

Data Sanitization

Risks and Standards

Presented by:
Michael Harstrick
Chief Global Development Officer
Garner Products, Inc.
MHarstrick@Garner-Products.com
www.garnerproducts.com



Shredding is an ANALOG solution to a DIGITAL problem.

Modern media is so densely recorded,
shredding is not a secure option for HDDs

Risk

Sanitization Options

Regulatory Environment

Independent Standards



142°



Data Controller- A person who determines the purposes for which and the manner in which any personal data are processed.



Data Processor- Any person (other than an employee of the data controller) who processes the data on behalf of the data.

Regulatory Environment

Best known:

HIPAA/HITECH: Enforced by DHS, OSC and individual state Attorneys General

GLBA: Enforced by FTS, US Treasury Dept., Fed, SEC NCUA and FDIC

FACTA: Enforced by DOJ

GDPR: Enforced by ICO in each EU country

These are what your customers are living with



Strategic intent:

PROTECT CUSTOMERS' PRIVACY

Data Regulations

Regulations common thread:

Pro:

Protect privacy and sanctity of consumer information in all forms

Con:

No clearly defined media sanitization requirements



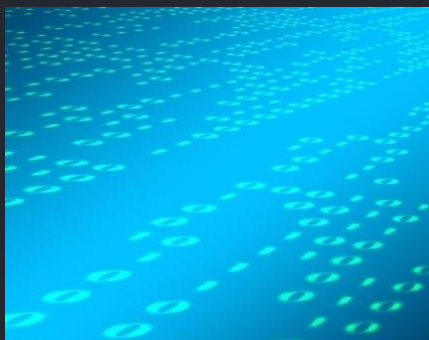
“Reasonable Requirement”

Regulations applicable to private industry for final disposition of personal information require the implementation of a reasonable sanitization process. (GDPR)

What is REASONABLE?



NIST: Sanitization Methods



Clear

- **Overwrite** that replaces target data with non-sensitive data
- Overwriting cannot be used for media that are damaged or not rewriteable, and may not address all areas of the device where sensitive data may be retained

Purge

- **Overwrite, block erase, and cryptographic erase**
- Degaussing renders a legacy magnetic device purged when the strength of the degausser is carefully matched to the media coercivity

Destroy

- **Incinerate, disintegrate, pulverize, melt.**
- Outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely
- The application of destructive techniques may be the only option when the media fails and other clear or purge techniques cannot be effectively applied to the media, or when the verification of clear or purge methods fails



Looking to Regulations

For Answers

There are guidelines available that are not arbitrary—these are a basis for best practices.

- NSA
- IRS 1075
- NIST 800-88 rev 2
- NAID AAA standards
- E2
- ~~– DoD Wipe~~



NSA Standards

Highest Protection Standard In The World.

Governments around the world use as their standard for **TOP SECRET** data destruction



NSA data destruction for TOP SECRET data requires:

- ✓ Shred (2mm particles)
- ✓ Incinerate
- ✓ Degauss with NSA-Listed Degausser

Before you leave the secure area.



UNCLASSIFIED

NSA/CSS Evaluated Products List for Magnetic Degaussers

March 2020

MAGNETIC DEGAUSSERS

VENDOR	DEVICE NAME / MODEL	TAPE: Oe RATING	HDD: Oe RATING	REMARKS
Advanced Design Corp.	MagWiper MW-2B	3000	L-5000, P-5000	
Applied Magnetic Laboratory, Inc.	AML-48G	Not Tested	L-5000, P-5000	Requires disk disassembly plus 1 full-contact pass with rotation
Data Security, Inc.	DD-1T	3000	L-5000, P-5000	
Data Security, Inc.	DD-FT	3000	L-5000, P-5000	
Data Security, Inc.	DDPM-2	3000	L-5000, P-5000	
Data Security, Inc.	LE-1	Not Tested	L-5000, P-5000	2 passes required with 90° rotation
Data Security, Inc.	LE-1	3000	L-5000, P-5000	
Data Security, Inc.	LE-1 w/Caddy Bolt	3000	L-5000, P-5000	
Data Security, Inc.	LE-1C	3000	L-5000, P-5000	
Data Security, Inc.	TE-1	2000	Not Tested	2 passes required with 90° rotation
Garner Products, Inc.	TS-1, TS-1XT Series	3000	L-5000, P-5000	
Intimus International	Intimus 20000	3000	L-5000, P-5000	
Proton Data Security	T-4	3000	L-5000, P-5000	
Proton Data Security	1000	Not Tested	L-750	2 passes required with 90° rotation
Proton Data Security	1100	Not Tested	L-5000, P-5000	Requires disk disassembly plus 1 full-contact pass with rotation
Proton Data Security	T-6	3000	L-5000, P-5000	

<https://www.nsa.gov/resources/everyone/media-destruction/>



GarnerProducts.com

Offered as a public service, please feel free to distribute.

NIST: Regulation Media Sanitization

NIST Special Publication 800
NIST SP 800-88r2

Guidelines for Media Sanitization

Ramaswamy Chandramouli
*Computer Security Division
Information Technology Laboratory*

Eric A. Hibbard
Samsung Semiconductor, Inc.

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-88r2>

September 2025



U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

NIST: Media Sanitization

The risk decision should include the potential consequence of disclosure of information retrievable from the media, the cost of information retrieval and its efficacy, and the cost of sanitization and its efficacy. Additionally, the length of time the data will remain sensitive should also be considered. These values may vary between different environments.

4.3.4. Control of Media

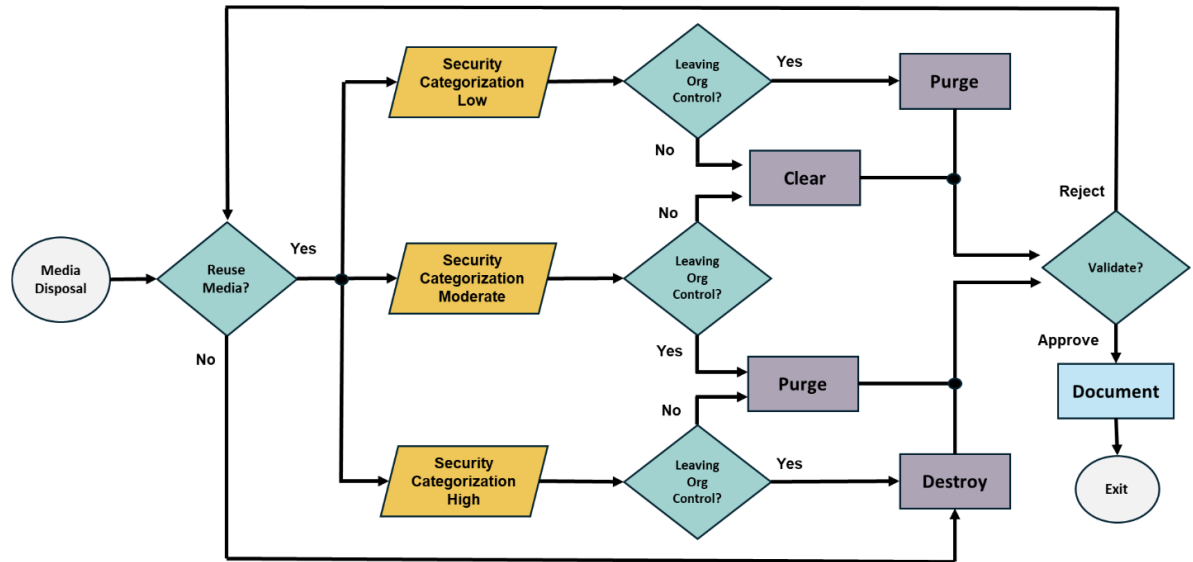
Organizational sanitization decisions are influenced by who has control and access to the media. This aspect must be considered when media leaves organizational control.

Media control can change when an ISM is returned from a leasing agreement, donated, resold to be reused outside of the organization, or sent to a recycling facility. For example:

- ISM under organizational control
 - ISM that are turned over (and securely transported) to a maintenance provider may still be considered to be under organizational control if contractual agreements are in place with the organization and the maintenance provider that specifically provides for the confidentiality of the information.
 - Maintenance being performed on an organization's site, under the organization's supervision, by a maintenance provider is also considered to be under the control of the organization.
- ISM not under organizational control (i.e., external control)
 - ISM that are being exchanged for warranty, cost rebates, or other purposes and will not be returned to the organization are considered to be out of organizational control.

