Tutorial on Disk Drive Data Sanitization

Gordon Hughes, UCSD CMRR (gfhughes@ucsd.edu)
Tom Coughlin, Coughlin Associates (tom@tomcoughlin.com)
April 26, 2007

Summary

Summary: user data is left on disk drives removed from computers and storage systems, creating a data security vulnerability that many users are unaware of. Recent Federal and state laws requiring secure erasure of user data expose companies to fines of $250,000 and responsible parties to imprisonment for 10 years.

Complete eradication of user data off drives can be accomplished by running data Secure Erasure utilities such as the freeware "HDDerase" downloadable here. It executes the Federally-approved (NIST 800-88) Secure Erase command in the ATA ANSI standard, which is implemented in all recent ATA drives greater than 15-20 GB. A similar command in the SCSI ANSI standard is optional and not yet implemented in drives tested. Normal Secure Erase takes 30-60 minutes to complete. Some ATA drives also implement the standard Enhanced Secure Erase command that takes only milliseconds to complete.

Table of Contents

Introduction

Data security has risen to be one of the highest concerns of computer professionals. Tighter legal requirements now exist for protecting user data from unauthorized use, and for both preserving and erasing (sanitizing) records to meet legal compliance requirements. This Tutorial document will address concerns and developments in the sanitization and protection of user data.

Overall data storage security entails protection at different levels and locations:

- Data at rest - drive data erasure
- Secure erase of all data blocks on disk drives
- Single file erasure
- Drive physical or magnetic destruction
- Data in motion - data encrypted during transport
- Protection of data and crypto keys during transport
- Transparency to users (automatic encryption)
- Drive internal encryption (data encrypted by storage device)
- Access level dependent upon key or password used to decrypt data
- Drive data sanitization
- Secure erasure of user data for drive disposal or reuse

The following table (**Table 1**) outlines comparative times to execute various approaches for data sanitization (erasure) as well as level of data sanitization security.

Table 1. Comparison of Various Data Sanitization Approaches

Type of Erasure	Average Time (100 GB)	Security	Comments
Normal File Deletion	Minutes	Very Poor	Deletes only file pointers, not actual data
DoD 5220 Block Erase	Up to several days	Medium	Need 3 writes + verify, cannot erase reassigned blocks
NIST 800-88 Secure Erase	1/2-2 hours	High	In-drive overwrite of all user accessible records
Enhanced Secure Erase	Seconds	Very high	Change in-drive encryption key

Data Loss is Rampant

The cardinal rule of computer storage design has been to protect user data at all costs. Disk drives supply primary mass storage for computer systems, designed to prevent accidental erasure of data. Techniques such as “recycle” folders and “Unerase” commands are common ways that operating systems try to prevent accidental sanitization of user data. Deletion of file pointers is standard to speeds data writing, because actual overwriting of file data is far slower. Drives use elaborate error detection and correction techniques to make sure that they don’t return incorrect user data.

All this means that true computer data erasure is an abnormal event. These measures taken to protect and speed access to user data can make that data vulnerable to recovery by unauthorized persons.

Following are some statistics on computer loss and theft[1]:

- Statistics show that 1 of every 14 laptops is stolen, and over 2,000 computers are stolen every day in this country. ((Information Week)
- A computer is stolen every 43 seconds
- Over 98% of stolen laptops are never recovered. (FBI)
- A survey of 769 corporate IT managers revealed that 64% had experienced laptop theft. (Tech Republic)

When a computer is lost or disposed of, active and discarded data typically remains stored on its hard disk drive. Even if users "delete" all their files, they can be recovered from "recycling" folders or by special utility programs such as Norton Unerase.

If data is not erased beyond recovery, data on disk drives that leave the physical control of owners can and often does fall into the hands of others. Data can be recovered with little effort, from discarded, warranty repaired, or resold disk drives. Many reports have been written on data recovered from discarded disk drives.[2,3] Each year hundreds of thousands of hard disk drives are retired. Some of these hard disk drives find their way back into the market and their data can be recovered unless it is erased securely.

