxes, such as 500. The user may be requesting that storage be allocated for 500 mailboxes for use with an email application. The application best practices for the email application may be codified using a script, rules, programming language, and the like, which map the requirements of 202 to the generic storage resource requirements of 204. In this example, the element 204 includes the generic storage resource requirements further annotated with application specific information as will be described in more detail below. In an embodiment, one or more candidate solutions or ways in which the resource provisioning request may be serviced may be specified in terms of the generic resource requirements. The example 200 illustrates a generic cache configuration solution and two possible or candidate storage pool solutions 204a and 204b. For each of these candidate solutions, the currently available resources of the data storage system may be examined to see if the provisioning request may be implemented in accordance with each candidate solution. In other words, each candidate solution specifies a cache configuration solution or amounts and types of data storage needed to fulfill the current provision request. The current state of available resources on the data storage system is examined to determine if it is possible to allocate resources as needed for each candidate solution. It may be that there are insufficient resources available on the data storage system so that one or more candidate solutions are eliminated. (For example, the data storage system may have little or no ability to modify its cache configuration.) In this example, candidate solution 204a indicates that 5 storage groups (SGs) may be formed in which each SG consists of storage for 100 mailboxes. Each SG may include 2 volumes of FAST storage of **capacity** SIZE1 for storing mail data, and 1 volume of CHEAP storage of **capacity** SIZE2 for logging purposes. Both of the foregoing are stored on storage which is PROTECTED or provides data protection in the event of device failure. Data protection may be a generic way of specifying some form of data redundancy such as mirroring, or other technique (e.g., RAID protection via parity information) by which data recovery is possible in the event of a data device failure. Candidate solution 204b indicates that a single SG may be formed consisting of storage for all 500 mailboxes. The SG may include 10 volumes of FAST storage of

capacity SIZE1 for storing mail data, and 5 volumes of CHEAP storage of **capacity** SIZE2 for logging purposes. In connection with solution 204b, additional CRITERIA may be specified of OWN GROUP. In one embodiment, OWN GROUP may be used to indicate that the storage allocated for use by the email application should be from a RAID group which does not share storage with any other application. Such criteria may affect the performance of servicing I/O requests for each application hosting data included in the same RAID group. In another embodiment, OWN GROUP may indicate that the data storage in connection with this single provisioning request should be in its own RAID group so that these particular 500 mailboxes do not share a same RAID group with other mailboxes for this email application or another application.

Description Paragraph - DETX (54):

Element 210 may represent results including the cache configuration and the different storage pools configured from the physical devices of the data storage system. In other words, element 210 may represent the cache configuration and the different storage pools configured from the physical devices as illustrated in FIG. 3 in accordance with data storage system best practices for a currently defined policy. (Note that application aware cache best practices may have different cache configurations for different proposed solutions. For example, if a 100 SG solution delivers higher disk performance, the cache requirements might be lower than the cache requirements for the 10 SG solution. Thus, the cache configuration is not necessarily independent of the solution selected.) Element 210 includes a cache which is 80% allocated to read cache and 20% allocated to write cache. Element 210 includes FAST storage pool A of SIZE X, and FAST storage pool A2 of SIZE X1. Element 210 may also include CHEAP storage pool B of SIZE Y. For purposes of illustration, a policy may be in effect which defines FAST storage as preferably formed from Fibre channel devices with a RAID-10 configuration of pairs of physical devices for mirroring, and CHEAP storage formed from ATA (Advanced Technology Attachment) devices with RAID-5 having 8 data drives and 1 parity drive (8+1). At data storage system startup time, FAST storage pool A and CHEAP storage pool B may be configured. At a first later point in time, 5 more Fibre channel drives may be added to the data storage system for additional storage **capacity** and processing may be performed to configure these 5 drives into storage pools for use with the techniques herein. In accordance with data storage system best practices, although RAID 10 may be preferred over other RAID levels and configurations, the data storage system best practices may note that 5 drives have been added and thus, to make use of all 5 drives, a RAID 5 configuration of 4 data drives and 1 parity drive may be preferred in this particular instance with the addition of an odd number of 5 drives. (The addition of drives and other application storage may cause a change to the cache configuration. Best practices can be applied each time something

changes in the system.) As such, the code implementing the data storage system best practices may result in formation of the FAST storage pool A2.

Description Paragraph - DETX (55):

For each candidate solution 204a and 204b, the different storage pools, currently available data storage **capacity,** and associated properties of 210b are examined in accordance with the following for each candidate solution: the type of storage (e.g., FAST or CHEAP), the amount of storage of the different types required to implement the solution, and the other criteria (e.g., OWN GROUP) and other attributes specified (e.g., PROTECTED).

Description Paragraph - DETX (69):

FIG. 7 illustrates an example of overall operation flow. The user enters an application description (step 710), which depending on the user's proficiency level may include only high level information such as the identity or type of application and scale information (e.g., email software and number of users, or network share and **capacity**). Storage is provisioned as described above (step 720). Cache is then configured (step 730), based on the application description and the corresponding storage objects as provisioned. The storage becomes available to the application (step 740). On an ongoing basis, the configuration is modified based on current conditions and parameters (step 750)

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S220	2	"7581061".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 08:53
S221	0	S220 and (density)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 08:53
S222	677	((policy or rule) with density).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 09:00
S223	2028	((policy or rule) with density).ab,ti.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 09:01
S224	13555	((policy or rule) with density)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 09:01
S225	1	15/804,772	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 09:04
S226	1	S225 and (error or reduc$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 09:04
S227	74	((policy or rule) same density same	US-PGPUB;	OR	ON	2019/10/21

		(error or fail$4 or bad or defect$6 or corrupt$5)).clm.	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			09:06
S228	316	((policy or rule) same density same (error or fail$4 or bad or defect$6 or corrupt$5)).ab,ti.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 09:06
S229	3392	((policy or rule) same density same (error or fail$4 or bad or defect$6 or corrupt$5))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 09:07
S230	20	S227 AND ((G06F17/5081 OR G06F17/5072 OR G06F17/5068 OR G06F11/104 OR G06F11/1076 OR G06F11/3696 OR G06F16/9027 OR G06F21/552 OR G06F21/566 OR G06F17/18 OR G06F17/5045 OR G06F21/554 OR G06F21/577 OR G11C29/785 OR G11C29/808).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 09:39
S231	707	((policy or rule) same density same (error or fail$4 or bad or defect$6 or corrupt$5) same (stor$4 or writ$4))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 09:46
S232	15	((policy or rule) same density same (error or fail$4 or bad or defect$6 or corrupt$5) same (stor$4 or writ$4)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 09:46
S233	34	((policy or rule) same density same (error or fail$4 or bad or defect$6 or corrupt$5) same (stor$4 or writ$4)).ab,ti.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 11:24
S234	707	((policy or rule) same density same (error or fail$4 or bad or defect$6 or corrupt$5) same (stor$4 or writ$4))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 11:27
S235	19	S234 AND ((G06F11/10 OR G06F16/27 OR G06F17/5068 OR G06F17/5072 OR G06F17/5077 OR G06F17/5081 OR G06F21/126 OR G06F21/566 OR G06F3/0604 OR G06F3/061 OR	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2019/10/21 11:27

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002
Page 190

		G06F3/0619 OR G06F3/0632 OR G06F3/0658 OR G06F3/0665 OR G06F3/0673 OR G06F3/068 OR G06F9/485).CPC.)	DERWENT; IBM_TDB			
S236	1	15/804,772	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 17:56
S237	1	S236 and ("605")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 17:56
S238	1	S236 and (programmable with processor)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 17:57
S239	1	S236 and (corrupt$5 or error)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 18:02
S240	184	(record$5 same (density or capacity) same (corrupt$5 or bad or fail$5 or error) same (disk or disc or track or magnetic)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 18:07
S241	23	S240 AND ((G11B27/36 OR G11B19/041 OR G11B20/12).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 18:16
S242	2	12/164,336	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 18:21
S243	2	S242 and (density or capacity or frequency)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/21 18:21

10/22/2019 7:42:58 AM
C:\Users\jlane\Documents\EAST\Workspaces\15896879.wsp

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002

DOCUMENT-IDENTIFIER: US 20020036852 A1

TITLE: Adaptive zone frequency compensation for disc drives

PATENT-FAMILY-ID: 34078756

Claims Text - CLTX (4):

3. A process of formatting a **recording** surface of a **disc** drive, wherein the **recording** surface is segmented into a plurality of radial zones each containing a plurality of concentric **tracks** on which data may be **recorded, the disc** drive further includes a head confronting the **recording** surface to transfer data between the head and **tracks on the recording** surface, the process comprising steps of: a) assigning a data frequency for each zone so that all of the zones have a nominal data **density** that is substantially the same; b) measuring an **error** rate of data transfer between the head at least one **track** in each zone; c) comparing the measured **error** rates to a predetermined maximum **error** rate; and d) for a zone whose **error** rate measured in step (b) exceeds the predetermined **error** rate, establishing a data frequency to define a data **density** substantially lower than the nominal data **density** so that an **error** rate for the zone is no greater than the predetermined **error** rate.

Claims Text - CLTX (20):

19. Apparatus for formatting a **recording** surface of a **disc** drive, wherein the **recording** surface is segmented into a plurality of radial zones each containing a plurality of concentric **tracks** on which data may be **recorded, the disc** drive further includes a head confronting the **recording** surface to transfer data between the head and **tracks on the recording** surface, the apparatus comprising: a writer for writing test data to at least one **track** in each zone at a data frequency for the respective zone so that all of the zones have a nominal data **density** that is substantially the same; frequency means for adjusting a data frequency for a zone having an **error** rate greater than a predetermined **error** rate at the nominal data **density** so that the adjusted data frequency defines a data **density** substantially lower than the nominal data **density and an error** rate for the zone is no greater than the predetermined **error** rate.

CPC Current Inventive Classification - CPCI (2):

G11B27/36 20130101

DOCUMENT-IDENTIFIER: US 20060061356 A1

TITLE: Disk testing apparatus, disk testing method, computer product, and disk apparatus

PATENT-FAMILY-ID: 36073304

Claims Text - CLTX (2):

2. The **disk** testing apparatus according to claim 1, wherein the test includes at least one of an **error** rate test and a side erase test, and the condition relaxing unit relaxes the condition of a **recording density** in a direction of circumference of a **disk,** when the result of the test is unsatisfactory only in the **error** rate test; in a direction of radius of the **disk,** when the result of the test is unsatisfactory only in the side erase test; and in the direction of circumference of the **disk,** when the result of the test is unsatisfactory in both the **error** rate test and the side erase test.

Claims Text - CLTX (7):

7. The **disk** testing method according to claim 6, wherein the test includes at least one of an **error** rate test and a side erase test, and the relaxing includes relaxing the condition of a **recording density** in a direction of circumference of a **disk,** when the result of the test is unsatisfactory only in the **error** rate test; in a direction of radius of the **disk,** when the result of the test is unsatisfactory only in the side erase test; and in the direction of circumference of the **disk,** when the result of the test is unsatisfactory in both the **error** rate test and the side erase test.

Claims Text - CLTX (9):

9. The computer-readable **recording** medium according to claim 8, wherein the test includes at least one of an **error** rate test and a side erase test, and the condition relaxing unit relaxes the condition of a **recording density** in a direction of circumference of a **disk,** when the result of the test is unsatisfactory only in the **error** rate test; in a direction of radius of the **disk,** when the result of the test is unsatisfactory only in the side erase test; and in the direction of circumference of the **disk,** when the result of the test

is unsatisfactory in both the **error** rate test and the side erase test.

CPC Current Additional Classification - CPCA (2):

G11B27/36 20130101

DOCUMENT-IDENTIFIER: US 20020036852 A1

TITLE: Adaptive zone frequency compensation for disc drives

PATENT-FAMILY-ID: 34078756

Claims Text - CLTX (4):

3. A process of formatting a **recording** surface of a **disc** drive, wherein the **recording** surface is segmented into a plurality of radial zones each containing a plurality of concentric **tracks** on which data may be **recorded, the disc** drive further includes a head confronting the **recording** surface to transfer data between the head and **tracks on the recording** surface, the process comprising steps of: a) assigning a data frequency for each zone so that all of the zones have a nominal data **density** that is substantially the same; b) measuring an **error** rate of data transfer between the head at least one **track** in each zone; c) comparing the measured **error** rates to a predetermined maximum **error** rate; and d) for a zone whose **error** rate measured in step (b) exceeds the predetermined **error** rate, establishing a data frequency to define a data **density** substantially lower than the nominal data **density** so that an **error** rate for the zone is no greater than the predetermined **error** rate.

Claims Text - CLTX (20):

19. Apparatus for formatting a **recording** surface of a **disc** drive, wherein the **recording** surface is segmented into a plurality of radial zones each containing a plurality of concentric **tracks** on which data may be **recorded, the disc** drive further includes a head confronting the **recording** surface to transfer data between the head and **tracks on the recording** surface, the apparatus comprising: a writer for writing test data to at least one **track** in each zone at a data frequency for the respective zone so that all of the zones have a nominal data **density** that is substantially the same; frequency means for adjusting a data frequency for a zone having an **error** rate greater than a predetermined **error** rate at the nominal data **density** so that the adjusted data frequency defines a data **density** substantially lower than the nominal data **density and an error** rate for the zone is no greater than the predetermined **error** rate.

CPC Current Inventive Classification - CPCI (2):

G11B27/36 20130101

DOCUMENT-IDENTIFIER: US 20040174627 A1

TITLE: Methods of optimizing recording current and setting recording density of hard disk drive

PATENT-FAMILY-ID: 32768468

Claims Text - CLTX (13):

12. A method of optimizing a **recording density** of a hard **disk** drive, comprising: measuring a rate of **errors** in data **recorded** on a target **track** under a predetermined adjacent **track** erasure (ATE) test condition; comparing the rate of **errors** with a predetermined threshold; and adjusting the **recording density** by changing **tracks** per inch (TPI) when the rate of **errors** is larger than the predetermined threshold.

Claims Text - CLTX (27):

26. A method, comprising: determining a range of values of a **recording** parameter for a hard **disk** drive; for at least one **recording** parameter value in the range, **recording** data on a target **track** a first predetermined number of times, **recording** data on **tracks** adjacent to a target **track** a second predetermined number of times, reading the data from the **tracks** adjacent to the target **track** a third predetermined number of times, and determining a number of **recording errors for the recording** parameter value; calculating a total of the **recording errors** for the respective **recording** parameter values; comparing the total to a predetermined threshold; if the total is greater than the predetermined threshold, setting a **recording density** of the hard **disk** drive to a first value; and if the total is not greater than the predetermined threshold, setting the **recording density** of the hard **disk** drive to a maximized value.

CPC Current Inventive Classification - CPCI (3):

G11B27/36 20130101

US-PAT-NO: 9280987

DOCUMENT-IDENTIFIER: US 9280987 B1

****Please see Images for: (Certificate of Correction) ****

TITLE: Methods and apparatus for selecting data density and track density values for magnetic recording media having variable bit aspect ratios

DATE-ISSUED: March 8, 2016

PATENT-FAMILY-ID: 55410493

Claims Text - CLTX (13):

13. A tangible machine-readable **recordable** storage medium, wherein one or more software programs when executed by one or more processing devices implement the following steps: obtaining a plurality of data **density** values as a function of a corresponding plurality of bit **error** rates; obtaining a plurality of **track density** values as a function of a corresponding plurality of bit **error** rates; determining a data **density/track density** correlation between the plurality of data **density** values and the plurality of **track density** values for at least one Sector **Error** Rate (SER); and determining a data **density** capability value and a **track density** capability value that provides an areal **density** capability (ADC) value that satisfies one or more predefined criteria using the data **density/track density** correlation.

CPC Current Inventive Classification - CPCI (5):

G11B27/36 20130101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/804,772	11/06/2017	Joshua Johnson	980.0023	2463

70440 7590 10/30/2019

SETTER ROCHE LLP
14694 Orchard Parkway
Building A, Suite 200
Westminster, CO 80023

EXAMINER	
LANE, JOHN A	

ART UNIT	PAPER NUMBER
2139	

NOTIFICATION DATE	DELIVERY MODE
10/30/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@setterroche.com

Office Action Summary	Application No. 15/804,772	Applicant(s) Johnson et al.	
	Examiner JOHN A LANE	Art Unit 2139	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 10/03/2019.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☑ This action is **FINAL.** 2b) ☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-36 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-36 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

1. This Office action is responsive to the amendment filed 10/03/2019. This Office action is a complete supplemental action to the final Office action mailed 10/25/2019.

2. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-36 are rejected under 35 U.S.C. 103 as being unpatentable over Olster et al. (US 2015/0052167) in view of Leow et al. (US 2002/0036852).

1. An apparatus comprising:

a storage device (**corresponds to "storage media", see [0022], [0026] and throughout Olster; corresponds to disk drive 100, see Fig. 1 of Leow**);

a device controller operatively coupled with the storage device (**corresponds to "controller…included with the storage media and/or storage node", see [0026] and throughout Olster; corresponds to controller/circuit board 128 and/or circuitry including frequency processor 308, see [0047], [0048] of Leow**) comprising a memory (**corresponds to "volatile memory and non-volatile memory", see [0024] and throughout Olster; corresponds to "BPI setting table may be stored in a controller (not shown)", see [0047] of Leow**); an application stored on the memory and comprising instructions (**corresponds to "software", "application program", "object code", "machine code", see [0020] and throughout Olster; programming of some kind appears to be inherent within the device of Leow**) that, when executed, direct the device controller to at least:

receive at least one storage device policy (**corresponds to "storage policy", "policy" or "polices", see [0030] and throughout Olster; corresponds to "capacity requirements of the disc drive", "error rate requirements", "BPI setting", see [0020], [0023] and throughout Leow**) wherein the at least one storage device policy indicates at least a storage density

(corresponds to "BPI setting", "selected data density", see [0017] and throughout Leow);

receive a storage request **(corresponds to "request", (see [0046], [0047] and throughout Olster; corresponds to signals generated by host computer (not shown), see [0014] of Leow)** to store content **(corresponds to "data" or "object" discussed throughout Olster; corresponds to "data" discussed throughout Leow)**;

store the content on the storage device at the storage density specified by the at least one storage device policy **(corresponds to "[t]he object including its constituent data portion may be stored among storage nodes and storage zones according to the storage policy…", see [0030] of Olster; "replication and placement component of a policy defines the replication and placement of data objects in the data storage system", see [0031] of Olster; "[t]he maximum size of the embedded object databases may be a configuration parameter…or parameter of the policy", see [0039] of Olster; corresponds to "density" discussed throughout Leow)**;

record storage information for the content on the memory, comprising at least a content identifier for the content **(corresponds to "metadata", "object identifier", (see [0039], [0040], [0041] and throughout Olster)**;

subsequent to storing the content, receive a content request for the content, comprising at least the content identifier for the content **(corresponds to "reading", see [0029]) "request" throughout Olster)**;

in response to the content request, retrieve from the memory the storage information for the content **(corresponds to reading metadata (see [0039], [0041] and [0049] of Olster)**;

recover the content from the storage device, at least in part according to the storage information **(corresponds to reading the file/data/object using metadata, object identifier, etc. of Olster)**; and

respond to the content request at least by returning the content.

26. An apparatus comprising:

a storage device **(discussed above)**;

a device controller operatively coupled with the storage device, comprising a memory, the device controller configured to receive content to be stored on the storage device **(discussed above)**;

a programmable processor configured to implement a storage device policy wherein the storage device policy indicated a least a storage density **(corresponds to "processors such as microprocessors", see [0020] and**

throughout Olster, see above with regard to Leow), the programmable processor communicatively coupled with the device controller such that the content received by the device controller to be stored on the storage device must pass though the programmable processor; and

an application stored on the memory and comprising instructions that, when executed, direct the device controller to at least store the content on the storage device after the content has been processed by the programmable processor at the storage density specified by the storage device policy (**discussed above**).

32. An apparatus comprising:

a storage device (**discussed above**);

a device controller operatively coupled with the storage device, comprising a memory (**discussed above**);

an application stored on the memory and comprising instructions that, when executed, direct the device controller to at least (**discussed above**):

receive a storage device policy, wherein the storage device policy indicates a plurality of storage densities **(discussed above)**;

differential content by content type;

store a first content on the storage device at a first density in accordance with the storage device policy **(corresponds to storing "documents, images, audio, videos", see [0060] of Olster; "[a]dditional fields may also be stored as metadata regarding the object such as a code or designator or text name for (a) the kind of data represented by the object, including, for example, image, video, audio, text document, and the like…", see [0039] of Olster; see also above regarding storing data in accordance with metadata and/or policy)**; and

store a second content on the storage device at a second density and in accordance with the storage device policy; and

wherein the first density and the second density differ **(corresponds to storing another type of data in accordance with metadata and/or policy)**.

Leow et al. teach (see [0006] and throughout as discussed above) decreasing/increasing/modifying the data densities (bits per in) (BPI) of tracks on disc memory to improve error rates. The error rates are determined by heads 111 failing to successfully read bits without an error (see [0026]). A reduction in density (BPI) spreads out the recorded data bits so that the data is not corrupted and the read/write heads are able to successfully read the data.

Because manipulating the data densities on disc memory improves error rates, it would have been obvious to use such a data density modification scheme in the device of Olster to improve reliability. Therefore, the claimed invention would have been obvious to one of ordinary skill in the art before the effective filing data of the claimed invention.

Independent claims 9, 16 and 21 define embodiments similar in scope to that of claim 1 and are rejected accordingly.

The remaining dependent claim features are expressly or inherently found in the applied art.

4. Applicant's arguments filed 10/03/2019 have been fully considered but they are not deemed to be persuasive.

Applicant should reconsider the rejection above in section 3 of the Office action with regard to the claimed "density". As stated in the Official notification in the prior Office action, storing or recording data in accordance with densities to manage errors/corruption/error rate on a disk appears to be well known as found in Leow.

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 C.F.R. section 1.136(a).

6. A SHORTENED STATUTORY PERIOD FOR RESPONSE TO THIS FINAL ACTION IS SET TO EXPIRE THREE MONTHS FROM THE DATE OF THIS ACTION. IN THE EVENT A FIRST RESPONSE IS FILED WITHIN TWO MONTHS OF THE MAILING

DATE OF THIS FINAL ACTION AND THE ADVISORY ACTION IS NOT MAILED UNTIL AFTER THE END OF THE THREE-MONTH SHORTENED STATUTORY PERIOD, THEN THE SHORTENED STATUTORY PERIOD WILL EXPIRE ON THE DATE THE ADVISORY ACTION IS MAILED, AND ANY EXTENSION FEE PURSUANT TO 37 C.F.R. □ 1.136(a) WILL BE CALCULATED FROM THE MAILING DATE OF THE ADVISORY ACTION. IN NO EVENT WILL THE STATUTORY PERIOD FOR RESPONSE EXPIRE LATER THAN SIX MONTHS FROM THE DATE OF THIS FINAL ACTION.

Any response to this final action should be mailed to:

Box AF

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

or faxed to:

(571) 273-8300, (for Official communications intended for entry)

Or:

(571) 273-4208, (for Non-Official or Draft communications, please label "Non-Official" or "DRAFT")

Or:

Via e-mail at Jack.Lane@uspto.gov (for Non-Official or Draft communications, please label “Non-Official or “DRAFT”)

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JOHN A LANE whose telephone number is 571 272-4208. The examiner can normally be reached on M-F 6:30am-6pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Reg Bragdon can be reached on 571 272-4204.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571 272-2100.

/JOHN A LANE/

Primary Examiner, Art Unit 2139

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/804,772	Johnson et al.
	Examiner	Art Unit
	JOHN A LANE	2139

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
EAST text search	04/29/2019	JAL
EAST to date	10/21/2019	JAL
STIC search	10/22/2019	JAL

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
711	ALL	04/29/2019	JAL

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/804,772	Filing Date 11/06/2017	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $40 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $210 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	04/24/2020	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 36	Minus	** 36	= 0		x $50 =	0
	Independent (37 CFR 1.16(h))	* 6	Minus	*** 6	= 0		x $230 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/EFREM WARREN/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	15/804,772	Filing Date	2017-11-06	Docket Number (if applicable)	980.0023	Art Unit	2139
First Named Inventor	Joshua Johnson et al.			Examiner Name	John A. Lane		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No ____

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

Applicant Signature

PTO/SB/30EFS (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/David J. Setter/	Date (YYYY-MM-DD)	2020-04-24
Name	David J. Setter	Registration Number	78758

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	15804772
Filing Date:	06-Nov-2017
Title of Invention:	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR
First Named Inventor/Applicant Name:	Joshua Johnson
Filer:	Stephen S. Roche/Karen Dainty
Attorney Docket Number:	980.0023

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	2253	1	700	700
Miscellaneous:				
RCE- 1ST REQUEST	2801	1	650	650
		Total in USD ($)		**1350**

Electronic Acknowledgement Receipt	
EFS ID:	39259218
Application Number:	15804772
International Application Number:	
Confirmation Number:	2463
Title of Invention:	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR
First Named Inventor/Applicant Name:	Joshua Johnson
Customer Number:	70440
Filer:	Stephen S. Roche/Karen Dainty
Filer Authorized By:	Stephen S. Roche
Attorney Docket Number:	980.0023
Receipt Date:	24-APR-2020
Filing Date:	06-NOV-2017
Time Stamp:	15:51:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1350
RAM confirmation Number	E20204NF55387149
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		2020-04-24-980-0023-RFOA.pdf	181440 8d63821b75f8b98468e641e6ba32dd7b220b0e03	yes	16
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Response After Final Action		1	1	
	Claims		2	8	
	Applicant Arguments/Remarks Made in an Amendment		9	16	
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	2020-04-24-980-0023-RCE.pdf	1349965 3290ef087f959e9f06db29cbe2d7b42c85c1bb90	no	3
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	32588 98c99a14c0eeacc874c5adbb90122e55e7bc46ad	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1563993		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Practitioner's Docket No. 980.0023 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Joshua Johnson et al. Confirmation No.: 2463

Application No.: 15/804,772 Art Unit: 2139

Filed: 11/06/2017 Examiner: Lane, John A.

For: DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR

Mail Stop: RCE
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT

In response to the final Office action dated 10/30/2019, please enter the present amendments and consider the following remarks.

AMENDMENTS

In the Claims:

1. (Currently Amended) An apparatus comprising:

a storage ~~**device**~~ **media**;

a device controller operatively coupled with the storage **media** ~~**device, comprising a memory;**~~

~~**an application stored on the memory and comprising instructions that, when executed, direct the device controller**~~ **configured** to at least:

receive**, from a host,** at least one storage device policy, wherein the at least one storage device policy indicates at least a ~~**storage density**~~ **recording method for writing content to the storage media**;

receive a storage request**, from the host,** to store content;

store the content on the storage ~~**device**~~ **media** ~~**at the storage density**~~ **by utilizing the recording method indicated** ~~**specified**~~ by the at least one storage device policy;

record storage information for the content on **[[the]] a** memory **of the device controller**, comprising at least a content identifier for the content;

subsequent to storing the content, receive a content request for the content, comprising at least the content identifier for the content;

in response to the content request, retrieve from the memory **of the device controller,** the storage information for the content;

recover the content from the storage ~~**device**~~ **media**, at least in part according to the storage information; and

respond to the content request at least by returning the content **to the host**.

2. (Currently Amended) The apparatus of claim 1, wherein the ~~**storage density indicated by the**~~ at least one storage device policy **further** comprises ~~**a recording path density**~~ **instructions that direct the device controller to differentiate the content by one or more content types and to assign a customized recording method to each of the one or more content types**.

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002
Page 224

3. (Currently Amended) The apparatus of claim 2, wherein the **recording method indicated by the** at least one storage device policy further comprises a head/media interface strength.

4. (Currently Amended) The apparatus of claim 3, wherein the **recoding method indicated by the** at least one storage device policy further comprises instructions related to media defect treatment on the storage ~~**device**~~ **media**.

5. (Currently Amended) The apparatus of claim 4, wherein the ~~**storage density**~~ **recording method** indicated by the at least one storage device policy further comprises **one or more of a recording path density or** a recording frequency.

6. (Currently Amended) The apparatus of claim 5, wherein the **recording method indicated by the** at least one storage device policy further comprises instructions to ~~**differentiate content by a content type**~~ **determine a priority level for the content wherein the priority level indicates how densely the content is stored.**

7. (Original) The apparatus of claim 1, wherein the content identifier is assigned by the device controller and is returned in a response to the storage request.

8. (Original) The apparatus of claim 1, wherein the instructions, when executed, direct the device controller to further:

reply to the storage request with a request for a storage device policy update;

receive a storage device policy update; and

update the storage device policy in accordance with the storage device policy update.

9. (Currently Amended) An apparatus comprising:

a storage ~~**device**~~ **media**;

a device controller operatively coupled with the storage **media** ~~**device, comprising a memory;**~~

~~**an application stored on the memory and comprising instructions that, when executed, direct the device controller**~~ **configured** to at least:

receive**, from a host,** at least one storage device policy, wherein the at least one storage device policy indicates at least a ~~**storage density**~~ **recording method for writing content to the storage media**;

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002
Page 225

store content on the storage **~~device~~** **media** **~~at the storage density~~** **by utilizing the recording method indicated** **~~specified~~** by the at least one storage device policy;

record storage information for the content on **[[the]]** **a** memory **of the device controller**, comprising at least a content identifier for the content;

subsequent to storing the content, receive a content request for the content, comprising at least the content identifier for the content;

in response to the content request, retrieve from the memory **of the device controller** the storage information for the content;

recover the content from the storage **~~device~~** **media**, according to the storage information and according to the at least one storage device policy; and

respond to the content request at least by returning the content **to the host**.

10. (Previously Presented) The apparatus of claim 9, wherein the at least one storage device policy comprises a command timeout.

11. (Previously Presented) The apparatus of claim 10, wherein the at least one storage device policy further comprises a read retry count.

12. (Previously Presented) The apparatus of claim 11, wherein the at least one storage device policy further comprises instructions related to background task controls.

13. (Currently Amended) The apparatus of claim 9, wherein the storage **media** **~~device~~** comprises a magnetic disk.

14. (Currently Amended) The apparatus of claim 9, wherein the storage **media** **~~device~~** comprises a solid-state memory device.

15. (Original) The apparatus of claim 9, wherein the content identifier is assigned by the device controller and is returned in a response to the storage request.

16. (Currently Amended) An apparatus comprising:

a storage **~~device~~** **media**;

a device controller operatively coupled with the storage **media** **~~device, comprising a memory;~~**

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002
Page 226

~~an application stored on the memory and comprising instructions that, when executed, direct the device controller~~ **configured** to at least:

receive**, from a host,** a storage policy, wherein the storage policy comprises **at least** a write-protection policy and ~~a storage density~~ **recording method for writing content to the storage media**;

receive**, from the host,** a storage request to store content;

store the content on the storage **media** ~~device at the storage density specified~~ by **utilizing the recording method of** the storage policy;

record storage information for the content on **[[the]] a** memory **of the device controller**, comprising at least a content identifier for the content;

subsequent to storing the content, receive a delete request for the content, comprising at least the content identifier for the content;

in response to the delete request, retrieve from the memory **of the device controller** the storage information for the content; and

respond to the delete request, indicating that the content was not deleted in accordance with the write-protection policy.

