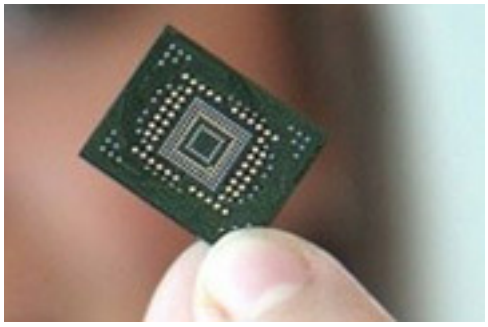
Researchers at the University of California at San Diego (UCSD) say data on SSDs is more difficult to erase than that on HDDs, in their study *"Reliably Erasing Data From Flash-Based Solid State Drives."*



The study tells how sanitising SSDs of data is a difficult task-- if not nearly impossible. Not even overwriting data several times ensures data erasure, as the researchers say they still recovered data on some products. As the paper says: "all single-file overwrite sanitization protocols failed: between 4% and 75% of the files' contents remained on the SATA SSDs."

USB flash drives fare similarly, with between 0.57% and 84.9% of data remaining on drive after an overwrite attempt.

The researchers conclusion remains; HDDs are easier to sanitise of data than SSDs. This is due to how SSDs work-- where in HDDs write and erase sectors are the same, flash memory consists of pages (containing 8K of data), and blocks (containing up to 2MB of data marked for erasing).

The security experts suggestion? Cryptographic erasure. This process involves the user first encrypting the SSD, then deleting the encryption keys on drive once the SSD is no longer in use. Some SSDs carry native hardware-based encryption; for others, encryption software is required.

Go Reliably Erasing Data From Flash-Based SSDs