There is an urgent need for a capability to reliably erase data and prevent access to data from retired computer hard disk drives for security and privacy reasons. Data sanitization needs arise differently depending upon the user application. Even consumer drives could use data sanitization to protect user privacy or for DRM purposes.

Data Sanitization Legal Requirements

While most people are aware of legal compliance regulations requiring long term retention of data, the same regulations also specify the need for protection of data for privacy and other reasons. Many of them also specify conditions and requirements for the sanitization of data. Strict local, state and Federal legislation protecting investors, consumers and the environment specify that organizations must be extremely careful when disposing of IT equipment that has outlived its usefulness.

There are several laws and regulations that relate to data retention and data sanitization on data storage devices like hard disk drives. Some US requirements are listed below:

Health Information Portability and Accountability Act (HIPAA)
Personal Information Protection and Electronic Documents Act (PIPEDA)
Gramm-Leach-Bliley Act (GLBA)
California Senate Bill 1386

---

[1] The U.K. Times Information Security Supplement, 27March2007
[2]T. Coughlin, Rumors of My Erasure Are Premature, Coughlin Associates, http://www.tomcoughlin.com/Techpapers/Rumors of my erasure,061803.pdf (2003)
[3] J. Garfinkel, A. Shelat, A Study of Disk Sanitization Practices, IEEE Security and Privacy, Jan.-Feb. 2003.

Sarbanes-Oxley Act (SBA)
SEC Rule 17a

The Federal Health Insurance Portability and Accountability Act (HIPAA) sets goals on keeping personal information secure in the health industry. If a company is found in non-compliance of HIPAA data security practices, the company may be exposed to a maximum fine of $250,000 and the responsible party can face a maximum of 10 years imprisonment.

There are several approved methods for data sanitization that satisfy these legal requirements or meet even more stringent corporate or government secrecy requirements. Many of them physically destroy disk drives to prevent any future use. Another data security measure is encryption of user data.. Secure data encryption from creation to destruction is approved by some regulatory compliance legislation to protect sensitive information. Federal document FIPS 142-2 sets cryptographic security requirements.

According to newly released data sanitization document NIST 800-88[4], acceptable methods include executing the in-drive Secure Erase command, and degaussing. These data sanitization methods erase data even against recovery even using exotic laboratory techniques. Such sophisticated techniques are threats to data privacy using specific drive technology knowledge with specialized scientific and engineering instrumentation, to attempt data recovery outside of the normal drive operating environment. They involve signal processing equipment and personnel with knowledge of specific drive engineering details, and can even involve removing the components from the hard disk drive for spin stand testing.

Secure erase is recognized by NIST 800-88 as an effective and secure way to meet legal data sanitization requirements.

[4] NIST Special Publication 800-88, **Guidelines for Media Sanitization**, August 2006

Legal Penalties for Failure to Sanitize Data

The following table[5] summarizes the fines and jail penalties for violation of the data security laws.

	Gramm-Leach-Bliley	Sarbanes-Oxley	FACTA	HIPAA
	Financial Services Modernization Act	Public Company Accounting Reform & Investor Protection Act	Fair and Accurate Credit Transaction Act	Health Insurance Portability & Accountability Act
Directors and Officers	$10,000	$1,000,000		$50,000 to $250,000
Institution	$100,000			
Years in Prison	5 to 12 years	20 years		1 to 10 years
FDIC Insurance	Terminated			
Impact on Operations	Cease and Desist			
Individual	$1,000,000		Civil Action	$25,000
Institution	1% of assets			

Data Sanitization in Hard Disk Drives

Four basic sanitization security levels can be defined: weak erase (deleting files), block erase (overwrite by external software), normal secure erase (current drives), and enhanced secure erase (see below). The CMRR at UCSD has established test protocols for software secure erase[6]. This downloadable freeware utility can be used to securely erase ATA drives. A commercial secure erase device is available, which can also erase SCSI and other drives[5].

