Phiston TECHNOLOGIES® INC.
Innovation, Ingenuity, Integrity

Why Software Erasure is Never 100% Trustworthy

Many companies offer software hard drive erasure. These solutions are not 100% reliable, as they don't fit the NSA/CSS data destruction requirements. Here's what works.

ABSTRACT

Many hard drive software solutions promise to wipe out media. However, there is a general misunderstanding about how these work and what levels of erasure they can truly achieve. For one, data destruction software can never completely destroy information stored in drives. Additionally, this method doesn't fit NSA/CSS requirements (and other security compliance guidelines) for secure data destruction. In this article, we will explain in detail why software erasure is not capable of truly destroying information, even if it promises to make a recovery impossible. We will also cover the limitations of this technique for different types of hard drives (such as magnetic ones, solid-state drives, and USB flash memories). Lastly, we will explain what you need to do if you want to comply with the most secure regulations, including using hard drive shredders and destroyers.

WHAT IS SOFTWARE HARD-DRIVE ERASURE, AND HOW DOES IT WORK?

Software erasure (also referred to as data wiping, data clearing, or data destruction) is a method for overwriting data on a hard drive that aims to delete files and destroy all digital media. This process is irreversible and renders the information irrecoverable.

Unlike basic file deletion, permanent data erasure removes all direct pointers to disk sectors, so you won't be able to see the cleared files using common software tools or repair tools. At the same time, this method leaves the disks operable, so you can use them again if you need to.

By erasing your hard drives using software, you can achieve certain requirements for data sanitation. In order to do this, you will need to select specific standards and verify the overwriting was completed successfully.

THE PROCESS OF ERASING DATA WITH SOFTWARE

The way software data erasure works is as follows: The application writes a stream of zeros, ones, or meaningless alpha-numeric data (pseudorandom) onto all the sectors of a hard drive. These mask each hard drive sector. Many data eradication programs give the user the option to do multiple overwrites, too.

Single-pass software erasure processes are generally considered sufficient for modern hard disk drives, but it's vital to ensure the program also does a verification pass to ensure the data has been removed. Many organizations also use these applications to target specific data for routine erasure, helping protect against hacking while also allowing users to save time by avoiding having to use software encryption.

Unfortunately, software erasure is not bulletproof. In many cases, you will still be able to recover data using drive repair software or disk repair software (for example, an HDD regenerator). This significantly raises the risk of identity theft and data breaches.

THE PROBLEM WITH SOFTWARE ERASURE

Many companies and institutions need to hold large volumes of confidential data, such as health records, social security numbers, state-issued verification cards, and credit card numbers and pins. As the need to store this data securely increases and technology changes rapidly, many organizations have had to turn to permanent data erasure solutions to deal with devices that need to be refurbished or retired.

One of the main issues with software data erasion is that it only works partially on flash-based media like USB flash drives and solid-state drives. The issue is that these devices can still keep remnant data that, although made inaccessible to the technique used for the erasure, can still be retrieved using the individual chips inside the drive (so, drive failure doesn't necessarily result in data erasure). For example, if there are bad sectors, these can be invisible to the host system and the erasing software. Any data stored in them would be recoverable.

As we mentioned above, drive failure (or partition management) doesn't equate inaccessible information. If you don't correctly erase the data stored in a disk that is retired or lost, it could become compromised. This, in turn, can lead to identity theft, financial impacts, threats to regulatory compliance, and loss of corporate reputation.

HIGH-PROFILE DATA BREACHES CAN HAPPEN

In the last twenty years, we've seen many high-profile incidents of data theft, including:

- **Lifeblood, 2008:** About 321,000 laptops containing personal information (such as social security numbers and dates of birth) went missing.
- **CardSystems Solutions, 2005:** 40 million accounts were exposed due to a credit card breach.
- **Compass Bank, 2008:** About 1,000,000 customer records were exposed when hard drives were stolen.
- **University of Florida College of Medicine, 2008**: 1,900 computers obtaining identifying information and photographs were improperly disposed of.