17. (Original) The apparatus of claim 16, wherein the storage policy and the delete request are received from the same source.

18. (Original) The apparatus of claim 16, wherein the storage policy and the delete request are received from different sources.

19. (Original) The apparatus of claim 16, wherein the delete request is a modification request.

20. (Original) The apparatus of claim 16, wherein the delete request is an overwrite request.

21. (Currently Amended) An apparatus comprising:

a storage ~~device~~ **media**;

a device controller operatively coupled with the storage **media** ~~device, comprising a memory;~~

~~an application stored on the memory and comprising instructions that, when executed direct the device controller~~ **configured** to at least:

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002
Page 227

receive a storage policy **from a host**, wherein the storage policy indicates at least a ~~**storage density**~~ **recording method for writing content to the storage media**;

receive**, from the host,** a storage request to store content;

store the content on the storage **media** ~~**device at the storage density**~~ **by utilizing the recording method** specified by the storage policy;

send storage information for the content to a remote location;

store lookup information comprising at least a content identifier for the content and an information pointer for the storage information;

subsequent to storing the content, receive a lookup request for the content, comprising at least the content identifier for the content;

in response to the lookup request, retrieve storage information for the content from the remote location, based at least in part on the information pointer; and

retrieve the content.

22. (Original) The apparatus of claim 21, wherein the information pointer is a network address.

23. (Original) The apparatus of claim 21, wherein the step of retrieving storage information further comprises sending an authentication to the remote location.

24. (Original) The apparatus of claim 21, wherein the information pointer is stored in a header attached to the content.

25. (Original) The apparatus of claim 21, wherein the information pointer is stored in a memory separate from to the content.

26. (Currently Amended) An apparatus comprising:

a storage ~~**device**~~ **media**;

a device controller operatively coupled with the storage **media** ~~**device**~~, comprising a memory, the device controller configured to receive content**, from a host,** to be stored on the storage ~~**device**~~ **media**;

a programmable processor configured to implement a storage device policy wherein the storage device policy indicates at least a ~~**storage density**~~ **a recording method**

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002
Page 228

for writing content to the storage media, the programmable processor communicatively coupled with the device controller such that the content received by the device controller to be stored on the storage ~~**device**~~ **media** must pass though the programmable processor; and

program instructions ~~**an application**~~ stored on the memory **of the device controller** ~~**and comprising instructions**~~ that, when executed, direct the device controller to at least store the content on the storage ~~**device**~~ **media** after the content has been processed by the programmable processor ~~**at the storage density**~~ **by utilizing the recording method** ~~**specified**~~ **indicated** by the storage device policy.

27. (Original) The apparatus of claim 26, wherein the programmable processor is unprogrammed when the apparatus is manufactured.

28. (Previously Presented) The apparatus of claim 26, wherein the programmable processor is configured to implement the storage device policy wherein the storage device policy further comprises instructions to encrypt content.

29. (Previously Presented) The apparatus of claim 26, wherein the programmable processor is configured to implement the storage device policy wherein the storage device policy further comprises instructions to identify a pattern in the content.

30. (Original) The apparatus of claim 29, wherein the pattern is a symbol or string.

31. (Original) The apparatus of claim 29, wherein the pattern is an image.

32. (Currently Amended) An apparatus comprising:

a storage ~~**device**~~ **media**;

a device controller operatively coupled with the storage **media** ~~**device, comprising a memory;**~~

~~**an application stored on the memory and comprising instructions that, when executed, direct the device controller**~~ **configured** to at least:

receive**, from a host,** a storage device policy, wherein the storage device policy indicates ~~**a plurality of storage densities**~~ **recording methods for writing content to the storage media wherein each recording method corresponds to a content type**;

~~differentiate~~ **identify the content type of** a first content **and the** ~~by a~~ content type **of a second content**;

store **[[a]] the** first content on the storage **media** ~~device at a first density~~ **by utilizing a first recording method of the more recording methods** in accordance with the storage device policy; and

store **[[a]] the** second content on the storage **media** ~~device at a second density~~ **by utilizing a second recording method of the recording methods** in accordance with the storage device policy wherein the first ~~density~~ **recording method** and the second ~~density~~ **recording method** differ.

33. (Currently Amended) The apparatus of claim 32, wherein the first **recording method includes a first** density and the second **recording method includes a second** density **and wherein the first density and the second density** are dictated by a slope at which the first content and the second content are stored on the storage **media** ~~device~~.

34. (Currently Amended) The apparatus of claim 32, wherein the first content and the second content are both stored on the storage ~~device~~ **media**.

35. (Previously Presented) The apparatus of claim 34, wherein the first content is an image, and the second content is not an image.

36. (Previously Presented) The apparatus of claim 34, wherein the first content and the second content are different content types.

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002
Page 230

REMARKS

Claims 1-36 are pending in the application. Claims 1-36 stand rejected. Claims 1-6, 9, 13, 14, 16, 21, 26, and 32-34 are herein amended. Claims 1, 9, 16, 26, and 32 are the independent claims. The Applicant respectfully requests consideration of the following remarks and allowance of the claims.

35 U.S.C. § 112 Rejection

Claim 2 ***was previously rejected*** under U.S.C. § 112(b). The applicant thanks the Examiner for the careful consideration of the Applicant's remarks and the removal of the U.S.C. § 112(b) rejection of claim 2.

35 U.S.C. § 102 Rejections

Claims 1-36 ***were previously rejected*** under 35 U.S.C. § 102(a)(2) as being anticipated by U.S. Patent Application Publication No. 2015/0052167 (*Olster*). The Applicant thanks the Examiner for the careful consideration of the Applicant's remarks and the removal of the 35 U.S.C. § 102(a)(2) rejection of claims 1-36.

35 U.S.C. § 103 Rejections

Claims 1-36 stand rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent Application Publication No. 2015/0052167 (hereinafter "*Olster*") in view of U.S. Patent Application Publication No. 2002/0036852 (hereinafter "*Leow*"). The Applicant disagrees. However, for the sole purpose of expediting prosecution, the Applicant has amended claims 1-6, 9, 13, 14, 16, 21, 26, and 32-34. The Applicant reserves the right to pursue any previous version of the claims, or variant thereof (broader or narrower), in this application or in one or more continuation applications.

Claims 1 recites, in part, "a device controller operatively coupled with the storage media configured to at least: receive, from a host, at least one storage device policy, wherein the at least one storage device policy indicates at least a recording method for writing content to the storage media; receive a storage request, from the host, to store content; store the content on the storage media by utilizing the recording method indicated by the at least one storage device policy." The

Applicant respectfully asserts that the art of record fails to render obvious at least these aspects of claim 1. For example, *Olster* is silent with regards to storing content on a storage media by utilizing a recording method for writing content to a storage media that is specified by a storage device policy and received from a host. At best, paragraph [0030] of *Olster* states the following:

> [0030] In some embodiments, files and other data may be partitioned into Smaller portions and stored as multiple objects among multiple storage media 160 in a storage node 150. Files and other data may be partitioned into smaller portions referred to as objects and stored among multiple storage nodes 150 in a storage zone. In one embodiment each object includes a storage policy identifier and a data portion. ***The object including its constituent data portion may be stored among storage nodes and storage zones according to the storage policy specified by the storage policy identifier included in the object***. Various policies may be maintained and distributed or known to the nodes in all zones in the distributed data storage system. The policies may be stored on and distributed from a client 102 to the data storage system 100 and to all zones in the data storage system and to all nodes in the data storage system.

While this paragraph specifically states, "[The] object including its constituent data portion may be stored among storage nodes and storage zones according to the storage policy specified by the storage policy identifier…" there is no reference to utilizing a recording method for writing content to a storage media to store content on the storage media. Instead, *Olster* discloses storing an object among storage zones according to the storage policies which is different than utilizing a recording method for writing content to a storage media. To further elaborate, in paragraph [0031], *Olster* presents a storage policy with two components, a replication and placement component and a searchability component. As taught by *Olster*, the replication and placement component defines the replication and placement of data objects in a storage system while the searchability component of the policy may specify metadata fields of an object group that are searchable. However, neither of these policies, when implemented, would result in a recording method for writing content to a storage media nor a device which utilizes a recording method for writing content to a storage media as required by claim 1.

As presently understood by the Applicant, *Olster* generally relates to a searchable data storage system that includes autonomous and independent storage zones, where each storage zone is made up of storage nodes and where each storage node is made up of storage devices. When a

data item is stored, a local database is updated with information about the newly stored data item. When a search for a data item is received, multiple searches are conducted across all storage devices in all nodes in all zones of the storage system. (see, e.g., Abstract and Figs. 1-2). Here, *Olster* presents a searchable and distributed database. For example, in paragraph [0025] *Olster* states, "a controller for a node or a designated node… may handle coordination, management and search queries. The coordination and management handled by the controller or primary node include the distribution and promulgation of storage and replication policies. The controller or primary node will also receive search queries from a server, distribute the search queries to all nodes in a storage zone, store the results of search queries as an object, and provide the results of the search to the requesting server." As such, *Olster* does not contemplate a storage controller or storage system which stores content on a storage media by utilizing a recording method, received from a host, for writing content to a storage media. Instead, *Olster* discloses a controller for a storage node which distributes storage policies and handles search queries.

To further illustrate this deficiency, paragraph [0039] of *Olster* states the following:

> [0039] ***When objects 310 are stored on the storage device, object specific information including certain metadata about the objects are stored in the object database 320. The object database 320 may be indexed according to the object identifier or OIDs of the objects stored on the storage device***. In one embodiment, each entry in the object database 320 is limited to 256 bytes or less of data per object. Thus the object data base may only store a small amount of information for each object. In alternative embodiments the object database is larger to allow for the storage of a larger number of fields or larger amount of object specific information or metadata. ***The maximum size of the embedded object databases may be a configuration parameter of the system or it may be a parameter of the policy that the objects are stored under***…

This paragraph specifically states, "When objects are stored on the storage device, object specific information including certain metadata about the objects are stored in the object database. The object database may be indexed according to the object identifier of OIDs of the object stored on the storage device." Here, *Olster* describes a storage device that creates a database that includes metadata relating to the content where the size of the database may be altered. However, *Olster* again fails to disclose a device that stores content on a storage media by utilizing a recording

method, received from a host, for writing content to the storage media. As such, claim 1 is not obvious over *Olster* for at least these reasons.

Similarly, *Leow* fails to overcome the shortcomings of *Olster*. As presently understood by the Applicant, *Leow* generally relates to a storage device whose recording data frequency is reduced for a first zone whose error rate is initially less than the predetermined error rate so that the first zone exhibits an error rate meeting the predetermined error rate. The data frequency for a second zone whose data transfer error factor initially exceeds the predetermined error rate is increased to restore any loss of storage capacity of the recording surface due to the reduced data frequency in the first Zone. By doing this, the error rate across the entire storage device is uniform without reducing the overall storage capacity of the storage device (see, e.g., Abstract and Figs. 1-2). Here, *Leow* presents a storage device, such as a magnetic disc hard drive, that will adjust the rate, or density, at which data is stored in order to normalize the error rate exhibited by the storage device. Although *Leow* does disclose altering the storage density of a storage device, *Leow* does not disclose or suggest a device that receives a storage device policy that indicates a recording method for writing content to a storage media. Furthermore, *Leow* fails to disclose or suggest a device that stores content on a storage media by utilizing the recording method, received from a host, for writing content to the storage media. At best, paragraph [0007] of *Leow* states the following:

> [0007] In one embodiment, a recording surface of a disc drive that failed to meet a predetermined error rate is re-formatted. The recording surface is segmented into a plurality of radial zones each containing a plurality of concentric tracks on which data may be recorded. The recording surface is originally formatted with a data frequency for each zone such that all of the zones have substantially the same data density. ***The data frequency is reduced for a first zone whose error rate is greater than the predetermined error rate, and is increased for a second zone whose error rate is less than the predetermined error rate.***

This paragraph specifically states, "[t]he data frequency is reduced for a first zone whose error rate is greater than the predetermined error rate, and is increased for a second zone whose error rate is less than the predetermined error rate." *Leow* again fails to disclose or suggest a suggest a device that stores content on a storage media by utilizing the recording method for writing content to the storage media nor does *Leow* overcome the deficiencies of *Olster*. As such,

claim 1 is not obvious over *Leow* for at least this reason. Furthermore, combining the distributed storage system as taught by *Olster* with error rate normalization techniques as taught by *Leow* still fails to render obvious every limitation of claim 1. As such, claim 1 is not obvious in view of *Olster* and *Leow* in combination.

Based on the above comments, neither *Olster* nor *Leow* – separately or in combination – render obvious all of the limitations of claim 1. Consequently, the prima facie case of obvious needed to sustain a 35 U.S.C. § 103 rejection is absent. Claim 1 is therefore allowable over the art of record and such indication is respectfully requested.

Independent claims 9, 16, 21, 26, and 32 include limitations similar to those of claim 1 and are therefore allowable for at least the same or similar reasons as discussed above for claim 1. Dependent claims 2-8, 10-15, 17-20, 22-25, 27-31, and 33-36, while separately allowable over the art of record, depend from otherwise allowable independent claims. Therefore, the Applicant respectfully contends that claims 2-8, 10-15, 17-20, 22-25, 27-31, and 33-36 are allowable for at least the reasons presented above in support of their respective independent claims, and such indication is respectfully requested.

Claim 2 as amended now recites, in part, "the recording method of the at least one storage device policy further comprises instructions that direct the device controller to differentiate the content by one or more content types and to assign a customized recording method to each of the one or more content types." The Applicant cannot find any teaching or reasonable suggestion of such a feature in *Olster* (or in any of the other cited references) of a device that differentiates "content by one or more content types" and assigns "a customized recoding method." As such, claim 2 is believed to be allowable for at least this additional reason.

Claim 6 as amended now recites, in part, "the recording method specified by the at least one storage device policy further comprises instructions to determine a priority level for the content wherein the priority level indicates how densely the content is stored." The Applicant cannot find any teaching or reasonable suggestion of such a feature in *Olster* (or in any of the other cited references) of a device that determines "a priority level for the content." As such, claim 6 is believed to be allowable for at least this additional reason.

Claim 29 recites, in part, "the storage device policy further comprises instructions to identify a pattern in the content." The Applicant cannot find any teaching or reasonable suggestion of such a feature in *Olster* (or in any of the other cited references) of a device that identifies "a

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002
Page 235

pattern in the content." As such, claim 29 is believed to be allowable for at least this additional reason.

Claim 33 as amended recites, in part, "the first recording method includes a first density and the second recording method includes a second density and wherein the first density and the second density are dictated by a slope at which the first content and the second content are stored on the storage media." The Applicant cannot find any teaching or reasonable suggestion of such a feature in *Olster* (or in any of the other cited references) of a device with storage densities where "the first density and the second density are dictated by a slope." As, such, claim 33 is believed to be allowable for at least this additional reason.

DEPENDENT CLAIMS

In view of the above remarks, a specific discussion of each dependent claim is considered to be unnecessary. Therefore, the Applicant's silence regarding any dependent claim is not to be interpreted as agreement with, or acquiescence to, the rejection of such claim or as waiving any argument regarding that claim.

RESERVATION OF RIGHTS

For the sake of conciseness and clarity, the Applicant may not have addressed every assertion or rejection made in the Office Action, particularly where the Applicant has presented amendments or arguments that the Applicant believes render such assertions/rejections moot. Therefore, the Applicant's silence regarding any such assertions or rejections does not constitute an admission or acquiescence regarding such assertions/rejections or a waiver of any argument relating to such assertions/rejections. The Applicant reserves the right to challenge at a later time any rejection or any factual or legal assertion made by the Office in relation to the present application. The Applicant does not admit that any of the references cited in the Office Action are prior art. The Applicant reserves the right to swear behind any cited reference at a later date, to the extent permitted by law.

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002
Page 236

NO DISCLAIMERS OR DISAVOWALS

Although the present communication may include alterations to the application or claims, or characterizations of claim scope or referenced art, the Applicant is not conceding in this application that previously pending claims are not patentable over the cited references. Rather, any alterations or characterizations are being made to facilitate expeditious prosecution of this application. The Applicant reserves the right to pursue at a later date any previously pending or other broader or narrower claims that capture any subject matter supported by the present disclosure, including subject matter found to be specifically disclaimed herein or by any prior prosecution. Accordingly, reviewers of this or any parent, child or related prosecution history shall not reasonably infer that the Applicant has made any disclaimers or disavowals of any subject matter supported by the present application.

CONCLUSION

The Applicant respectfully submits that the amendments and remarks have overcome the rejections and that the pending claims are in condition for allowance. Accordingly, the Applicant requests that the rejections be withdrawn and that a Notice of Allowance be issued.

The Applicant is paying the fees for a three-month extension of time and an RCE with this response. No additional fees are believed to be due for this response. Should the Office determine fees are necessary, however, the Office is hereby requested to contact the undersigned to arrange for payment.

REQUEST FOR A TELEPHONE INTERVIEW

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned.

Respectfully submitted,

/David J. Setter/
SIGNATURE OF PRACTITIONER
David J. Setter, Reg. No. 78,758
Stephen S. Roche, Reg. No. 52,176
Setter Roche LLP
Telephone: (720) 293-9822
E-mail: steve@setterroche.com

Correspondence address:

CUSTOMER NO. 70440
Setter Roche LLP
1860 Blake Street, Suite 100
Denver, CO 80202

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

70440 7590 05/11/2020

SETTER ROCHE LLP
1860 Blake Street
Suite 100
Denver, CO 80202

EXAMINER
LANE, JOHN A

ART UNIT	PAPER NUMBER
2139	

DATE MAILED: 05/11/2020

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/804,772	11/06/2017	Joshua Johnson	980.0023	2463

TITLE OF INVENTION: DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0.00	$0.00	$500	08/11/2020

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PTOL-85 (Rev. 02/11)

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

70440 7590 05/11/2020
SETTER ROCHE LLP
1860 Blake Street
Suite 100
Denver, CO 80202

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/804,772	11/06/2017	Joshua Johnson	980.0023	2463

TITLE OF INVENTION: DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0.00	$0.00	$500	08/11/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
LANE, JOHN A	2139	711-156000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑Issue Fee ❑Publication Fee (if required) ❑Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002
Page 240

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/804,772	11/06/2017	Joshua Johnson	980.0023	2463

70440 7590 05/11/2020

SETTER ROCHE LLP
1860 Blake Street
Suite 100
Denver, CO 80202

EXAMINER	
LANE, JOHN A	

ART UNIT	PAPER NUMBER
2139	

DATE MAILED: 05/11/2020

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 02/11)

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 15/804,772	Applicant(s) Johnson et al.	
	Examiner JOHN A LANE	Art Unit 2139	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to the amendment and RCE filed 04/24/2020.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 1-36 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☑ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☑ Examiner's Amendment/Comment
6. ☐ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/JOHN A LANE/
Primary Examiner, Art Unit 2139

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

The application has been amended as follows:

In the Claims:

Claim 26, line 7, delete "a" (1st occurrence).

Claim 32, line 14, delete "more".

2. Claims 1-36 are allowable over the prior art of record.

Any response to this action should be mailed to:

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

or faxed to:

(571) 273-8300, (for Official communications intended for entry)

Or:

(571) 273-4208, (for Non-Official or draft communications, please label "Non-Official" or "DRAFT")

Or:

Via e-mail at Jack.Lane@uspto.gov (for Non-Official or Draft communications, please label "Non-Official or "DRAFT")

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Jack Lane whose telephone number is 571 272-4208. The examiner can normally be reached on Mon-Fri 7:30AM-6:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Reg Bragdon can be reached on 571 272-4204.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571 272-2100.

/JOHN A LANE/
Primary Examiner, Art Unit 2139

Notice of References Cited	Application/Control No. 15/804,772	Applicant(s)/Patent Under Reexamination Johnson et al.	
	Examiner JOHN A LANE	Art Unit 2139	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20180121136-A1	05-2018	ISHIYAMA; Masahiro	G11C8/12	1/1
*	B	US-9619429-B1	04-2017	Wang; Tianqing	G06F3/06	1/1
*	C	US-20180349035-A1	12-2018	Ellis; Jackson	G06F3/0673	1/1
*	D	US-20180260154-A1	09-2018	Dronamraju; Ravikanth	G06F3/068	1/1
*	E	US-20160313943-A1	10-2016	HASHIMOTO; Daisuke	G06F3/0659	1/1
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/804,772	Johnson et al.
	Examiner	Art Unit
	JOHN A LANE	2139

CPC						
Symbol					Type	Version
G06F	/	3	/	0632	F	2013-01-01
G06F	/	3	/	0673	I	2013-01-01
G06F	/	3	/	0604	I	2013-01-01
G06F	/	3	/	0658	I	2013-01-01
G06F	/	3	/	068	I	2013-01-01
G06F	/	3	/	0665	I	2013-01-01
G06F	/	3	/	0619	A	2013-01-01
G06F	/	3	/	061	A	2013-01-01

CPC Combination Sets							
Symbol					Type	Set	Ranking	Version
	/		/					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	36	
/JOHN A LANE/ Primary Examiner, Art Unit 2139	04 May 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	26	11A and 11C

U.S. Patent and Trademark Office — Part of Paper No.: 20200504

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002
Page 247

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/804,772	Johnson et al.
	Examiner	**Art Unit**
	JOHN A LANE	2139

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06F	/	12	/	00

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	36	
/JOHN A LANE/ Primary Examiner, Art Unit 2139	04 May 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	26	11A and 11C

U.S. Patent and Trademark Office — Part of Paper No.: 20200504

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002
Page 248

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/804,772	Johnson et al.
	Examiner	**Art Unit**
	JOHN A LANE	2139

☑ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	10	10	19	19	28	28								
2	2	11	11	20	20	29	29								
3	3	12	12	21	21	30	30								
4	4	13	13	22	22	31	31								
5	5	14	14	23	23	32	32								
6	6	15	15	24	24	33	33								
7	7	16	16	25	25	34	34								
8	8	17	17	26	26	35	35								
9	9	18	18	27	27	36	36								

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	36	
/JOHN A LANE/ Primary Examiner, Art Unit 2139	04 May 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	26	11A and 11C

U.S. Patent and Trademark Office Part of Paper No.: 20200504

Meta Platforms, Inc. and Samsung Electronics Co. Ltd. - Ex. 1002
Page 249

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/804,772	Johnson et al.
	Examiner	Art Unit
	JOHN A LANE	2139

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
EAST text search	04/29/2019	JAL
EAST to date	10/21/2019	JAL
STIC search	10/22/2019	JAL
EAST text search	05/04/2020	JAL

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
711	ALL	04/29/2019	JAL

DYNAMIC SINGLE TO MULTIPLE BIT PER CELL MEMORY BAUER, Mark E; TALREJA, Sanjay S; KWONG, Phillip Mu-Lee; MILLS, Duane R; ROZMAN, Rodney R (Inventors). INTEL CORPORATION (Assignee). **WO 1995034074 A1**. (Published 14 Dec 1995). **US 6097637 A**. ... coding. However, other types of data, such as code, is more difficult to encode for operation with an error correction system. Because the integrity of data storage is more critical for some types of data than for others, it is desirable to store some types of data in a low density memory while storing other types of data in a high density memory.

Addressing modes for a dynamic single bit per cell to multiple bit per cell memory Wells, Steven E; Robinson, Kurt B (Inventors). INTEL CORPORATION (Assignee). **US 5515317 A**. (Published 07 May 1996). ... coding. However, other types of data, such as code, are more difficult to encode for operation with an error correction system. Because the integrity of data storage is more critical for some types of data than for others, it is desirable to store some types of data in a low density memory while storing other types of data in a high density memory

DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR Johnson, Joshua; Bruner, Curt; Reh, Jeffrey; Squires, Christopher; Wilson, Brian (Inventors). Gaea LLC (Assignee). US 20180129439 A1. (Published 10 May 2018). Your inventors In an embodiment, a storage device is provided. A device controller with a memory is coupled with the storage device. The memory stores an application with instructions that direct the controller to receive a storage device policy. The instructions further direct the controller to store content from a storage request in accordance with the storage device policy, and record storage information, including at least a content identifier, to the memory. Subsequent to storing the content, the instructions further direct the controller to retrieve the content according to the storage information received in a storage request. According to an implementation, the instructions further provide instruction to refuse a delete request in accordance to the storage information. According to an implementation, the instructions provide direction to store the storage information at a remote location.

15804772 Search Strategy-Dialog

Databases: Abstracts in New Technology & Engineering, British Library Inside Conferences, Computer and Information Systems Abstracts, Ei Compendex®, Electronics & Communications Abstracts, Gale Group Computer Database™, Inspec®, Jane's Defense & Aerospace News, NTIS: National Technical Information Service, SciSearch®: a Cited Reference Science Database

Set#	Searched for	Results
S1	storage N/2 (policies or policy or rule$1 or guideline$1)	12525*
S2	storage N/2 density or recording N/2 path N/2 density or areal N/2 density	60908*
S3	(critical or high N/1 priority) N/3 data	110185*
S4	(lower or smaller or low or small or less or lesser) N/2 (s2 or density)	886047*
S5	(Avoid* or prevent*) N/3 (defect$1 or error$1)	186714*
S6	AU("Johnson, Joshua" or "Bruner, Curt" or "Reh, Jeffrey" or "Squires, Christopher" or "Wilson, Brian" or "Johnson, J" or "Bruner, C" or "Reh, J" or "Squires, C" or "Wilson, B")	35086*
S7	(storing or saving) and s3 and s4	120°
S8	s7 and s1	1°
S9	s7 and s5	6°
S10	s7 and s6	0°
S11	s1 and s2 and s3	2°
S12	s1 N/100 s2	30°
S13	s12 and s6	0°
S14	s12 AND YR(<=2018)	28°

Search Strategy

Databases: Argentina Patents Fulltext, Australia Patents Fulltext, Austria Patents Fulltext, Belgium Patents Fulltext, Brazil Patents Fulltext, Canada Patents Fulltext, China Patents Fulltext, Denmark Patents Fulltext, Derwent Patents Citation Index®, Derwent World Patents Index®, Eurasia Patents Fulltext, European Patents Fulltext, Finland Patents Fulltext, France Patents Fulltext, Germany Patents Fulltext, Global Patents Bibliographic, Great Britain Patents Fulltext, India Patents Fulltext™, Ireland Patents Fulltext, Italy Patents Fulltext, Japan Patents Fulltext, JAPIO - Patent Abstracts of Japan, Korea Patents Fulltext, Luxembourg Patents Fulltext, Mexico Patents Fulltext, Monaco Patents Fulltext, Netherlands Patents Fulltext, Norway Patents Fulltext, Portugal Patents Fulltext, Russia Patents Fulltext, Spain Patents Fulltext, Sweden Patents Fulltext, Switzerland Patents Fulltext, United States Patents Fulltext, WIPO PCT Patents Fulltext

Set#	Searched for	Results

S1	storage N/2 (policies or policy or rule$1 or guideline$1)	82301
S2	storage N/2 density or recording N/2 path N/2 density or areal N/2 density	185389
S3	(critical or high N/1 priority) N/3 data	195999
S4	(lower or smaller or low or small or less or lesser) N/2 (s2 or density)	3282908
S5	(Avoid* or prevent*) N/3 (defect$1 or error$1)	1205779
S6	AU("Johnson, Joshua" or "Bruner, Curt" or "Reh, Jeffrey" or "Squires, Christopher" or "Wilson, Brian" or "Johnson, J" or "Bruner, C" or "Reh, J" or "Squires, C" or "Wilson, B")	15332
S7	CPC("G06F 3/0632" or "G06F 3/0673" or "G06F 3/0604" or "G06F 3/061" or "G06F 3/0619" or "G06F 3/0658" or "G06F 3/0665" or "G06F 3/068")	86250
S8	(storing or saving) N/50 s3 N/50 s4	8
S9	s8 N/100 s1	0
S10	s8 N/100 s5	0
S11	s8 and s6	0
S12	s8 and apda(<=20170120)	8
S13	s8 and apda(<=20170120)	7°
S14	s1 N/50 s2 N/50 s3	0°
S15	s1 N/50 s2	49°
S16	s15 N/50 s5	0°
S17	s15 and s7	3°
S18	s17 and apda(<=20170120)	2°

IP.COM

Complete Main Concept Text
==========
Storage policy storage density invention stores critical or high priority data at a low or lower density

==========
Earliest Priority Date: To 2017-01-20
De-dup: Simple Family Numbers

Patent Collections
==========
US Patents
US Designs
US Applications
EPO Patents
EPO Applications
China Patents
China Applications
Japan Patents
Japan Applications
Korea Patents
Korea Applications
WIPO Applications
Argentina Patents
Argentina Applications
Brazil Patents
Brazil Applications

Canada Patents
Canada Applications
Chile Patents
Chile Applications
Colombia Applications
Costa Rica Applications
Cuba Patents
Cuba Applications
Dominican Republic Applications
Ecuador Patents
Ecuador Applications
El Salvador Applications
Guatemala Applications
Honduras Applications
Mexico Patents
Mexico Applications
Nicaragua Patents
Panama Applications
Peru Applications
Trinidad & Tobago Patents
Uruguay Applications
Austria Patents
Austria Applications
Belarus Patents
Belgium Patents
Belgium Applications
Bosnia & Herzegovina Patents
Bosnia & Herzegovina Applications
Bulgaria Patents
Bulgaria Applications
Croatia Patents
Croatia Applications
Czech Republic Patents
Czech Republic Applications
Czechoslovakia Patents
Czechoslovakia Applications
Denmark Patents
Denmark Applications
Estonia Patents
Estonia Applications
EUIPO Patents
Finland Patents
Finland Applications
France Patents
France Applications
Germany Patents
Germany Applications
Great Britain Patents
Great Britain Applications
Greece Patents
Greece Applications
Hungary Patents
Hungary Applications
Iceland Patents
Iceland Applications
Ireland Patents
Ireland Applications
Italy Patents
Italy Applications
Latvia Patents
Latvia Applications
Lithuania Patents
Lithuania Applications
Luxembourg Patents
Malta Patents
Monaco Patents
Montenegro Patents
Montenegro Applications
Netherlands Patents
Netherlands Applications
Norway Patents
Norway Applications
Poland Patents
Poland Applications
Portugal Patents
Portugal Applications
Republic of Moldova Patents
Republic of Moldova Applications
Romania Patents
Romania Applications
San Marino Patents
San Marino Applications
Serbia Patents
Serbia Applications
Slovakia Patents
Slovakia Applications
Slovenia Patents
Spain Patents
Spain Applications
Sweden Patents
Sweden Applications
Switzerland Patents
Switzerland Applications
Ukraine Patents
Yugoslavia/Serbia and Montenegro Patents
Yugoslavia/Serbia and Montenegro Applications
Armenia Patents
Australia Patents
Australia Applications
Cyprus Patents
Gulf Cooperation Council Patents
Hong Kong Patents
India Patents
India Applications
Indonesia Patents
Indonesia Applications
Israel Applications
Jordan Patents
Kyrgyzstan Patents
Macao Applications
Malaysia Patents
Mongolia Patents
New Zealand Patents
Philippines Patents
Philippines Applications
Saudi Arabia Patents
Singapore Patents
Singapore Applications
Taiwan Patents
Taiwan Applications
Tajikistan Patents
Tajikistan Applications
Thailand Applications

Uzbekistan Patents
Vietnam Patents
Algeria Patents
ARIPO Patents
ARIPO Applications
Egypt Patents
Kenya Patents
Malawi Patents
Morocco Patents
Morocco Applications
OAPI Patents
South Africa Patents
Tunisia Applications
Zambia Patents
Zimbabwe Patents
EAPO Patents
EAPO Applications
Georgia Patents
Georgia Applications
Kazakhstan Patents
Kazakhstan Applications
Russia Patents
Russia Applications
Turkey Patents
Turkey Applications

NPL Collections
==========
IEEE Xplore Publications: IEEE Periodicals
IEEE Xplore Publications: IEEE Conferences
IEEE Xplore Publications: IEEE Standards
IEEE Xplore Publications: IEEE Early Access
IEEE Xplore Publications: IET Periodicals
IEEE Xplore Publications: IET Conferences
IEEE Xplore Publications: SMPTE Periodicals
IEEE Xplore Publications: SMPTE Conferences
IEEE Xplore Publications: SMPTE Standards
IEEE Xplore Publications: MIT Press eBooks
IEEE Xplore Publications: Wiley-IEEE eBooks
IEEE Xplore Publications: IBM Periodicals
IEEE Xplore Publications: URSI Periodicals
IEEE Xplore Publications: VDE Conferences
IEEE Xplore Publications: Periodicals from China
IP.com Prior Art Database: The IP.com Journal
IP.com Prior Art Database: Internet Society RFC
IP.com Prior Art Database: IBM TDB Archive
IP.com Prior Art Database: Legacy Journals
IP.com Prior Art Database: Software Patent Institute
OnePetro.org: Periodicals at OnePetro.org
OnePetro.org: Conferences at OnePetro.org
OnePetro.org: Standards at OnePetro.org
Other Literature: IBM Redbooks
Other Literature: PubMed Central

Version #2
Classic Syntax limited to: storage NEAR2 density

US007581061B2

(12) **United States Patent**
Miyagaki et al.