The examples above do not consider relevant legal, regulatory, or statutory requirements associated with certain types of sensitive data, which can treat the loss of organizational control of ISM that have not been sanitized as a data breach.

NIST: Sanitization and Disposition Decision Flow



NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

IEEE 2883

Intent to encourage
re-use
Detailed criteria for
Purge

Must be purchased

METHOD	TECHNIQUE	DATA TYPE
CLEAR	LOGICAL overwrite, block erase	NON-SENSITIVE
PURGE	LOGICAL & PHYSICAL overwrite, block erase, cryptographic erase, degauss	SENSITIVE
DESTRUCT	PHYSICAL Disintegrate, incinerate, melt	SENSITIVE

ISO 21964

Rehash of DIN 66399

Shred only Categories from 1-7 15 yr+ old



Level 1-3

Suitable for **general documents** or internal documents that don't require high security.

Shred in strips



Level 4

Recommended for **confidential data**, like personal information or financial records.

Shred with criss cut



Level 5-7

Used for highly sensitive or **top-secret** data that requires the highest level of protection.

Shred with criss cut
shape 5mm²

ICT Asset Recovery Standard 8.0

ADISA Asset Recovery Standard is a standard for providing data sanitisation services.

ICT Asset Recovery Standard incorporates GDPR compliance. It also helps to define risk management using DIAL analysis, and requires evidence or documentation of sanitisation procedure.



DIAL (Data Impact Assurance Level)

- Data type
- Volume
- Potential threat
- Impact of a data breach



E-Steward/R2

Policies and
Procedures-no data
sanitization standard

NAID AAA

Policies and
procedures-no
data sanitization
standard

ITAD Consequences

You are a data processor.

You want your customer to contractually assure you that the media has been sanitized—before it comes to you.



If you are contracted to destroy media that has not been sanitized:

You must have a sanitization
technique that meets regulatory
guidelines;
You must have a tracking system
that captures every sanitization
by serial number so you can
prove compliance.



CERTIFICATE OF ERASURE & DESTRUCTION



Serial No.: WMAYW0074986
Incident No.: 01
Date/Time: 2019-11-20 18:34:09
Degaussed: 22620 G (PASS)
Destroyed: PD-5: 24 mm SSD: No
User ID: 1123
Witness ID: N/A
JPG File: 20191120-183144_WMAYW0074986.jpg
JPG File 2: 20191120-183358_WMAYW0074986.jpg



Serial No.: WCAVW118892
Incident No.: 01
Date/Time: 2019-11-20 18:37:32
Degaussed: 22590 G (PASS)
Destroyed: PD-5: 24 mm SSD: No
User ID: 1123
Witness ID: N/A
JPG File: 20191120-183717_WCAVW118892.jpg
JPG File 2: 20191120-183717_WCAVW118892.jpg

Serial No.: 6VYH5Z4Z
Incident No.: 01
Date/Time: 2019-11-20 18:40:37
Degaussed: 22380 G (PASS)
Destroyed: PD-5: 24 mm SSD: No
User ID: 1123
Witness ID: N/A
JPG File: 20191120-184037_6VYH5Z4Z.jpg
JPG File 2: 20191120-184037_6VYH5Z4Z.jpg

Serial No.: W629P63
Incident No.: 01
Date/Time: 2019-11-20 18:47:57
Degaussed: 22650 G (PASS)
Destroyed: PD-5: 24 mm SSD: No
User ID: 1123
Witness ID: N/A
JPG File: 20191120-184757_W629P63.jpg
JPG File 2: 20191120-184757_W629P63.jpg



Page: 1 of 2
info@garner-products.com

0 Time + 0 Distance = 0 Risk



Thank You

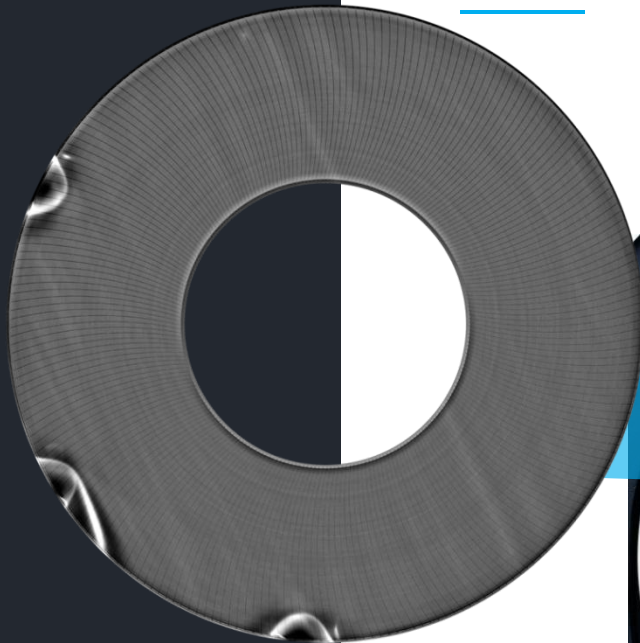
Michael Harstrick
Chief Global Development Officer
Garner Products, Inc.
MHarstrick@Garner-Products.com
www.garnerproducts.com



GarnerProducts.com

Offered as a public service, please feel free to distribute.

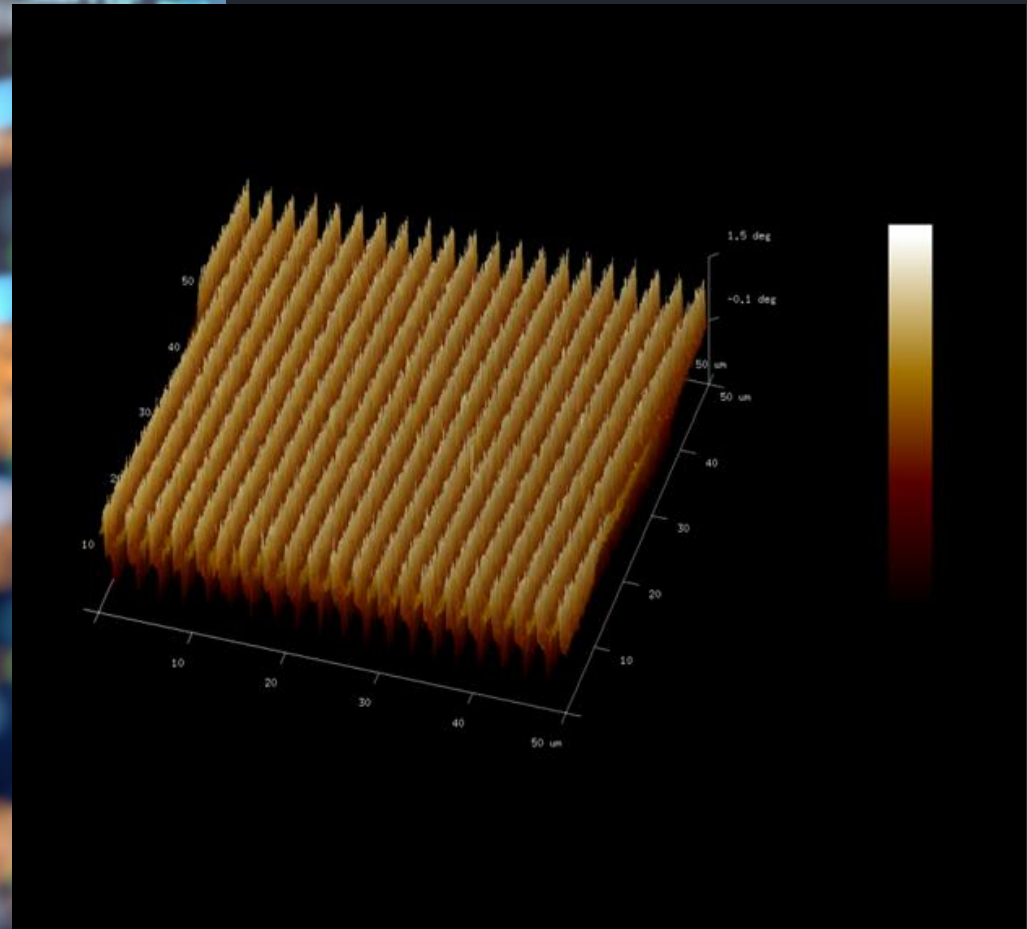
Magnetic Media



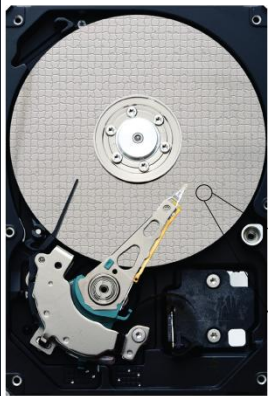
MFM Image

MFM image of data on a
HDD platter.