Block erase is most commonly used. While it significantly better than no erase, or file deletion, or drive formatting, it is vulnerable to malware and incomplete erasure of all data blocks. Examples are data blocks reassigned by drives, multiple drive partitions, host protected areas, device configuration overlays, and drive faults.

Normal secure erase is approved by NIST 800-88 for legal sanitization of user data up to Confidential. Enhanced secure erase should qualify for higher levels, but it's not currently covered in 800-88 (no method to do it was known before encrypting disk drives came on the market). Enhanced secure erase now exists in Seagate drives, and these drives are under evaluation by the CMRR.

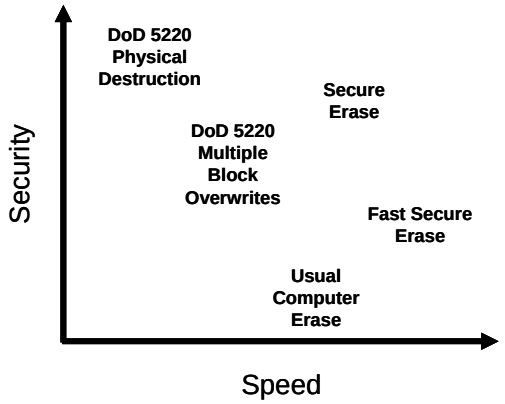
These four erasure protocols exist because users make tradeoffs between sanitization security level and the time required. A high security protocol that requires special software

[5] From Ensconce Data Technology, Inc, www.deadondemand.com

[6] G. Hughes, CMRR Secure Erase Protocols, http:/cmrr.ucsd.edu/Hughes/

and days to accomplish will be avoided by most users, making it little used and of limited practical value. For example, the old data overwrite document DoD 5220 calls for multiple block overwrites of Confidential data, which can take more than a day to complete in today's large capacity drives. So users make tradeoffs between the time required to erase data and the risk that the next drive user may know and use recovery techniques which can access weakly erased data. **Figure 1** shows tradeoffs in security level vs. speed of erasure for various erasure options.

Figure 1. Security vs. Speed of Completion of Various Modes to Erase Data on Hard Disk Drives



For all but top-secret information, users will usually turn to erasure methods that take minutes rather than hours or days. They will select a method that gives them an acceptable level of security in a reasonable time window.

Physical Drive Destruction

To positively prevent data from recovery, disks can be removed from disk drives and broken up, or even ground to microscopic pieces. (Actually, simple disk bending is highly effective, particularly in emergency situations.) Obsolete government document DoD 5220.22M required physical destruction of the storage medium (the magnetic disks) for data classified higher than Secret. Even such physical destruction is not absolute if any remaining disk pieces are larger than a single 512-byte record block in size, about 1/125" in today's drives. As linear and track densities increases, the maximum allowable size of disk fragments become ever smaller Destroyed disk fragments of this size have been studied by the CMRR[2]. Magnetic microscopy is used to image stored recorded media bits.

Some storage products are more easily destroyed than hard disk drives, such as magnetic disk data cartridges, tape cartridges, secure USB drives, and optical media.

Disk Drive Degaussing

Degaussers are used to erase magnetic data on disk drives. They create high intensity magnetic fields that erase all magnetic recordings in a hard disk drive, including the sector header information on drive data tracks (information necessary for drive head positioning and data error recovery). In addition, track and disk motor magnets are often also erased

by degausser magnetic fields. Like physical destruction, when a disk drive has been successfully degaussed it is no longer useable.

The CMRR evaluates commercial degaussers for data sanitization.

Drive designers continually increase the linear density of magnetic recording to create higher data storage capacity per disk. This raises the disk magnetic coercivity, the field required to write bits on the magnetic media. As the magnetic coercivity increases, the fields required to erase the data on recorded disks increases. Thus an older degausser may not fully erase data on a newer hard disk drive. New perpendicular recording drives may not be erasable by present degaussers designed for past longitudinal recording drives.