(10) **Patent No.: US 7,581,061 B2**
(45) **Date of Patent: Aug. 25, 2009**

(54) **DATA MIGRATION USING TEMPORARY VOLUME TO MIGRATE IIIGII PRIORITY DATA TO HIGH PERFORMANCE STORAGE AND LOWER PRIORITY DATA TO LOWER PERFORMANCE STORAGE**

(75) Inventors: **Atsushi Miyagaki**, Odawara (JP); **Koji Yasuta**, Hiratsuka (JP)

(73) Assignee: **Hitachi, Ltd.**, Tokyo (JP)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 472 days.

(21) Appl. No.: **11/640,324**

(22) Filed: **Dec. 18, 2006**

(65) **Prior Publication Data**

US 2008/0104343 A1 May 1, 2008

(30) **Foreign Application Priority Data**

Oct. 30, 2006 (JP) 2006-294300

(51) **Int. Cl.**
G06F 12/00 (2006.01)
G06F 3/06 (2006.01)
G06F 13/00 (2006.01)
G06F 13/28 (2006.01)
G06F 11/00 (2006.01)

(52) **U.S. Cl.** **711/114**; 711/4; 711/100; 711/111; 711/112; 711/147; 711/148; 711/154; 711/161; 711/162; 711/165; 711/117; 714/5; 714/6; 714/7

(58) **Field of Classification Search** ..... None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,177,883	B2 *	2/2007	Yagawa	707/104.1
7,475,206	B2 *	1/2009	Murotani et al.	711/162
2004/0006572	A1	1/2004	Hoshino et al.	
2005/0203964	A1	9/2005	Matsunami et al.	

FOREIGN PATENT DOCUMENTS

JP	2003-303052	4/2002
JP	2004-295457	3/2003

* cited by examiner

Primary Examiner—Sanjiv Shah
Assistant Examiner—Marwan Ayash
(74) *Attorney, Agent, or Firm*—Stites & Harbison, PLLC; Juan Carlos A. Marquez, Esq.

(57) **ABSTRACT**

The storage control device of the present invention uses a temporary volume to move data rapidly between volume groups. The storage control device forms a plurality of volume groups by grouping volumes of the same performance. At least one or more temporary volumes are each pre-provided in the respective volume groups. The control section calculates and manages the priority levels of the respective data. The data with the highest priority level in the lower volume group are copied beforehand to the temporary volume in the upper volume group at a time when the data are not being accessed by the host. As a result, data can be moved rapidly when data migration is executed and so forth.

15 Claims, 24 Drawing Sheets

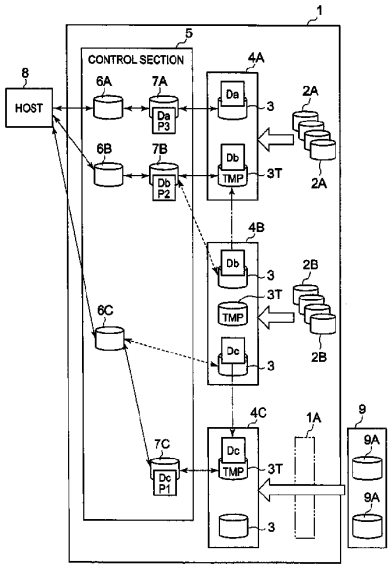


FIG. 1

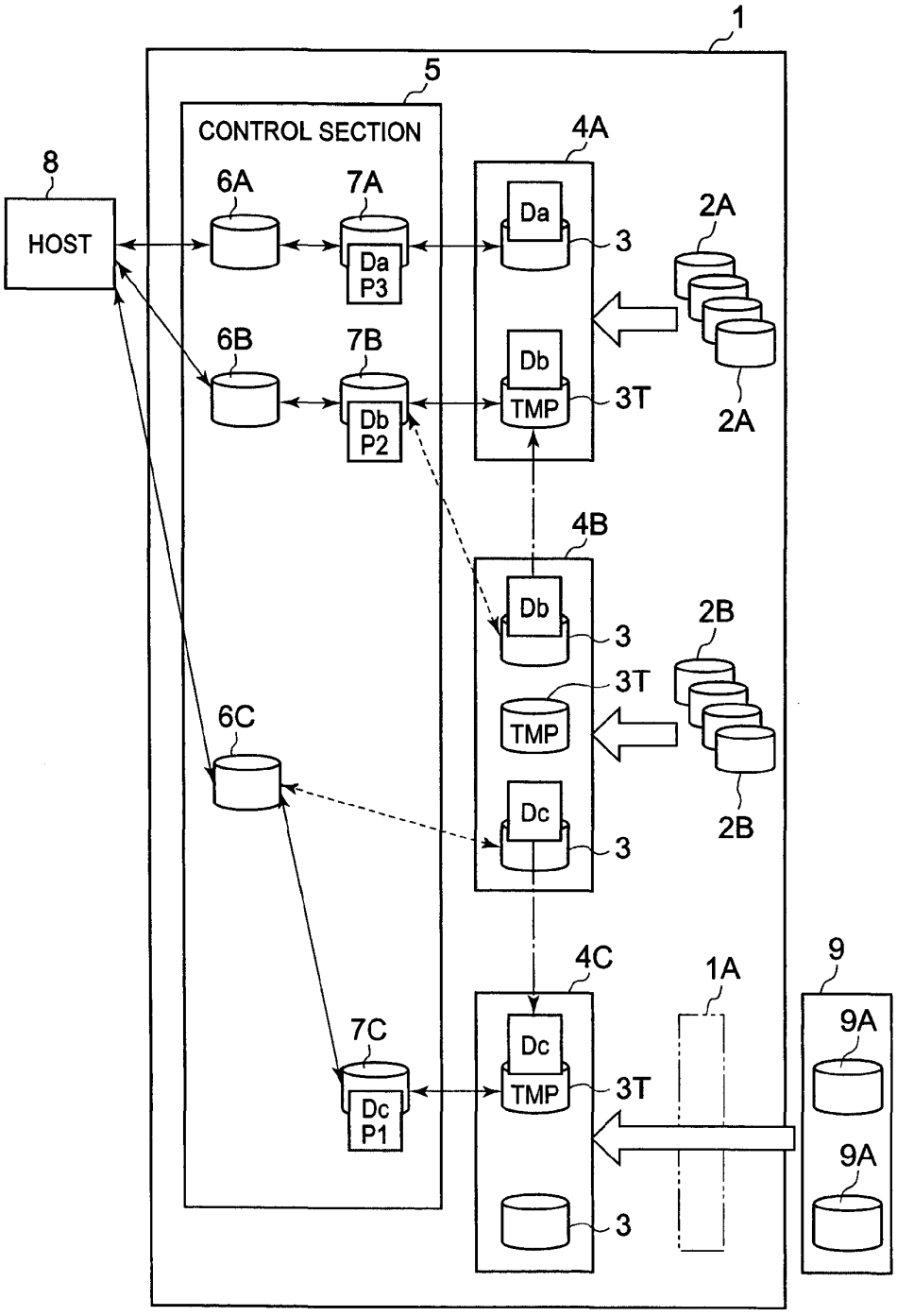

1
5
CONTROL SECTION
8
HOST
6A
7A
Da
P3
4A
Da
3
2A
6B
7B
Db
P2
Db
TMP
3T
2A
4B
Db
3
2B
3T
TMP
6C
Dc
3
2B
4C
1A
9
9A
7C
Dc
P1
Dc
TMP
3T
9A
3

FIG. 2

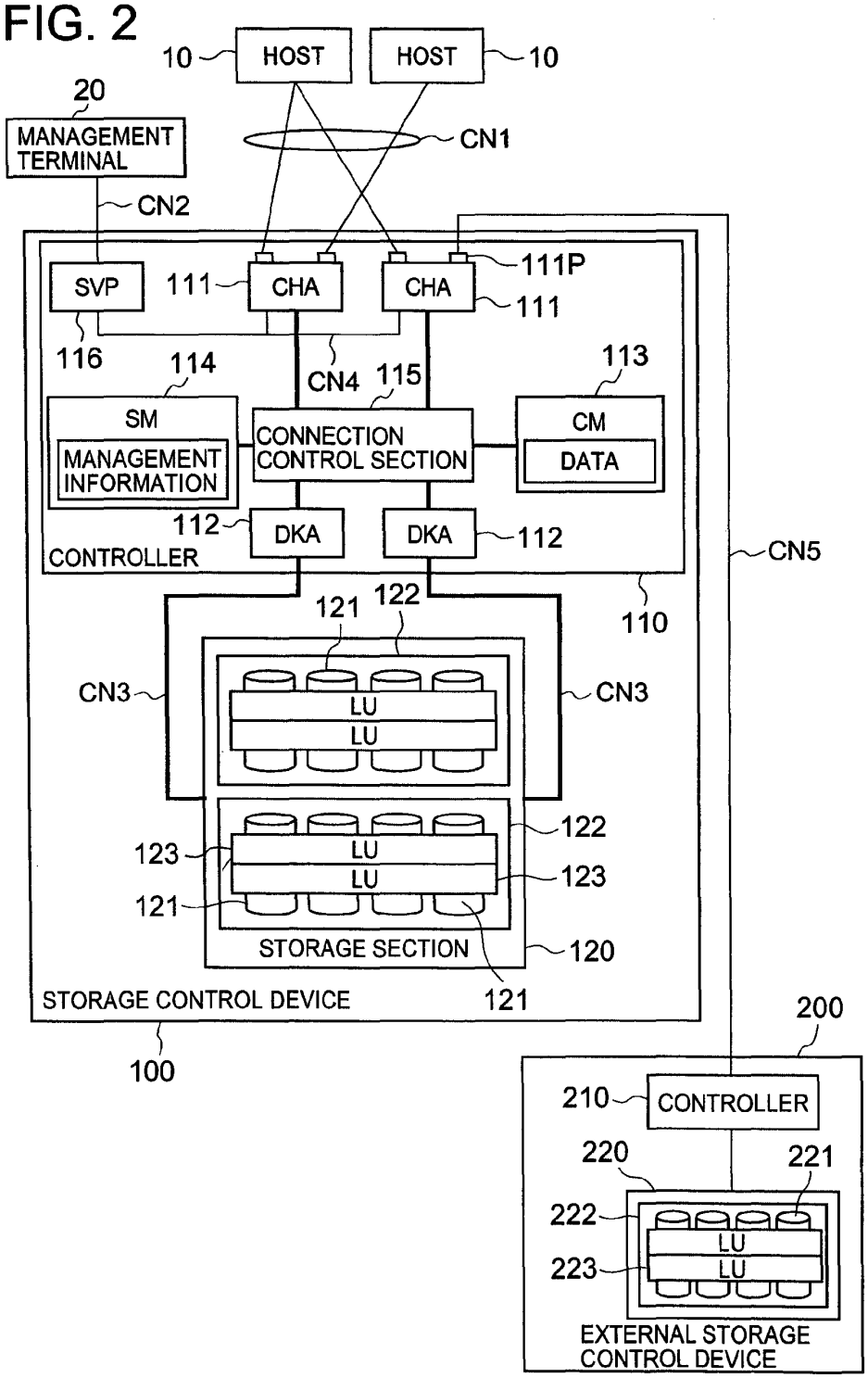

10
HOST
HOST
10
20
MANAGEMENT TERMINAL
CN1
CN2
SVP
111
CHA
CHA
111P
111
116
114
CN4
115
113
SM
MANAGEMENT INFORMATION
CONNECTION CONTROL SECTION
CM
DATA
112
DKA
DKA
112
CONTROLLER
CN5
110
121
122
CN3
CN3
LU
LU
122
123
LU
LU
123
121
STORAGE SECTION
120
STORAGE CONTROL DEVICE
121
100
200
210
CONTROLLER
220
221
222
LU
223
LU
EXTERNAL STORAGE CONTROL DEVICE

FIG. 3

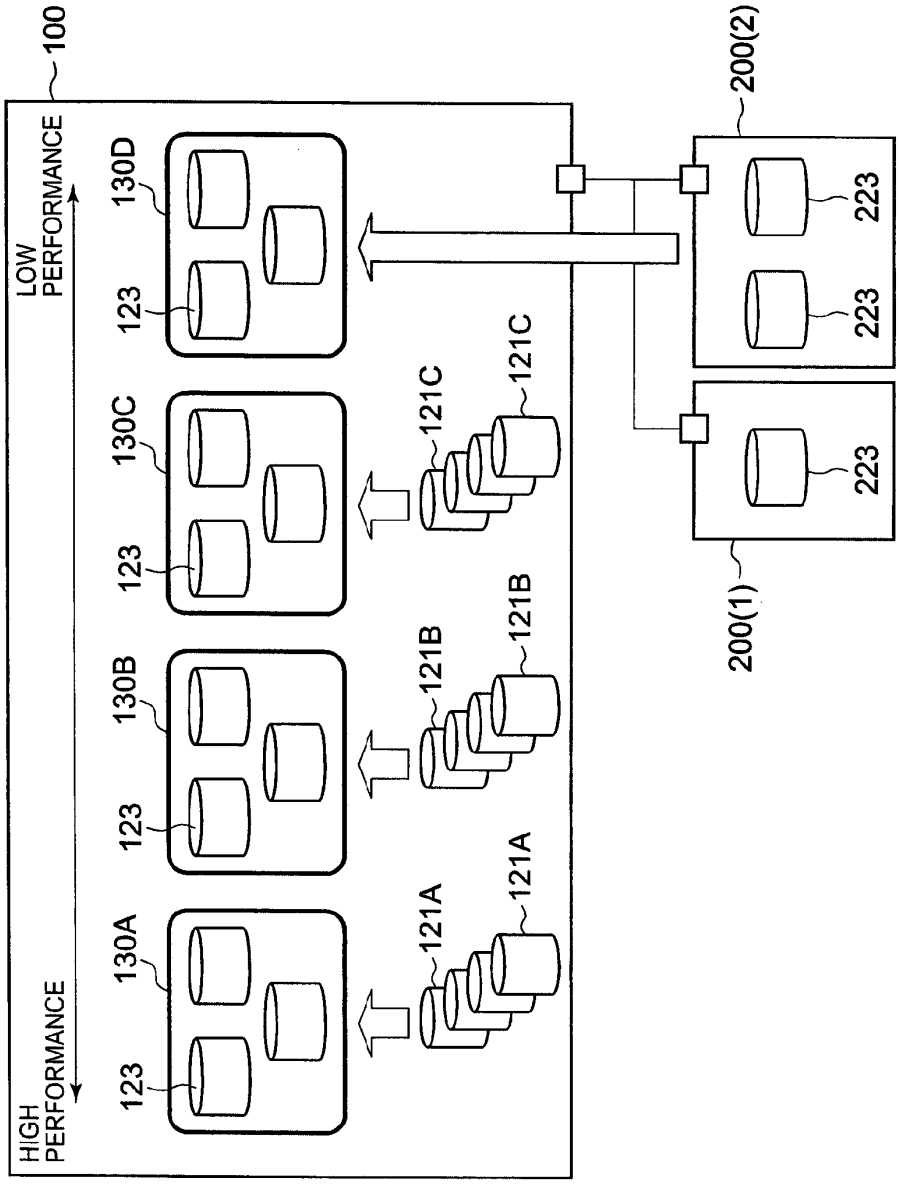

100
HIGH PERFORMANCE
LOW PERFORMANCE
130A
130B
130C
130D
123
121A
121B
121C
200(1)
200(2)
223

FIG. 4

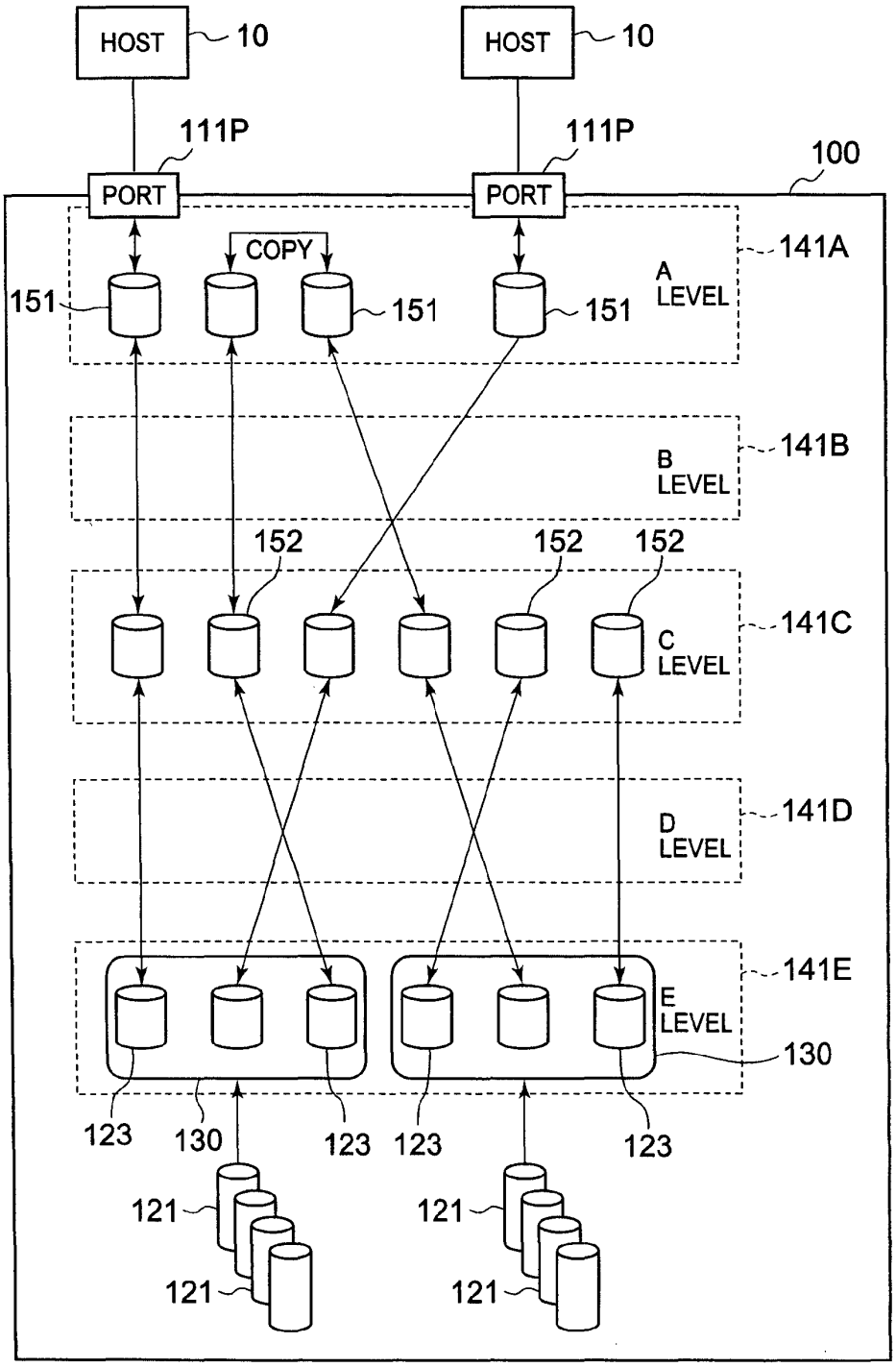

HOST
10
HOST
10
111P
111P
100
PORT
PORT
COPY
141A
151
151
151
A
LEVEL
141B
B
LEVEL
152
152
152
141C
C
LEVEL
141D
D
LEVEL
141E
E
LEVEL
130
123
130
123
123
123
121
121
121
121

FIG. 5

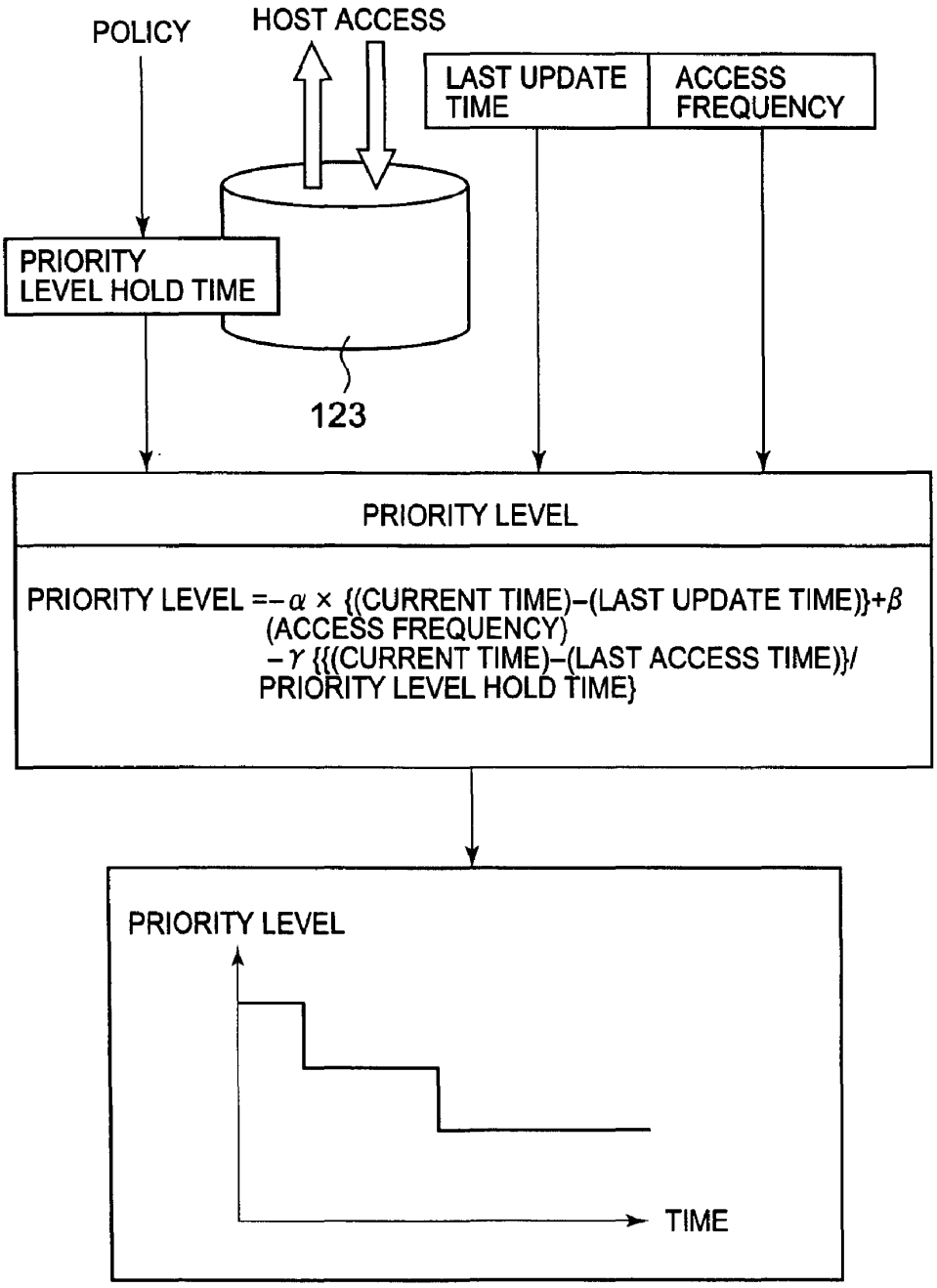

POLICY
HOST ACCESS
LAST UPDATE TIME
ACCESS FREQUENCY
PRIORITY LEVEL HOLD TIME
123
PRIORITY LEVEL
PRIORITY LEVEL =−α × {(CURRENT TIME)−(LAST UPDATE TIME)}+β (ACCESS FREQUENCY) −γ {{(CURRENT TIME)−(LAST ACCESS TIME)}/ PRIORITY LEVEL HOLD TIME}
PRIORITY LEVEL
TIME

FIG. 6

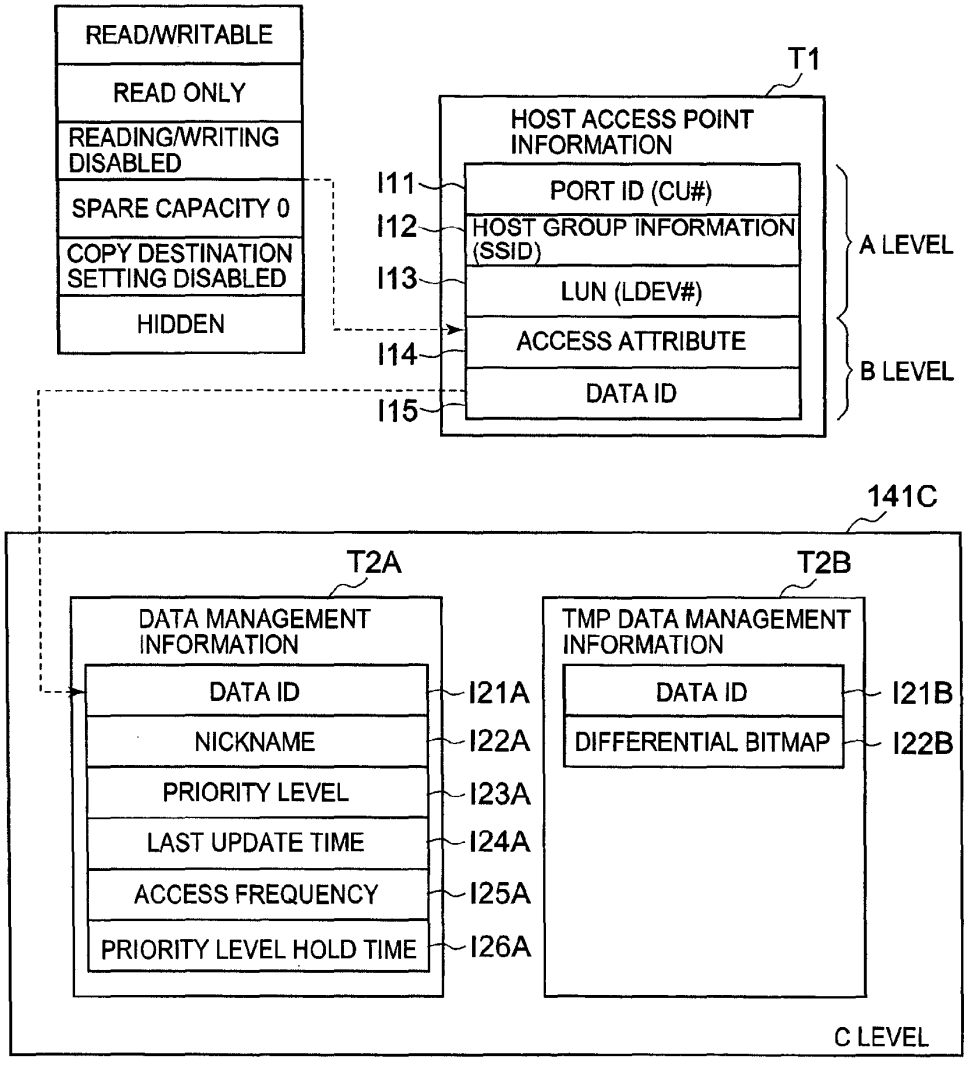

READ/WRITABLE
READ ONLY
READING/WRITING DISABLED
SPARE CAPACITY 0
COPY DESTINATION SETTING DISABLED
HIDDEN
T1
HOST ACCESS POINT INFORMATION
I11
PORT ID (CU#)
I12
HOST GROUP INFORMATION (SSID)
I13
LUN (LDEV#)
ACCESS ATTRIBUTE
I14
DATA ID
I15
A LEVEL
B LEVEL
141C
T2A
DATA MANAGEMENT INFORMATION
DATA ID
I21A
NICKNAME
I22A
PRIORITY LEVEL
I23A
LAST UPDATE TIME
I24A
ACCESS FREQUENCY
I25A
PRIORITY LEVEL HOLD TIME
I26A
T2B
TMP DATA MANAGEMENT INFORMATION
DATA ID
I21B
DIFFERENTIAL BITMAP
I22B
C LEVEL

