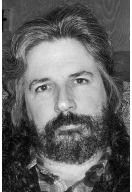


ROBERT G. FERRELL

/dev/random



Robert is a semiretired hacker with literary and musical pretensions who lives on a small ranch in the Texas Hill Country with his wife, five high-maintenance cats, and a studio full of drums and guitars.

rgferrell@greatambience.com

KNOW WHAT I LIKE ABOUT ONLINE auctions? Well, several things actually, but in this case I'll confine my enthusiasm to the juicy low-hanging fruit known as storage media. I'm talking "previously owned" hard disks, thumb drives, micro drives, memory sticks, compact flash cards, SM cards, and all the other variations on that theme to be found for sale to the highest bidder. Even old DLT tapes, Zip disks, and their somewhat archaic ilk can be had, for those with the equipment to read them. What is it about these utterly commonplace devices, you may well ask, that waxes my elephants? It is the treasures nestled deep in their binary bowels, of course: intact data. The number of people who yank media out of a computer or digital camera and ship it off to a never-met buyer without even bothering to delete the contents is, to choose but one from the stable of modifiers that apply, staggering. Even among those who make some attempt at sanitization, the belief that simply deleting files on a hard disk is sufficient to obliterate data is as widespread as it is erroneous. That minor misconception is what makes disk-diving entertaining.

I'm not going to cover the basics of file systems and the mechanisms for deletion of data therefrom, because I strongly suspect most anyone reading this already knows all about that sort of thing—probably more than I do, in fact. I will instead press onward and mention that the public record is liberally littered with examples of carelessly cast-off bits. Customer profiles, patient files, Privacy Act data, confidential transactions, student grades, personal communications, pirated music and video, homegrown pr0n, and just about every other embarrassing and potentially actionable manifestation of our obsession with archiving ones and zeroes for posterity are there for the bidding and the winning and the fondling. Garfinkel and Shelat in 2003 estimated that only 9% of used drives bought off an auction site fit into the "properly cleansed" category, while something like 17% still contained intact operating systems as well as user data. I'm not talking about

data recoverable only using expensive forensics suites or scanning tunnel microscopy, either. I mean plug it in, boot it up, read 'em, and reap.

Although I don't have figures at hand concerning other forms of removable data storage, I would expect them to suffer from a similar lack of deletion diligence. There have been marketing campaigns touting thumb drives, for example, as "disposable" storage. All storage is disposable, as far as that goes. Despite prolific coverage of "dumpster diving" as a lucrative technique for intelligence gathering, people still tend quite naively to equate disposal with oblivion. One of my best friends as a child was the son of a small-town garbage man. (Yep, that's what we called them back then. They hadn't come up with "sanitation engineer" yet.) His dad would find some truly amazing things in the trash on occasion: completely functional electronics, toys still in their original packaging, intact china, perfectly serviceable furniture, and so on. My buddy had, as a result, the single largest personal collection of plastic model parts in the known universe: closets and bedrooms and storage sheds full of them. If we were children today, I figure his dad would be bringing home operational thumb drives and flash memory cards for us. They're not as easy to build room-filling space stations out of, but we'd manage somehow. Nerds are nothing if not resourceful.

Giggling at embarrassing vacation photos someone thought they'd dispatched forever or riffling through breathy emails to an old lover are invasions of someone's privacy, admittedly, but they don't come close, damage-wise, to the ever more popular hobby of identity theft. Aye, there's the rub, or rather, jagged laceration, where unsanitized media are concerned. When your Social Security number, bank account, date of birth, and online passwords are in the hands of the profit-minded, you're in a world of hurt. There's an awful lot of mayhem that can be perpetrated in your name in this case and—here's the really dicey part—even though you're the victim here, it's up to *you* to prove you didn't do it. The "innocent until proven guilty" principle, which has already taken a terrific tossing around in recent years, goes right out the window and splatters messily on the pavement far below. Meanwhile, the bad guy has moved on to buying stuff using someone else's identity, blissfully unconcerned with the years it will take you to rebuild your besmirched reputation in the eyes of the financial sector. All because you, or more likely some company with whom you once did business, couldn't be bothered to wipe before flushing.

Here, of course, is where the whole concept gets seriously scary. No matter how careful you are with your personal data on equipment you control, there's not much you can do about the appalling lack of security at the myriad institutions with whom you've shared this information. Just stop and think how many hard drives in the world have your private data stored on them, any one of which falling into the wrong hands could shred your life quite thoroughly. On second thought, maybe it's better if you *don't* think about it too much. There's enough bad news permeating our daily existence as it stands now without adding yet another worry based on an event with a fairly low statistical probability of occurring, like a hurricane or a supervolcano eruption or an asteroid strike or avian flu or global warming or Lyme disease or . . . Sorry, my world view has been deteriorating steadily since I ran out of selective serotonin reuptake inhibitors the other day.

Returning briefly to the subject of used media, the Data Protection Gurus say that if you'll take the simple preliquidation precaution of overwriting everything with zeroes or ones you'll foil all but the most determined and well-funded illicit data recovery efforts. I go them one better, though. Before I discard old media, I overwrite everything with twos.*

*The "two" is stamped into the head of a twelve-pound sledgehammer.