Written by **Beverly K. Eakman** on May 25, 2011

Service Versus Surveillance: Has Computer Technology Outpaced the Legal System?

First, the short version: Privacy? "Fuggedaboudit!" You can encrypt your messages, lock your laptop and password-protect your various accounts till your fingers fall off. You can purchase "gee-whiz" software packages to control spam and spyware, construct endless filters to screen unwanted e-mail and phone calls. You can install parent-control devices on your TV, inputting "prohibited" keywords till you're blue in the face. You can report abuse and "scrub" old computers.

Still, you will come up short. In fact, you may wind up creating such a maze of conflicting virus-protectors, screening protocols and passwords that your computer, TV, telephone and DVR are rendered inoperable and non-repairable, especially if you have "bundled" these services. Refusing surveys and other cross-matchable data-collection instruments will help you temporarily. Evading surveillance cameras, directional laser-based detection devices, shredding documents and purchasing sensors to stem eavesdropping and voice/facial recognition may buy you time … or ensure that you "do time," depending.

Welcome to the world of computer forensics.

Those who watch TV programs like *CSI* tend to think of forensics as applying only to crime-solving techniques. But the term has morphed into "figuring out how the heck stuff works."

Therein lies the problem. The genius who fixes your computer can also create an illicit backup file that takes your financial data and identity to the cleaners. The legal system will be helpless in the face of technologies that it doesn't comprehend, Top Secret military projects notwithstanding. Everyone is essentially "flying blind" because, as new ways of accessing and manipulating data are discovered, even fewer legal precedents and guidelines are in place. The Supremes might know who leaked, stole, or transmitted data and who eluded detection devices, but chances are they can't explain how it was accomplished. Even when they do, they throw up their hands in the face of a Digital-World-on-Steroids that recognizes no legal boundaries.

It's a twenty-first-century *Catch-22*. It's like knowing, technically, how your great-grandmother canned tomatoes, but even following her directions word-for-word never daring to actually eat the product two months later for fear of poisoning yourself.

Last weekend a perfect example surfaced. It was buried inadvertently in a news story about Dominique Strauss-Kahn, the International Monetary Fund (IMF) chief who allegedly raped and sodomized a hotel maid at the Softel Hotel in New York.

Now, far be it from most of us to condone sexual assault, but two interesting facts emerged from Chris Hawley's May 21 story detailing this and other horror stories from hotel maids and housekeepers employed in tony hotels and resorts nationwide. Most such crimes, the reporter found, go unreported for fear of retribution. But labor groups have heard them loud and clear.

That said, two factoids jumped off the page:

- That viewing pornography is well-known to be a prelude to sexual assaults, even though political correctness dictates otherwise, referring to porn as a "victimless crime"; and
- That hotel management frequently assigns male housekeepers to rooms *if a computer divulges* that the guest in question has viewed pornography in his room.

Both revelations are huge, the first because the public has been lied to concerning the real-world effects of pornography, and the second because computers apparently can, and do, contain specialized software and hardware that make it possible to spy on the television activities of guests (and maybe other things, too), not just after-the-fact when the guest must pay up, but *in real time.*

Most people have long known about the mini-cam, which can be installed into a lamp or other common fixture, as well as key-stroke and e-mail spying by employers, or "cookies" deftly inserted onto computers — usually under the umbrella of marketing or security. But few expect that hotel management would go so far as to monitor, *in real time*, one's television-watching, leaving the door wide open to eavesdropping on video-conferences and more.

There is a difference, of course, between private and government surveillance, but the lines are becoming increasingly blurred as government partners with the private sector, thereby compromising the concept of entrapment, thanks to the overabundance of pathways and signals through which data can now flow.

In 2002, the legal system was still trying to decide whether the Internet, for legal purposes, was like a public park, a public telephone (as in an old-style booth) or a freeway. Or had the Internet (not merely the PC) already evolved into a form of private property, in which case it carried some measure of privacy protection? But even if such protection did apply, what about minor children, especially when their parents remain clueless about technology? To complicate matters, private property rights already were being dismantled piece by piece by the same government that was supposed to be concerned about protecting your "privileged" information.