Scale is about $\frac{1}{2}$ width of
human hair.



Shred Risk



1 in² of hard drive = 1.3 Tb
2,000 bytes per page = Paper
Sheet Equivalent (PSE)
1.3 Tb = 8,125,000 PSE
1 mm² = 125,969 PSE



NSA Shred Requirement is 2 mm²

2 mm² = 503,876 PSE

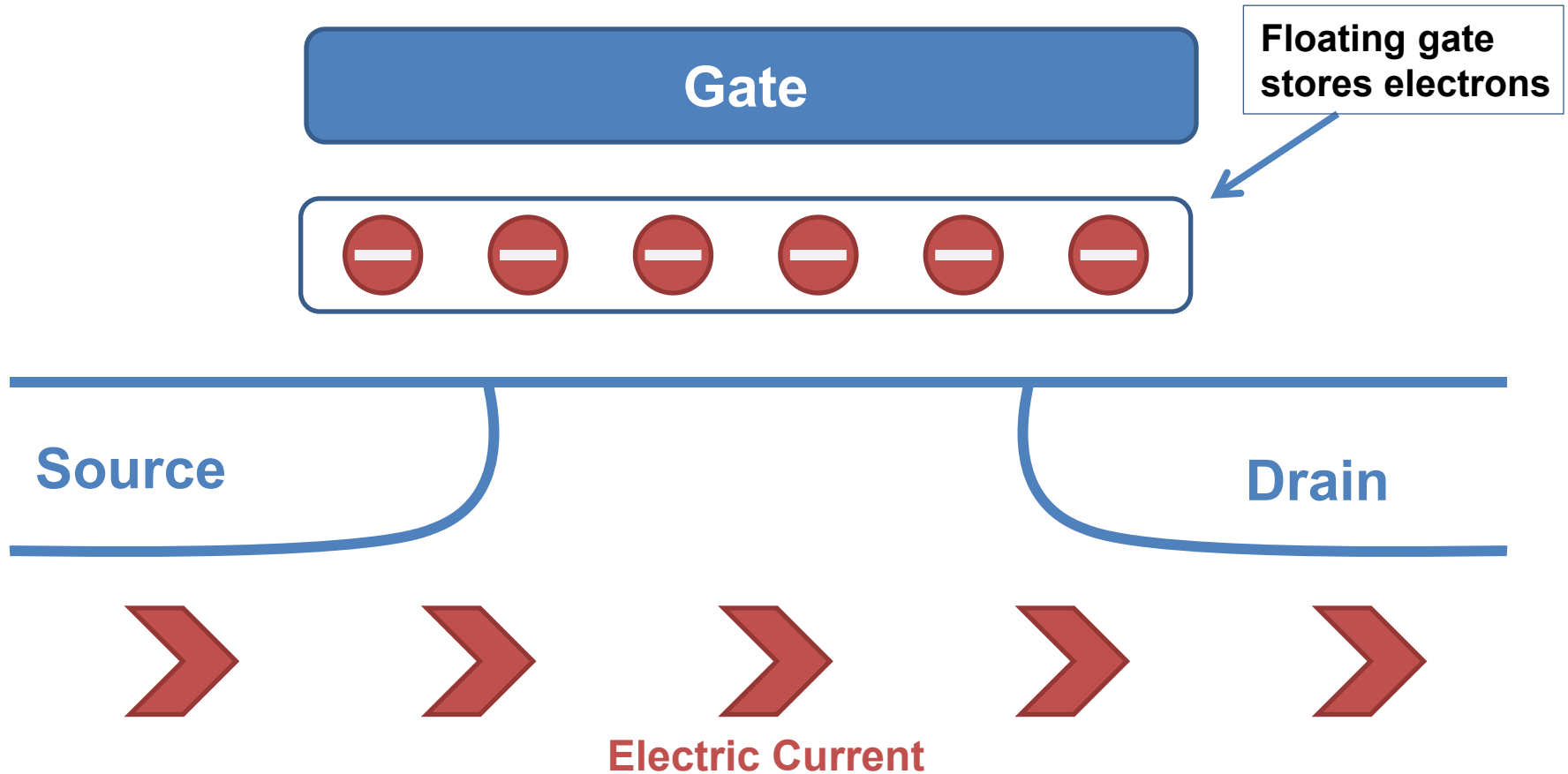
2.52 Pallets
of Paper

or

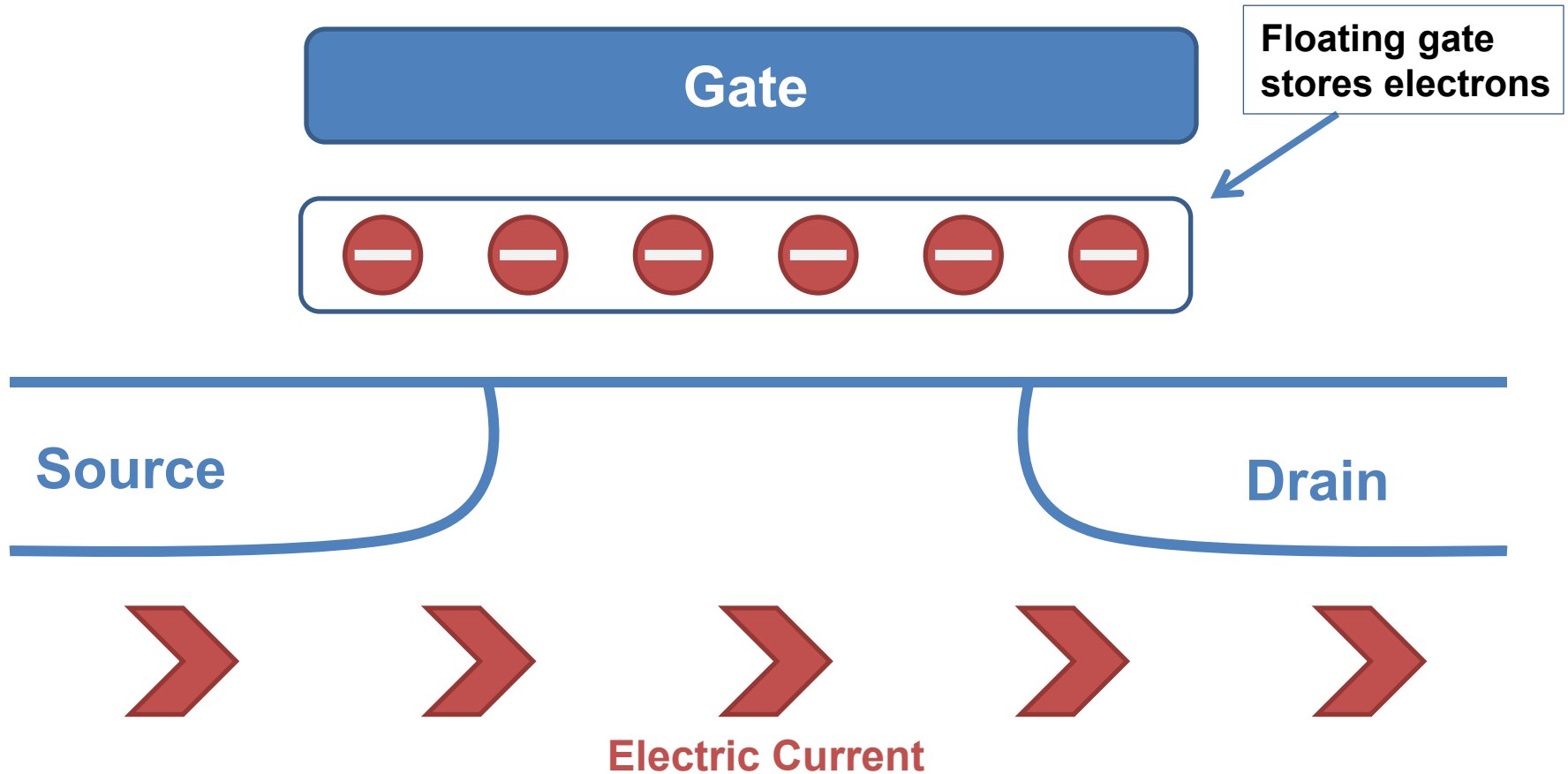
15 Sets
Encyclopedia
Britannica



How information is stored on an SSD



How information is stored on an SSD



How Real is the Risk?