FIG. 7

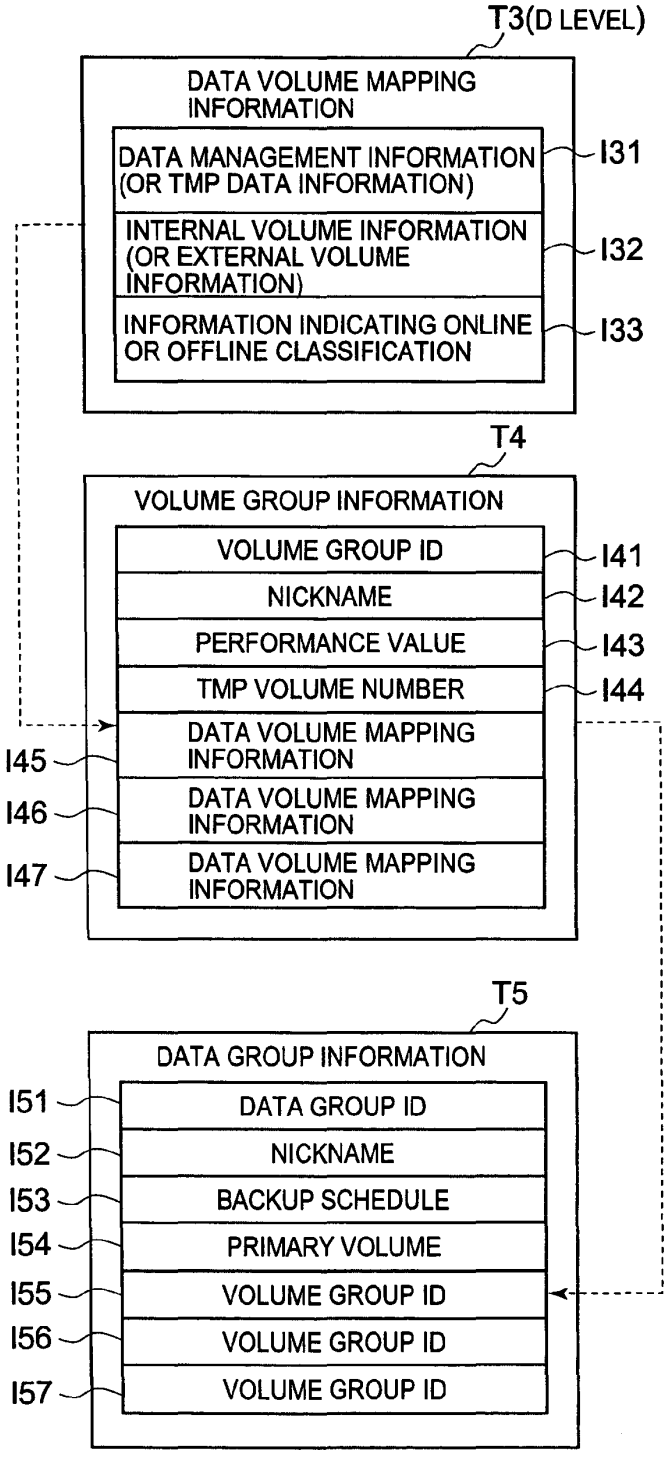

T3(D LEVEL)
DATA VOLUME MAPPING INFORMATION
DATA MANAGEMENT INFORMATION (OR TMP DATA INFORMATION)
I31
INTERNAL VOLUME INFORMATION (OR EXTERNAL VOLUME INFORMATION)
I32
INFORMATION INDICATING ONLINE OR OFFLINE CLASSIFICATION
I33
T4
VOLUME GROUP INFORMATION
VOLUME GROUP ID
I41
NICKNAME
I42
PERFORMANCE VALUE
I43
TMP VOLUME NUMBER
I44
I45
DATA VOLUME MAPPING INFORMATION
I46
DATA VOLUME MAPPING INFORMATION
I47
DATA VOLUME MAPPING INFORMATION
T5
DATA GROUP INFORMATION
I51
DATA GROUP ID
I52
NICKNAME
I53
BACKUP SCHEDULE
I54
PRIMARY VOLUME
I55
VOLUME GROUP ID
I56
VOLUME GROUP ID
I57
VOLUME GROUP ID

FIG. 8

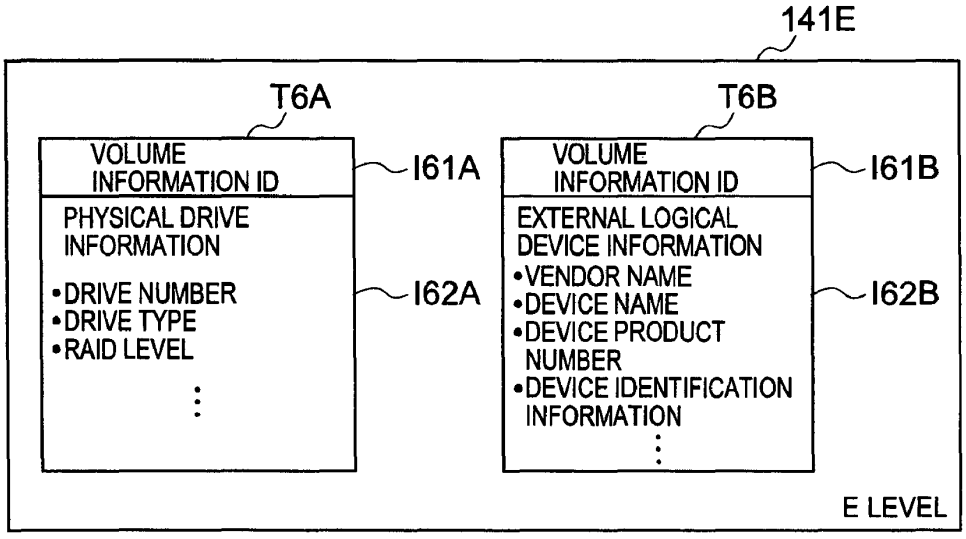

141E
T6A
T6B
VOLUME INFORMATION ID
I61A
VOLUME INFORMATION ID
I61B
PHYSICAL DRIVE INFORMATION
•DRIVE NUMBER
•DRIVE TYPE
•RAID LEVEL
I62A
EXTERNAL LOGICAL DEVICE INFORMATION
•VENDOR NAME
•DEVICE NAME
•DEVICE PRODUCT NUMBER
•DEVICE IDENTIFICATION INFORMATION
I62B
E LEVEL

FIG. 9A

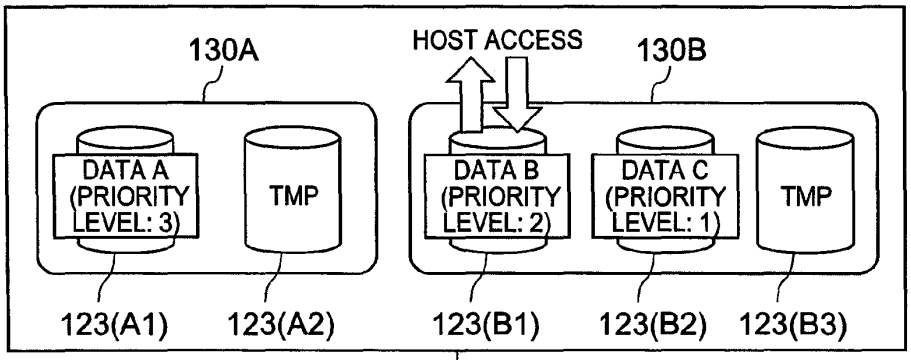


FIG. 9B

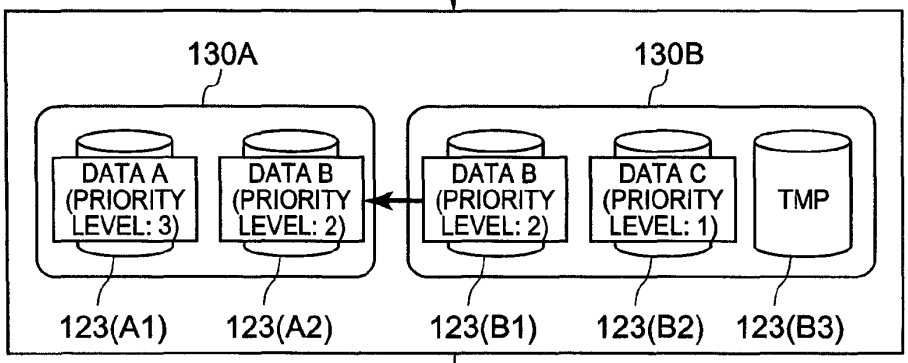


FIG. 9C

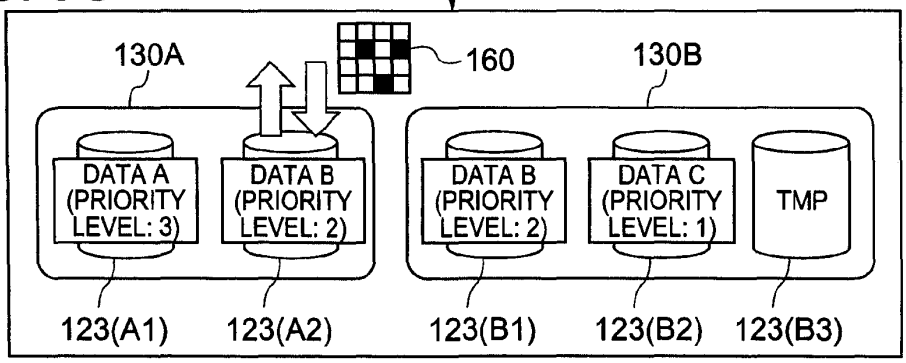


FIG. 10A

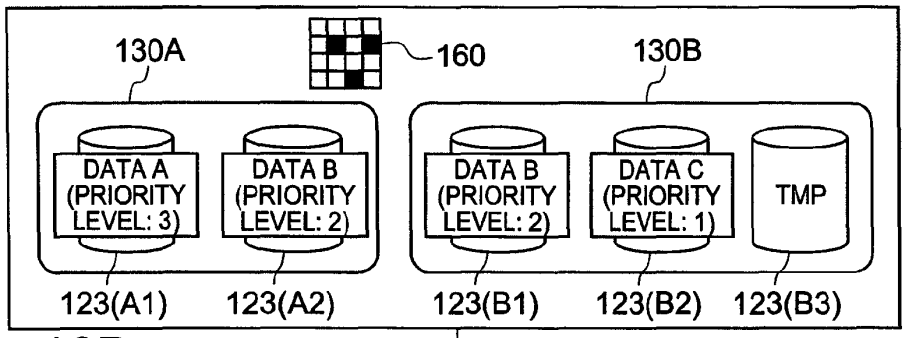


FIG. 10B

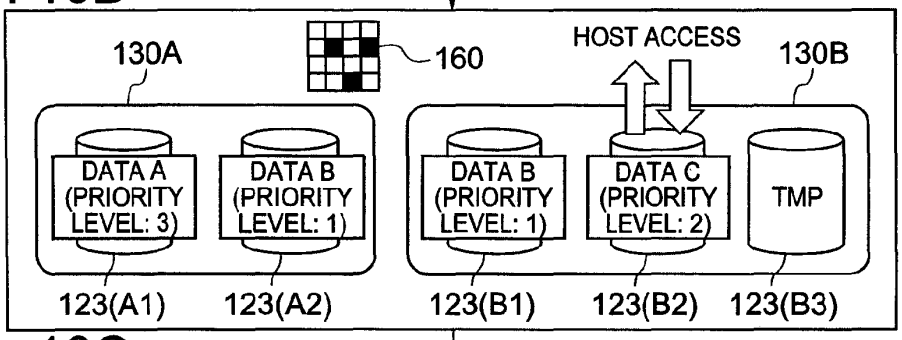


FIG. 10C

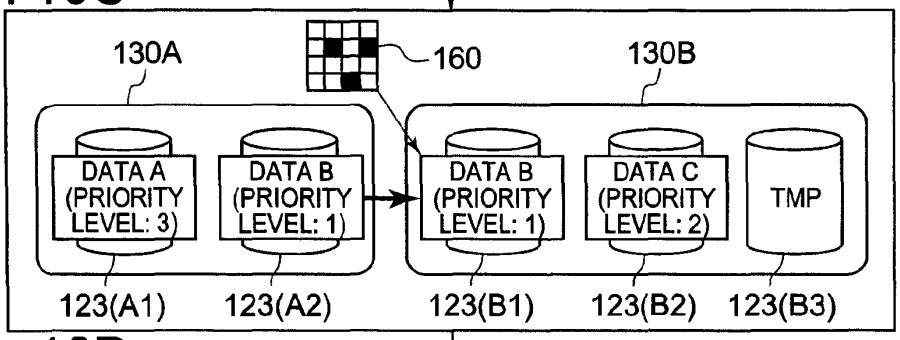


FIG. 10D

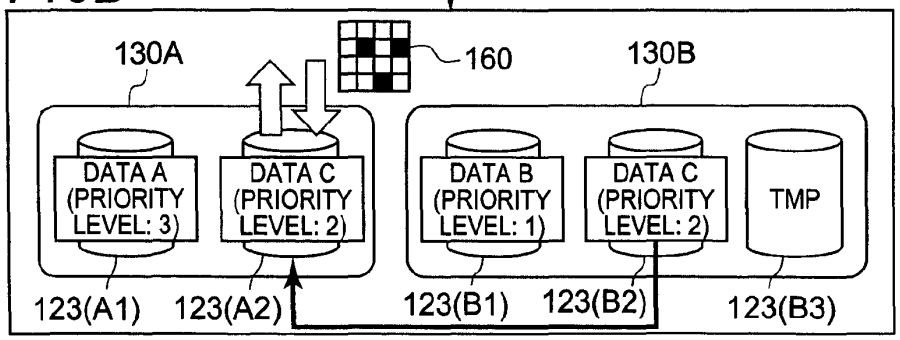


FIG. 11A

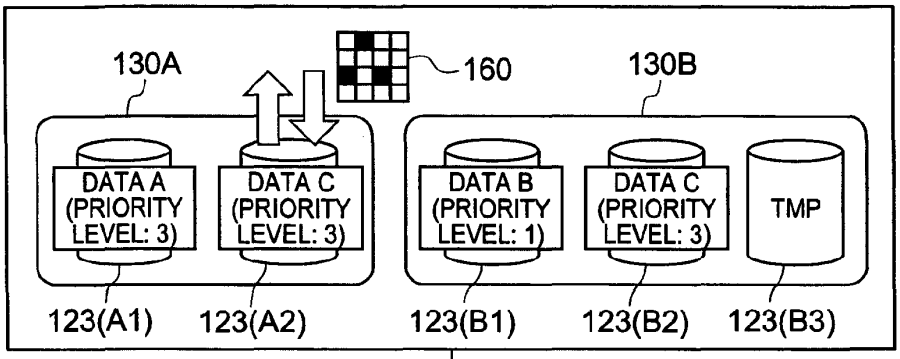


FIG. 11B

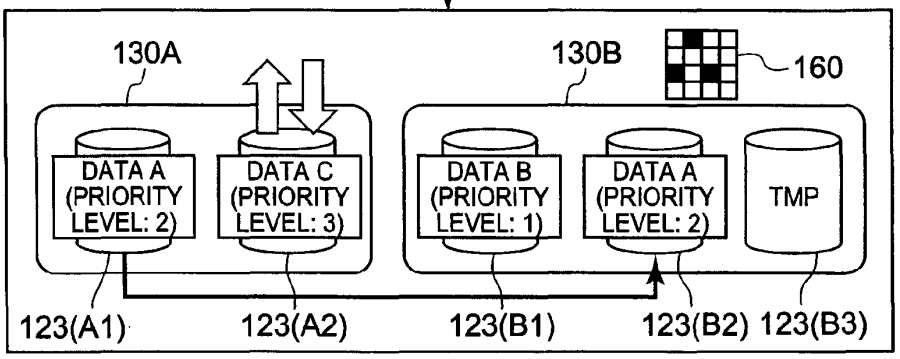


FIG. 12

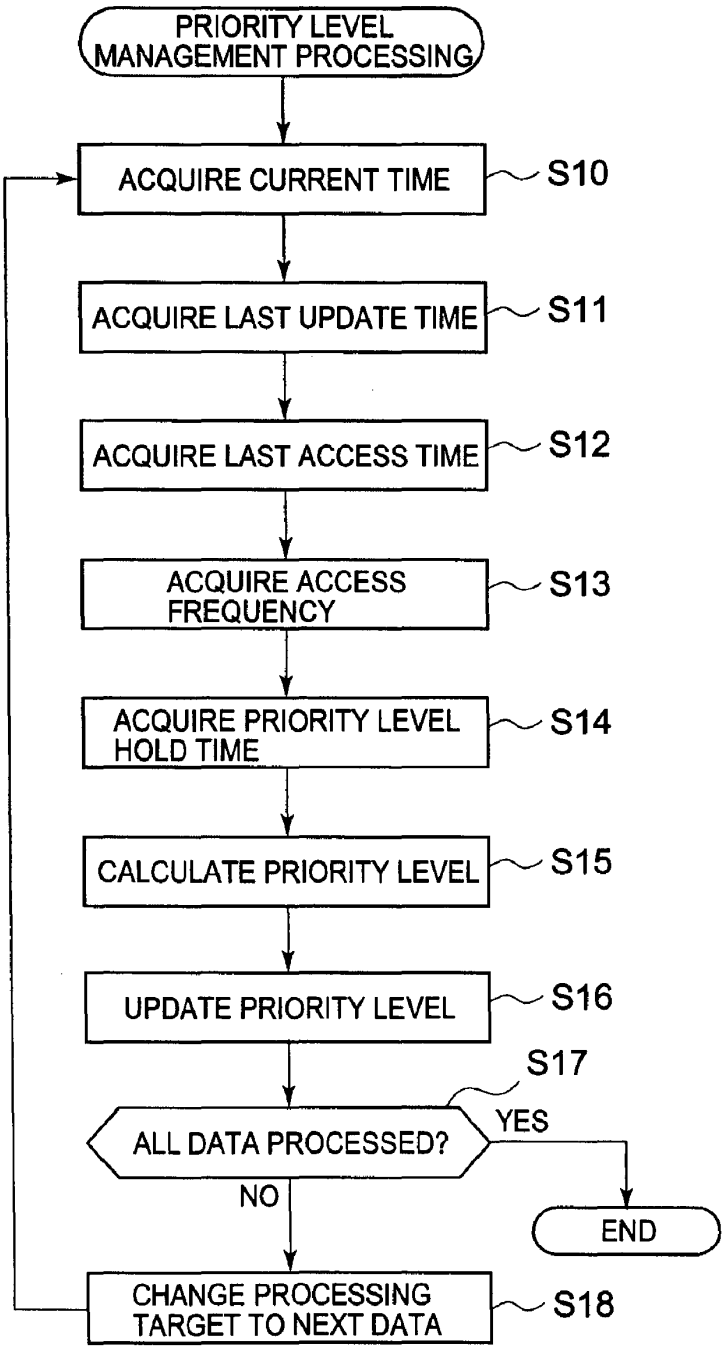

PRIORITY LEVEL MANAGEMENT PROCESSING
ACQUIRE CURRENT TIME
S10
ACQUIRE LAST UPDATE TIME
S11
ACQUIRE LAST ACCESS TIME
S12
ACQUIRE ACCESS FREQUENCY
S13
ACQUIRE PRIORITY LEVEL HOLD TIME
S14
CALCULATE PRIORITY LEVEL
S15
UPDATE PRIORITY LEVEL
S16
S17
ALL DATA PROCESSED?
YES
NO
END
CHANGE PROCESSING TARGET TO NEXT DATA
S18

FIG. 13

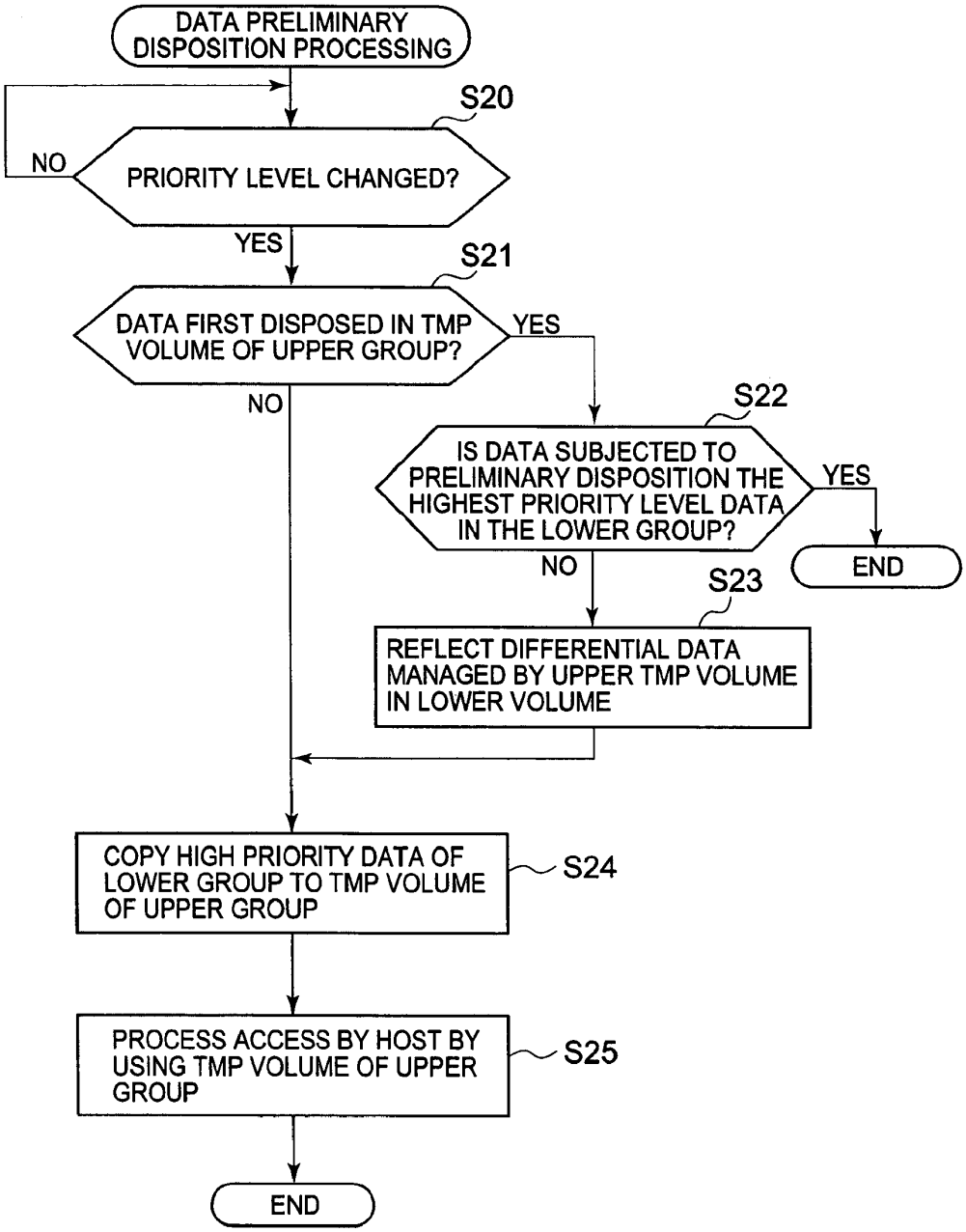

DATA PRELIMINARY DISPOSITION PROCESSING
S20
NO
PRIORITY LEVEL CHANGED?
YES
S21
DATA FIRST DISPOSED IN TMP VOLUME OF UPPER GROUP?
YES
NO
S22
IS DATA SUBJECTED TO PRELIMINARY DISPOSITION THE HIGHEST PRIORITY LEVEL DATA IN THE LOWER GROUP?
YES
END
NO
S23
REFLECT DIFFERENTIAL DATA MANAGED BY UPPER TMP VOLUME IN LOWER VOLUME
COPY HIGH PRIORITY DATA OF LOWER GROUP TO TMP VOLUME OF UPPER GROUP
S24
PROCESS ACCESS BY HOST BY USING TMP VOLUME OF UPPER GROUP
S25
END

FIG. 14

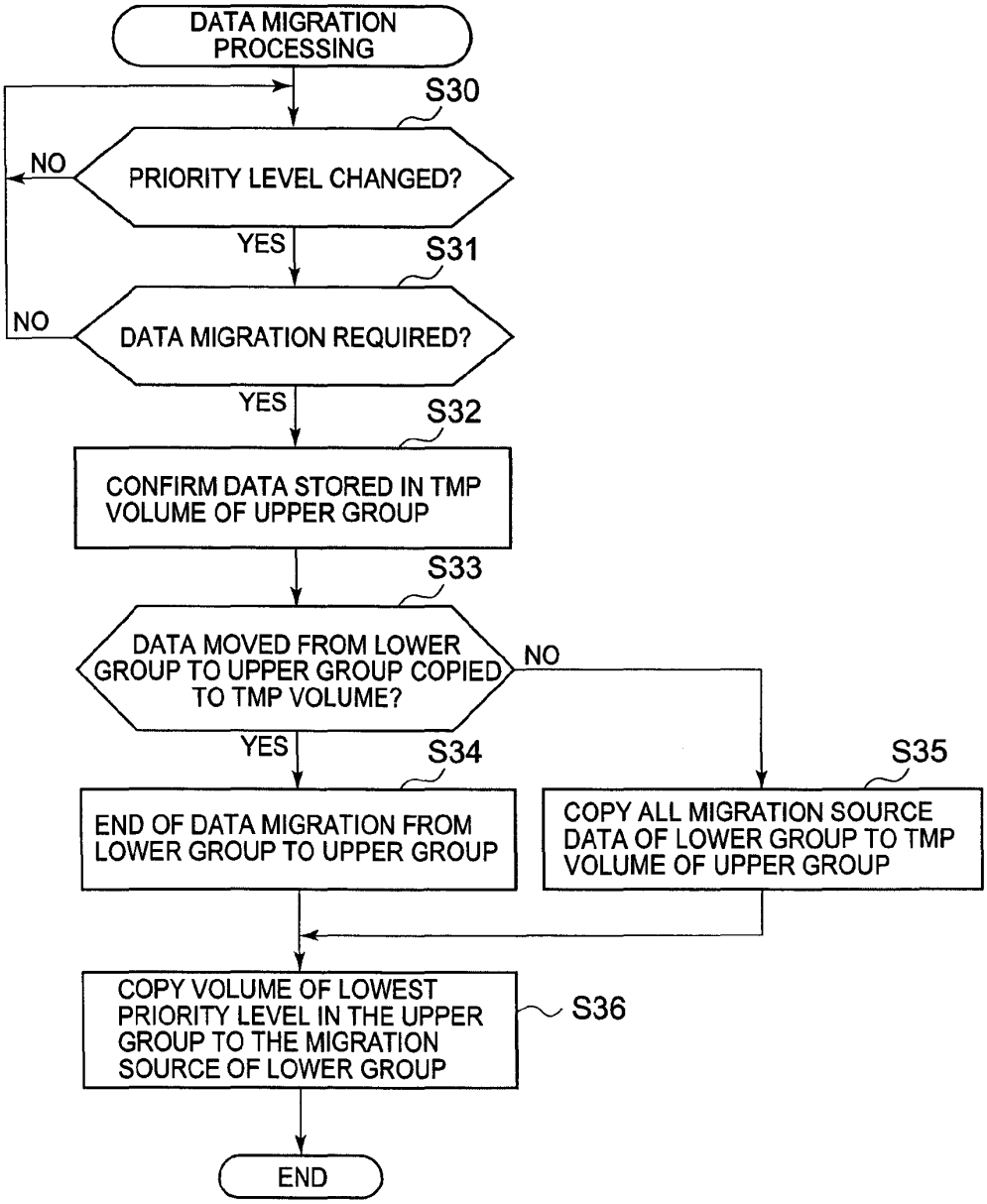

DATA MIGRATION PROCESSING
S30
PRIORITY LEVEL CHANGED?
NO
YES
S31
DATA MIGRATION REQUIRED?
NO
YES
S32
CONFIRM DATA STORED IN TMP VOLUME OF UPPER GROUP
S33
DATA MOVED FROM LOWER GROUP TO UPPER GROUP COPIED TO TMP VOLUME?
NO
YES
S34
END OF DATA MIGRATION FROM LOWER GROUP TO UPPER GROUP
S35
COPY ALL MIGRATION SOURCE DATA OF LOWER GROUP TO TMP VOLUME OF UPPER GROUP
COPY VOLUME OF LOWEST PRIORITY LEVEL IN THE UPPER GROUP TO THE MIGRATION SOURCE OF LOWER GROUP
S36
END