SOFTWARE ERASURE AND REGULATORY COMPLIANCE

Due to security concerns and breaches like the ones mentioned above, many industries and governments have put regulations in place to try to mitigate the risk of unauthorized exposure of confidential government and corporate data. In the United States, some of these regulations include:

- **HIPAA:** The Health Insurance Portability and Accountability Act, or HIPAA, is a federal law established in 1996 that created standards for the protection of sensitive patient health information.

- **FACTA:** The Fair and Accurate Credit Transactions Act of 2003, or FACTA, allows consumers to get free credit reports every 12 months and contains (among many regulations) several provisions for the prevention of identity theft.
- **PCI DSS:** The Payment Card Industry Data Security Standard, or PCI DSS, is used to handle credit card information from major brands and requires them to maintain secure networks and systems and implement access control measures.
- **NSA/CSS:** The National Security Agency/Central Security Service, or NSA/CSS, contains performance requirements for disposing of, sanitizing, and destroying media that contains sensitive or classified information. In this case, only NSA-listed tools can be used for deleting data.

If a company or organization fails to comply with these industry standards and government regulations, they can incur fines, be found civilly and criminally liable, and face damage to their reputation.

Although pre-testing for sector abnormalities and making sure hard drives are in working order before erasing the information can help with sanitation, many of the regulations listed above will only accept these solutions if they can overwrite the data a number of times and verify it's truly gone or, in most cases, require erasure via physical destruction.

A SAFER ALTERNATIVE FOR ERASING DATA: PHYSICAL DESTRUCTION

The only way to permanently and irrevocably get rid of all traces of data is to use drive destructions; for example, by using a hard drive crushing machine or hard disk destroyer machine.

The safest way to destroy a hard drive and all the data contained in it is to shred it or degauss it. Let's go through these techniques in a little more detail.

Shredding Hard Drives

You've probably heard of shredders, which are typically used for destroying confidential documents. Shredding is the most effective way to destroy a hard drive, too, as it turns it into many tiny pieces that cannot be put together again - thus erasing all the data forever.

There are many companies that offer shredding services for optical discs (such as DVDs and CDs), removable storage devices (like SD cards, USB flash drives, and compact flash cards), as well as microfilm, tapes, floppy disks, and of course solid state drives. At Phiston Technologies, we use high-speed industrial-grade shredders with excellent crushing power and interlocking grinders to do the job.

Shredding a hard drive, as you might expect, makes it unusable. This solution is an excellent choice for solid state drives (or SSDs) because they store the data in microchips that need to be destroyed, not merely sanitized as it would happen in software erasure.

Degaussing Hard Drives

Degaussers are machines that eliminate the magnetic fields stored on a divide (for example, a tape or a hard drive). They do this by sending a magnetic pulse through the device, which instantly sanitizes all data.

Degaussers are a highly specialized piece of equipment, as the magnetic fields they generate can disrupt the iron oxide coatings of hard disk plates. There are different types of degaussers, including electromagnetic degaussers (which pass electrical charges through a coil to generate a field. Sub-types include the rotating coil degausser and the pulse degausser), and permanent magnet degaussers (which use magnets made from rare earth materials and don't require electricity to operate).

Degaussing has some limitations in terms of how you can use the method to erase data. Mainly, that it does not work on SSD drives and newer enterprise drives. This is why degaussing alone is no longer considered a standalone destruction method.

Degaussing also destroys the physical medium, albeit partially. Many forms of magnetic storage media can be reused after the degaussing process is finished, but this applies mostly to older types, such as VHS video cassettes, floppy disks, and reel-to-reel audio tape. For modern hard disks, though, degaussing will damage the storage system. This happens because these devices have an infinitely variable read-write head positioning mechanism reliant of a servo control data that is also recorded onto the magnetic media. Degaussing removes all the stored data and the server patterns.

Crushing, Pulverizing, and Disintegrating Hard Drives

Other options for destroying hard drives include using an HDD destroyer or drive crusher. You can also pulverize the media (using pneumatics to smash SSDs and HDDs into pieces and render them inoperable). Many organizations looking to destroy classified information use these methods.