Future generations of magnetic recording media may use very high magnetic coercivity disks to achieve areal densities greater than 500 gigabits per square inch. These drives may have technology using laser light in the magnetic write element of the disk drive, to raise the temperature of a spot on the magnetic medium in order to lower the magnetic coercivity to the point where the write element can record a bit on the very high coercivity magnetic media. For disk drives using this Heat or Thermally Assisted Magnetic Recording (HAMR/TAMR) technology the degausser field required to erase the disk drive at room temperatures may be impossible or impractical to achieve. In this case the drive may have to be physically destroyed.

"Hybrid drives" are now being introduced for notebook or laptop computers that have flash memory write cache on hard disk drive circuit boards. Magnetic degaussing would not affect any resident data on such semiconductor memory chips. Data on these non-volatile semiconductors would have to be sanitized using some other technique. For all these reasons degaussing of all the data on hard disk drives will become increasingly impractical.

Nondestructive Data Erasure

Sanitization of data on a hard disk drive is not a simple task. Deleting a file merely removes its name from the directory structure's special disk sectors. The user data remains in the drive data storage sectors where it can be retrieved until the sectors are overwritten by new data. Reformatting a hard disk drive clears the file directory and severs the links between storage sectors, but the user data remains and can be recovered until the sectors are overwritten. Software utilities that overwrite individual data files or an entire hard drive are susceptible to error or malicious virus attack, and require constant modifications to accommodate new hardware and evolving computer operating systems.

It is difficult for external software to reliably sanitize user data stored on a hard disk drive. Many commercial software packages are available using variations of DoD 5220, making as many as 35 overwrite passes. But in today's drives, multiple overwrites are no more effective than a single overwrite. And even the minimum four passes DoD 5220 requires can take more than a day today's high capacity hard disk drive. In busy IT facilities, such time requirements tempt IT personnel to take short cuts.

DoD 5220 overwriting has other vulnerabilities, such as erasing only to a drive's Maximum Address, which can be set lower than its native capacity; not erasing reallocated (error) blocks; or miss extra partitions. External overwrites cannot access the reallocated sectors on most drives, and any data once recorded is left on these sectors. These sectors could conceivably be recovered and decoded by exotic forensics. While enterprise-class drives and drive systems (SCSI/FC/SAS/iSCSI) allow software commands to test all the user blocks for write and read ability, mass market drives (PATA/SATA) cannot read, write, or detect reassigned blocks since they have no logical block address for a user to access.

The Secure Erase (SE) command was added to the open ANSI standards that control disk drives, at the request of CMRR at UCSD. The ANSI T13.org committee oversees the ATA interface specification (also called IDE) and the ANSI T10.org committee governs the SCSI interface specification.

Secure erase is built into the hard disk drive itself and thus is far less susceptible to malicious software attack than external software utilities.

The SE command is implemented in all ATA interface drives manufactured after 2001 (drives with capacities greater than 15 GB), according to testing by CMRR. A standardized internal secure erase command also exists for SCSI drives, but is optional and not currently implemented in SCSI drives tested.

Secure erase is a positive easy-to-use data destroy command, amounting to "electronic data shredding." Executing the command causes a drive to internally completely erase all possible user data record areas by overwriting, including g-list records that could contain readable data in reallocated disk sectors (sectors that the drive no longer uses because they have hard errors).

SE is a simple addition to the existing "format drive" command present in computer operating systems and storage system software, and adds no cost to hard disk drives. Because the Secure Erase command is carried out within hard disk drives, no additional software is required either.

Secure erase does a single on-track erasure of the data on the disk drive, after technical testing at CMRR showed that multiple on-track overwrite passes gave no additional erasure.