FIG. 15A

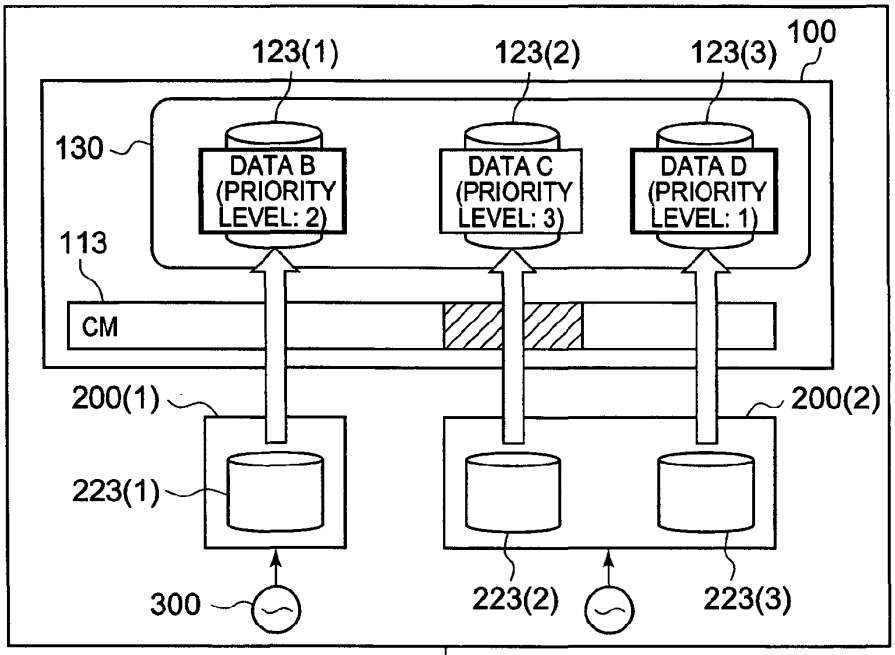


FIG. 15B

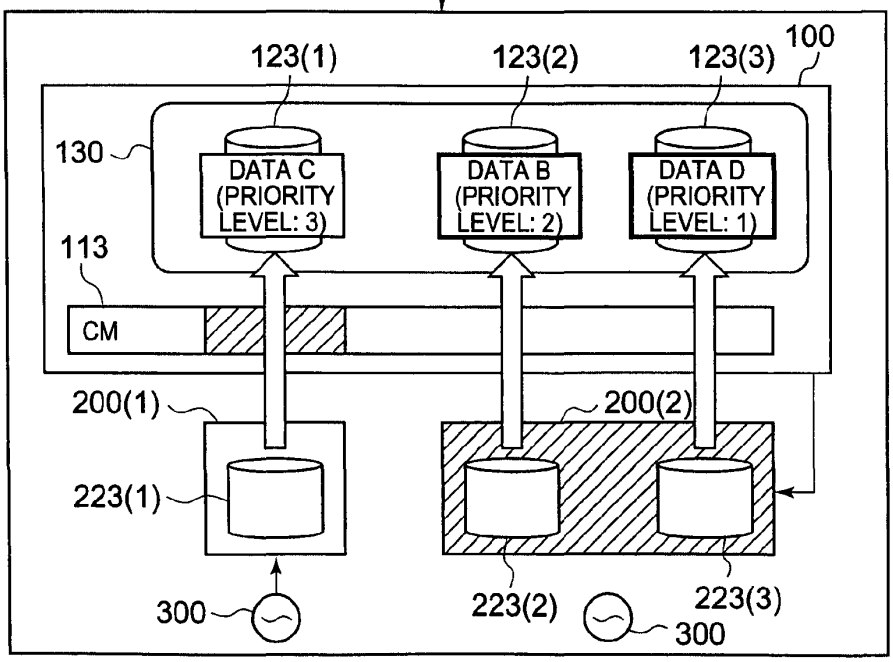


FIG. 16

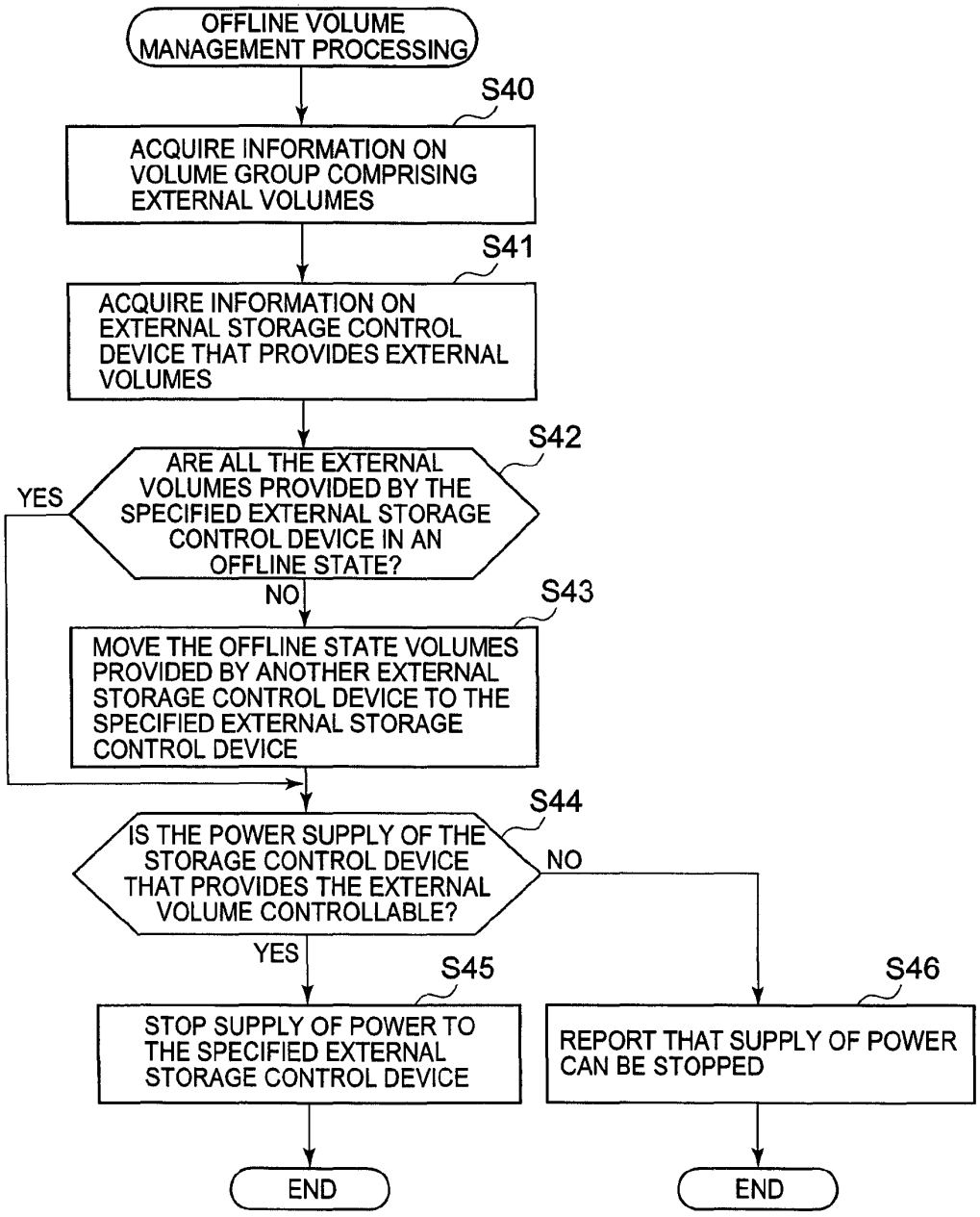

OFFLINE VOLUME MANAGEMENT PROCESSING
S40
ACQUIRE INFORMATION ON VOLUME GROUP COMPRISING EXTERNAL VOLUMES
S41
ACQUIRE INFORMATION ON EXTERNAL STORAGE CONTROL DEVICE THAT PROVIDES EXTERNAL VOLUMES
S42
ARE ALL THE EXTERNAL VOLUMES PROVIDED BY THE SPECIFIED EXTERNAL STORAGE CONTROL DEVICE IN AN OFFLINE STATE?
YES
NO
S43
MOVE THE OFFLINE STATE VOLUMES PROVIDED BY ANOTHER EXTERNAL STORAGE CONTROL DEVICE TO THE SPECIFIED EXTERNAL STORAGE CONTROL DEVICE
S44
IS THE POWER SUPPLY OF THE STORAGE CONTROL DEVICE THAT PROVIDES THE EXTERNAL VOLUME CONTROLLABLE?
NO
YES
S45
STOP SUPPLY OF POWER TO THE SPECIFIED EXTERNAL STORAGE CONTROL DEVICE
S46
REPORT THAT SUPPLY OF POWER CAN BE STOPPED
END
END

FIG. 17

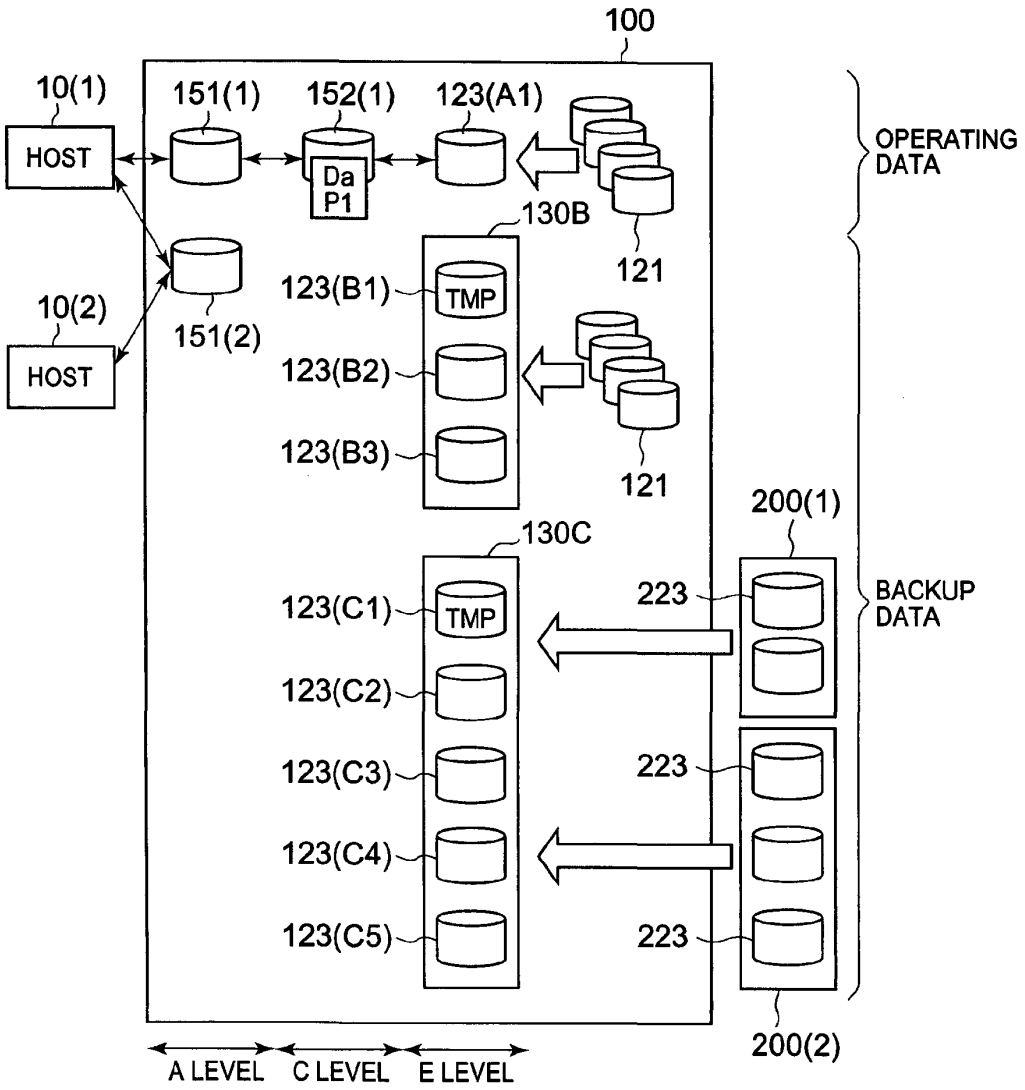

100
10(1)
HOST
151(1)
152(1)
Da
P1
123(A1)
OPERATING
DATA
121
130B
123(B1)
TMP
123(B2)
123(B3)
121
10(2)
HOST
151(2)
200(1)
130C
123(C1)
TMP
223
BACKUP
DATA
123(C2)
123(C3)
223
123(C4)
123(C5)
223
200(2)
A LEVEL
C LEVEL
E LEVEL

FIG. 18

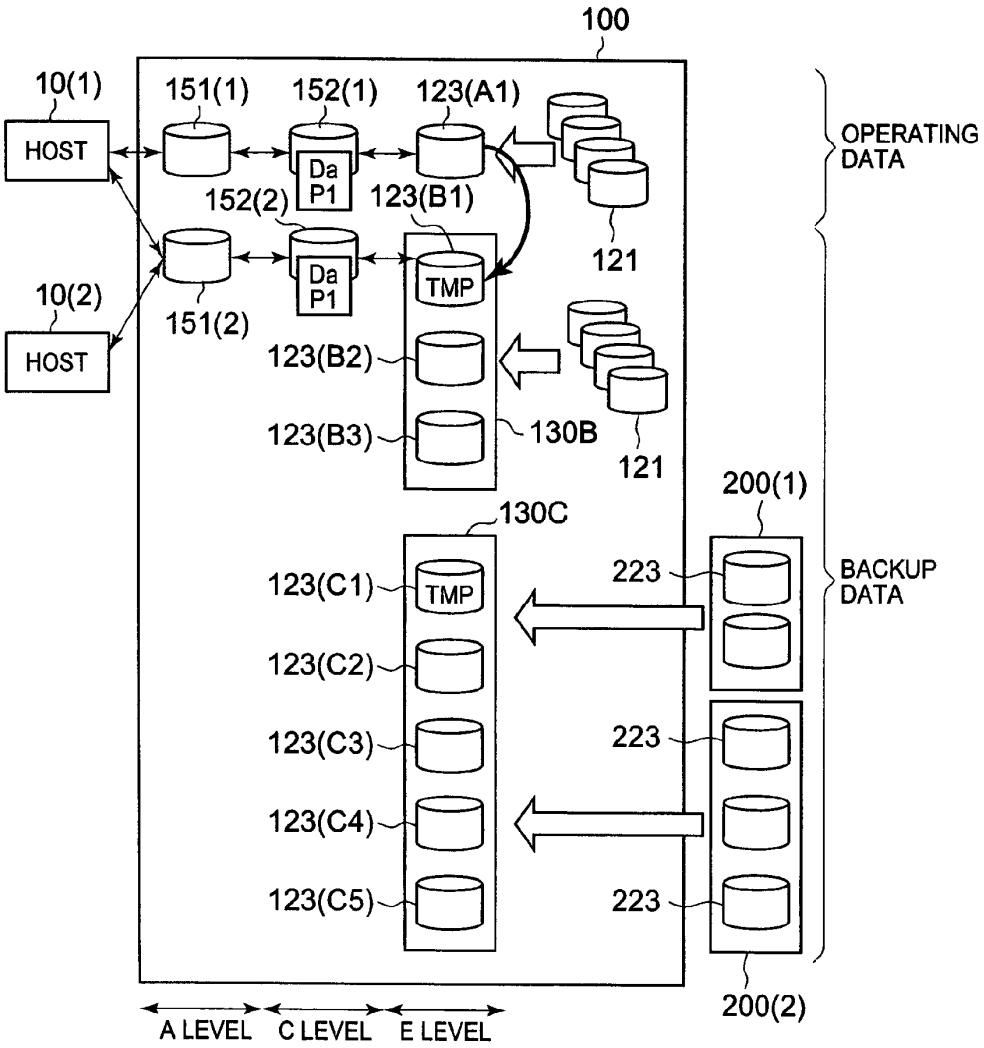

100
10(1)
HOST
151(1)
152(1)
123(A1)
Da
P1
152(2)
123(B1)
121
OPERATING
DATA
10(2)
HOST
151(2)
TMP
123(B2)
123(B3)
130B
121
200(1)
130C
123(C1)
TMP
223
BACKUP
DATA
123(C2)
123(C3)
223
123(C4)
123(C5)
223
200(2)
A LEVEL
C LEVEL
E LEVEL

FIG. 19

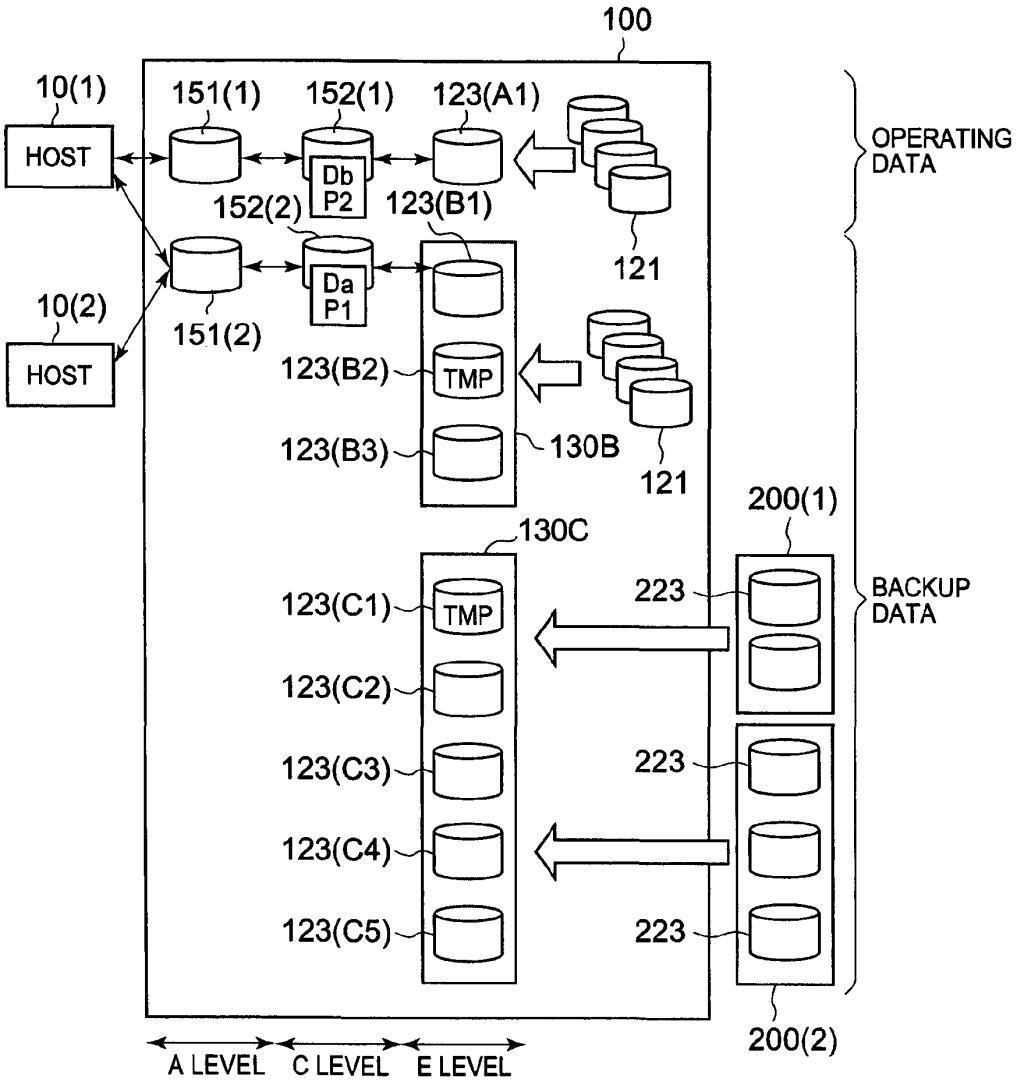

100
10(1)
HOST
151(1)
152(1)
123(A1)
Db
P2
152(2)
123(B1)
121
OPERATING DATA
10(2)
HOST
151(2)
Da
P1
123(B2)
TMP
123(B3)
130B
121
200(1)
130C
123(C1)
TMP
223
BACKUP DATA
123(C2)
123(C3)
223
123(C4)
123(C5)
223
200(2)
A LEVEL
C LEVEL
E LEVEL

FIG. 20

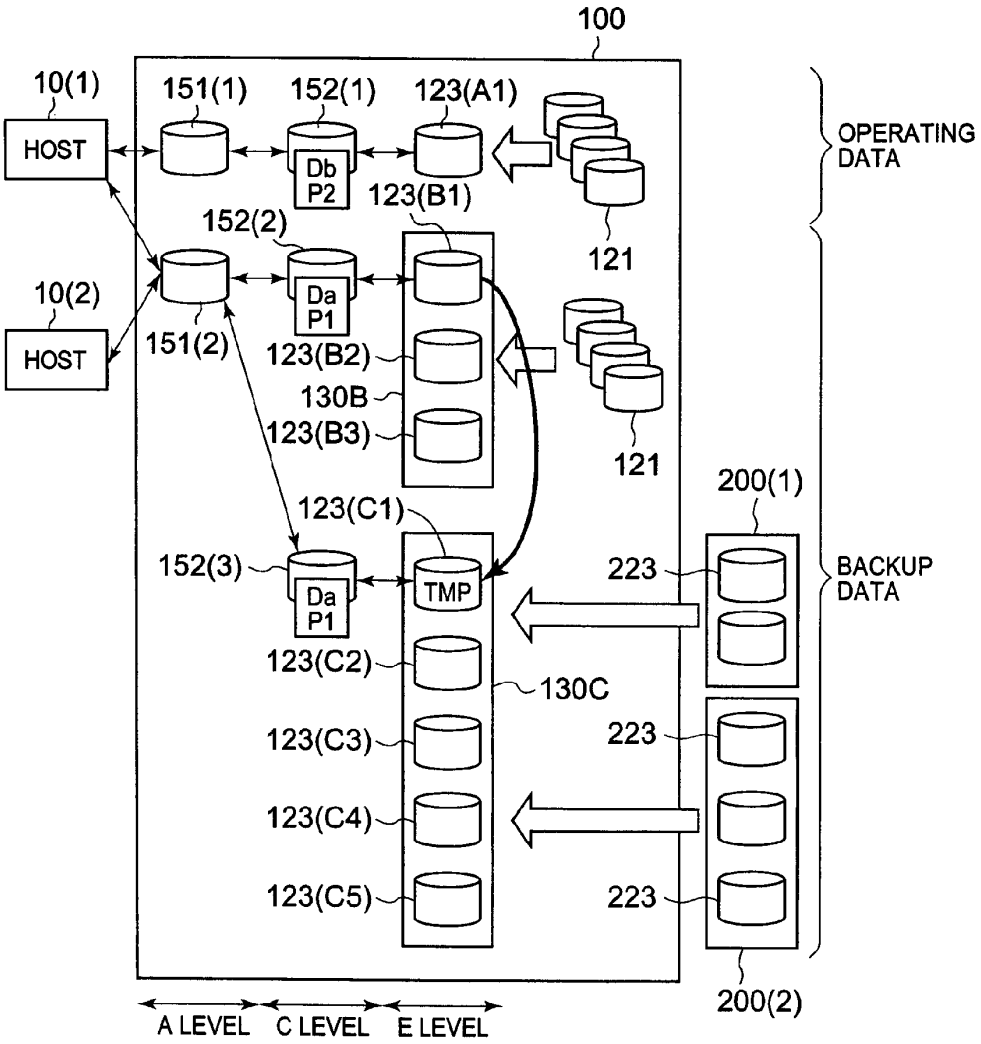

100
10(1)
HOST
151(1)
152(1)
123(A1)
Db
P2
123(B1)
OPERATING
DATA
121
152(2)
Da
P1
10(2)
HOST
151(2)
123(B2)
130B
123(B3)
121
200(1)
123(C1)
152(3)
Da
P1
TMP
223
BACKUP
DATA
123(C2)
130C
123(C3)
223
123(C4)
123(C5)
223
200(2)
A LEVEL
C LEVEL
E LEVEL

FIG. 21

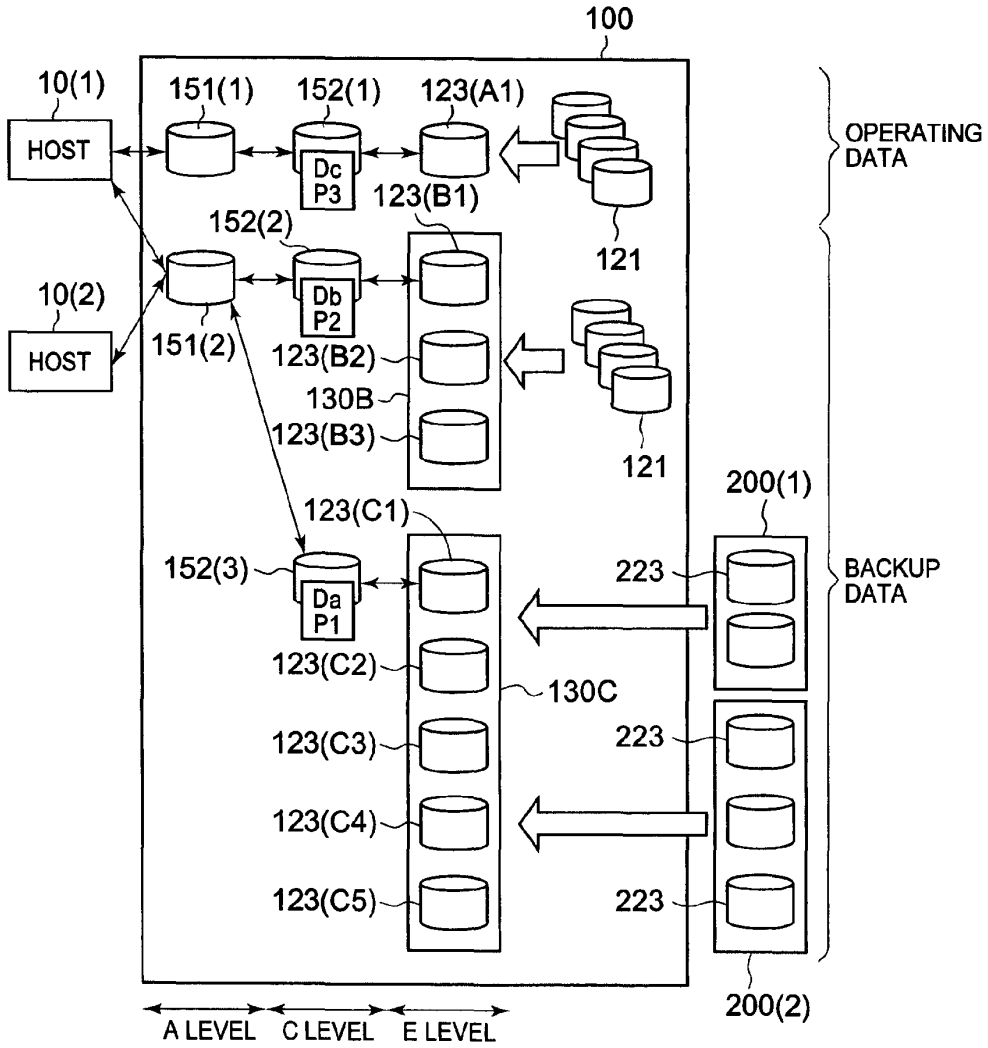

100
10(1)
HOST
151(1)
152(1)
123(A1)
Dc
P3
123(B1)
OPERATING
DATA
121
152(2)
10(2)
HOST
Db
P2
151(2)
123(B2)
130B
123(B3)
121
200(1)
123(C1)
152(3)
Da
P1
223
BACKUP
DATA
123(C2)
130C
123(C3)
223
123(C4)
123(C5)
223
200(2)
A LEVEL
C LEVEL
E LEVEL

FIG. 22

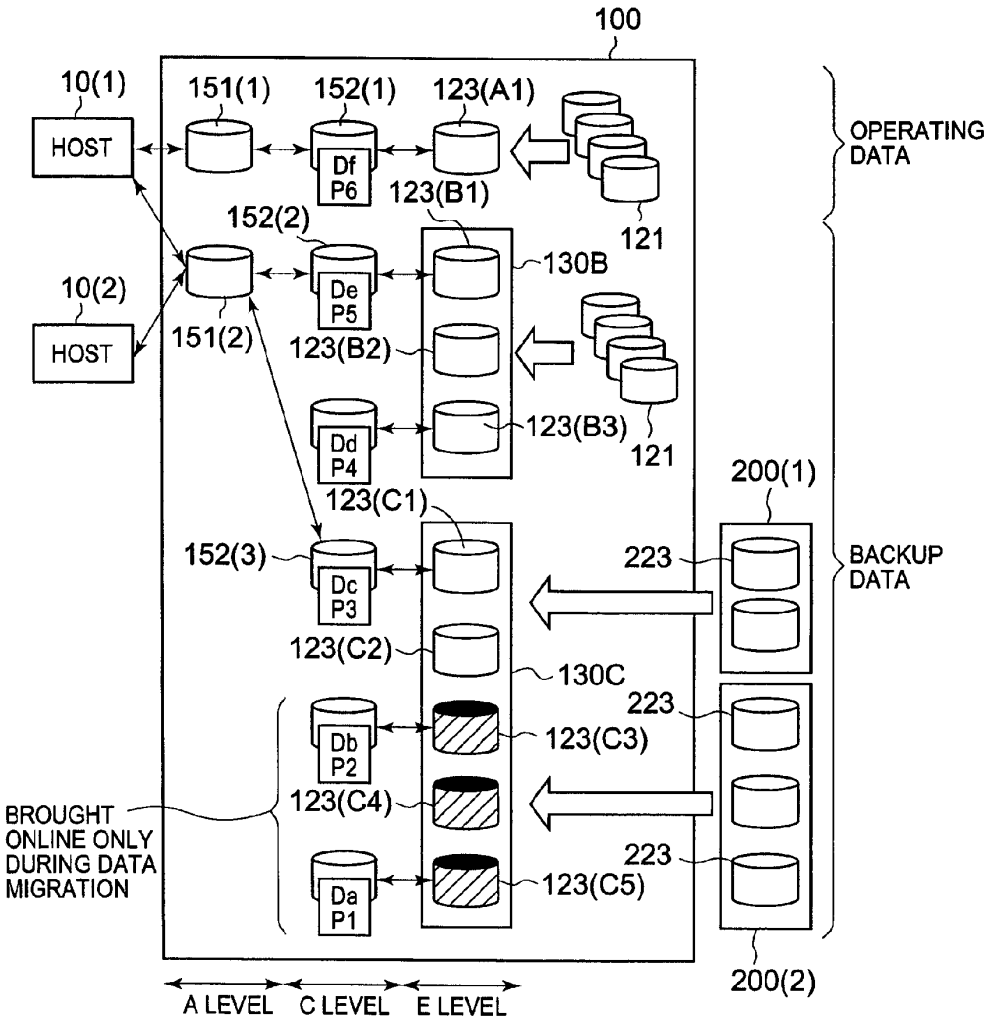

100
10(1)
HOST
151(1)
152(1)
123(A1)
Df
P6
123(B1)
121
OPERATING DATA
152(2)
130B
10(2)
HOST
151(2)
De
P5
123(B2)
123(B3)
121
Dd
P4
123(C1)
200(1)
152(3)
Dc
P3
223
BACKUP DATA
123(C2)
130C
223
Db
P2
123(C3)
123(C4)
BROUGHT ONLINE ONLY DURING DATA MIGRATION
223
Da
P1
123(C5)
200(2)
A LEVEL
C LEVEL
E LEVEL