GARFINKEL

Purchased a large number of hard drives, found significant amounts of data-easily

2003

NAID

Study in Australia

2013

NAID

Study in US: **40%** had recoverable PII...using off the shelf or free software

2017

2007

CHEO RESEARCH

Replicated findings

2016

BLANCCO

Study: **35%** had recoverable PII



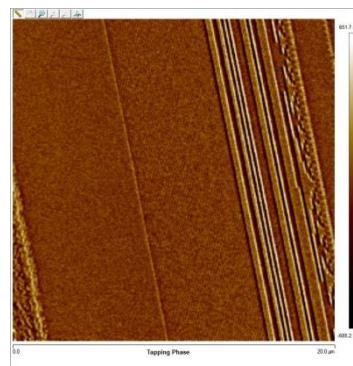
Degauss

Magnetic media is recorded by having a surface that can be magnetized.

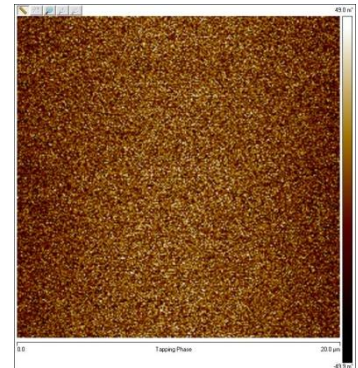
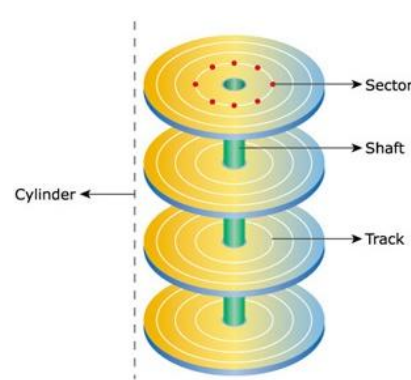
Data is applied by creating a magnetic pattern (domain) that can be read by read/write head

Strength of field is measured in Oersteds:

- Oersted is the measurement of resistance of the field to being erased, referred to as coercivity of the media.
- Modern HDDs have a coercivity of up to 5000 oe, modern tape up to 3000 oe.
- **Strength of the field applied is measured in gauss. One gauss kills one Oersted.**



Magnetic Force Microscopy



Magnetic Force Microscopy

Degaussing

Magnetic Media

Vast majority of storage media is magnetic

About 400 million HDDs sold each year

Tape is still the backup medium of choice especially for archiving

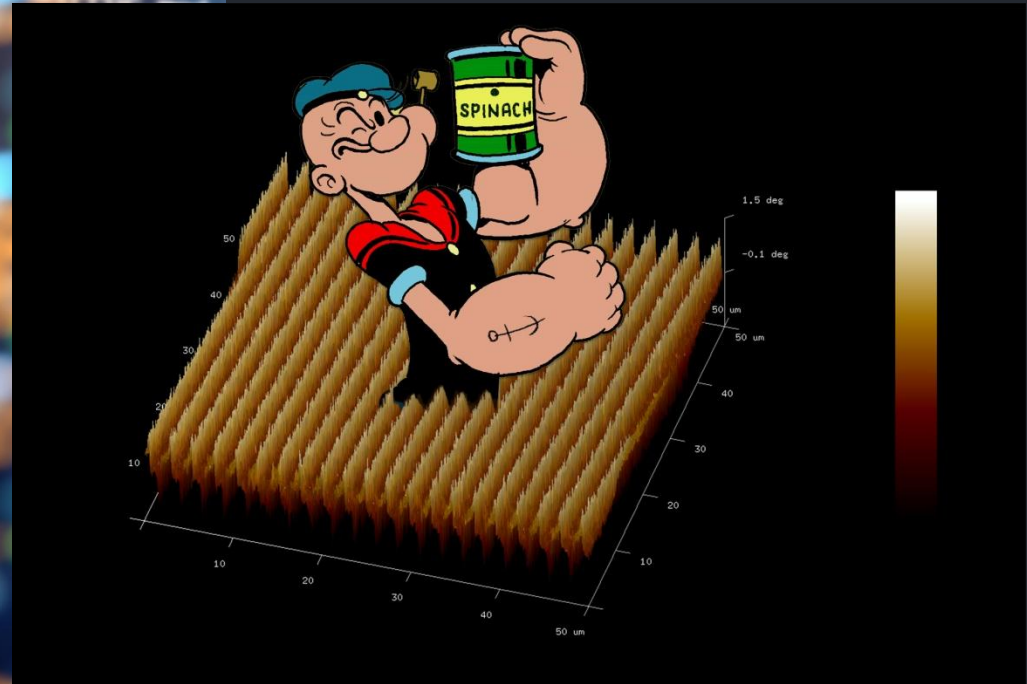
Emergent magnetic storage techniques such as HAMR and MAMR will keep magnetic media competitive for years

Emergent tape technologies will keep tape competitive for years

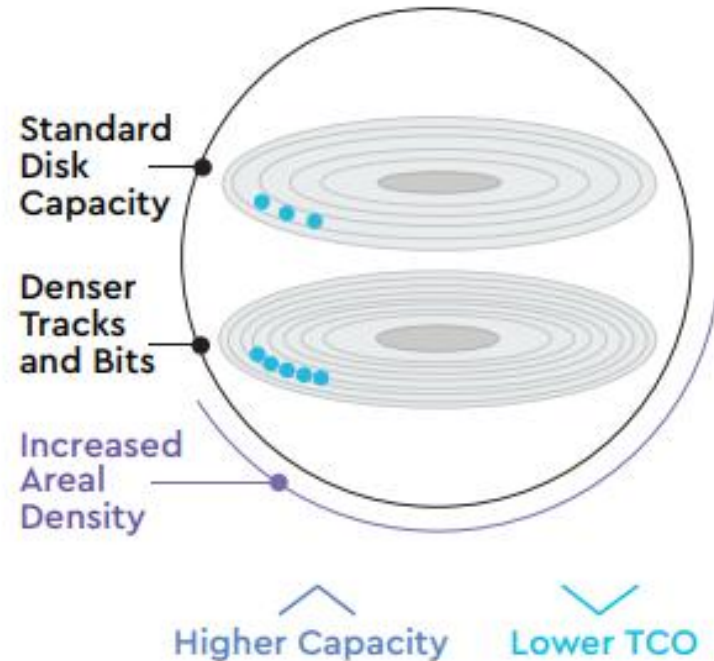
MFM Image

MFM image of data on a HDD platter.

Scale is about $\frac{1}{2}$ width of human hair.



