Digital evidence: Today's fingerprints

Electronic world increasingly being used to solve crimes

By Michael Coren
CNN

(CNN) -- Police and prosecutors are fashioning a new weapon in their arsenal against criminals: digital evidence. The sight of hard drives, Internet files and e-mails as courtroom evidence is increasingly common.

"Digital evidence is becoming a feature of most criminal cases," said Susan Brenner, professor of law and technology at the University of Dayton School of Law, in an e-mail response for this article. "Everything is moving in this direction."

Digital evidence may play a significant role in the trial of pop superstar Michael Jackson on charges of child molestation.

Computers were among the items authorities in California seized during their search of Jackson's Neverland Ranch in November 2003. Once the territory of child pornography and computer fraud, digital evidence figures into every crime that can leave an electronic trail.

The changing world of technology is challenging courts to keep pace with new laws addressing potential evidence and preserving privacy, legal analysts say.

Police officials say that the U.S. war on terrorism may create a shortage of digital analysts at the local law enforcement level.

In the wired world, almost every crime intersects with the digital realm at one time or another.

"Digital evidence is simply a number of rows of ones and zeros ... whenever a computer is used to facilitate a crime," said Fred Demma, an expert on computer crime at the U.S. Air Force's computer research laboratory in Rome, New York.

Laptops, digital cameras, phones and hard drives provide mountains of raw data for experts to sift through, part of the expanding field of computer forensics.
A single file, credit card purchase or stray e-mail message can provide the proof that clinches a case.

"It's incredibly important," said Jeffrey Toobin, senior legal analyst for CNN. "Data such as e-mail has become indispensable, particularly in the prosecution of white-collar crime."

**Digital search**

Law enforcement officials hope to become as technologically savvy as the criminals they pursue.

"In modern day era of crime ... what you're going to find is a room full of computers, telephone lines and a network address and that's about it," Demma said. "In many cases, that's what you start with."

That may be enough, some investigators say.

The NYPD's computer crime squad, founded in 1995, has taken on a wide range of criminal activity -- from pedophilia to corporate espionage -- using a team of technicians and specially trained detectives.

Every year, it has put more and more people behind bars, said John Otero, the squad's commanding officer.

"If I were to tell you we are 100 percent caught up to the bad guys, I'd be lying," said. Otero. "We're always in a catch-up situation. The key is to be so close to their tail they don't have the chance to breathe ."

One section of Otero's 32-member squad scours the Internet for potential child molesters, drug dealers and others who may engage in illegal activities.

Another investigates suspicious activity by setting up electronic wiretaps and sifting through data logs that detectives can investigate within hours -- the shelf life for many electronic clues.

In one recent case, the NYPD seized a computer of a child pornographer, assumed his identity and continued the ruse to launch 43 spinoff investigations and arrests across Europe and North America.

"Ultimately, it's still an investigation and it comes down to good police work," Otero said. "All NYPD is using are the tools available to us to keep up with these guys."
Legal strategy

Law governing digital evidence still lags behind the reality of cyber-crime. There are few legal precedents to guide judges who often have little experience in the mercurial world of digital technology.

"It makes life difficult ... because law changes very slowly," said the University of Dayton’s Brenner. "We have judges who did not grow up with computers and so many do not understand the technology and issues it raises."

There is also a bottleneck of highly trained personnel to comb through evidence. Police report an acute shortage of detectives and lawyers trained in electronic police work.

"Part of the biggest obstacles we've had to overcome is having to get savvy lawyers and judges to understand what we do," Otero said.

The fight against terrorism means people with these skills will remain at a premium, potentially depriving smaller police departments of such personnel.

The demand is only likely to increase as the volume of cases with digital evidence increases, according to the Department of Justice.

"Cyber-crime is obviously something that is a national priority," said Steve Bunnell, chief of the criminal division at the U.S. attorney's office in Washington, D.C., which recently established a cyber-crime division.

"Computer crimes are something that crosses borders. ...There is really a premium on getting the right and left hand working together," Bunnell said.

Courtrooms and universities are welcoming more lawyers specializing in electronic crime. They are setting the stage for the evolution of "cyber-law" as the debate over digital evidence -- and what limits may be put on it -- is raging among legal scholars and law enforcement, Brenner said.

"Our search and seizure laws evolved in a bricks and mortar era and therefore are not well suited for a digital environment," she said.

Police must now re-evaluate how they obtain evidence. Information obtained in an electronic search can be thrown out if it violates the Fourth Amendment's protection against unreasonable searches and seizures.

But how far does protection extend on a computer hard drive? What about e-mails and files sent over the Internet?
Some judges at the state and federal level have restricted the conduct of electronic searches by law enforcement, insisting officers follow certain procedures or methodologies. Police and prosecutors disagree, arguing that a judge can only issue warrants, not dictate its terms.

"This is a new issue," Brenner said. "In the real world, police go execute a warrant to find stolen tires ... and bring them back, end of story.

"In digital searches, police search for a computer, find the computer, bring it back and then subject the data on it to various kinds of searches."

The thorny questions about privacy and the sanctity of personal data loom as digital technology is inextricably linked to our daily lives.

Brenner predicts we will need to revisit the laws designed during an earlier, simpler age.

"I'm not sure you can say we 'choose' to use technology today," she said. "And I think the situation will only become that much worse."