FIG. 23

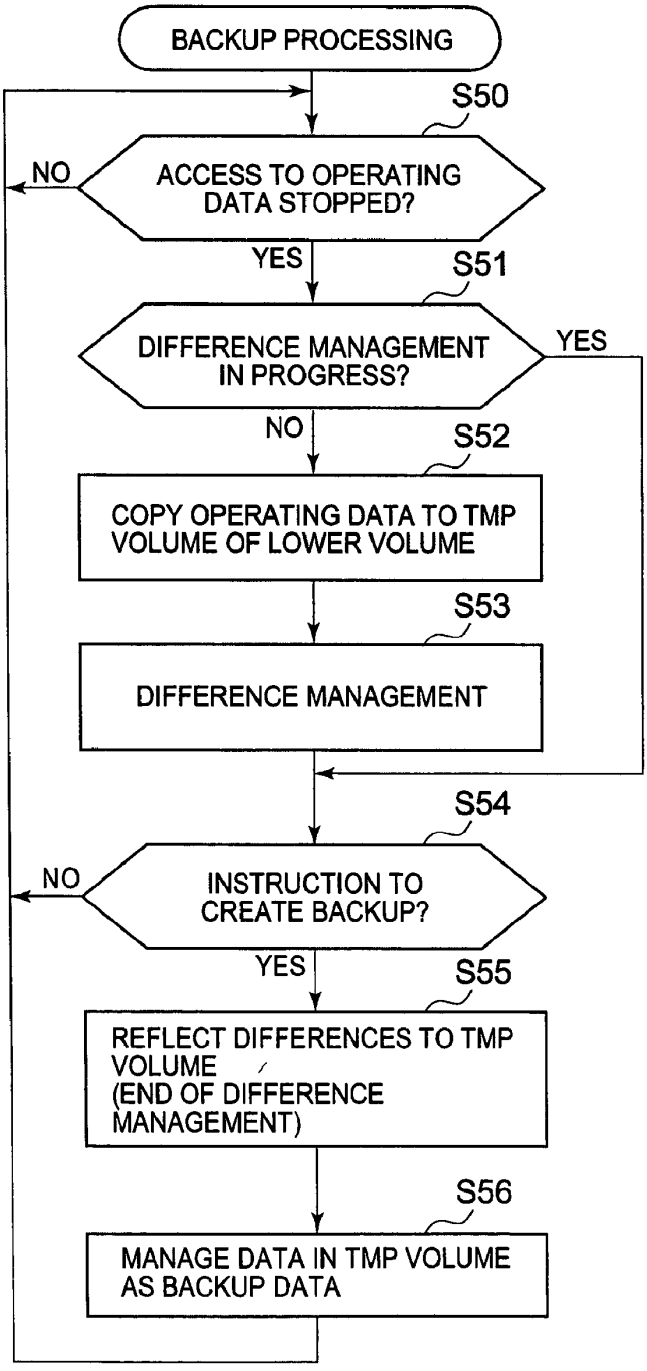
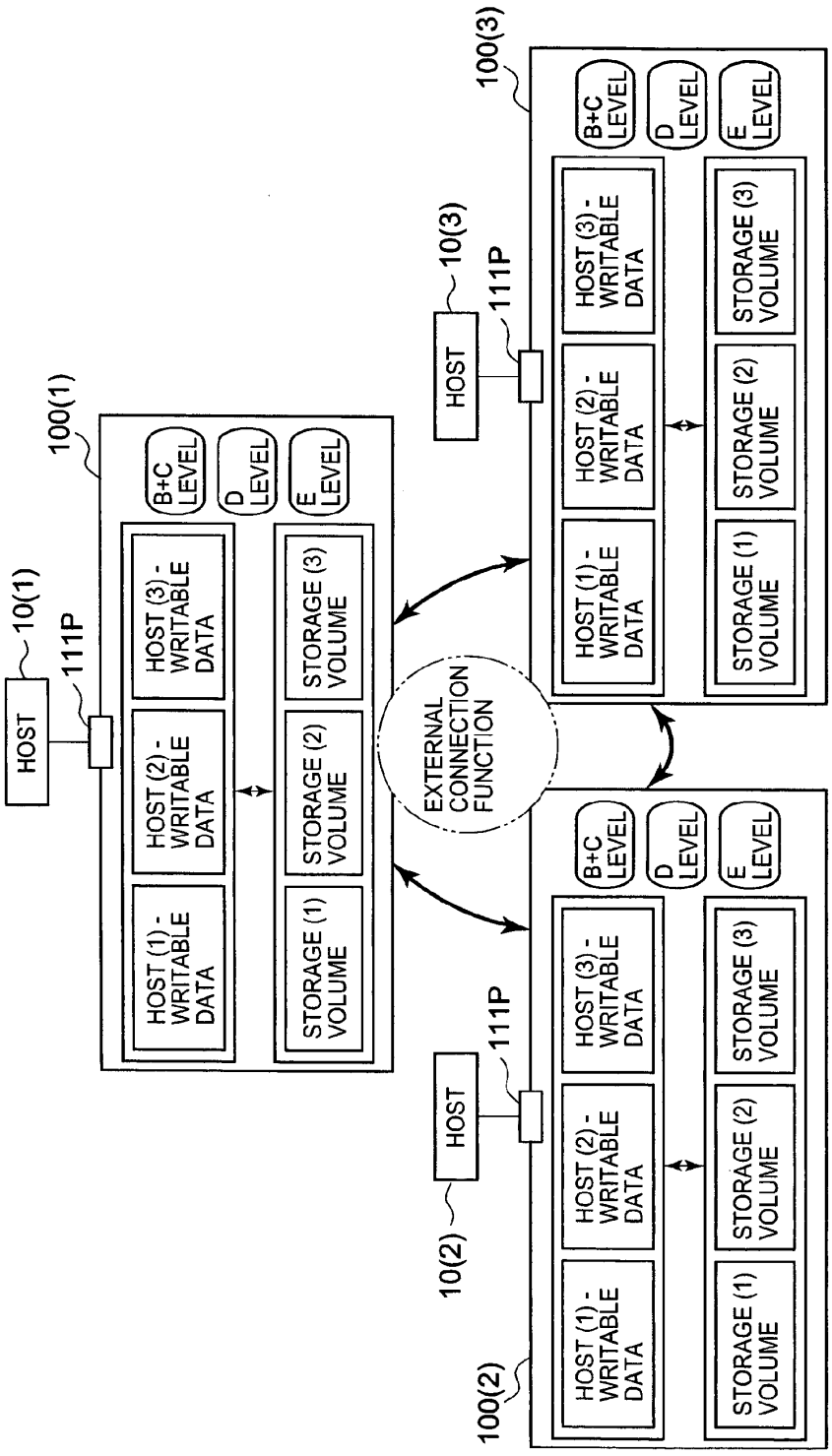

BACKUP PROCESSING
S50
ACCESS TO OPERATING DATA STOPPED?
NO
YES
S51
DIFFERENCE MANAGEMENT IN PROGRESS?
YES
NO
S52
COPY OPERATING DATA TO TMP VOLUME OF LOWER VOLUME
S53
DIFFERENCE MANAGEMENT
S54
INSTRUCTION TO CREATE BACKUP?
NO
YES
S55
REFLECT DIFFERENCES TO TMP VOLUME (END OF DIFFERENCE MANAGEMENT)
S56
MANAGE DATA IN TMP VOLUME AS BACKUP DATA

FIG. 24


100(1)
100(2)
100(3)
10(1)
10(2)
10(3)
HOST
111P
HOST (1) - WRITABLE DATA
HOST (2) - WRITABLE DATA
HOST (3) - WRITABLE DATA
STORAGE (1) VOLUME
STORAGE (2) VOLUME
STORAGE (3) VOLUME
B+C LEVEL
D LEVEL
E LEVEL
EXTERNAL CONNECTION FUNCTION

DATA MIGRATION USING TEMPORARY VOLUME TO MIGRATE HIGH PRIORITY DATA TO HIGH PERFORMANCE STORAGE AND LOWER PRIORITY DATA TO LOWER PERFORMANCE STORAGE

CROSS-REFERENCE TO RELATED APPLICATIONS

This application relates to and claims priority from Japanese Patent Application No. 2006-294300 filed on Oct. 30, 2006, the entire disclosure of which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a storage control device and a data migration method for the storage control device.

2. Description of the Related Art

In government, government administration offices, local self-governing bodies, enterprises, and educational institutions, and so forth, for example, data are managed by using relatively large-scale storage systems to handle large quantities of data of a variety of types. Such storage systems are constituted by a storage control device such as a disk array device. The disk array device is constituted by providing a multiplicity of disk drives in the form of an array and provides a RAID (Redundant Array of Independent Disks)-based storage region, for example. At least one or more logical volumes (logical storage devices) are formed in physical storage regions provided by a disk drive group. The logical volumes are provided for programs that run on a host computer. The host computer (abbreviated as 'host' hereinbelow) is able to read and write data from and to the logical volumes by transmitting predetermined commands.

The amount of data to be managed is increasing on a daily basis in line with the advances of a computerized society. However, the value of data is not fixed and the evaluation of a lot of data drops as time elapses. A procedure for managing data in accordance with the value of data is known as ILM (Information Lifecycle Management), for example. Therefore, a data migration technology that changes the storage location of data in accordance with the value of the data has been proposed (Japanese Application Laid Open No. 2004-295457).

Meanwhile, a technology that automatically generates parameters that are used by tools for setting storage devices on the basis of storage device constitution information and policies that are established by the user has also been proposed (Japanese Application Laid Open No. 2003-303052).

In the conventional technology mentioned in Japanese Application Laid Open No. 2004-295457, when the re-arrangement of data has been determined, it is necessary to copy data constituting the migration target from the migration source to the migration destination after preparing a storage device for storing the data at the migration destination. Hence, although there is also variation depending on the total size of the data constituting the migration target, it takes a long time until the data migration is complete and user convenience is low.

SUMMARY OF THE INVENTION

The present invention was conceived in view of the above problems and an object of the present invention is to provide a storage control device and a data migration method for the storage control device that make it possible to improve user convenience with respect to data migration. A further object of the present invention is to provide a storage control device and a data migration method for the storage control device that makes it possible to improve user convenience and shorten the data migration time by moving at least a portion of the data in advance by using a temporary volume that is pre-prepared in each volume group before data migration is determined. Yet another object of the present invention is to provide a storage control device and a data migration method for the storage control device that makes it possible to improve user convenience which is able to automatically judge the value of data and move data in a relatively short time to a logical volume that depends on the value of the data. Further objects of the present invention will become evident from the following description of the embodiments.

In order to achieve the above object, the storage control device according to the present invention is a storage control device that comprises a plurality of storage drives for storing data used by a higher level device and a controller that controls data inputs and outputs between each of the storage drives and the higher level device, comprising: a plurality of logical volumes formed on the basis of physical storage regions of the respective storage drives; a plurality of volume groups each formed by grouping a plurality of each of the respective logical volumes; a priority level management section provided in the controller that detects and manages each of the priority levels of the data stored in the respective logical volumes on the basis of an access request issued by the higher level device; and a data migration section provided in the controller that moves the data between the respective volume groups on the basis of the respective priority levels managed by the priority level management section, wherein, among the respective logical volumes in the respective volume groups, at least one or more of the logical volumes is established as a temporary volume which is used for the migration of the data; and the data migration section uses the temporary volume to move migration target data between the respective volume groups beforehand.

In the embodiment of the present invention, the data migration section uses the temporary volume to move the migration target data between the respective volume groups before the migration of the migration target data has been determined.

In the embodiment of the present invention, the respective volume groups are ranked in accordance with the types of the respective logical volumes that constitute the respective volume groups.

In the embodiment of the present invention, the respective storage drives are classified as storage drives of a plurality of types each of which has a different performance, and the respective volume groups are ranked from a volume group with the highest rank to a volume group with the lowest rank in accordance with the type of the storage drive in which the respective logical volumes constituting the respective volume groups are provided.

In the embodiment of the present invention, the data migration section uses the temporary volume to move the migration target data between the respective volume groups so that the data of a high priority level are located in a volume group of a higher rank and data of a low priority level are located in a volume group of a lower rank.

In the embodiment of the present invention, the priority level management section detects and manages the priority levels of each of the data on the basis of the last time the higher level device accessed the respective data and the frequency with which the higher level device has accessed the respective data.

In the embodiment of the present invention, the priority level management section detects and manages the priority level for each of the respective data on the basis of the last time the higher level device accessed the respective data, the frequency with which the higher level device has accessed the respective data, and a priority level hold time that is preset for the respective data.

In the embodiment of the present invention, the data migration section selects data with the highest priority level among the respective data contained in a migration source volume group of a relatively low rank as the migration target data and copies the migration target data beforehand to the temporary volume contained in a migration destination volume group that is one rank higher.

In the embodiment of the present invention, the data migration section uses the migration target data copied to the temporary volume in the migration destination volume group to process an access request issued by the higher level device to the migration target data.

In the embodiment of the present invention, the data migration section manages the differences between the temporary volume in the migration destination volume group and a migration source logical volume in the migration source volume group with respect to the migration target data.

In the embodiment of the present invention, the data migration section reflects the differences to the migration source logical volume when the priority level of the migration target data is lowered by the priority level management section and copies other data set at the highest priority level in the migration source volume group to the temporary volume in the migration destination volume group.

In the embodiment of the present invention, the data migration section copies backup target data stored in a backup target logical volume that exists in a higher ranking volume group to a temporary volume in a lower ranking volume group beforehand.

In the embodiment of the present invention, the data migration section manages differences between the backup target logical volume and the temporary volume in the lower ranking volume group with respect to the backup target data and ends the backup by reflecting the differences in the temporary volume when an instruction to execute a backup is issued.

In the embodiment of the present invention, the controller controls each of (1) an access path management level that manages access points accessed by the higher level device, (2) a volume management level that manages the respective logical volumes, (3) an intermediate management level that manages management information related to the data stored in the volume management level and associations between the access points and the logical volumes.

In the embodiment of the present invention, the intermediate management level is constituted comprising a first level that manages the management information, a second level that manages the relationship between the access points and the first level, and a third level that manages the association between the first level and the volume management level.

In the embodiment of the present invention, at least one specified volume group among the respective volume groups is constituted by a virtual logical volume that is associated with another logical volume that exists in a plurality of different storage control devices; and the controller allocates cache memory in the controller when the virtual logical volume has been set to the online state and does not allocate the cache memory when the virtual logical volume has been set to the offline state.

In the embodiment of the present invention, the controller stores low priority level data in the specified virtual logical volumes associated with the other logical volumes in the specified other storage control device and, when the specified virtual logical volumes have all been set to the offline state, reports the fact that the supply of power to the specified other storage control device can be stopped or automatically stops the supply of power to the specified other storage control device.

In a data migration method according to another aspect of the present invention that uses a storage control device that comprises a plurality of storage drives for storing data used by a higher level device and a controller that controls data inputs and outputs between each of the storage drives and the higher level device, the controller executes: a step of generating each of a plurality of volume groups by grouping a plurality of each of a plurality of logical volumes formed on the basis of the physical storage regions of the respective storage drives according to the performance of the respective storage drives and setting at least one or more logical volumes among the respective logical volumes in the respective volume groups as a temporary volume for moving data; a step of detecting and managing the priority levels of the data stored in the respective logical volumes on the basis of an access request issued by the higher level device; and a step of using the temporary volume to move data between the respective volume groups before data migration is determined so that the high priority level data are stored in a volume group associated with a higher performance storage drive and the low priority level data are stored in a volume group associated with a lower performance storage drive.

All or some of the means, functions and steps of the present invention can sometimes be constituted as computer programs that are executed by a computer system. When all or part of the constitution of the present invention is constituted by a computer program, the computer program can be distributed by securing the program to various storage media or can be transmitted via a communication network, for example.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is an explanatory diagram of an overview of an embodiment of the present invention;

FIG. **2** is a block diagram of the constitution of the storage control device;

FIG. **3** is an explanatory diagram of an aspect in which volumes are managed in groups in accordance with the performance of the disk drive;

FIG. **4** is an explanatory diagram of the management levels in the storage control device;

FIG. **5** is an explanatory diagram of a priority level calculation method;

FIG. **6** is an explanatory diagram of the constitution of information that is managed on levels A, B, and C;

FIG. **7** is an explanatory diagram of the constitution of information that is managed on level D;

FIG. **8** is an explanatory diagram of the constitution of information that is managed on level E;

FIG. **9** is an explanatory diagram of preliminary disposition processing in which data of a lower volume are copied to a higher temporary volume beforehand;

FIG. **10** is an explanatory diagram of processing in a case where preliminary disposition has failed;

FIG. **11** is an explanatory diagram of processing to move data of a higher volume to a lower volume;

FIG. **12** is a flowchart of priority management processing;

FIG. **13** is a flowchart of data preliminary disposition processing;

FIG. **14** is a flowchart of data migration processing;

FIG. **15** is an explanatory diagram of an aspect according to a second embodiment in which a volume corresponding with an external storage control device is shifted to an offline state and the supply of power to the external storage control device is stopped;

FIG. **16** is a flowchart of processing for managing offline state volumes;

FIG. **17** is an explanatory diagram of an initial state before backup processing of a storage control device according to a third embodiment;

FIG. **18** is an explanatory diagram that follows on from FIG. **17**;

FIG. **19** is an explanatory diagram that follows on from FIG. **18**;

FIG. **20** is an explanatory diagram that follows on from FIG. **19**;

FIG. **21** is an explanatory diagram that follows on from FIG. **20**;

FIG. **22** is an explanatory diagram that follows on from FIG. **21**;

FIG. **23** is a flowchart that shows backup processing; and

FIG. **24** is an explanatory diagram of the overall constitution of a storage system in which the storage control device according to a fourth embodiment is used.

DESCRIPTION OF THE SPECIFIC EMBODIMENTS

FIG. **1** is a constitution explanatory diagram that provides an overview of an embodiment of the present invention. The storage control device **1** of this embodiment is connected to a host **8** which is a higher level device and an external storage control device **9** which is another storage control device. The host **8** is constituted as a computer device such as a mainframe computer or a server computer, for example. The external storage control device **9** is another storage control device that exists outside the storage control device **1** and comprises logical volumes **9**A.

The storage control device **1** is constituted comprising a plurality of disk drives **2**A and **2**B, a plurality of logical volumes **3**, a plurality of volume groups **4**, and at least one control unit **5**, for example.

The disk drives **2**A and **2**B are constituted as hard disk drives of a plurality of types of differing performance and reliability, for example. One disk drive **2**A is constituted as a hard disk drive of a relatively high performance and the other disk drive **2**B is constituted as a hard disk drive of a relatively low performance. Further, disk-type storage media need not necessarily be used for the disk drives **2**A and **2**B. The disk drives **2**A and **2**B can also use other storage devices other than hard disk drives. For example, a constitution that uses semiconductor memory devices (including flash memory devices), holographic memory, optical disk devices, magneto-optical disk devices, and magnetic tape devices or the like is also possible. When no particular distinction is made between the disk drives hereinbelow, disk drives **2**A and **2**B are sometimes referred to as disk drives **2**.

The logical volumes **3** are logical storage regions that are provided in physical storage regions of the disk drives **2** and can also be called logical storage devices. As shown in the following embodiments, one or a plurality of logical volumes **3** can be generated by using a storage region that one or a plurality of disk drives **2** comprise. In this embodiment, the sizes of the respective logical volumes **3** are the same for the sake of the convenience of the invention.

A volume group **4** groups the logical volumes **3** according to the performance (or reliability) of the respective logical volumes **3**. That is, each volume group **4** is constituted by a plurality of logical volumes **3** of the same type. For example, the storage control device **1** comprises a group **4**A of high-performance logical volumes **3** that is established in the storage region of the high-performance disk drive **2**A and a group **4**B of low-performance logical volumes **3** that is established in the storage region of the low-performance disk drive **2**B.

FIG. **1** shows one each of volume group **4**A which comprises high-performance logical volumes **3** and volume group **4**B which comprises low-performance logical volumes **3** for the sake of convenience in the invention. The constitution is not limited to the above constitution, however. A plurality of high-performance volume groups **4**A and a plurality of low-performance volume groups **4**B can also be provided and a medium-performance volume group which comprises logical volumes of medium performance can also be provided.

In addition, the logical volumes contained in another volume group **4**C correspond to the logical volume **9**A in the external storage control device **9**. That is, whereas the respective logical volumes **3** in the volume groups **4**A and **4**B are provided in physical storage regions of the disk drives **2**A and **2**B respectively, the respective logical volumes **3** in the volume group **4**C are constituted as virtual logical volumes that use the logical volumes **9**A in the external storage control device **9** that is located outside the storage control device **1**.

In other words, whereas the data in the respective logical volumes **3** that constitute the volume groups **4**A and **4**B are stored in the disk drives **2**A and **2**B respectively of the storage control device **1**, the data in the respective logical volumes **3** that constitute the volume group **4**C are stored in the logical volumes **9**A in the external storage control device **9** that exists outside the storage control device **1**. For example, by directly matching the respective logical volumes **3** in the volume group **4**C with the respective logical volumes **9**A in the external storage control device **9**, the storage destination of the data can also be established as the logical volumes **9**A in the external storage control device **9** (also called the external volumes **9**A). Further, for example, by establishing an intermediate storage level **1**A between the logical volumes **3** in the volume group **4**C and the external volume **9**A, the constitution of the external volume **9**A can also be suitably changed and used. For example, one external volume **9**A can also be divided and mapped to a plurality of logical volumes **3** or the storage regions of a plurality of external volumes **9**A can be brought together and mapped to one or a plurality of logical volumes **3**.

A control unit **5** which is a controller controls the overall operation of the storage control device **1**. The control unit **5** is constituted as a computer device that comprises a microprocessor, a cache memory, a program memory, and a data I/O control circuit or the like, for example. The control unit **5** implements processing to input/output data to/from the logical volumes **3**, data migration processing between the volume groups **4**, and backup processing and so forth as a result of the microprocessor reading and executing a pre-stored program, for example.

The control unit **5** comprises access points **6**A, **6**B, and **6**C and management volumes **7**A, **7**B, and **7**C. The access points **6**A, **6**B, and **6**C (when no particular distinction is made, they are referred to as access points **6**) are points that are identified as access targets by the host **8** and can also be considered to be virtual volumes that are accessed by the host **8**. More specifically, the access points **6** are constituted by matching identification information for specifying port numbers, LUN (Logical Unit Numbers) and access target data. The access

points **6** are windows that are accessed by the host **8** and the places where data are actually stored are the logical volumes **3**.

The management volumes **7**A, **7**B, and **7**C (when no particular distinction is made, they are referred to as 'management volumes **7**') are information for managing the relationships of correspondence between the access points **6** and logical volumes **3** and the priority levels of the data stored in the logical volumes **3**. The access points **6** and logical volumes **3** are linked by the management volumes **7**.

An example of the method for calculating the priority level will be made clear by the following embodiments. To describe this first in simple terms, the control unit **5** calculates the frequency with which the host **8** accesses the respective data, the times that the host **8** ultimately updates the respective data, and the times (ultimate lead times) at which the host **8** ultimately accesses the respective data, and calculates the priority levels of the respective data by considering priority level hold times. The priority hold times are the times at which the priority level established for the data is maintained. The priority level established for the data is not changed until the priority level hold time has elapsed even when other parameters (access frequency, last update time, and last access time) have changed. Although default values are prepared for the priority level hold times, optional times can be set by the user.

The priority levels of the data stored in the logical volumes **3** are managed by the management volumes **7**. In other words, the priority levels of the data stored in the logical volumes **3** are separated from the data units and managed within the management volumes **7**. Hence, the priority levels of the data can be changed without changing the data stored in the logical volumes **3** simply by rewriting the priority levels in the management volumes **7**. Further, the logical volumes **3** accessed by the host **8** can be switched without the knowledge of the host **8** simply by rewriting the relationships between the access points **6** and the logical volumes **3** in the management volumes **7**.

Let us now turn our attention once again to the volume groups **4**. Each of the volume groups **4** is provided with at least one or more temporary volumes **3**T. In other words, among the plurality of logical volumes **3** that constitute the respective volume groups **4**, at least one or more logical volumes **3** are always used as temporary volumes **3**T. That is, it is probable that any of the logical volumes **3** in the volume groups **4** will be used as temporary volumes **3**T.

The temporary volumes **3**T are temporary storage regions that are used for data migration between the respective volume groups **4**. Data are able to migrate in an upward or downward direction. The upward direction signifies the direction in which data are stored in higher performance logical volumes **3** and the downward direction signifies the direction in which data are stored in lower performance logical volumes **3**. As mentioned earlier, the respective volume groups **4** are ranked into a plurality of levels from the highest rank volume group **4**A to the lowest rank volume group **4**C in accordance with their performance and reliability and so forth.

The host **8** normally uses the highest ranked logical volume **3** to perform a variety of task processing. Task processing can include database processing, electronic mail processing, and customer management processing and so forth, for example. Data Da that are currently used by the host **8** are stored in the logical volume **3** in the volume group **4**A. Suppose that the priority level of the data Da is "3". In this embodiment, the higher the value, the higher the priority level is. That is, data of priority level "3" have a higher value than data of priority level "2".

Data Db are stored in a logical volume **3** in the volume group **4**B located one rank below the volume group **4**A. The priority level of data Db is "2" and also has the highest priority level in the volume group **4**B. The host **8** is able to access the data Db that are stored in the logical volume **3** in the volume group **4**B from the access point **6**B via the management volume **7**B.

When the host **8** is not accessing the data Db, the control unit **5** copies the data Db from the logical volume **3** in the volume group **4**B to the temporary volume **3**T in the volume group **4**A. The control unit **5** copies the data Db while managing the differences between the migration source logical volume **3** and the migration destination temporary volume **3**T. The control unit **5** then rewrites the information of the management volume **7**B and connects the access point **6**B and the temporary volume **3**T in the volume group **4**A.

The access request from the host **8** to the data Db is processed as follows. In the case of the write request, the write data are written to the migration destination temporary volume **3**T. The address of the write data written to the temporary volume **3**T is managed by difference management information such as a differential bitmap. In the case of a read request for data that have already been copied to the temporary volume **3**T, the data requested by the host **8** are read from the temporary volume **3**T. In the case of a read request for data that has not yet been copied to the temporary volume **3**T, the access point **6**B and the logical volume **3** in the volume group **4**B are re-connected and the data requested by the host **8** are read from the logical volume **3** in the volume group **4**B.

Thus, the data Db of the highest priority level in the lower volume group **4**B are copied beforehand to the temporary volume **3**T in the upper volume group **4**A by using the time during which the data Db are not being accessed by the host **8**. An access request from the host **8** is then processed by using the higher performance temporary volume **3**T.

In cases where the re-arrangement of data is performed on the basis of the priority levels of the respective data, the probability that the data Db of the highest priority level in the lower volume group **4**B will migrate to the upper volume group **4**A is high. Because the data Db has already been copied to the temporary volume **3**T in the upper volume group **4**A, the control unit **5** rewrites the information of the management volume **7**B to make the storage destination of the data Db the volume **3**T. As a result of the storage destination being officially changed, the temporary volume **3**T is treated as a primary logical volume.

Among the data in the upper volume group **4**A, data of the lowest priority level are made to migrate to the volume group **4**B which is one volume group below. After the data migration is complete, the logical volume **3** in which data of the lowest priority level are stored is employed as a temporary volume **3**T. Thus, in each volume group **4**, the logical volume **3** that stores the data of the lowest priority level is used as the new temporary volume **3**T.

A case where the priority level of the data Db is changed to a low level after copying the data Db to a temporary volume **3**T in the upper volume group **4**A may also be considered. In cases where the data Db which has been copied to the temporary volume **3**T of the migration destination volume group **4**A does not have the highest priority level in the migration source volume group **4**B, the preliminary arrangement of data Db has failed. In this case, the control unit **5** reflects the differences managed by the migration destination temporary volume **3**T to the migration source logical volume **3**. The temporary volume **3**T in the migration destination volume group **4**A is used as is as a temporary volume and employed as a migration destination volume for other data.

In another respect, data can also be made to migrate from top to bottom using the temporary volume **3**T. For example, when data Dc of priority level "1" is considered, in cases where the host **8** is not accessing data Dc, the data Dc can be pre-copied to the temporary volume **3**T in the lower volume group **4**C. The control unit **5** copies data Dc from the logical volume **3** to the temporary volume **3**T while managing the difference between the migration source logical volume **3** and the migration destination temporary volume **3**T.

When the host **8** issues a write request to the data Dc, the control unit **5** writes write data to the migration source logical volume **3** and manages the address of the write data by means of a differential bitmap or the like. When a read request for data Dc is issued by the host **8**, the control unit **5** reads the data from the migration source logical volume **3** and transmits the data to the host **8**.

When the re-arrangement of the data is performed on the basis of the priority level of the respective data, the probability that migration to the lower volume group **4**C will be determined for the data Dc of the lowest priority level in the volume group **4**B is high. Because the data Dc has already been copied to the temporary volume **3**T in the lower volume group **4**C, the control unit **5** is able to complete the migration of data Dc simply by reflecting the differences from the time copying is started until data re-arrangement is executed in the temporary volume **3**T. After the migration of data Dc is complete, the control unit **5** rewrites the information of the management volume **7**C to connect the access point **6**C and the temporary volume **3**T in the volume group **4**C. The temporary volume **3**T is used as a storage destination volume of the data Dc. The data of the highest priority level in the lowest volume group **4**C migrates to the volume group **4**B that is one volume group higher. Hence, the logical volume **3** in which the data are stored is used as the new temporary volume **3**T.

In FIG. **1**, one each of the temporary volumes **3**T are shown in the respective volume groups **4** due to space limitations. However, as mentioned earlier, the constitution may also be such that a plurality of temporary volumes which are an upper temporary volume which is to be used for upward migration from bottom to top and a lower temporary volume which is to be used for downward migration from top to bottom are provided in the respective volume groups **4**. Further, because there is no need to provide an upper temporary volume in the highest volume group **4**A, only one temporary volume need be provided.

Let us know consider volume group **4**C. The respective logical volumes **3** in the volume **4**C are made to correspond with the respective logical volumes **9**A in the external storage control device **9**. When all the logical volumes **3** in the volume **4**C are then set to an offline state, the control unit **5** is able to report the fact that the supply of power to the external storage control device **9** can be stopped to the user. Alternatively, when the control unit **5** is able to control the power supply device that supplies power to the external storage control device **9**, the control unit **5** is also able to automatically stop the supply of power to the external storage control device **9**.

As mentioned earlier, in this embodiment, the volume group **4**C is constituted by the external volumes **9**A and the number of volumes **3** that are set to the online state can be set. An online-state volume signifies a volume that is placed in a state where same is capable of processing an access request from the host **8** directly.

A resource that is required for access processing such as a cache memory is allocated to the online-state logical volumes **3**. In contrast, the resources required for access processing such as the cache memory are not allocated to the offline-state logical volumes **3**. Hence, the running costs of the storage control device **1** can be reduced by preventing the futile allocation of resources to the logical volumes **3** that are not being accessed by the host **8**. The number of logical volumes **3** in the online state in the volume group **4**C is preset. When there exist logical volumes **3** for which the number of volumes that are able to enter the online state is exceeded, the logical volumes **3** that store data of a low priority level in the volume group **4**C are set to the offline state.

According to the embodiment of this constitution, at least one or more temporary volumes **3**T are created beforehand in the respective volume groups **4** and the temporary volumes **3**T are used to implement data migration between the respective volume groups **4**. Hence, in comparison with a case where a migration destination volume is generated when the time to perform data migration has come, user convenience can be raised by shortening the time required for the data migration.

In this embodiment, data of the migration target are copied to the temporary volumes **3**T before data migration is determined. Hence, when data migration is determined, data can be caused to migrate immediately simply by establishing the relationships of correspondence between the access points **6** and logical volumes **3** and reflecting the differences, and user convenience can be raised by shortening the data migration time.

In this embodiment, the values of the respective data are judged on the basis of the priority levels thereof and the storage destinations of the data are changed in accordance with the priority levels of the respective data. Hence, data can be stored in suitable logical volumes **3** in accordance with the values of the data and the disk drives **2** can be used effectively. That is, a situation where the high-performance logical volumes **3** that are constituted on the basis of the high-performance disk drives **2**A are occupied by data of low value can be prevented and data of a high usage value can be stored in high-performance logical volumes **3** by the user. The embodiment will be described in more detail hereinbelow.

First Embodiment

FIG. **2** is a block diagram that shows the constitution of the important parts of the storage control device of this embodiment. A host **10** is, for example, a computer device that comprises information processing resources such as a CPU (Central Processing Unit) and memory and so forth, and is constituted as a personal computer, work station, server computer, or mainframe computer, or the like, for example.

The host **10** comprises a communication control section for accessing a storage control device **100** via a communication network CN**1**, and an application program such as database software, for example.

Depending on the case, a LAN (Local Area Network), a SAN (Storage Area Network), the Internet, a dedicated line, a public line, or the like, for example, can be suitably used as the communication network CN**1**. Data communications via a LAN are performed in accordance with the TCP/IP protocol, for example. When the host **10** is connected to the storage control device **100** via the LAN, the host **10** requests data inputs and outputs in file units by specifying the file name. When the host **10** is connected to the storage control device **100** via the SAN, the host **10** requests data inputs and outputs in block units in accordance with the fiber channel protocol.

A management terminal **20** is a computer device for managing the constitution and so forth of the storage control device **100** and can be operated by the user such as the system manager, for example. The management terminal **20** is connected to the storage control device **100** via the communica-

tion network CN2. The user is able to set the priority level hold times of the respective data via the management terminal 20.