EAMR



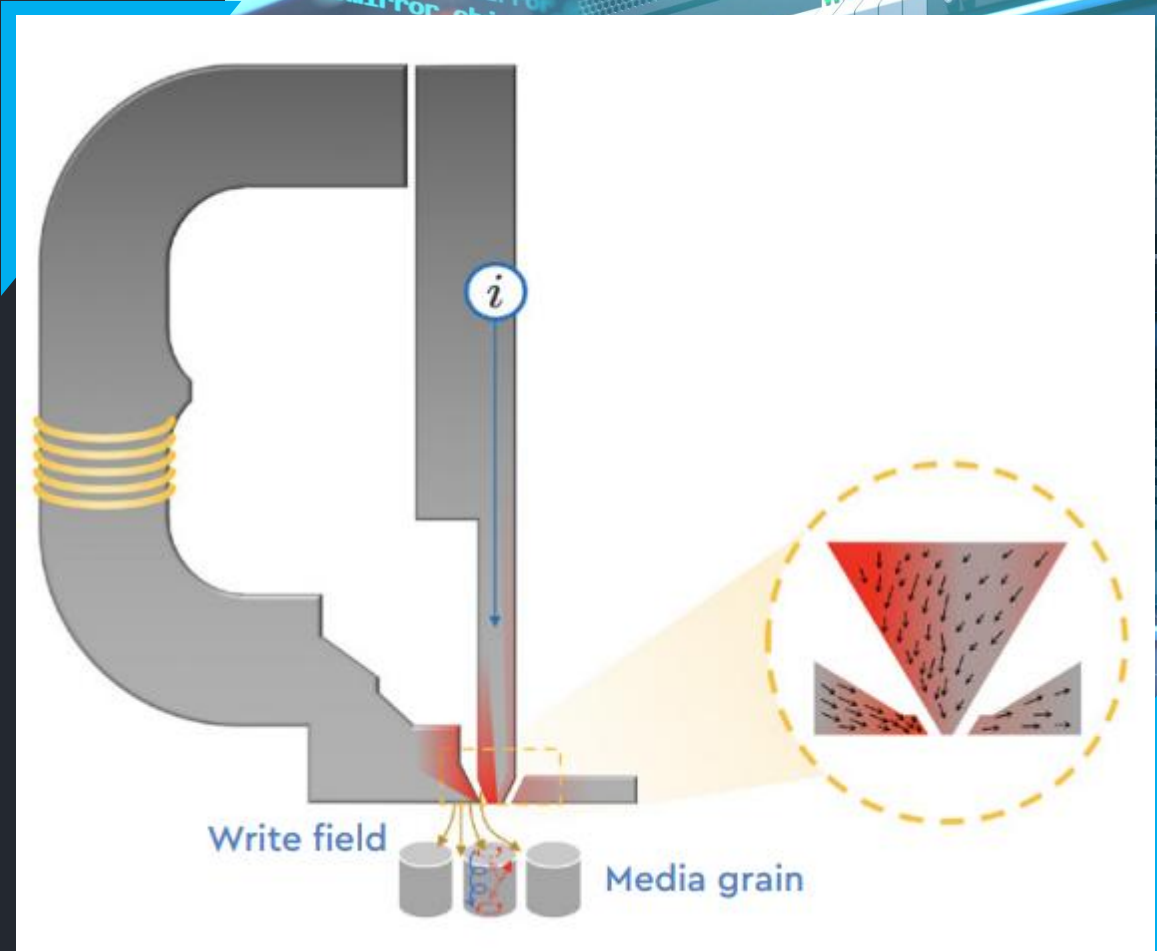
More precise write operations mean more data can be written on the platter, increasing its areal density.

Read / Write Head

EAMR

Applies electrical current to the main pole of the read/write head, *during write*, generate and additional magnetic field for magnetization flip of media bits, and reducing jitter.

This creates a more consistent write signal.



Magnetic Recording Trilemma

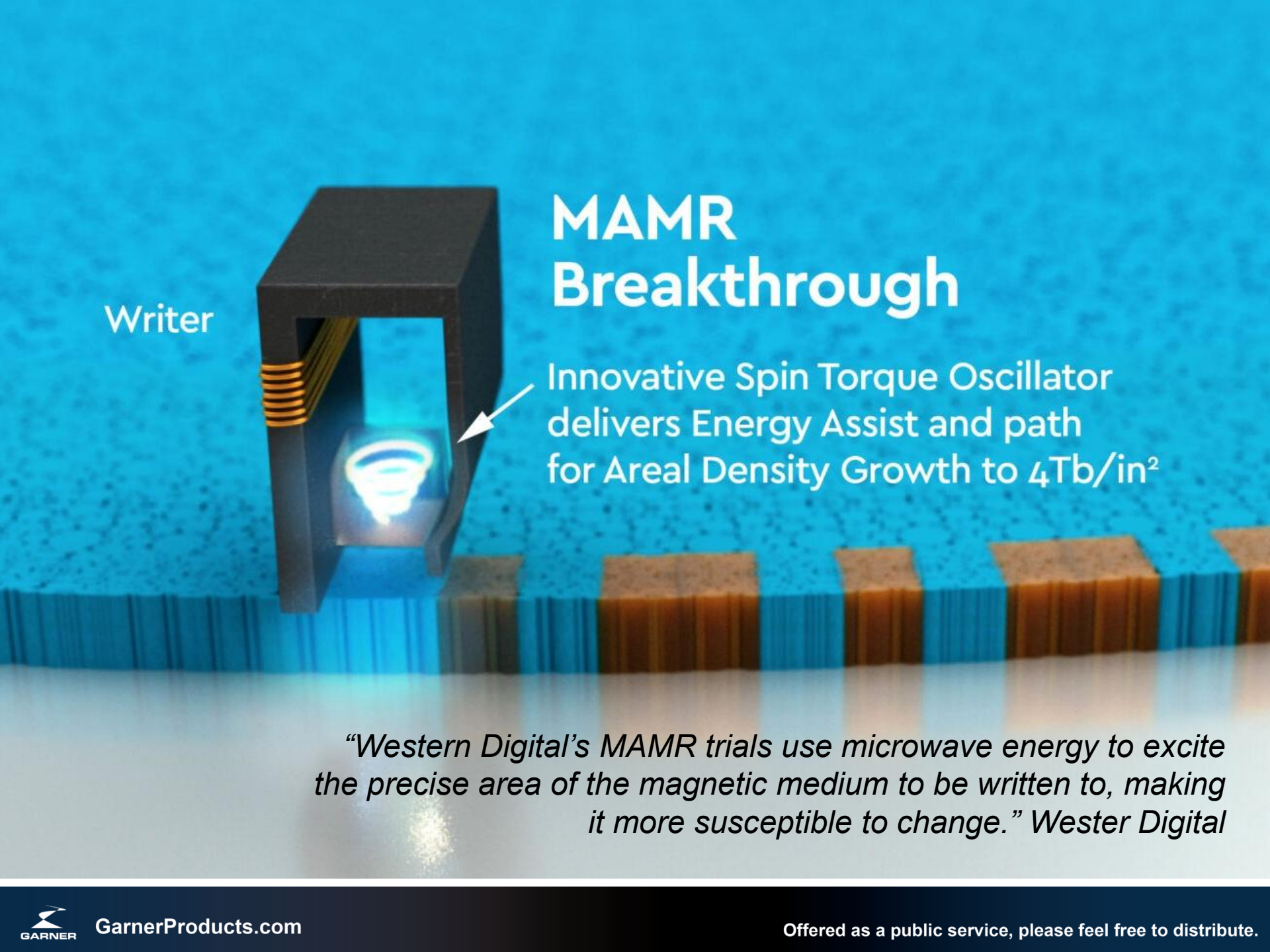
3 competing factors

The maximum usable data density on a magnetic recording device is limited by three competing factors:

- Magnetic coercivity—the strength of magnetic field required to demagnetize a domain—must be high enough to prevent the separately recorded grains from influencing one another and corrupting data

- The field strength of the write head must be high enough to overcome the coercivity of the medium

- Finally, the size of the field generated by the write head must be small enough so as not to overwrite adjacent areas