Secure erase has been approved by the U.S. National Institute for Standards and Technology (NIST), Computer Security Resource Center[7]. NIST document 800-88 approves SE at a higher security level than external software block overwrite utilities like as Norton Government Wipe, and it meets the legal requirements of HIPAA, PIPEDA, GLBA, and Sarbanes-Oxley.

Software overwrite utilities running in protected execution environments (e.g. running inside file system hardware like RAID arrays or inside secure computers) could be verified

[7] *NIST Computer Security Resource Center, Special Publication 800-88: Guidelines for Media Sanitization, August 2006*

secure under NIST 800-88. For the most sensitive data, the government requires physical destruction of drives.

Drive manufacturers today are pursuing higher security secure erase (including secret data), via in-drive data encryption (see below)

Enhanced Secure Erase via Data Encryption

Recently, 2.5-inch hard disk drives for laptop computers have been introduced which encrypt user data before recording—internal full data encryption[8,9] Such drives provide protection of data should the laptop or drive be lost or stolen, and even provide high protection from forensic data recovery. These drives also offer a new, instantaneous way to sanitize data on a hard disk drive – by securely discarding the encryption key.

Why encrypt data at rest in drives instead of in computers, such as by user application programs that access the data? Because computer level data encryption defeats the purpose of many important data management functions, such as incremental backup, continuous data protection, data compression, de-duplication, virtualization, archiving, content addressable storage, advanced routing, and thin provisioning[10]. Defeating these operations causes significant penalties to enterprise storage companies in data access speed and cost,. Each of these operations exploits the structure of user data, and needs to inspect the data. They become inefficient or nonfunctional if the data has been randomized by encryption. For example, data compression ratios may fall from more than 2:1 to less than 1:1, because compressing random data can expand it instead. De-duplication won't find identical data sets if they are encrypted by different users.

Computer level encryption could be employed with in-drive encryption as well, the double encryption does no harm and provides additional security. In-drive encryption can relieve encryption key management problems inherent in removable storage, like laptop disk drives or tape backups. In fact, hardware-based tape drive encryption may become widespread[11] by 2007 due to widely publicized losses of backup tape reels containing identity theft data on millions of people.

Full Disk Encryption (FDE) Enhanced Secure Erase," ("FDE-SE"), securely changes the internal drive encryption key, to render encrypted user data on disk indecipherable. This is enabled via the Enhanced SE command in the present ATA ANSI specs.

FDE SE encryption needs to be tested for protection against advanced forensic analysis. The results will determine the erasure security data level - Confidential, Secret, Top Secret, or higher. The US Commerce Department prohibits most 256-bit and higher encryption

[8] *G. Hughes, "Wise Drives", IEEE Spectrum, August 2002*

[9] *e.g. Seagate Momentus 5200 drives*

[10] *Storage* magazine, October 2006

[11] *Storage* magazine, December 2006

export overseas, limiting FDE E-SE to AES-128-bit encryption (since disk drives are a global industry).

AES-256 bit encryption in FDE drives could allow FDE SE at a somewhat higher security level. Note that a FDE E-SE operation amounts to double AES-128, because the data encrypted by the discarded key is decrypted by the new key, and AES is a symmetric encryption scheme. It would appear that a brute force attack on double AES-128 requires the same computational effort as single AES-256.

For paranoid-level security, the cypt-text in an FDE disk drive could be eliminated by a Normal OW SE done after the FDE E-SE.

An open industry standard for FDE is being worked on by the Trusted Computing Group overall specification (the Storage Working Group in trustedcomputinggroup.org). Drive members of the TCG include Seagate, HGST, Fujitsu and WD. SE via encryption may be included, consistent with the ANSI open standards for ATA drives (t13.org)

CMRR has begun testing FDE-SE drives. They take less than 15 milliseconds to complete an Enhanced SE; while a 750 GB ATA-interface HDD can take over an hour to erase using conventional Secure Erase (or many hours using external overwrite software).