The storage control device 100 can be constituted as a disk array system that comprises a multiplicity of disk drives 121, for example. In addition to comprising inherent unique storage resources (disk drives 121), the storage control device 100 is also able to utilize storage resources (disk drives 221) that an external storage control device 200 comprises. As will be described subsequently, the storage control device 100 provides the host 10 with storage resources that the external storage control device 200 comprises as its own logical volumes (logical units).

The storage control device 100 is broadly categorized as the controller 110 and the storage section 120. The controller 110 is constituted comprising, for example, a plurality of channel adapters ('CHA' hereinbelow) 111, a plurality of disk adapters ('DKA' hereinbelow) 112, a cache memory 113, a shared memory 114, a connection control section 115, and a service processor ('SVP' hereinbelow) 116.

The respective CHA111 perform data communications with the host 10. Each CHA111 comprises at least one communication port 111P for communicating with the host 10. Each CHA111 is constituted as a microcomputer system that comprises a CPU or memory or the like respectively and analyzes and executes a variety of commands that are received from the host 10. A network address for identifying each of the CHA111 (IP address or WWN, for example) is allocated to each CHA111. Each CHA111 can also behave individually as NAS (Network Attached Storage). When a plurality of hosts 10 exist, each CHA111 individually receives and processes a request from each host 10.

Each DKA112 exchanges data between the disk drives 121 that the storage system 120 comprises. Each DKA112 is constituted as a microcomputer system that comprises a CPU or memory or the like as per the CHA111. Each DKA112 is connected via a communication network CN3 such as a SAN to the respective disk drives 121.

Each DKA112 writes the data that the CHA111 receives from the host 10 and data read from the external storage control device 200, for example, to a predetermined address of a predetermined disk drive 121. Further, each DKA112 reads data from the predetermined address of the predetermined disk drive 121 and transmits the data to the host 10 or external storage control device 200.

When data are input and output to and from the disk drive 121, each DKA112 converts the logical address to the physical address. The logical address is an address that indicates the block position of a logical volume 123 and is known as an LBA (Logical Block Address). Each DKA112 performs data access in accordance with a RAID configuration when the disk drive 121 is being managed in accordance with RAID. For example, each DKA 112 writes the same data to separate disk drive groups (RAID groups 122) or executes parity computation and writes data and parities to the disk drive groups.

The cache memory 113 stores data received from the host 10 or external storage control device 200 or stores data read from the disk drive 121. A variety of management information and control information and so forth for use in the operation of the storage control device 100 are stored in the shared memory (sometimes called the 'control memory') 114.

Further, any one or a plurality of the disk drives 121 may be used as a cache disk. Further, the cache memory 113 and shared memory 114 can also be constituted as separate memories, part of the storage region of the same memory can also be used as the cache region and the other storage regions can also be used as control regions.

The connection control section 115 mutually connects the respective CHA111, the respective DKA112, the cache memory 113, and the shared memory 114. The connection control section 115 can be constituted as a crossbar switch that performs data transmissions by means of a high-speed switching operation, for example.

The SVP116 is connected to the respective CHA111 via the communication network CN4 such as a LAN, for example. The SVP116 is able to access information of the respective DKA112, cache memory 113, and shared memory 114 via the CHA111. The SVP116 collects information relating to the various states in the storage control device 100 and supplies this information to the management terminal 20. The user is able to learn the various states of the storage control device 100 via the screen of the management terminal 20. Further, the user is able to set the access path between the host 10 and the logical volume 123, for example, via the SVP116 from the management terminal 20 and set the priority level hold time, and so forth. The SVP116 reflects the information input by the user as the management information and so forth.

The storage section 120 comprises a plurality of disk drives 121. As the disk drives 121, various storage devices such as hard disk drives, flexible disk drives, magnetic tape drives, semiconductor memory drives, and optical disk drives and the equivalents thereof can be employed, for example. Further, disks of different types such as FC (Fibre Channel) disks, SATA (Serial AT Attachment) disks and ATA disks, for example, can also be mixed in the storage section 120.

One RAID group (also called a 'parity group', for example) 122 is formed by a plurality of disk drives 121. One or a plurality of logical volumes 123 of a predetermined size or an optional size can be provided in the physical storage region of the RAID group 122. Further, one or a plurality of logical volumes 123 can also be provided in the storage region of a single disk drive 121. For the sake of the convenience of the invention, this embodiment will be described by taking the example of a case where the respective logical volumes 123 are the same size.

Further, the storage control device 100 comprises a virtual internal volume based on the disk drives 221 of the external storage control device 200. The virtual internal volume is provided to the host 10 in the same way as the internal volumes 123 that are generated on the basis of the disk drives 121 in the storage control device 100.

The external storage control device 200 is a separate storage control device that exists outside the storage control device 100 and is therefore called an external storage control device in this embodiment. If the storage control device 100 is called a first storage control device, the external storage control device 200 is called a second storage control device. The storage control device 100 and external storage control device 200 are connected via a communication network CN5 such as a SAN. Hence, if the storage control device 100 is known as the connection source storage control device, the external storage control device 200 is known as the connection destination storage control device. Although only one external storage control device 200 is shown in FIG. 2, a plurality of external storage control devices 200 can be connected to the storage control device 100 as shown in FIG. 3 and so forth.

The communication network CN5 that connects the storage control devices 100 and 200 can be constituted as a communication network that is separate from the communication network CN1 that is used for data I/O that connects the host 10 and storage control device 100. As a result, there is limited influence on communications between the host 10 and the storage control device 100 and data and commands and so forth can be sent and received between the storage control

devices **100** and **200**. The constitution may instead be such that the communication network CN**1** and communication network CN**3** are constituted as a shared communication network.

The external storage control device **200** comprises, for example, a controller **210** and a plurality of disk drives **221**. The controller **210** is connected to the storage control device **100** via a communication port and a communication network CN**5**. As mentioned earlier for the storage control device **100**, a RAID group **222** is constituted by a plurality of disk drives **221** and logical volumes **223** are provided in the RAID group **222**.

The external storage control device **200** can also have substantially the same constitution as that of the storage control device **100** and can also have a simpler constitution than the storage control device **100**. The disk drive **221** of the external storage control device **200** is used as an internal storage device of the storage control device **100**.

FIG. **3** is an explanatory diagram that schematically shows the constitution of the logical volumes **123** managed by the storage control device **100**. The plurality of disk drives **121** of the storage section **120** are categorized into disk drives **121**A, **121**B, and **121**C of a plurality of types and of different performance and reliability. For example, the first type of disk drive **121**A is a high-performance and high-reliability disk drive such as an FC disk. The second type of disk drive **121**B is a relative high-performance and high-reliability disk drive such as an SAS (Serial Attached SCSI) disk, for example. The third type of disk drive **121**C is a relatively low-performance and low-reliability disk drive such as a SATA disk, for example. Further, the above drive types are illustrations and the present invention is not limited to disk drives of the above types.

As a result of collecting disk drives of the same performance and reliability, the volume groups **130**A, **130**B, and **130**C are formed. When no particular distinction is made, the volume groups are called volume groups **130**. The volume group **130**A of the highest rank is a group of high-performance logical volumes **123** generated on the basis of the high-performance disk drive **121**A. The volume group **130**B which is one volume group below the highest rank volume group **130**A is a group of medium-reliability logical volumes **123** generated on the basis of the medium-performance disk drive **121**B. The volume group **130**C which is one further rank below the highest rank volume group **130**A is a group of low-reliability logical volumes **123** generated on the basis of the low-performance disk drive **121**C.

The lowest rank volume group **130**D is a group of logical volumes **123** that correspond with the logical volumes **223** in the external storage control device **200**. When the logical volume **123** in the storage control device **100** is called an internal volume, the logical volumes **223** in the external storage control device **200** can be called an external volume. In this embodiment, the lowest rank volume group **130**D is constituted as a set of external volumes **223**.

As described subsequently, in this embodiment, the value of the respective data is measured and managed by means of a particular index such as the priority level. Further, the storage location of the respective data is determined in accordance with the priority level. The higher the priority level of the data, the higher the volume group **130** the data are moved to. The lower the priority level of the data, the lower the volume group **130** that the data are moved to. At least one or more provided temporary volumes are employed in the respective volume groups **130** in the migration of data between volume groups.

Further, 'high performance' and 'low performance' refer to relative expressions that are employed for an understanding of the present invention and, even when a low-performance disk drive **121**C is used, the reliability of the storage control device **100** remains intact.

FIG. **4** is an explanatory diagram that schematically shows the constitution of a plurality of levels that are formed in the storage control device **100**. The storage control device **100** is provided, in order starting from the side closest to the host **10**, with an A level **141**A, B level **141**B, C level **141**C, D level **141**D, and E level **141**E.

A level **141**A which is closest to the host **10** is an access path management level that manages the access path from the host **10** to the logical volumes **123**. A level **141**A manages the ports **111**P and access points **151** and so forth. Further, an enclosure-internal volume copy such as one whereby a volume is copied from one volume to another volume within the storage control device **100** is also executed by forming a copy pair by means of a plurality of access points **151** that are accessed by the host **10**, which is managed by A level **141**A.

B level **141**B is provided in a position below A level **141**A. B level **141**B is a mapping level for managing the relationships of correspondence between A level **141**A and C level **141**C. B level **141**B manages the relationship between the access points **151** and management volumes **152**. Which access point **151** is accessed by which logical volume **123** can be managed by B level **141**B. That is, the actual access destination volume **123** can be switched without changing the access point **151** accessed by the host **10**. Further, access attributes can also be set in B level **141**B.

C level **141**C is provided below B level **141**B. C level **141**C forms an 'intermediate management level' together with B level **141**B and a subsequently described D level **141**D. C level **141**C manages the values of data stored in the logical volume **123** as priority levels. The priority levels are managed separately from the logical volume **123** in which data are stored.

D level **141**D is provided below C level **141**C. D level **141**D is a second mapping level for managing the relationship between C level **141**C and E level **141**E. D level **141**D controls which logical volume **123** is managed by which management volume **152**.

E level **141**E is a volume management level for classifying and managing the respective logical volumes **123** in volume groups **130** according to performance and reliability.

FIG. **5** is an explanatory diagram of a priority calculation method. As parameters for calculating the priority level, the access frequency, last update time (and last access time), and priority level hold time, for example, are used. The user is able to set arbitrary times as priority level hold times in accordance with the data migration policy. The last update time, last access time, and access frequency are obtained by analyzing the access request issued by the host **10**.

The priority level is calculated using the following equation, for example.

$$\text{Priority level} = -\alpha \times \{(\text{current time}) - (\text{last update time})\} + \beta(\text{access frequency}) - \gamma\{\{\text{current time}\} - (\text{last access time})\}/\text{priority level hold time}\} \quad \text{(Equation 1)}$$

Although initial values are each prepared for the respective coefficients α, β, and γ in Equation 1, the user is also able to suitably adjust the values of the coefficients. The computation result of $\gamma\{\{\text{current time}\} - (\text{last access time})\}/\text{priority level hold time}\}$ discards figures below the decimal point.

According to Equation 1, the closer the last update time, the higher the priority level. According to Equation 1, the higher the access frequency, the higher the priority level. According

to Equation 1, each time the priority level hold time elapses after the time the data were last accessed, the priority level drops stepwise. Therefore, as shown at the bottom of FIG. **5**, the priority level of the data drops stepwise as time elapses. However, the graph shown in FIG. **5** schematically shows an example in which the priority level changes in order to permit an understanding of the invention. This does not mean that the priority level of all the data changes as shown in FIG. **5**.

FIG. **6** is an explanatory diagram of information managed by A level **141**A, B level **141**B, and C level **141**C. The host access point information T**1** is managed by A level **141**A and B level **141**B.

The host access point information T**1** is information that defines the access path and so forth whereby the host **10** accesses the data. The host access point information T**1** comprises, for example, the management items of port ID_I**11**, host group information I**12**, LUN_I**13**, access attribute I**14**, and data ID_I**15**. Further, the case above is one where the so-called host **10** is an open-system host. In the case of a main frame-system host, the port ID is changed to the CU (Command Unit) number, the host group information is changed to the SSID (Subsystem ID), and the LUN is changed to the LDEV number.

The access attribute I**14** can be set to the values of readable and writeable, read-only, read and write-prohibited, spare capacity **0**, copy destination setting prohibited, and a hidden value, for example. The spare capacity **0** is an attribute that sends back a response to the effect that there is absolutely no spare capacity irrespective of the value for the actual spare capacity in response to a capacity inquiry command from the host **10**. A hidden value is an attribute in which a response to the inquiry command from the host **10** is not sent back and is hidden.

Data ID is identification information for uniquely specifying the respective data managed by the storage control device **100**. The port ID (CU number), host group information (LDEV number), and LUN (SSID) are managed by A level **141**A. The access attribute and data ID are managed by B level **141**B.

Data management information T2A and TMP data management T2B which are managed by C level **141**C are shown at the bottom of FIG. **6**. Data management information T2A is information for managing data stored in the respective logical volumes **123**. The TMP data management information T2B is information for managing data stored in temporary volumes at least one of which is provided in each of the volume groups **130**.

Data management information T2A includes the management items of data ID_**121**A, nickname I**22**A, priority level I**23**A, last update time I**24**A, access frequency I**25**A, and priority level hold time I**26**A, for example. Further, here, the last access time is also managed within the last update time I**24**A. The nickname is information for specifying data simply.

The TMP data management information T2B manages data ID_I**21**B and differential bitmap I**22**B, for example. The differential bitmap I**22**B is difference management information for managing differences between data copied first to the temporary volume and copy source (migration source) data.

FIG. **7** shows information and so forth managed by D level **141**D. The data volume mapping information T**3** is managed by D level **141**D. The data volume mapping information T**3** is information indicating the relationship of correspondence between data and the logical volumes **123**. The information T**3** comprises, for example, data management information I**31**, internal volume information I**32**, and information I**33** distinguishing whether the logical volumes are online or offline.

Either data management information T2A or TMP data management information T2B shown in FIG. **6** is set as the data management information I**31**. Either internal volume information T**6**A or external volume information T**6**B described subsequently in FIG. **8** is set as the internal volume information I**32**. Information indicating whether the logical volumes **123** are in an online state or offline state is set as item I**33**.

Volume group information T**4** is information for managing the respective volume groups **130**. The volume group T**4** comprises, for example, volume group ID_I**41**, nickname I**42**, performance value I**43**, TMP volume number I**44**, and a plurality of data volume mapping information items I**45** to I**47**.

The volume group ID_I**41** is information for uniquely specifying a volume group **130**. The nickname I**42** is information for simply specifying the volume group **130**. The performance value I**43** is information indicating a value related to the performance of the volume group **130**. Performance-related information can include the type of disk drive **121** and the access speed or the like, for example. The TMP volume number I**44** is information indicating the number of temporary volumes provided in the volume group **130**. The data volume mapping information items I**45** to I**47** are information for specifying the data volume mapping information T**3** shown at the top of FIG. **7**.

The data group information T**5** is management information that is to be used in the backup processing. The data group information T**5** manages, for example, a data group ID_I**51**, nickname I**52**, a backup schedule I**53**, a primary volume I**54**, and at least one or more volume groups ID_I**55** to I**57**.

The data group ID_I**51** is information for specifying a data group that forms a copy pair from a primary volume and secondary volume. The nickname is information for simply specifying the data group. The backup schedule I**53** is information indicating the schedule for backing up the data of the primary volume. The primary volume I**54** is information for specifying a primary volume. The volume groups ID_I**55** to I**57** are information for specifying volume group information T**4**. By using the data group information T**5**, it is possible to manage which data of which primary volume are backed up to which logical volume **123** of which volume group **130** with which timing.

FIG. **8** is an explanatory diagram of an internal volume information T**6**A and external volume information T**6**B managed by E level **141**E. The internal volume information T**6**A is information for managing a logical volume **123** that exists in the storage control device **100**. The external volume information T**6**B is information for managing a logical volume **223** that exists in the external storage control device **200**.

The internal volume information T**6**A comprises, for example, a volume ID_I**61**A and physical drive information I**62**A. The physical drive information I**62**A stores information relating to the RAID group **122** and disk drive **121** and so forth in which the logical volume **123** specified by a volume ID_I**61**A is provided. For example, information (the drive number) for specifying the disk drive **121** in which the logical volume **123** is provided can include the type of the disk drive **121**, the RAID level of the RAID group **122**, and the capacity and so forth.

The external volume information T**6**B comprises a volume ID_I**61**B and an external logical device information I**62**B, for example. The external logical device information I**62**B stores information for specifying the logical volumes **223** in the

external storage control device **200**. For example, this information includes the name of vendor that supplies the external storage control device **200**, the product name of the external storage control device **200**, the product number of the external storage control device **200**, and identification information for accessing the logical volumes **223** (the port numbers, LUNs, and volume numbers, for example).

The method for causing data to migrate between the respective volume groups **130** on the basis of the priority level will now be described on the basis of the FIGS. **9** to **11**. The details of the method for determining the priority level, the method for data migration, and the method for copying the data first before the data migration will be described subsequently together with the individual figures.

FIG. **9** is an explanatory diagram of an aspect in which data of a high priority level are made to migrate to a upper volume group **130** before data migration is started. Processing in which data of a high priority level are copied to the temporary volume in the upper volume group before data migration is executed is known as preliminary disposition processing. In the following description, the volume group **130**A will be described as the upper volume group and the volume group **130**B will be described as the lower volume group by way of example.

FIG. **9**A shows a state prior to starting the preliminary disposition processing. Data A of priority level "3" are stored in the logical volume **123** (A1) of the upper volume group **130**A. The volume **123** (A2) is set as the temporary volume. Data B of priority level "2" are stored in the logical volume **123** (B1) of the lower volume group **130**B and data C of priority level "1" are stored in the logical volume **123** (B2). The volume **123** (B3) is set as the temporary volume.

When the lower volume group **130**B is considered, data B is accessed by the host **10** frequently and the priority level is set as "2". Therefore, the priority level of data B has a larger priority level than the priority level "1" of other the data stored in the lower volume **130**B and the highest priority level in the data stored in the lower volume group **130**B. Therefore, data B has a high probability of migrating to the upper volume group **130**A during the next data migration processing.

As shown in FIG. **9**B, the controller **110** copies data B that has the highest priority level in the lower volume group **130**B to the temporary volume **123** (A2) in the upper volume group **130**A when a time comes when the host **10** is not accessing data B. That is, in the preliminary disposition processing, a copy pair is established in which the logical volume **123** (B1) that stores the data B of the highest priority level in the lower volume group **130**B is the copy source and the temporary volume **123** (A2) in the upper volume group **130**A is the copy destination.

As shown in FIG. **9**C, the data copying from the lower logical volume **123** (B1) to the upper temporary volume **123** (A2) is performed while differences are managed. The differential bitmap **160**, for example, is used for the difference management.

When an access request to data B is issued by the host **10**, the controller **110** basically processes an access request by using data B stored in the upper temporary volume **123** (A2).

That is, the write data received by the host **10** are written in the temporary volume **123** (A2). The difference produced by the update of write data is recorded in the differential bitmap **160**. The data for which reading has been requested by the host **10** are read from the temporary volume **123** (A2). When the reading of the data that exist only in the copy source logical volume **123** (B1) has been requested, the controller **110** reads the data from the logical volume **123** (B1) and transmits the data to the host **10**.

Further, the data of the highest priority level in the lower volume group are also copied beforehand to the temporary volume **123** (B3) in the lower volume group **130**B.

Thus, the data B of the highest priority level in the lower volume group **130**B are copied to the temporary volume **123** (A2) in the upper volume group **130**A beforehand and the access request from the host **10** is processed using the temporary volume **123** (A2). The upper temporary volume **123** (A2) is formed on the basis of the higher performance disk drive **121** and, therefore, the access request can be processed rapidly and the responsiveness of the storage control device **100** can be improved.

FIG. **10** is an explanatory diagram of processing in a case where the preliminary disposition of data B fails. The priority level of the respective data A to C are calculated and updated at regular and irregular intervals. FIG. **10**A shows an aspect at a time where the preliminary disposition of data B is complete. At this point in time, the latest stored content of data B is held in the upper temporary volume **123** (A2) and the stored content when the preliminary disposition is started is stored in the lower logical volume **123** (B1). The difference between the volume **123** (A2) and the volume **123** (B1) is managed by the differential bitmap **160**.

Therefore, after completing the preliminary disposition, data B are stored in both the volume **123** (A2) and volume **123** (B1) of different types. Therefore, when a fault is produced in either volume **123** (A2) or volume **123** (B1), the latest data B can be obtained using the other volume.

The priority level of data changes gradually with time in accordance with the state of being accessed by the host **10**. Hence, as shown in FIG. **10**B, a situation where the priority level of data B that are copied to the upper temporary volume **123** (A2) subsequently drops from "2" to "1" may also be considered. In FIG. **10**B, while the priority level of data B drops by one, the priority level of data C increases from "1" to "2".

Therefore, as shown in FIG. **10**C, the controller **110** uses data B in the differential bitmap **160** and upper temporary volume **123** (A2) to place data B in the lower logical volume **123** (B1) in the latest state. Thus, after data B have been written back from temporary volume **123** (A2) to logical volume **123** (B1), the controller **110** copies data C with the highest priority level from the logical volume **123** (B2) to the temporary volume **123** (A2).

Ultimately, the controller **110** uses data C stored in temporary volume **123** (A2) to process access requests from the host **10** as described in the preliminary disposition processing of data B (FIG. **10**D).

FIG. **11** is an explanatory diagram of data migration processing that re-disposes the respective data in the logical volumes **123** which each have a suitable performance, in accordance with the priority level of the respective data. FIG. **11**A shows the state prior to the start of data migration processing. The data Dc with the highest priority level in the lower volume group **130**B are pre-stored in the temporary volume **123** (A2) in the upper volume group **130**A by the preliminary disposition processing mentioned earlier. The differences between the volume **123** (A2) and volume **123** (B2) are managed by the differential bitmap **160**. Access requests from the host **10** are processed by using data Dc in the upper temporary volume **123** (A2).

However, at the point shown in FIG. **11**A, the formal storage destination (storage destination device) for data Dc is copy source volume **123** (B2). The upper temporary volume **123** (A2) is only used as a temporary storage destination for data Dc.

FIG. **11**B shows the result of data migration processing being executed. Here, the priority levels of the respective data Da, Db, and Dc are first calculated and, as a result, the priority level of data Da is lowered from "3" to "2".

The priority level of data Dc has a high priority level and is unchanged at "3". Therefore, the movement of data Dc from lower volume group **130**B to upper volume group **130**A is determined. As a result of the above preliminary disposition processing, data Dc are copied beforehand to the temporary volume **123** (A**2**) in the upper volume group **130**A and the controller **110** processes an access request from the host **10** by using data Dc that have been copied to the temporary volume **123** (A**2**).

Therefore, the data Dc that are copied beforehand to the temporary volume **123** (A**2**) hold the latest state. Hence, the controller **110** rewrites information managed in C level **141**C and D level **141**D and establishes the temporary volume **123** (A**2**) as a storage device for data Dc. That is, the data migration from lower volume group **130**B to upper volume group **130**A is completed directly simply by rewriting the management information.

As a result of data Dc migrating to the upper volume group **130**A, volume **123** (B**2**) which is the migration source can be used as a second temporary volume. Therefore, the controller **110** copies data Da with the lowest priority level in the upper volume group **130**A from the upper logical volume **123** (A**1**) to the lower temporary volume **123** (B**2**). In other words, the controller **110** establishes a copy pair of the volume **123** (A**1**) and volume **123** (B**2**) and manages differences between the two volumes by means of a differential bitmap **160** until the data migration is complete.

FIG. **12** is a flowchart that shows the priority level management processing. The subsequent respective processes that include this processing are implemented as a result of the controller **110** executing a predetermined program. Further, the respective flowcharts that will be subsequently described provide an overview of the processing to the extent required in order to understand and implement the present invention and sometimes differ from the actual program. The modification, addition, and deletion of steps can be suitably performed by a person skilled in the art.

The controller **110** acquires information related to the current time from the timer and counter and so forth provided in the controller **110**, for example (S**10**). The controller **110** acquires the last update time (S**11**), the last access time (S**12**), the access frequency (S**13**), and the priority level hold time (S**14**). The controller **110** then calculates the priority level by using Equation 1 above (S**15**) and rewrites the priority level in the data management information T**2**A to the latest value (S**16**).

The controller **110** judges whether the priority level has been calculated for all the data (S**17**). When unprocessed data remain (S**17**: NO), the controller **110** changes the processing target to the next data (S**18**) and returns to S**10**. When a priority level calculation and update are complete for all data, the processing ends.

FIG. **13** is a flowchart showing the preliminary disposition processing. The controller **110** judges whether the priority level has been changed (S**20**). When the priority levels have been changed by the priority level management processing (S**20**: YES), the controller **110** judges whether data of the highest priority in the lower volume group have been copied beforehand to the temporary volume in the upper volume group (S**21**). That is, the controller **110** judges whether the data of the migration target have been copied beforehand to the migration destination volume group before the data migration processing has started.

When data of the highest priority have been copied beforehand to the upper temporary volume (S**21**: YES), the controller **110** judges whether the data that have been pre-copied have the highest priority level in the lower volume group (S**22**). In cases where the data currently with the highest priority level in the lower volume group have already been copied to the temporary volume in the upper volume group, this processing is terminated.

In contrast, when the priority level of the data of the lower volume that was first disposed in the previous preliminary disposition processing is changed and is not the highest priority level in the lower volume group (S**22**: NO), the previous preliminary disposition fails. Therefore, the controller **110** places the data in the lower volume in the latest state by writing the differential data managed by the upper temporary volume to the copy source lower volume (S**23**).

When the data of the highest priority level have not been pre-copied to the upper temporary volume in the lower volume group (S**21**: NO), the controller **110** copies data of the highest priority level in the lower volume group to the temporary volume in the upper volume group (S**24**). The differences between the lower volume which is the copy source and the upper temporary volume which is the copy destination are managed by the upper volume group. The controller **110** uses the data that have been copied to the upper temporary volume to process an access request from the host **10** (S**25**).

FIG. **14** is a flowchart that shows data migration processing. The controller **110** judges whether the priority level has changed (S**30**). Thereafter, the controller **110** judges whether data migration is necessary (S**31**).

When it is judged that the priority levels of at least part of the data have been changed (S**30**: YES) and data must be moved (S**31**: YES), the controller **110** starts data migration as described below.

In S**31**, for example, it is judged whether data migration is to be performed on the basis of the data migration preset by the user. For example, when the user pre-designates the execution time of the data migration, the controller **110** judges whether the designated execution time has arrived.

When the start of data migration is determined, the controller **110** confirms the data stored in the temporary volume in the upper volume group (S**32**). The controller **110** judges whether data for which migration from the lower volume group to the upper volume group has been determined have already been copied to the upper temporary volume (S**33**).

As a result of the preliminary disposition processing, data of a high priority level are pre-copied to the upper temporary volume before the data migration processing is started. Hence, the controller **110** judges in S**33** whether the preliminary disposition has succeeded.

When the preliminary disposition has succeeded (S**33**: YES), the controller **110** terminates the data migration from the lower volume group to the upper volume group by rewriting the management information of the data first disposed (S**34**).

When the preliminary disposition fails as a result of the change in priority levels (S**33**: NO), the controller **110** copies the data with the highest priority level in the lower volume group to the temporary volume in the upper volume group (S**35**).

Finally, the controller **110** moves data of the lowest priority level by copying data of the lowest priority level in the upper volume group to the specified volume in the lower volume group (S**36**). The specified volume is volume **123** (B**2**) shown in FIG. **11**B, for example. That is, the specified volume is a

volume in the lower volume group for which new data can be accepted for the data migration from the lower volume group to the upper volume group.

The embodiment affords the following effects on account of having the above constitution. In this embodiment, the constitution is such that data are made to migrate between respective volume groups by using the temporary volume provided in each volume group. Hence, the time required for the data migration can be shortened and user convenience improves.

In this embodiment, the constitution is such that data of the migration target are pre-copied to the temporary volume in the volume group which has been preset as the migration destination before the data migration is performed. Therefore, data migration can be rapidly completed and user convenience improves.

In this embodiment, the constitution is such that the value of the data is judged and the respective data are then disposed in volumes of suitable performance. Hence, disk drives **121** whose performance and reliability differ can also be effectively used and user convenience improves.

In this embodiment, the constitution is such that the priority level is changed each time the priority level hold time designated by the user has elapsed. Hence, the value of the data that cannot be measured simply from the access frequency and last access time and so forth can be assessed.

In this embodiment, the constitution is such that one temporary volume is prepared in each of the volume groups and a logical volume capable of accepting new data in accordance with the completion of data migration is used as another temporary volume. Therefore, the volume of the storage control device **100** can be effectively used and user convenience can be improved while suppressing an increase in costs.

Second Embodiment

The second embodiment of the present invention will now be described on the basis of FIGS. **15** and **16**. The subsequent embodiments that include this embodiment correspond to modified examples of the first embodiment above. In this embodiment, the supply of power to the external storage control devices **200** is stopped by setting the external volumes **223** provided by the external storage control devices **200** to an offline state as far as is possible and the power consumption amount of the whole storage system is reduced.

FIG. **15** is an explanatory diagram that shows an aspect in which volumes in an offline state are grouped in the external storage control devices **200** and the power supply to the external storage control devices **200** is stopped. As shown in FIG. **15**A, the volume group **130** is constituted by logical volumes **123**(**1**) to **123**(**3**) corresponding to the external volumes **223**(**1**) to **223**(**3**).

The external volume **223**(**1**) of the first external storage control device **200** (**1**) corresponds to the logical volume **123**(**1**) and the priority level of the data B stored in the logical volume **123** (**1**) is "2". Accurately speaking, the logical volume **123** (**1**) exists virtually and the actual storage of data B is in the external volume **223** (**1**).

Likewise, the first external volume **223** (**2**) of the second external storage control device **200**(**2**) corresponds to the logical volume **123** (**2**) and the priority level of data C stored in the logical volume **123** (**1**) is "3". The other external volume **223** (**3**) of the second external storage control device **200** (**2**) corresponds to the logical volume **123** (**3**) and the priority level of the data stored in the logical volume **123**(**3**) is "1".

The number of volumes that can be set in the online state in the volume group **130** is assumed to be one. Therefore, the storage control device **100** sets only the logical volume **123** (**2**) that stores the data of the highest priority level among the three logical volumes **123** (**1**) to **123** (**3**) to the online state and sets the logical volumes **123** (**1**) and **123** (**3**) to the offline state.

Thus, the storage control device **100** allocates the storage region of the cache memory **113** only to the logical volume **123** (**2**) in the online state. The storage region of the cache memory **113** is not allocated to the offline-state logical volumes **123** (**1**) and **123** (**3**). By allocating the storage region of the cache memory **113** only to the online state logical volume **123** (**2**), the cache memory **113** can be efficiently used and the costs of the storage control device **100** can be reduced. Further, the resources allocated only to the online state logical volume are not limited to the cache memory **113**. However, here, for the sake of expediency in the description, the cache memory **113** will be explained by way of example.