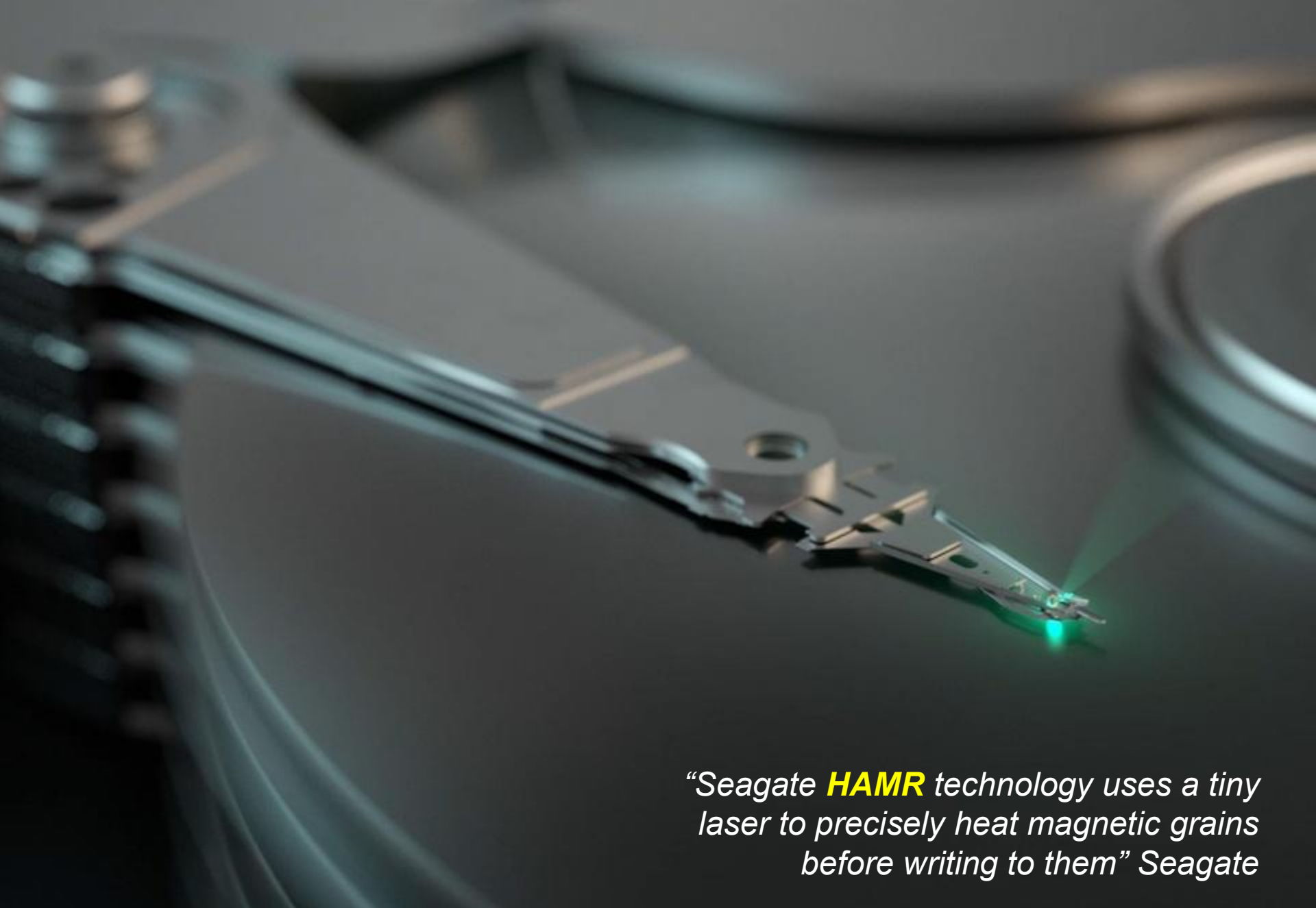


Writer

MAMR Breakthrough

Innovative Spin Torque Oscillator
delivers Energy Assist and path
for Areal Density Growth to 4Tb/in²

“Western Digital’s MAMR trials use microwave energy to excite the precise area of the magnetic medium to be written to, making it more susceptible to change.” Western Digital



*“Seagate **HAMR** technology uses a tiny laser to precisely heat magnetic grains before writing to them” Seagate*

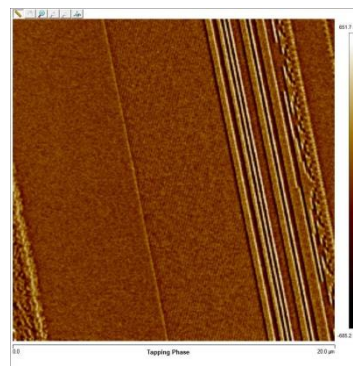
Degauss

Magnetic media is recorded by having a surface that can be magnetized.

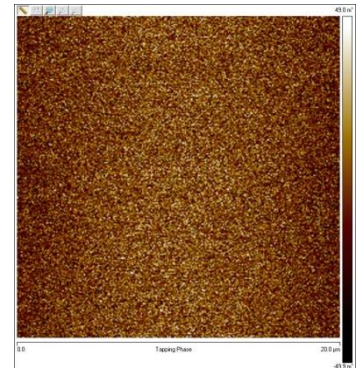
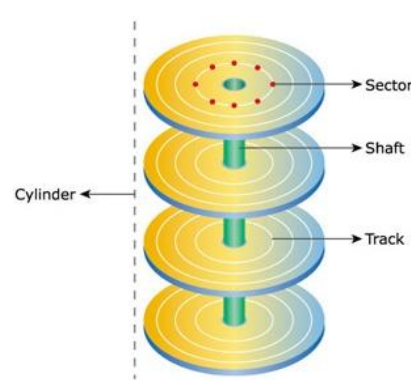
Data is applied by creating a magnetic pattern (domain) that can be read by read/write head

Strength of field is measured in Oersteds:

- Oersted is the measurement of resistance of the field to being erased, referred to as coercivity of the media.
- Modern HDDs have a coercivity of up to 5000 oe, modern tape up to 3000 oe.
- **Strength of the field applied is measured in gauss. One gauss kills one Oersted.**



Magnetic Force Microscopy



Magnetic Force Microscopy

Degaussing

Why it Matters

NSA wants a safety margin

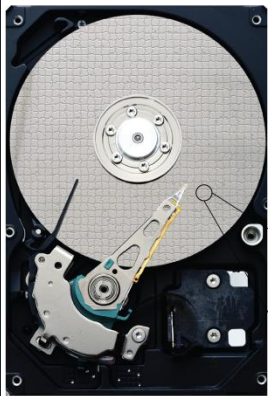
NSA: wants safety margin

Today media is 5,000 oe.

Degrade machine performance by 25%, then want 3 to 1 margin of Oe to Gauss

This generation HAMR (testing) is 6,500-7,500 oe....needs a 30,000 Gauss degausser.

Shred Risk



1 in² of hard drive = 1.3 Tb
2,000 bytes per page = Paper
Sheet Equivalent (PSE)
1.3 Tb = 8,125,000 PSE
1 mm² = 125,969 PSE



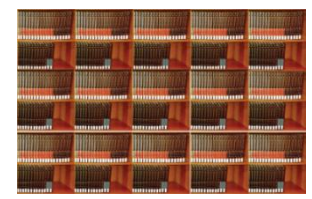
NSA Shred Requirement is 2 mm²

2 mm² = 503,876 PSE

2.52 Pallets
of Paper

or

15 Sets
Encyclopedia
Britannica



Shred Risk

Let's do the Math:

1 in² of hard drive = 1.3 Tb

1.3 Tb ÷ 8 (8 bits = 1 byte) = bytes

**2,000 bytes per page = Paper Sheet
Equivalent (PSE)**

1.3 Tb = 8,125,000 PSE

1 in² ÷ 645 sq mm = 1 mm²

8,125,000 PSE ÷ 645 = 125,969 PSE

1 mm² = 125,969 PSE

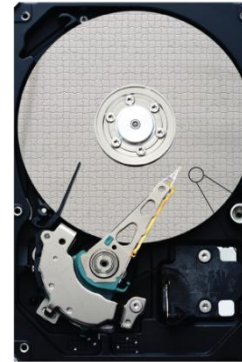
1 mm² x 4 = 2 mm²

125,969 PSE x 4 = 503,876 PSE



2 mm² = 503,876 PSE

NSA Shred Requirement is 2 mm²



2 mm² = 503,876 PSE

**2.52 Pallets
of Paper**

or

**15 Sets
Encyclopedia
Britannica**



Best Practice: Magnetic Media

0 Time + 0 Distance = No Risk

- Bring an NSA EPL degausser into the secure area
- Destroy on site at the time.
- Add a tracking system that captures:
 - ✓ Serial number
 - ✓ JPG image of the drive
 - ✓ Successful degauss
 - ✓ date/time/location/operator, etc.
 - ✓ Downloadable Certificate of Destruction.