Computer Forensics Data Recovery

Forensics recovery uses exotic data recovery techniques by experts with advanced equipment. Its normal purpose is to recover data from failed hard disk drives, and for legal discovery. Forensic companies can successfully recover unerased but protected data in a disk drive using electronic instrumentation. However, the secure erase commands discussed above erase all user data on the disk drive beyond physical disk drive forensic recovery. Drives old enough to permit such attack are too old to have the Secure Erase built-in command.

Paranoid-level recovery concerns based on hypothetical schemes are sometimes proposed by people not experienced in actual magnetic disk recording, claiming the possibility of data recovery even after physical destruction. One computer forensics data recovery company claims to be able to read user data from a magnetic image of recorded bits on a disc, without using normal drive electronics[12]. Reading back tracks from a disk taken out of a drive and tested on a spin stand was practical decades ago, but no longer with today's microinch-size tracks.

The time required by exotic technologies is itself a barrier to data recovery and increases data security. Also, accessing data from magnetic images requires overcoming almost a dozen successive magnetic recording technology hurdles. Even if these hurdles were overcome, about an hour would be required to recover a single user data block out of millions on a disk. Recovering substantial amounts of data in less than months requires that the disk be intact and undamaged, so that heads can be flown over it to obtain data playback

[12] www.actionfront.com

signals; then overcoming these technology hurdles. Simply bending a disk makes this nearly impossible, so physical damaging drives to warp their disks makes recovery practically impossible.

Other "experts" claim that limited information can be recovered from unerased track edges. But this has been shown to be false by tests at CMRR13. Such recovery also presumes detailed technical knowledge of the drive's magnetic recording design. Charles Sobey at ChannelScience.com wrote an illuminating article on drive-independent data recovery, showing how difficult these hurdles are.[14]

Secure Erasure Implementation and Certification

CMRR has studied secure erase for the Federal Government for many years, and its research[4] demonstrates three distinct protocols for user data deletion:

Weak deletion by users deleting files in public operating systems such as Windows or Linux ("usual computer erase' in Figure 1). This deletes only file directory entries, not the user data itself.

Block overwrite utilities overwrite all user accessible blocks (at the time of overwriting). It gives a higher level of deletion confidence than file erase, and these utilities claim to meet Federal Government requirements in DoD 5220. Today's hard drive technology has obsoleted this document, and NIST 800-88 should be used instead.

Disk drive Secure Erase is a drive command defined in the ANSI ATA and SCSI disk drive interface specifications, which runs inside drive hardware. It completes in about 1/8 the time of 5220 block erasure.

CMRR provides verification and certification of data erasure effectiveness for the government as well as drive companies and may be the most experienced organization in the world on disk drive data erasure. It is one of the few public organizations with detailed knowledge of drive internal technology. CMRR requested the SE command now in the T13.org ATA specification. For Normal Erase mode the spec requires that the SECURITY ERASE UNIT command write binary zeroes to all user accessible data areas. Note that ATA reassigned blocks are not user accessible because they have no user address. CMRR verification testing shows that the erasure security is at the Purge level of NIST 800-88, because drives having the command also randomize user bits before storing on magnetic media. The erasure verify DoD 5220 requires (which is often forgotten), is via in-drive internal write fault detection hardware, which takes no additional time. This reduced execution time increases user willingness to erase drives. CMRR measured test times were up to days for DOD 5220 but the drive normal Secure Erase can complete in 15-45 minutes.

[13] *T. M. Coughlin and G. F. Hughes, "Secure Erase of Disk Drive Data," IDEMA Insight Magazine, pp. 22-25, Summer 2002*

[14] See white papers at http://www.actionfront.com/ts_whitepaper.aspx

Data Sanitization in the Real World

The security erase command is available to all users, the Federal government, and in commercial drive erasure products[15]. In a typical recent 2006 month there were 622 downloads of the freeware secure erase utility from the CMRR web site (http://cmrr.ucsd.edu/hughes/SecureErase.html). This is significantly higher than the historic past average of 109 downloads per month, arguably caused by increasing interest in Secure Erase. (Downloads in early 2006 averaged in the middle three hundreds per month.)

