# 9.1.5 Data Destruction Facts

When you dispose of a computer, sell used hardware, or erase important information, it's crucial to destroy all of the data on a device. It's not enough to delete the data. Reformatting the hard drive is not even sufficient. If other people can access your computer, they can use data remanence, the residual representation of erased data, to recover information. You must damage the hardware so badly that the remanence is gone.

The benefits if data destruction include:

- Protect your business
- Protect your customers
- Protect your employees
- Optimize your hard disk space

The following table identifies various ways to destroy data:

| Data Destruction Techniques | Description |
|---|---|
| Burning | *Burning* is the method of building a small fire somewhere legal and safe. Use metal tongs to burn your documents one by one or a few at a time. It's important to ensure that each document is turned into ash--if sensitive information escapes the flames and flies away, it might fall into the wrong hands. |
| Shredding | *Shredding* is running a hard disk through a disk shredder, physically destroying the drive. |
| Pulping | *Pulping* is a way of removing all traces of ink from paper by using chemicals and then mashing the paper into pulp. Since these chemicals can ruin carpet and clothing, you should perform this process outside and use protective gloves. |
| Pulverizing | *Pulverizing* is like shredding, except that it uses a punch press or hammer system to crush a hard disk into a pile of metal confetti. |
| Degaussing | *Degaussing* purges the hard disk by exposing it to high magnetic pulse that destroys all of the data on the disk. It also ruins the motors inside the drive. |
| Purging | *Purging* is the removal of sensitive data, making sure that the data cannot be reconstructed by any known technique. |
| Wiping | *Wiping* is a software-based method of overwriting data to completely destroy all electronic data residing on a hard disk drive or other digital media. Wiping uses zeros and ones to overwrite data onto all sectors of the device. By overwriting the data on the storage device, the data is rendered unrecoverable and achieves data sanitization. |

Now that we have discussed ways to permanently dispose of information, let's switch gears to talk about the legal requirements of data destruction, starting with data sovereignty. Data sovereignty is the concept that information stored in binary digital form is subject to government laws and regulations. Data sovereignty laws are created to maintain privacy and prevent foreign countries from subpoenaing, or searching, another country's data. Data sovereignty laws evolve rapidly as cloud services and other new storage options emerge.

It's imperative that you stay current with data sovereignty laws because every business must comply with state and federal data destruction regulations. Data sovereignty laws protect citizens from identity theft, companies from security breaches, and clients from privacy issues. They specify when, how, and what data you are allowed to destroy. Requirements vary depending on location, so make sure you comply with the most up-to-date version of both state and federal regulations. In the US, you will have to follow laws dictated by three government acts:

| Government Act | Description |
|---|---|
| HIPAA | HIPAA stands for Health Insurance Portability and Accountability Act. HIPAA protects medical records and personal health information. Companies that provide healthcare insurance handle HIPAA-protected information. And, of course, companies that provide health-related services also handle HIPAA-protected information. |
| FACTA | FACTA, the Fair and Accurate Credit Transactions Act, was created to protect against identity theft. It applies to the disposal of consumer reports and related information. FACTA includes credit reports, credit scores, employment history information, check writing history, insurance claims, residential or tenant history, and medical history. Every business handles FACTA-protected information, and every business must comply with FACTA laws. |
| FISMA | FISMA, the Federal Information Security Management Act, protects government information. It is primarily concerned with proper data destruction and has detailed disposal requirements. |

Companies should have data retention policies and procedures for storing and destroying information. By law, organizations must retain certain information for specified time periods, and your business probably has additional records to keep and maintain. Always make absolutely certain that it is okay to destroy papers, data, and drives.

You are responsible for the destruction of data, but it's always a good idea to let the following individuals know when you plan to destroy any data:

- The owner of the data
- The steward or custodian of the data
- The privacy officer in your company