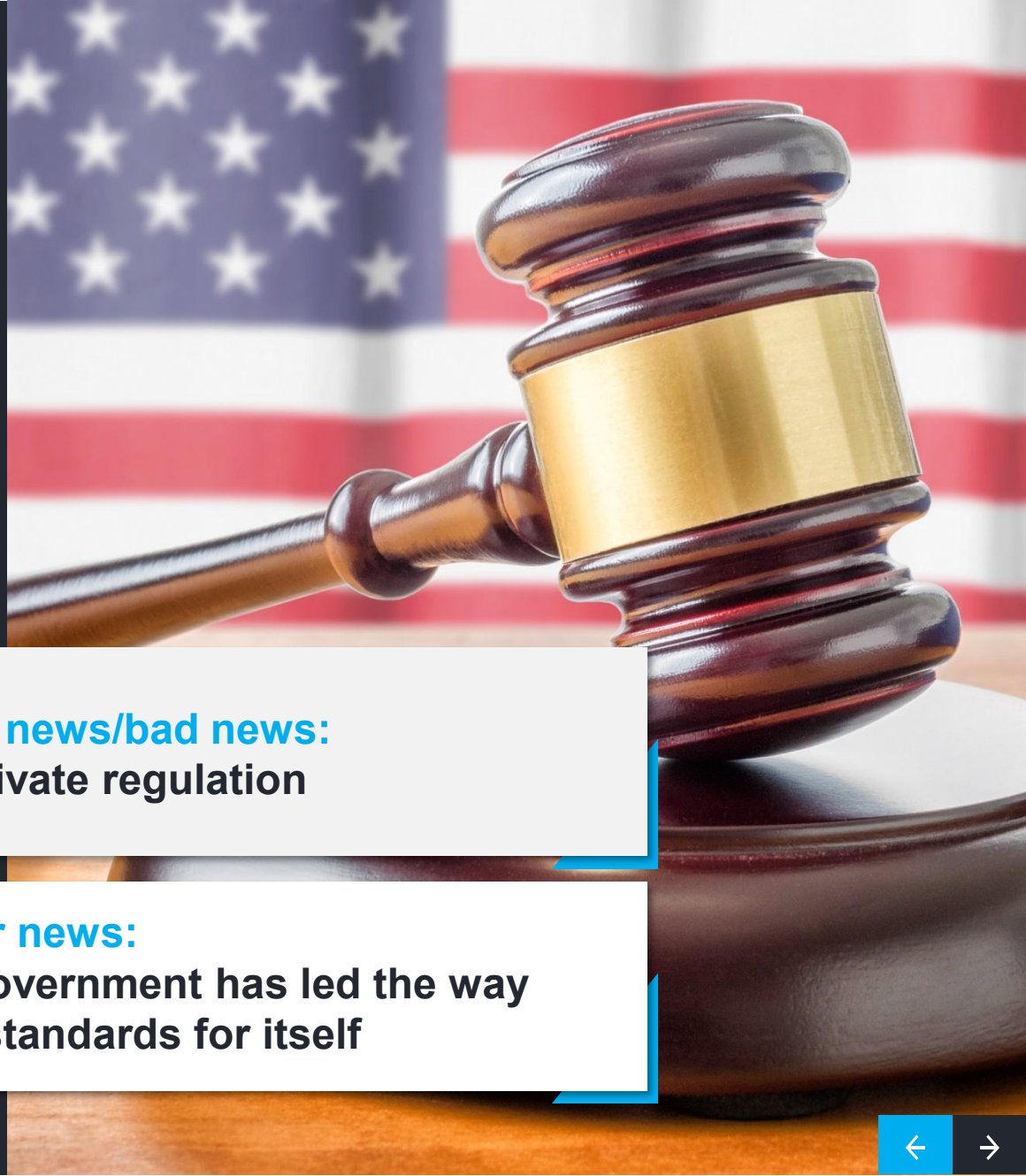


Data Regulations

Regulations
common thread:

Good news/bad news:
No private regulation

Better news:
US Government has led the way
with standards for itself



NSA Standards

Highest Protection Standard In The World.

Governments around the world use as their standard for **TOP SECRET** data destruction



NSA data destruction for TOP SECRET data requires:

- ✓ Shred (2mm particles)
- ✓ Incinerate
- ✓ Degauss with NSA-Listed Degausser

Before you leave the secure area.



UNCLASSIFIED

NSA/CSS Evaluated Products List for Magnetic Degaussers

March 2020

MAGNETIC DEGAUSSERS

VENDOR	DEVICE NAME / MODEL	TAPE: Oe RATING	HDD: Oe RATING	REMARKS
Advanced Design Corp.	MagWiper MW-2B	3000	L-5000, P-5000	
Applied Magnetic Laboratory, Inc.	AML-48G	Not Tested	L-5000, P-5000	Requires disk disassembly plus 1 full-contact pass with rotation
Data Security, Inc.	DD-1T	3000	L-5000, P-5000	
Data Security, Inc.	DD-1T	3000	L-5000, P-5000	
Data Security, Inc.	DDPM-2	3000	L-5000, P-5000	
Data Security, Inc.	LE-1	Not Tested	L-5000, P-5000	2 passes required with 90° rotation
Data Security, Inc.	LE-1	3000	L-5000, P-5000	
Data Security, Inc.	LE-1 w/ Caddy Bolt	3000	L-5000, P-5000	
Data Security, Inc.	LE-1C	3000	L-5000, P-5000	
Data Security, Inc.	TE-1	2000	Not Tested	2 passes required with 90° rotation
Garner Products, Inc.	TS-1, TS-1XT Series	3000	L-5000, P-5000	
Intimus International	Intimus 20000	3000	L-5000, P-5000	
Proton Data Security	T-4	3000	L-5000, P-5000	
Proton Data Security	1000	Not Tested	L-750	2 passes required with 90° rotation
Proton Data Security	1100	Not Tested	L-5000, P-5000	Requires disk disassembly plus 1 full-contact pass with rotation
Proton Data Security	T-6	3000	L-5000, P-5000	

<https://www.nsa.gov/resources/everyone/media-destruction/>



GarnerProducts.com

Offered as a public service, please feel free to distribute.

IRS: Regulations Media Sanitization



Publication 1075

**Tax Information Security Guidelines
For Federal, State and Local Agencies**

Safeguards for Protecting Federal Tax Returns
and Return Information



IRS 1075: Media Sanitization: Government Standards

FTI furnished or stored in electronic format must be destroyed in the following manner:

- Electronic media (e.g., hard drives, tapes, CDs, and flash media) must be destroyed according to guidance in [Section 9.3.10.6, Media Sanitization \(MP-6\)](#), and [Section 9.4.7, Media Sanitization](#). Electronic media containing FTI must not be made available for reuse by other offices or released for destruction without first being subjected to electromagnetic erasing. If reuse is not intended, the tape must be destroyed by burning or shredding in accordance with applicable standards (see Table 13, Media Sanitation Techniques).
- Destroy microfilms (microfilm, microfiche, or other reduced image photo negatives) by burning.

Whenever physical media leaves the physical or systemic control of the agency for maintenance, exchange, or other servicing, any FTI on it must be destroyed by sanitizing according to guidance in [Section 9.3.10.6, Media Sanitization \(MP-6\)](#), and [Section 9.4.7, Media Sanitization](#). FTI must be purged from the media prior to allowing release.

When using either method for destruction, every third piece of physical electronic media must be checked to ensure appropriate destruction of FTI.

Hand tearing, recycling, or burying information in a landfill are unacceptable methods of disposal.

8.4 Other Precautions

FTI must never be disclosed to an agency's agents or contractors during disposal without legal authorization and destruction must be witnessed by an agency employee.

