

# LAW and ORDER

## USB Memory Devices

by Kevin Gordon

When discussing USB memory devices, it could be called "the good, the bad, and the ugly." Such USB devices can provide great benefits and advantages to the average agency but can also cause great damage and concerns. As with everything in the computer world, change comes quickly. Regardless of what you refer to them as, USB memory sticks, jump drives, Iomegas, thumb drives, etc, what was expensive and limited is increasingly inexpensive and expansive.

A 128MB memory stick was an amazing amount of storage when it arrived on the scene, compared to 100mb of zip drives. Very quickly we saw 512MB, 1GB and Seagate recently introduce their pocket sized 5GB palm sized pocket hard drive. That 5GB is about 3500 times the capacity of a floppy disk. Compare that 5 gig with the total storage your first computer had!

I recently purchased a Seagate 5GB for less than \$100. I'm not sure what surprised me most, the 5GB size or the less than \$100 price. That 5GB is a lot of information to be able to store. It is also a lot of information to be able to lose.

The good uses of such memory devices are only limited to your imagination, just as the bad uses are only limited by the imagination of others. Many small departments only have a few PCs, which may or may not be networked. I recently visited several area agencies, all less than 10 officers. Several had two computers, not linked. One was for administration and one was for the chief.

In many such agencies data is not being systematically backed up. USB memory devices, if used properly, are a blessing to these departments. Such agencies may use them to backup files, store digital photos, hold reports which may be simple word processing documents, report templates, PowerPoint presentations, or just to transfer files from laptop to desktop or desktop to desktop if not networked.

The devices will last anywhere from 10,000 to 100,000 erase/write operations but you must keep in mind, the device can fail. Remember, most officers carry two magazines not because of the common need of more ammo, but because magazines can fail.

Officer Mike Bazzell serves as the Information Technology Officer for Alton, IL PD as well as the Computer Systems Administrator for the City of Alton. Bazzell points out "the corruption of data on these devices is much more likely than on more stable data storage, such as a hard drive. If the device is removed before being cleanly un-mounted, the chance of corruption increases."

USB devices are more easily misplaced or lost. I don't recall ever misplacing my original bag phone but I've misplaced my small, pocket size cell phone countless times. We all know the smaller it is, the more useable it is, the more loseable it is, even if that isn't a word.

If you use a USB device, you should assume that any and all data that is stored on it could disappear at any time. This may be due to the physical absence of the unit, by theft or loss, or the failure of the unit itself. If used to back up data, remember which is the back up. Replacing the new data with the old by accident is an all too common and simple error. It happens quite often, not due to user ignorance, but usually user distraction which is very common at a PD.

Sometimes simple is best. Just adding "BU" to the name of the back up file immediately reminds you which is the backup versus the original. If just transferring files, make sure you delete the files in question from the device when done for both security sake and the previous mentioned accidental replacement of new with old.

The bad uses may certainly include someone using the memory stick to steal your agency data, but

typically the more realistic problem is someone in the department losing the unit that accidentally ends up in the wrong hands. We have all read about folks who misplaced a laptop, a digital camera, USB, or other storage device that had sensitive material whether personal or business and the resulting problems.

An agency USB device may contain arrest reports including juvenile offender information, photos, confidential intelligence information, etc. Even if not overly sensitive, regardless of how minor the data is, someone will still have to answer for how it came up missing.

When asked about mitigation, Bazzell boiled it down to two methods, avoidance and decryption. "With the avoidance strategy, no data is stored on the memory stick that can be considered private. This strategy is limiting, especially determining exactly what constitutes private data.

An ideal encryption strategy allows any data to be stored on the memory stick but renders the data useless without the required encryption key, which is usually a strong password, but can also be a biometric such as a thumbprint. Some USB memory sticks include their own encryption algorithms and formats, but often the encryption used is either unproven or inadequate, and the memory sticks are more expensive."

Even if the department doesn't use such encryption, which most will not due to the additional cost, departments can certainly take steps to protect department information. Departments should consider at least a policy concerning memory devices so officers have direction. A simple policy of what will be used to back up or transfer files, when it will happen, who will do it, etc.

If USB storage devices will be used, they should be purchased by the agency and employees should not be allowed to use their own. There is no control in that. Most administrators were concerned about viruses from old floppy disks and online connection but forget that USB storage devices can also contain viruses that could do catastrophic damage to the department computer systems, the ugly side.

As difficult as it is for some folks in our business, don't be afraid to ask others for their input and advice. Most likely there is a younger, and yes, less experienced officer than you in the department, who just so happens to have 10 times the experience you may have in the computer field. Use that knowledge to benefit the department.

*Kevin Gordon spent 25 years in law enforcement and retired as a chief of police. He may be reached at [Kevin@KGordon.com](mailto:Kevin@KGordon.com).*

**This article was printed in Law and Order Magazine, February 2006.**