When I was detailed to the Justice Department's civil rights office, I responded to letters of complaint from the public. One month, out of the blue, I noticed five separate messages from individuals in different states complaining that no one at Justice was returning phone calls left on a toll-free number apparently aimed at stopping (i.e., tracking down) sources of fraud and pornographic e-mails sent to private homes with children. *Toll free number? What toll-free number?* I wondered.

I combed the e-mails again, and one person gave an actual number. So, I called it. Sure enough, the

computerized voice instructed the caller to describe the nature of the problem and leave a name and call-back number. Except no one had apparently returned any calls. *What the ____?*

So, I did some sleuthing. Turns out that while the intention was praiseworthy, the Department had no idea how to respond, and no means of tracking down sources emanating from all over the world, then bounced around the World Wide Web before landing in somebody's Inbox or Junk file.

Nine years later, not much has changed, except digitalization — which turned out to be a game-changer making any resolution even more difficult. Whereas the now-obsolete POTS (plain old telephone system) relied on a mass of switches which routed calls that could at least be easily traced, the newest computerized routing systems involve fiber-optics, cables and digital signals utilizing secondary addresses and IPs (Internet Protocols). Instead of tracing a call, for example, marketing enterprises "track bandwidth," usually surreptitiously, in order to later sell you something either by snail-mail or Internet or telephone — all easily located. Often you will find a long disclaimer when you access a site to purchase something — a pop-up message so complicated that most people just click on "I agree" to be done with it and move on. Online retailers and Facebook are just two examples. The method is known among experts as "affinity marketing." TV-polling systems don't need to ask your permission; they just go to the service provider.

Meanwhile, a hotel chain or cruise ship may create dedicated TV channels to services of various kinds: for example, invitations to attend a lecture in a certain dining room, to sign up for this-or-that promo, to list your purchases and room charges to date. It's all accessible via the room's remote control. Then there's on-demand TV that sometimes includes recently missed episodes of your favorite show, adult entertainment, kids' shows, food networks, and whatnot.

Some establishments may block or decline certain categories of channels entirely: say, "adult" channels or even religious broadcasts. There's probably an override. But most people are clueless concerning high-tech gizmos. They don't know how computers work. Indeed, most never knew how their 1950s-style black telephones worked, either.

As for those awesome, wall-sized touch-screens on modern crime-dramas such as *NCIS: Los Angeles*: Yes, they exist. They really can pull up a driver's license obtained under an alias and juxtapose it with a fingerprint or an enlarged and enhanced view of the same person emerging from a vehicle on the freeway via a revenue-camera (fraudulently called a "traffic cam"), then match for facial recognition — all in the name of security. But this is hugely expensive (*government to taxpayer: So what?*), and, more to the point, leads to the same technologies being available in perpetuity for ulterior purposes. According to a high-level source, who wishes to remain unidentified (for obvious reasons), increasingly software and hardware are compatible so as to share information.

Thus, if some day a video conference shows you decrying, say, gay-pride days, or sharing religious messages (*read "hate speech"*) or even denouncing the management where you work — what do you call that? Is it discriminatory? Is it "spying"? Is it "trespassing on private property"? Free speech or assembly?

Now, one can make a case that possession or transmittal of child porn is illegal, or in the case of a hotel, that the security of employees is at stake. But surveillance is still surveillance. Today it's child porn, tomorrow it's Christian broadcasts by the politically inconvenient.

The bottom line is that *technology is never un-invented*. Once deployed, we're stuck with it. The tie-breaker could be national security, "ongoing investigation," or even trespassing and "probable cause,"

but in our increasingly relativistic society, at least the last two are increasingly seen as a throwback to an earlier time — anachronisms.

In essence, we have stripped our nation of the very standards Congress might once have used to determine an updated legal basis that assures individual rights in a constitutional Republic.

Beverly K. Eakman began her career as a teacher in 1968. She left to become a science writer for a NASA contractor. She went on to serve as a former speechwriter for the Voice of America and do research-writing for two other federal agencies, including the U.S. Dept. of Justice. She has authored six books, scores of feature articles and op-eds covering education policy, mental-health, data-trafficking, privacy and political strategy. Her most recent works include **Walking Targets: How Our Psychologized Classrooms have Produced a Nation of Sitting Ducks** *and the blockbuster 2011 Edition of her seminar manual,* **How To Counter Group Manipulation Tactics** *(Midnight Whistler Publishers). Mrs. Eakman can be reached via her website at* BeverlyEakman.com/.