In order to help organizations crush, pulverize, and disintegrate hard drives, many companies have developed specifically designed machines that work with hard drives and SSDs. Because of how they are built, both these types of drives require different crushing mechanisms. Crushing a drive does not guarantee, on its own, that the data will not be recoverable.

If you use a disintegrator, you can break down a hard drive by pushing it through a conveyor belt system with a knife that cuts slices of the drive into small particles. For example, the MediaDice All Media Disintegrator can break down media into less than 2mm by 2mm pieces, making them impossible to reassemble. The main drawbacks of these machines are that they have special electrical requirements and heavy ventilation, which makes them unsuitable for office environments.

Melting Hard Drives

There's another method we should mention for permanently and physically destroying data, although this is absolutely not recommended as it can be extremely harmful to both human health and the environment. It is melting the hard drives by dipping them into acid. The process destroys both the platters and the housing, and although it's a very effective way of getting rid of the information for good, it's also the most dangerous option on this list.

The process of melting a hard drive involves the use of nitric and hydrochloric acid, both of which can harm human tissues and skin. These substances should only be handled using protective gear. Occupational exposure to hydrochloric acid can rapidly lead to spasm of the throat and suffocation. Nitric acid vapors are also highly corrosive and its manufacture releases nitrous oxide (which is 265 times more harmful to the climate than carbon dioxide) into the atmosphere.

Drilling on Hard Drives

Lastly, a homemade approach to physically destroying hard drives is to drill holes in its platter. You don't need any complex machinery to do this, but this method won't always guarantee the digital media will be entirely unrecoverable. For one, it would be extremely hard to ensure the drill goes through the correct places that can ensure the data is truly destroyed.

Although it might be enticing to take matters into your own hands, especially as an individual, there are a few essential considerations you should keep in mind when attempting to smash hard drives yourself. First of all, breaking these devices down will result in sharp shards that can cause serious injury. Secondly, if your business uses a large number of drives, this method will be unsafe and unreasonable. Thus, it's not recommended as a data destruction solution for companies.

SHOULD YOU USE A THIRD-PARTY SERVICE TO DESTROY YOUR DRIVES?

A popular way to dispose of hard drives is to hire a third-party specialist that can use a hard drive destruction device (for instance a hard drive destroyer) to physically tear them down so you can be certain the data is unrecoverable.

Hiring a third-party company offers several advantages, but there are risks, too. Here's how doing this in-house can be more beneficial:

- **Control:** If you send your drives to another company, they might claim to destroy them, yet something could go wrong, and the data could become compromised. By doing this in-house, you can be sure you are following the correct processes, so the drives are correctly destroyed.
- **Security:** When working with a third-party service, you will need to transport the drives to the facility. This transportation already involves a risk of data breaches or loss, something that won't be a worry if you have an HDD shredding machine or degaussing machine within your company.

- **Cost:** If you need to dispose of several drives, having your own erasure machines in-house will help you save money in the long term. This is because third-party services charge a significant amount for destroying drives.
- **Sustainability:** As you won't need to transport the drives to a different location, having your own machines is more sustainable and can reduce your company's carbon footprint.

USING PHISTON PRODUCTS TO DESTROY DATA FOR GOOD

If you want to have complete control over the disposal of your old hard drives, you should consider our data destruction products.

Phiston Technologies is the leader in physical data destruction and is also responsible for making the most innovative and competitive products to secure your confidential data. All of Phiston's products are engineered with government and private entities' standards in mind and follow all regulations to avoid security breaches.

We offer HDD destroyers, SSD destroyers, disintegrators, degaussers, and secure scanners so you can always be certain your data is unrecoverable and complies with all safety requirements. Request a quote today, and we'll get back to you ASAP!

THE PHISTON ADVANTAGE

At Phiston Technologies, we believe in innovation, proactive product development, and secure destruction of data.

Our goal is simple: destroying your media to preserve and promote data security. We build products to ensure complete media destruction.

As data storage continues to evolve, so will the need to advance current data destruction products. Phiston will always be ready to provide security solutions to keep your organization safe and in compliance.

Phiston as a company is a leader in end-of-cycle media destruction and has various products that can handle all. Our clients include some of the largest tech companies in the world, and our devices are deployed across all 50 states and in 49 different countries.