

# Making Copies

David Dindak  
Coast to Coast Data Search  
[david@2mypi.com](mailto:david@2mypi.com)

We've all had to copy a stack of confidential papers for work, medical, loans, mortgages or to send the next great American novel we just wrote to our publisher. I've seen people at the local copy shop furtively looking around and checking out the clientele to insure no one gets a look at their information. I've even seen a guy run back from the parking lot to check the copy machine one more time for any papers left behind.

What he didn't know, is that every scrap of paper he copied was sitting in the hard drive of the photocopier just waiting to be stolen.

CBS news sent a correspondent to a warehouse in New Jersey to buy photocopiers. Out of a selection of 6,000, they bought 4 for a total of \$1,200. What they found ... was identity thief heaven.

Using a free forensic software program found on the internet, they extracted tens of thousands of documents in 12 hours. They found bank records and personnel information. But the best find was from a copier previously used by Affinity Health Plan which stored medical information on nine people.

Since 2002 photocopiers have been manufactured with hard drives. About 90% of the office and public copiers are leased and are more likely to be resold with the information still available.

In 2007 many manufacturers have installed built-in technology to erase or encrypt the information in the hard drive. But the problem lies with the machines that are still in circulation from 2002 - 2006.

If you must copy confidential material, use your personal copier. It is less likely that a thief will go after a smaller copy machine when an office copier would yield much more. If you do not have a personal copier and must use a public machine, find out when it was manufactured and their policy on protecting your privacy.