As shown in FIG. **15**B, the storage control device **100** sets the logical volumes **123** (**2**) and **123** (**3**) to the offline state by switching the storage locations of data B and data C. The switching of the storage destination devices for data B and data C can be implemented by using the temporary volume provided in the other volume group **130**. For example, if data B are copied from volume **123** (**1**) to the temporary volume, data C are copied from volume **123** (**2**) to volume **123** (**1**), and data B are copied from the temporary volume to volume **123** (**2**), data B can be stored in volume **123** (**2**) and data C can be stored in volume **123** (**1**).

As a result of switching the storage locations of data B and data C, logical volumes **123** (**2**) and **123** (**3**), which are mapped to external volumes **223** (**2**) and **223** (**3**) of the second external storage control device **200** (**2**) are each set to the offline state. Hence, no inconvenience of any kind is produced for the storage system even when the operation of the second external storage control device **200** (**2**) is stopped. This is because the external volumes **223** (**2**) and **223** (**3**) correspond to offline state volumes not used by the host **10**.

Therefore, the storage control device **100** stops the supply of power to the second external storage control device **200** (**2**). As a result, the power consumption of the whole storage system is reduced and the operating costs of the storage system drop.

FIG. **16** is a flowchart showing the processing for managing offline-state volumes. The controller **110** acquires information on the volume group **130** constituted by the external volumes **223** of the external storage control devices **200** (S**40**). Thereafter, the controller **110** acquires information relating to the external storage control devices **200** (S**41**).

The controller **110** judges whether all the external volumes **223** provided by the specified external storage control devices **200** among the plurality of external storage control devices **200** are in an offline state (S**42**). More accurately, the controller **110** judges whether the logical volumes **123** corresponding with the respective external volumes **223** of one external storage control device **200** are all in the offline state.

When there is a mixture of online state external volumes **223** and offline state external volumes **223** in the specified external storage control device **200** (S**42**: NO), as shown in FIG. **15**, the controller **110** causes the offline state external volume **223** provided by the other external storage control device **200** to migrate to the specified external storage control device **200** (S**43**).

That is, more accurately speaking, when the states of the plurality of logical volumes **123** that correspond with the plurality of external volumes **223** in the specified external storage control device **200** are divided into an online state and offline state, the controller **110** changes the data storage des-

tination so that all of the external volumes **223** in the specified external storage control device **200** correspond to the offline state logical volumes **123** (S43).

The controller **110** then judges whether the supply of power to the specified external storage control device **200** can be controlled by the controller **110** (S44). For example, when both the storage control device **100** and the specified external storage control device **200** each comprise an interface or the like for sending and receiving commands and signals and so forth for controlling the supply of power remotely (S44: YES), the supply of power to the specified external storage control device **200** can be automatically stopped by means of a command from the controller **110** (S45).

In contrast, when the supply of power to the specified external storage control device **200** cannot be controlled by an instruction from the controller **110** (S44: NO), the controller **110** informs the user that the supply of power to the specified external storage control device **200** can be stopped via the management terminal **20** (S46).

This embodiment with this constitution also affords the same effects as those of the first embodiment. In addition, in this embodiment, a temporary volume is used to match an offline state logical volume **123** with an external volume **223** in the specified external storage control device **200** and the supply of power to the specified external storage control device **200** can be stopped. Hence, the amount of power consumption of the storage system is reduced and operating costs can be saved.

Third Embodiment

A third embodiment will now be described with respect to FIGS. **17** to **23**. In this embodiment, a temporary volume is used to create a backup of the backup-target volume beforehand before a backup instruction is issued.

FIGS. **17** to **22** are explanatory diagrams of an aspect in which backup target data Da which are stored in the primary volume **123** (A1) are backed up automatically and stepwise. The primary volume **123** (A1) used by the host **10** is made to correspond with the access point **151** (1) by means of the management volume **152** (**1**). The initial priority level of the data (operating data) Da of the backup target is assumed to be "1".

As shown in FIG. **18**, the controller **110** copies data Da from the primary volume **123** (A1) to temporary volume **123** (B1) provided in lower volume group **130**B which is one volume group lower when a time comes when the host **10** is not accessing data Da. The management volume **152**(**2**) for managing the data copied to the temporary volume **123** (B1) then manages the priority level of the data Da copied to the temporary volume **123** (B1). The controller **110** manages the differences between the primary volume **123** (A1) and temporary volume **123** (B1) produced after copying is complete in the primary volume **123** (A1).

As shown in FIG. **19**, when backup processing of data Da is started as a result of the backup schedule or an instruction from the user, the controller **110** reflects the differences between the primary volume **123** (A1) and temporary volume **123** (B1) in data Da in the temporary volume **123** (B1). The controller **110** then sets temporary volume **123** (B1) as the device for storing data Da. In other words, based on the subsequent management, the data Da stored in the volume **123** (B1) are treated as real data. As a result, the backup of data Da is complete.

The host **10** uses the primary volume **123** (A1) as is after the backup processing is complete and interrupts the work processing. New operating data Db are stored in the primary volume **123** (A1).

As shown in FIG. **20**, the data Da which are stored in volume **123** (B1) are backup data and, therefore, the frequency with which these data are accessed by the host **10** is low. Therefore, the priority level of data Da gradually drops lower. Thereafter, as a result of data migration processing, data Da are made to migrate to the temporary volume **123** (C1) in the lower volume group **130**C.

As shown in FIG. **21**, the new operating data Db are also copied to the temporary volume **123** (B1) in the lower volume group **130**B when a time comes when the host **10** is not accessing data Db as illustrated by FIG. **18**.

As shown in FIG. **22**, by repeating the above operation, a backup of data in the primary volume **123** (A1) is created automatically and the older the backup the lower the volume group **130** the data are disposed in.

The host **10** is then able to access backup data of the desired age simply by switching the connection to the access point **151** (**2**) for accessing the backup data. The backup data of the age desired by the host **10** can be supplied to the host **10** simply by switching the relationship between the access point **151** (**2**) of the backup data and the management volumes **152** (**2**) and **152** (**3**) that manage backup data of the respective ages within the storage control device **100**. Furthermore, in FIG. **22**, although numerals have only been provided for only two management volumes **152** (**1**) and **152** (**2**) due to space constraints, the management volume **152** is prepared for the respective backup data.

Further, the logical volumes **123** (C3), **123** (C4), and **123** (C5) which correspond with the external storage control device **200** (**2**) in FIG. **22** are each set to offline states. The respective volumes **123** (C3) to **123** (C5) are each set temporarily to the online state only when data are moved.

FIG. **23** is a flowchart showing the above backup processing. The controller **110** judges whether access by the host **10** to the operating data has been interrupted (S50). When access by the host **10** to the operating data has been interrupted (S50: YES), it is judged whether the differences with respect the operating data are being managed (S51). When differences are being managed (S51: YES), data currently being used for the operation have sometimes already been copied to the lower temporary volume. Hence, S52 and S53 below are skipped and the processing moves to S54.

When difference management has not been performed on the operating data (S51: NO), the controller **110** copies the operating data to the temporary volume in the lower volume group (S52) and starts difference processing (S53). A differential bitmap **160**, for example, is used in the difference management.

The controller **110** judges whether an instruction to create a backup has been provided (S54). For example, when it is judged, based on the backup schedule, that the backup creation time has arrived, the controller **110** reflects the differences to the temporary volume to which the operating data have been copied (S55). Thereafter, data stored in the temporary volume are managed as backup data of the operating data (S56). As a result, the backup processing of the operating data ends.

The embodiment with this constitution also affords the same results as those for the first embodiment. In addition, in this embodiment, a backup of the operating data can be created automatically by using the temporary volume and user convenience improves. Further, because the operating data are copied to the temporary volume beforehand, a backup of

the operating data can be created rapidly simply by writing the differences produced after copying to the temporary volume. Hence, the backup time can be shortened and user convenience can be improved.

Fourth Embodiment

A fourth embodiment will now be described based on FIG. **24**. In this embodiment, a plurality of storage control devices **100** (**1**), **100** (**2**), and **100** (**3**) are mutually connected using an external connection function and the volumes that the respective storage control devices **100** (**1**) to **100** (**3**) comprise are each managed on level E of the respective storage control devices **100** (**1**) to **100** (**3**). Further, due to space constraints in FIG. **24**, 'storage control device' is displayed as 'storage'. 'Storage (**1**)' in FIG. **24** denotes the storage control device **100** (**1**), 'storage (**2**)' denotes 'storage control device **100** (**2**)', and 'storage (**3**)' denotes 'storage control device **100** (**3**). Likewise, 'host (**1**)' denotes host **10** (**1**), 'host (**2**)' denotes host **10** (**2**), and 'host (**3**)' denotes host **10** (**3**).

The external connection function is a function whereby one storage control device incorporates the volumes of another storage control device as if the volumes of the other storage control device were its own volumes as was mentioned earlier with regard to the storage control device **100** and external storage control device **200**. By creating virtual volumes that are mapped to the other storage control devices among the respective storage control devices **100** (**1**) to **100** (**3**), the respective storage control devices are able to incorporate and use volumes of the other storage control device.

The respective storage control devices **100** (**1**) to **100** (**3**) are each managed using the respective data on level B and C and limits are set for the hosts capable of updating the respective data. That is, update-related constraints are set so that data are not updated by a host other than a host that has been permitted beforehand. Further, the respective hosts **10** (**1**) to **10** (**3**) are set so that all the data can be read.

Data migration processing is performed so that the respective data in the storage system are disposed in the storage control devices connected to the host with the highest access frequency among the respective storage control devices **100** (**1**) to **100** (**3**).

Moreover, the present invention is not limited to the above embodiments. A person skilled in the art is able to perform a variety of additions and modifications and so forth within the scope of the present invention.

What is claimed is:

1. A storage control device that comprises a plurality of storage drives for storing data used by a higher level device and a controller that controls data inputs and outputs between each of the storage drives and the higher level device, comprising:

a plurality of logical volumes formed on the basis of physical storage regions of the respective storage drives;

a plurality of volume groups each formed by grouping a plurality of each of the respective logical volumes;

a priority level management section that is provided in the controller and that detects and manages each of the priority levels of the data stored in the respective logical volumes on the basis of an access request issued by the higher level device; and

a data migration section provided in the controller that moves the data between the respective volume groups on the basis of the respective priority levels managed by the priority level management section,

wherein, among the respective logical volumes in the respective volume groups, at least one or more of the logical volumes is established as a temporary volume which is used for the migration of the data;

wherein the respective storage drives are classified as storage drives of a plurality of types each of which has a different performance, and the respective volume groups are ranked from a volume group with the highest rank to a volume group with the lowest rank in accordance with the type of the storage drive in which the respective logical volumes constituting the respective volume groups are provided, and

wherein the data migration section selects data with the highest priority level among the respective data contained in a migration source volume group of a relatively low rank as the migration target data and copies the migration target data beforehand to the temporary volume contained in a migration destination volume group that is one rank higher,

wherein the data migration section uses the temporary volume to move the migration target data between the respective volume groups before the migration destination of the migration target data has been determined.

2. The storage control device according to claim **1**, wherein the respective volume groups are ranked in accordance with the types of the respective logical volumes that constitute the respective volume groups.

3. The storage control device according to claim **2**, wherein the data migration section uses the temporary volume to move the migration target data between the respective volume groups so that the data of a high priority level are located in a volume group of a higher rank and data of a low priority level are located in a volume group of a lower rank.

4. The storage control device according to claim **1**, wherein the priority level management section detects and manages the priority levels of each of the data on the basis of the last time the higher level device accessed the respective data and the frequency with which the higher level device has accessed the respective data.

5. The storage control device according to claim **1**, wherein the priority level management section detects and manages the priority level for each of the respective data on the basis of the last time the higher level device accessed the respective data, the frequency with which the higher level device has accessed the respective data, and a priority level hold time that is preset for the respective data.

6. The storage control device according to claim **1**, wherein the data migration section uses the migration target data copied to the temporary volume in the migration destination volume group to process an access request issued by the higher level device to the migration target data.

7. The storage control device according to claim **6**, wherein the data migration section manages the differences between the temporary volume in the migration destination volume group and a migration source logical volume in the migration source volume group with respect to the migration target data.

8. The storage control device according to claim **7**, wherein the data migration section reflects the differences in the migration source logical volume when the priority level of the migration target data is lowered by the priority level management section and copies other data set at the highest priority level in the migration source volume group to the temporary volume in the migration destination volume group.

9. The storage control device according to claim **1**, wherein the data migration section copies beforehand backup target data stored in a backup target logical volume that exists in a higher ranking volume group to a temporary volume in a lower ranking volume group.

10. The storage control device according to claim 9, wherein the data migration section manages differences between the backup target logical volume and the temporary volume in the lower ranking volume group with respect to the backup target data and ends the backup by reflecting the differences in the temporary volume when an instruction to execute a backup is issued.

11. The storage control device according to claim 1, wherein the controller controls each of (1) an access path management level that manages access points accessed by the higher level device, (2) a volume management level that manages the respective logical volumes, (3) an intermediate management level that manages management information related to the data stored in the volume management level and associations between the access points and the logical volumes.

12. The storage control device according to claim 11, wherein the intermediate management level is constituted comprising a first level that manages the management information, a second level that manages the relationship between the access points and the first level, and a third level that manages the association between the first level and the volume management level.

13. The storage control device according to claim 1, wherein at least one specified volume group among the respective volume groups is constituted by a virtual logical volume that is associated with another logical volume that exists in a plurality of different storage control devices; and the controller allocates cache memory in the controller when the virtual logical volume has been set to the online state and does not allocate the cache memory when the virtual logical volume has been set to the offline state.

14. The storage control device according to claim 13, wherein the controller stores low priority level data in the specified virtual logical volumes associated with the other logical volumes in the specified other storage control device and, when the specified virtual logical volumes have all been set to the offline state, reports the fact that the supply of power to the specified other storage control device can be stopped or automatically stops the supply of power to the specified other storage control device.

15. A data migration method that uses a storage control device that comprises a plurality of storage drives for storing data used by a higher level device and a controller that controls data inputs and outputs between each of the storage drives and the higher level device,

wherein the controller executes:

a step of generating each of a plurality of volume groups by grouping a plurality of each of a plurality of logical volumes formed on the basis of the physical storage regions of the respective storage drives according to the performance of the respective storage drives and setting at least one or more logical volumes among the respective logical volumes in the respective volume groups as a temporary volume for moving data;

a step of detecting and managing each of a plurality of priority levels of the data stored in the respective logical volumes on the basis of an access request issued by the higher level device;

a step of classifying the respective storage drives as storage drives of a plurality of types each of which has a different performance, and ranking the respective volume groups from a volume group with the highest rank to a volume group with the lowest rank in accordance with the type of the storage drive in which the respective logical volumes constituting the respective volume groups are provided; and

a step of selecting data with the highest priority level among the respective data contained in a migration source volume group of a relatively low rank as the migration target data and copying the migration target data beforehand to the temporary volume contained in a migration destination volume group that is one rank higher,

a step of using the temporary volume to move migration target data between the respective volume groups before data migration is determined so that the high priority level data are stored in a volume group associated with a higher performance storage drive and the low priority level data are stored in a volume group associated with a lower performance storage drive.

* * * * *

US-PAT-NO: 10365857

DOCUMENT-IDENTIFIER: US 10365857 B2

TITLE: Memory system

DATE-ISSUED: July 30, 2019

PRIOR-PUBLICATION-INFORMATION:

DOCUMENT-IDENTIFIER	DOCUMENT-DATE
US 20180121136 A1	May 3, 2018

PATENT-FAMILY-ID: 62021475

Primary Examiner - XP (1):

Lane; John A

Claims Text - CLTX (6):

6. The memory system according to claim 1, wherein the identifier is received from the **host** in connection with a **write** command, and the controller is configured to select the non-volatile memory die so that a difference between program-erase cycles of the selected non-volatile memory die and minimum program-erase cycles of the plurality of non-volatile memory dies within the selected die set is within an allowable difference, and which has a highest assigned priority among the non-volatile memory dies within the selected die set having the difference within the allowable difference, when the received **write** command includes a **policy** indicating that wear leveling is to be preferentially considered.

Claims Text - CLTX (7):

7. The memory system according to claim 1, wherein the identifier is received from the **host** in connection with a **write** command, and the controller is configured to select the non-volatile memory die based on the number of uncompleted processes to be executed therein in order of the assigned priorities of the non-volatile memory dies within the selected die set, when the received **write** command includes

a **policy** indicating that a **writing** speed is to be preferentially considered.

Bibliographic Data

Application No: 15/804,772

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No ☐ Met After Allowance

Verified and Acknowledged: /JOHN A LANE/ (Examiner's Signature) (Initials)

Title: DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/06/2017	711	2139	980.0023
RULE			

APPLICANTS

Gaea LLC, Niwot, CO,

INVENTORS

Joshua Johnson Frederick, CO, UNITED STATES

Curt Bruner Niwot, CO, UNITED STATES

Jeffrey Reh Longmont, CO, UNITED STATES

Christopher Squires Boulder, CO, UNITED STATES

Brian Wilson Zumbro Falls, MN, UNITED STATES

CONTINUING DATA

This application has PRO of 62448826 01/20/2017

This application has PRO of 62418742 11/07/2016

This application has PRO of 62418785 11/07/2016

This application has PRO of 62418687 11/07/2016

This application has PRO of 62418775 11/07/2016

This application has PRO of 62418764 11/07/2016

This application has PRO of 62418780 11/07/2016

This application has PRO of 62418510 11/07/2016

This application has PRO of 62418696 11/07/2016

This application has PRO of 62418759 11/07/2016

This application has PRO of 62418773 11/07/2016

This application has PRO of 62418730 11/07/2016

This application has PRO of 62418768 11/07/2016

This application has PRO of 62418724 11/07/2016

This application has PRO of 62418717 11/07/2016

This application has PRO of 62418561 11/07/2016

This application has PRO of 62418693 11/07/2016

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

11/21/2017

**** SMALL ENTITY ****

STATE OR COUNTRY

UNITED STATES

ADDRESS

SETTER ROCHE LLP
1860 Blake Street
Suite 100
Denver, CO 80202
UNITED STATES

FILING FEE RECEIVED

$2,070

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S213	1	15/804,772	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 11:08
S214	1	S213 and (method)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 11:08
S215	5	"20150052167"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 11:12
S216	2	S215 and ((policy or policies) same (bit or bpi or density))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 11:15
S217	6	"20020036852"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 11:15
S218	0	S217 and ((policy or policies) same (bit or bpi or density))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 11:18
S219	2	S217 and (bit or bpi or density)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 11:20
S220	2	"7581061".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 11:29

S221	2	S220 and (polic$4 or method or density)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 11:29
S223	4	"5515317".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 11:33
S224	1	S223 and (polic$4 or method or density)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 11:33
S225	1350	((jack or john) and lane).xp.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 11:34
S226	4	S225 and ((stor$5 or writ$4) with (polic$4) with (host or server or cpu)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 11:35
S227	2	S215 and ((policy or policies) same (host or server or cpu))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 11:49
S228	2	S215 and ((policy or policies) same (host or server or cpu or client))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 12:07
S229	2	S215 and ((policy or policies or criteria) same (host or server or cpu or client))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 12:11
S230	1	S217 and ((policy or policies or criteria or metadata or meta adj3 data or bpi or table))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 12:15
S231	1	S213 and (writ$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 12:23

S232	1	S213 and (writ$4 same (polic$4 or method))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 12:24
S233	1	S213 and (writ$4 with method)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 12:30
S234	2	S215 and (policy or policies or criteria)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 12:36
S235	0	S217 and (policy or policies or criteria)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 12:42
S236	0	S217 and (parameter)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 12:42
S237	6342	(reg$6 and bragdon).xp. or (glen$3 and gossage).xp. or (kevin and verbrugge).xp. or (gary and portka).xp. or (brian and peugh).xp.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 12:53
S238	19	S237 and ((stor$5 or writ$4) with (polic$4) with (host or server or cpu)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 12:53
S239	50	S237 and ((stor$5 or writ$4) with (polic$4 or criteria or parameter) with (host or server or cpu)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 12:54
S240	6	S225 and ((stor$5 or writ$4) with (polic$4 or criteria or parameter) with (host or server or cpu)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 12:54
S241	1	S217 and ((BPI or bits) same (content or data or request$4))	US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	2020/05/01 13:08

			JPO; DERWENT; IBM_TDB			
S242	1	S225 and (writ$3 same (policy or policies or criteria or rule) same (content or data or request$4) same type).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/01 13:13
S243	1	15/993719	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 17:31
S244	1	15/453949	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 17:33
S245	8	"20160313943" or "20110107042" or "8959284".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 17:43
S246	4	S245 and (polic$4 or rule or criteria or parameter)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 17:43
S247	4	"9619429".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 17:49
S248	1	S247 and (polic$4 or rule or criteria)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 17:50
S249	1	15/804,772	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 17:56
S250	1	S249 and type	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 17:57

S251	0	S247 and (densit$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 18:00
S252	3	"20160313943"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 23:02
S253	2	S252 and (writ$5 same (polic$4 or rule or criteria or parameter))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 23:03
S254	0	S252 and (polic$4 or rule)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 23:03
S255	6342	(reg$6 and bragdon).xp. or (glen$3 and gossage).xp. or (kevin and verbrugge).xp. or (gary and portka).xp. or (brian and peugh).xp.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 23:07
S256	1350	((jack or john) and lane).xp.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 23:07
S257	7692	S255 or S256	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 23:07
S258	10	S256 and (writ$5 same (policy or rule)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 23:08
S259	78	S257 and (writ$5 same (policy or rule)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 23:36
S260	4	"9619429".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	2020/05/03 23:41

			JPO; DERWENT; IBM_TDB			
S261	1	S260 and ((writ$5 or record$4 or access$4) same (type or content))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 23:41
S262	1	S260 and ((polic$4 or rule or criteria or parameter) same (type or content or data))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/05/03 23:42

5/4/2020 7:45:22 AM
C:\Users\jlane\Documents\EAST\Workspaces\15896879.wsp

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

70440 7590 05/11/2020
SETTER ROCHE LLP
1860 Blake Street
Suite 100
Denver, CO 80202

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

Karen Dainty	(Typed or printed name)
/Karen Dainty/	(Signature)
August 11, 2020	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/804,772	11/06/2017	Joshua Johnson	980.0023	2463

TITLE OF INVENTION: DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0.00	$0.00	$500	08/11/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
LANE, JOHN A	2139	711-156000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Gaea LLC

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Niwot, CO

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ☒ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required) ❑ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

☒ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Stephen Roche/ Date August 11, 2020

Typed or printed name Stephen Roche Registration No. 52,176

PTOL-85 Part B (08-18) Approved for use through 01/31/2020 OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Electronic Patent Application Fee Transmittal

Application Number:	15804772
Filing Date:	06-Nov-2017
Title of Invention:	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR
First Named Inventor/Applicant Name:	Joshua Johnson
Filer:	Stephen S. Roche/Karen Dainty
Attorney Docket Number:	980.0023

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	500	500

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**500**

Electronic Acknowledgement Receipt	
EFS ID:	40250512
Application Number:	15804772
International Application Number:	
Confirmation Number:	2463
Title of Invention:	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR
First Named Inventor/Applicant Name:	Joshua Johnson
Customer Number:	70440
Filer:	Stephen S. Roche/Karen Dainty
Filer Authorized By:	Stephen S. Roche
Attorney Docket Number:	980.0023
Receipt Date:	11-AUG-2020
Filing Date:	06-NOV-2017
Time Stamp:	13:43:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$500
RAM confirmation Number	E20208AD46043235
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	2020-08-11-980-0023-85b-Issue-Fee-Transmittal.pdf	94523 11c589b8e35bef20ddf69c169d8f2e31ac0bf82a	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30585 9c83ac0ee6663e04ec762346bdaafc57304461c4	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	125108		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/804,772	09/15/2020	10776023	980.0023	2463

70440 7590 08/26/2020

SETTER ROCHE LLP
1860 Blake Street
Suite 100
Denver, CO 80202

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Joshua Johnson, Frederick, CO;
Gaea LLC, Niwot, CO;
Curt Bruner, Niwot, CO;
Jeffrey Reh, Longmont, CO;
Christopher Squires, Boulder, CO;
Brian Wilson, Zumbro Falls, MN;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

IR103 (Rev. 10/09)

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16990433
	Filing Date	2020-08-11
	First Named Inventor	Joshua Johnson
	Art Unit	2827
	Examiner Name	
	Attorney Docket Number	980.0023c1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5596458	A	1997-01-21	EMO, et al.	
	2	6195218	B1	2001-02-27	GUTTMANN, et al.	
	3	8151077	B1	2012-04-03	BAUER, et al.	
	4	9280987	B1	2016-03-08	BAO, et al.	
	5	9619429	B1	2017-04-11	WANG, et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020036852	A1	2002-03-28	LEOW, et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16990433
	Filing Date	2020-08-11
	First Named Inventor	Joshua Johnson
	Art Unit	2827
	Examiner Name	
	Attorney Docket Number	980.0023c1

	2	20040174627	A1	2004-09-09	KIM, et al.	
	3	20060061356	A1	2006-03-23	MAKIFUCHI, et al.	
	4	20100218177	A1	2010-08-26	MIURA	
	5	20140172930	A1	2014-06-19	MOLARO, et al.	
	6	20150052167	A1	2015-02-19	OLSTER, et al.	
	7	20160313943	A1	2016-10-27	HASHIMOTO, et al.	
	8	20180121136		2018-05-03	ISHIYAMA	
	9	20180260154	A1	2018-09-13	DRONAMRAJU, et al.	
	10	20180349035	A1	2018-12-06	ELLIS, et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

EFS Web 2.1.18

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16990433
	Filing Date	2020-08-11
	First Named Inventor	Joshua Johnson
	Art Unit	2827
	Examiner Name	
	Attorney Docket Number	980.0023c1

	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16990433
	Filing Date	2020-08-11
	First Named Inventor	Joshua Johnson
	Art Unit	2827
	Examiner Name	
	Attorney Docket Number	980.0023c1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

✓ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Stephen S. Roche/	Date (YYYY-MM-DD)	2020-11-10
Name/Print	Stephen S. Roche	Registration Number	52176

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt	
EFS ID:	41085949
Application Number:	15804772
International Application Number:	
Confirmation Number:	2463
Title of Invention:	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR
First Named Inventor/Applicant Name:	Joshua Johnson
Customer Number:	70440
Filer:	Stephen S. Roche/Melissa Eichten
Filer Authorized By:	Stephen S. Roche
Attorney Docket Number:	980.0023
Receipt Date:	10-NOV-2020
Filing Date:	06-NOV-2017
Time Stamp:	15:42:52
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	2020-11-10_980-0023c1_IDS.pdf	1035421 e0994826e5dd8e74f2c25974def70a8278c2c6bc	no	5

Warnings:

Information:	
Total Files Size (in bytes):	1035421

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Joshua Johnson et al.	Confirmation No.: 2463
Application No.: 15/804,772	Art Unit: 2139
Filed: 11/06/2017	Examiner: Lane, John A.

For: DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR

Commissioner for Patents
Office of Data Management Attention: Certificates of Correction Branch
P.O. Box 1450
Alexandria, VA 22313-1450

REQUEST FOR CERTIFICATE OF CORRECTION UNDER 37 C.F.R. § 1.322

The Patentee hereby requests issuance of a Certificate of Correction to correct mistakes in U.S. Patent No. 10,776,023 which were incurred through the fault of the Patent Office. Form SB/44 is submitted herewith which lists the corrections to be made.

It is respectfully requested that a Certificate of Correction be issued to correct the errors in the Letters Patent.

No fees are believed due in connection with this submission. Should the Office determine that fees are necessary, however, the Office is hereby requested to contact the undersigned to arrange for payment of the applicable fees.

Respectfully submitted,

/Stephen S. Roche/
SIGNATURE OF PRACTITIONER
Stephen S. Roche, Reg. No. 52,176
Setter Roche Smith & Shellenberger LLP
Telephone: (720) 562-2280
E-mail: steve@setterroche.com

Correspondence address:

CUSTOMER NO. 70440
Setter Roche LLP
1860 Blake Street, Suite 100
Denver, CO 80202

PTO/SB/44 (09-07)
Approved for use through 03/31/2023. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 10,776,023

APPLICATION NO.: 15/804,772

ISSUE DATE : September 15, 2020

INVENTOR(S) : Joshua Johnson et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 36, Claim 26, line 22, delete "specified"

Column 36, Claim 32, line 55, delete"density"

MAILING ADDRESS OF SENDER (Please do not use Customer Number below):
Setter Roche Smith & Shellenberger LLP
1860 Blake Street, Suite 100
Denver, CO 80202

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt	
EFS ID:	43788874
Application Number:	15804772
International Application Number:	
Confirmation Number:	2463
Title of Invention:	DATA STORAGE DEVICE WITH CONFIGURABLE POLICY-BASED STORAGE DEVICE BEHAVIOR
First Named Inventor/Applicant Name:	Joshua Johnson
Customer Number:	70440
Filer:	Stephen S. Roche/Melissa Eichten
Filer Authorized By:	Stephen S. Roche
Attorney Docket Number:	980.0023
Receipt Date:	16-SEP-2021
Filing Date:	06-NOV-2017
Time Stamp:	17:58:08
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Certificate of Correction	2021-09-16_980-0023_CoCRequest.pdf	110945 f85944ac1280c08dda1823d23a49425b291677a5	no	1

Warnings:

Information:					
2	Request for Certificate of Correction	2021-09-16_980-0023_CoC.pdf	174831 d9c593d18b5000b2d3e0a1e973f464a77c71eb74	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	285776	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 10,776,023 B2
APPLICATION NO. : 15/804772
DATED : September 15, 2020
INVENTOR(S) : Joshua Johnson et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Claims

Column 36, Claim 26, Line 22, delete “specified”

Column 36, Claim 32, Line 55, delete “density”

Signed and Sealed this
Nineteenth Day of October, 2021

Drew Hirshfeld
Performing the Functions and Duties of the
Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Northern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
4:26-cv-00348-P	3/26/2026	Northern District of Texas

PLAINTIFF	DEFENDANT
GAEA, LLC	Meta Platforms, Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	10,776,023	9/15/2020	GAEA, LLC
2	11,327,669	5/10/2022	GAEA, LLC
3	11,907,553	2/20/2024	GAEA, LLC
4	12,265,715	4/1/2025	GAEA, LLC
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
Karen Mitchell	s/Wendy Camargo	03/26/2026

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

Print Save As... Reset

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:26-cv-264	3/23/2026	Eastern District of Texas

PLAINTIFF	DEFENDANT
Gaea, LLC	Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	10,776,023	9/15/2020	Gaea, LLC
2	11,327,669	5/10/2022	Gaea, LLC
3	11,907,553	2/20/2024	Gaea, LLC
4	12,265,715	4/1/2025	Gaea, LLC
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading		
	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1			
2			
3			
4			
5			

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Print Save As... Reset