The Washington Times
www.washingtontimes.com

What is evidence?

By Richard W. Rahn
Published May 22, 2004

Have you seen any of the photos of Jane Fonda and John Kerry together back when he was a war protester? Do you know which of the photos are real and which are phony? Digital technology has made it easy to create pictures that purport to show something that never was.

The late-night television comedians and many Internet pranksters create pictures showing the famous in funny situations, most often in good fun.

The fun ends for both the accused and law enforcement officials when what is presented is said to be photographic evidence of a crime. We remember the famous pictures of Josef Stalin with his colleagues who, as they were physically liquidated, were also airbrushed out of the pictures.

However, a competent expert could examine an original negative or photo and tell if it had been altered. In the digital world, proving a photo is real can be almost impossible. The new technologies make it easier to both frame someone and create doubt about actual photographic evidence.

Life has suddenly become more risky for news editors. The editor of the London Daily Mirror, Piers Morgan, was just fired for publishing fake photographs of British troops abusing Iraqi prisoners. His newspaper had to apologize both to the British military and their readers. In the new digital world, the rules have changed. The mere presentation of a photo is no longer sufficient evidence for anything unless you know who took it and when, and the photographer's motivation and reputation.

In the age of terrorism, jumping to conclusions based on a digital photograph can have terrible consequences if the act portrayed is not independently verified.

When it comes to our computers, the situation is far worse. Law enforcement officers often seize the computer of suspected wrongdoers to see what compromising material may have been retained. Our problem is almost all our computers have wire or wireless connection to the Web. We thus are subject to outsiders dumping things into our computers without our knowledge or, even worse, having our browsers hijacked and used by outsiders for committing a crime.

Most "cookies" placed in our computers are harmless and used by marketers to gain information about our search patterns and/or speed information from certain Web sites to our computers. Browser hijackings are not harmless; they are malicious programs. Purveyors of kiddy porn, financial criminals, and terrorists, all without our knowledge, could use our computers without entering our premises.

There have been news reports about a man jailed for child porn though he claimed a browser hijacker placed porno images of children on his computer. Without knowing whether this particular story is true, it is technically possible. Everyone is at risk from personal enemies and unscrupulous law enforcement authorities who will find it relatively easy, if they so choose, to place compromising material on our computers.

Evidence tampering and salting has always been a problem -- remember the Los Angeles police scandals a decade ago? The difference now is false evidence can be planted on anyone by a scalawag anyplace on Earth who has access to the Internet.

The new digital technologies also allow the almost perfect replication of voices, signatures and even works of art. Some biometric identifications, such as fingerprints, can also be digitally copied and misused.

It is important all those who reply on information that can be or has been digitized treat it with some degree of caution or even skepticism. In law, there are "rules of evidence" that must be followed in legal proceedings. The basic prerequisites of admissibility of evidence are relevance, materiality and competence. Evidence is considered "competent" if it meets certain traditional requirements of reliability.

The problem for law enforcement, the courts and even the press is that "traditional requirements of reliability" for pictorial, electronic and documentary evidence are no longer sufficient because of the new digital technologies. Relying on old standards will cause too many innocent people to be wrongly accused or convicted.

The solution is for those in the legal system, as well as the public at large, to demand collaborating evidence before coming to conclusions based on digital evidence alone.

Richard W. Rahn is a senior fellow of the Discovery Institute and an adjunct scholar of the Cato Institute.