The Department of Justice, state tax agencies, and SSA may be exempted from the requirement of having agency personnel witness destruction by a contractor. If a contractor is used:

- The contract must contain safeguard language in [Exhibit 7, Safeguarding Contract Language](#) as appropriate to the contract to ensure the protection of FTI.
- Destruction of FTI must be certified by the contractor when not witnessed by an agency employee.
- It is recommended that the agency periodically observe the process to ensure compliance with security of FTI until it reaches a non-disclosable state and that an approved destruction method is utilized.
- If the agency has legal authority to disclose FTI to a disposal contractor and chooses one that is National Association for Information Destruction (NAID) certified, the agency will not be required to complete an internal inspection every 18 months of that facility. However, it must maintain a copy of, and periodically validate the NAID certification.

IRS 1075: Media Sanitization: Government Standards

Media and Sanitization Techniques

Exhibit 11

Exhibit 11 Media Sanitization Techniques

The technique for clearing, purging, and destroying media depends on the type of media to be sanitized.

Table 13 – Media Sanitization Techniques

Media Type	Clear	Purge	Destroy
Magnetic Disks			
Floppy disks	Overwrite media with agency-approved software and validate the overwritten data	Degauss with a NSA/CSS- approved degausser	• Incinerate floppy disks and diskettes by burning them in a licensed incinerator • Shred
ATA hard drives	Overwrite media with agency-approved and validated overwriting technologies/methods/ tools	• Secure erase, • Degauss, or • Disassemble and degauss the enclosed platters	• Incinerate hard disk drives by burning them in a licensed incinerator • Shred • Pulverize • Disintegrate
USB removable drives	Overwrite media with agency-approved and validated overwriting technologies/methods/ tools	• Secure erase, • Degauss with a NSA/CSS-approved degausser, or • disassemble and degauss enclosed platters with a NSA/CSS-approved degausser	• Incinerate hard disk drives by burning them in a licensed incinerator • Shred • Pulverize • Disintegrate
Zip drives	Overwrite media with agency-approved and validated overwriting technologies/methods/ tools	Degauss with a NSA/CSS-approved degausser	• Incinerate disks and diskettes by burning the zip disks in a licensed incinerator • Shred
SCSI drives	Overwrite media with agency-approved and validated overwriting technologies/methods/ tools	• Secure erase • Degauss with a NSA/CSS-approved degausser, or • Disassemble and degauss the enclosed platters with a NSA/CSS-approved degausser	• Incinerate hard disk drives by burning them in a licensed incinerator • Shred • Pulverize • Disintegrate

Media Sanitization Techniques

Exhibit 11

(Table 13, Media Sanitization Techniques continued)

Media Type	Clear	Purge	Destroy
Magnetic Tape			
Reel and cassette	Overwrite on a system similar to the one originally used to record the data (e.g., overwrite classified or sensitive VHS format video signals on a comparable VHS format recorder); overwrite all portions of the magnetic tape one time with known, nonsensitive signals	Degauss with a NSA/CSS-approved degausser	• Incinerate by burning the tapes in a licensed incinerator • Shred
Optical Disks			
CD/DVDs	N/A; see Destroy method column	N/A; see Destroy method column	Destroy in the following order of recommendations: • Remove the information-bearing layers of DVD media with a commercial optical disk grinding device • Incinerate optical disk media (reduce to ash) with a licensed facility • Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimension of five millimeters and surface area of 25 mm².[§]

[§] This particle size is the one currently acceptable. Any disk media shredders obtained in future should reduce CDs and DVDs to a surface area of .25 mm.

NAID AAA Standards



Extensive process and procedure controls

- **Degaussing** - Must be with NSA EPL machine-or independently approved.*
- **Secure Erase** - No product list limitation.*
- **Overwriting** - No product list limitation, but overwrite and verify software must come from different manufacturers. No standard against/for online vs onsite overwriting.*
- **Shredding** - No particle size limitation or target. To specs agreed with client.

***All methods submitted are tested by outside lab for security.**

How do you sell secure sanitization?

Confused?

Start with risk:

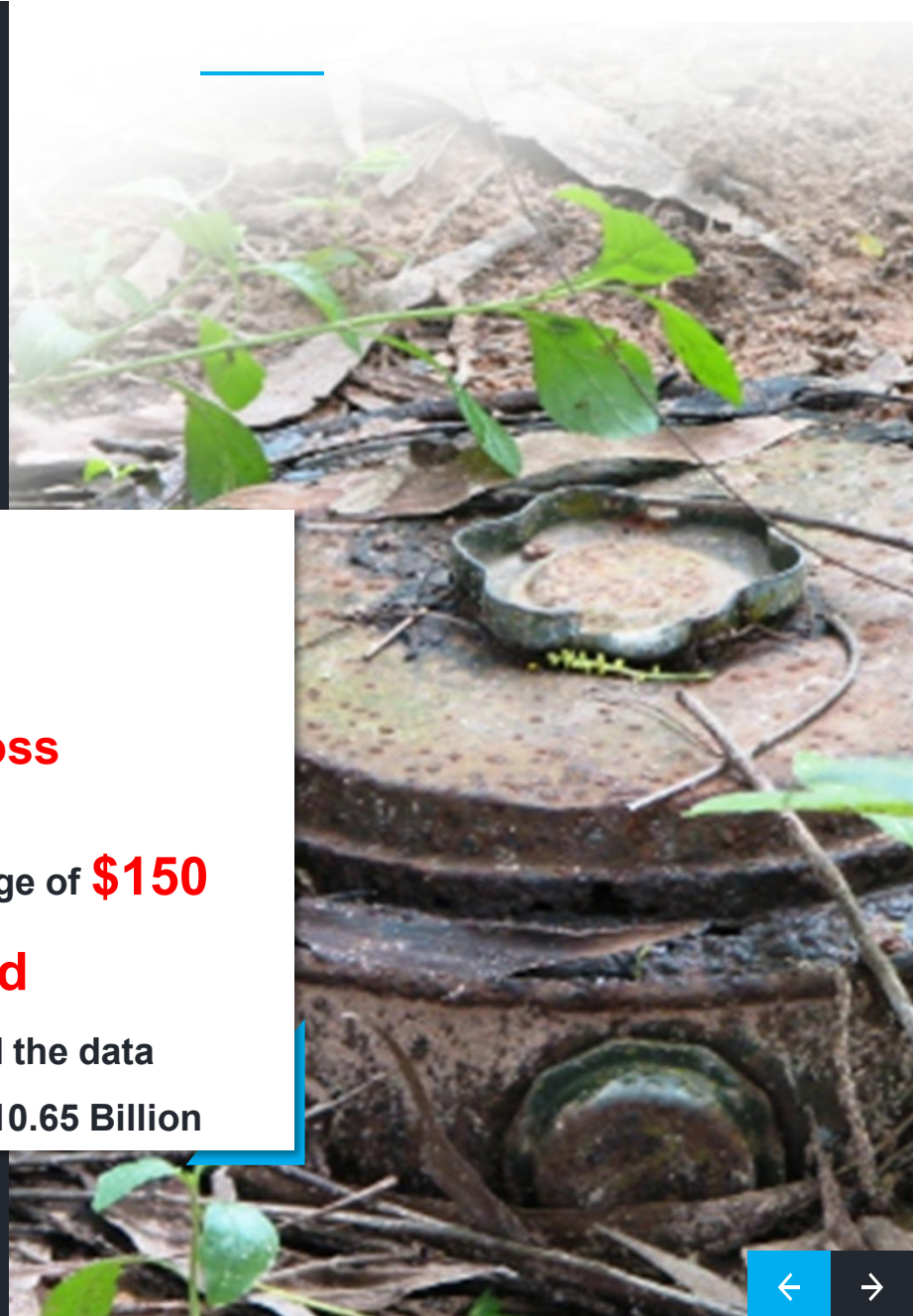
→ **Cost of loss x Probability of loss**

In 2019 data breaches cost an average of **\$150**

per name breached

to the company that lost/revealed the data

A 1TB drive=71MM pages of data=\$10.65 Billion





- 20,000 Gauss
- 15 Seconds
- 105 lbs



- 10,000 Gauss
- 3 Seconds
- 59 lbs



- 10,000 Gauss
- 8 Seconds
- 34 lbs

Triple Stage Actuator

EAMR

HDDs have Higher density with more accurate positioning, tracks can be written closer together.