The Department of the Navy licensed secure erase to erase data from disk drives. Some commercial vendors are also selling products using Secure Erase, such as Esconce Data Technology[15].

About the Authors

UCSD CMRR does certification of secure erase and other data sanitization procedures. Contact Gordon Hughes of UCSD CMRR for more information. See http://cmrr.ucsd.edu/hughes

Coughlin Associates provides data storage consulting and market and technology analysis of the data storage industry. Visit www.tomcoughlin.com or call 408-871-8808 for more information.

[15] Digital Shredder, Ensconce Technology, ensconcedata.com

Glossary

ANSI T-10	ANSI standards committee overseeing SCSI interface specification
ANSI T-13	ANSI standards committee that overseas the ATA interface specification
ATA	Advanced Technology Attachment, also known as IDE this interface was developed to connect disk drives in which the drive controller is integrated in the disk drive. This interface is moving from parallel (PATA) to serial (SATA) interfaces
CMRR	Center for Magnetic Recording Research at UCSD provides research on various magnetic recording topics as well as related technology
Delete	A command that moves a file to a recycle folder where it is kept with its links intact until the recycle folder is emptied.
Degauss	To apply a high enough magnetic field to a magnetic recording device to erase all the magnetic data stored on it. See magnetic coercivity.
FDE	Full Disk Encryption is a method to do encryption of the data on a hard disk drive where the encryption and code keys are managed by the internal drive electronics
FDE-SE	Data sanitization performed by throwing away the key for the encrypted data. Without the encryption key decoding the data is difficult
DoD 5220	Actually DoD Directive 5220.22M, “National Industrial Security Program Operating Manual," January 1995 specifies the use of 3 overwrites to erase data on a hard disk drive
Encryption	To encode data. Hard disk drives are often encrypted to protect the data they contain from unauthorized access
GLBA	Gramm-Leach-Bliley Act
HAMR	Heat Assisted Magnetic Recording (also known as Thermally Assisted Magnetic Recording, TAMR)

HIPAA	Health Information Portability and Accountability Act
Longitudinal Recording	Magnetic recording in which the magnetized regions of the recording medium have their magnetization pointing in the plane of the medium
Magnetic Coercivity	A technical measure of the external magnetic field necessary to cause the magnetic state of a recording medium to half erase. Completely erasing a magnetic recording requires applying a field of about twice the magnetic coercivity. In 1980, disk media coercivity was about 300 Oersted; today it can exceed 4000 and an effective degausser must be thirteen times as powerful.
NIST SP800-88	National Institute of Standards and Technology Guidelines for Media Sanitization, released August 2006
PATA	See ATA
Perpendicular Recording	Magnetic recording in which the magnetized regions of recording medium have their magnetization pointing out of the plane of the medium
PIPEDA	Personal Information Protection and Electronic Documents Act
Recycle Folder	A computer location where “deleted” files are kept until the recycle folder is emptied
SATA	See ATA
SBA	Sarbanes-Oxley Act
SE	Secure Erase is data sanitization by overwriting the data on the hard disk drive. This usually included overwriting the data left in the reallocated defect sectors. Enhanced SE is done by changing or eliminating a disk drive encryption key.
SCSI	Small Computer System Interface, an interface originally used by Apple and UNIX computers to connect hard disk drives to computers. Also widely used for storage arrays. SCSI commands are used in Fibre Channel disk drives for array

	applications. Serial Attached SCSI or SAS is displacing the older parallel SCSI interfaces.
Secure Erase (SE):	A technique for sanitizing all the data stored on a hard disk drive using internal commands. The data erased can include reallocated defect sectors
TAMR	See Heat Assisted Magnetic Recording (HAMR)
TCG	Trusted Computing Group. This group works on data security standards and is in charge of the FDE specification
Unerase	To recover data “deleted” from a drive, possible because only file pointers to drive data are normally erased, not actual user data