The World's Largest Information Center

I asked ten people "Who has the world's largest information center?" and got the following replies:

1) "I don't know and I don't care." (3)
2) "NASA—who else needs to know that much?" (2)
3) "Oliver North—before he shredded it all." (1)
4) "The United Nations or the Pentagon." (1)
5) "The IRS—they audited me this year." (2)
6) "Probably Uncle Sam. Who else wants to know everything about everybody?" (1)

I suppose it is comforting to know that 10% of the population can guess correctly that the US government is the world's largest information center. Not only is Uncle Sam the biggest information depository, he is also the largest publisher of information. When I asked my ten subjects "What one thing has enabled the US government to become the world's largest information center?," the percentage of subjects responding "technology has enabled the US government to become the world's largest information center" jumped to an impressive 80%. From this little exercise, one could draw the following conclusions:

1) In spite of the fact that the information technologies are still in their infancy or as Apple Computer Chairman, John Scully, declared in a recent keynote address, "We're at about the same stage of evolution...as the automobile industry was in...1917," people know that technology makes possible both the creation and the dissemination of information.
2) The fact that 80% of those asked know that technology has made the government a massive information center tells us nothing of what they understand about how the government uses technology to maintain its standing as the world's largest information center.

How many taxpayers know and understand the implications of the fact that they have enabled their government to embrace the new technologies to the tune of $17 billion dollars annually? According to the Office of Management and Budget, part of that $17 billion is used by the agencies of the Federal Government to purchase over 200,000 microcomputers per year. One would think that with a $17 billion dollar expenditure, the government would not rely on paper. Ironically enough, according to the May 1988 issue of *Government Executive*, the government still does most of its work *on* paper, *with* paper, and *in* paper. This, in spite of the fact that an aura of belt-tightening supposedly exists when government is being asked to do more with less. Aren't the new technologies supposed to be a "godsend" in such an era because they enable fewer people to do more work faster and efficiently?

Although there are those enthusiastic souls who see technology as a godsend with unprecedented potential for saving taxpayers money, very few of these enthusiasts ever mention the great potential for abuse that exists as the result of an annual $17 billion dollar government investment in the new technologies.

Not long ago, the government used its arsenal of technologies to ferret out fraud in the Department of Health and Human Services. The agency's giant IBM computer technologies were used to compare a list of everyone on the Social Security pension rolls with a comparable list of every Medicare recipient who had died. The search/comparison project uncovered over 8,000 dead people to whom Social Security pension checks were still being sent. "In some cases," Phillip Elmer-DeWitt was quoted in *U.S. News and World Report*, "the checks were being cashed by impostors, and the U.S. Treasury was being robbed."

Identifying and removing the deceased from Social Security pension rolls is saving U.S. taxpayers over $50 million; so far, over 500 people have been convicted on fraud charges. However, in order to identify the cheaters, the computer search opened the records of more than 30 million innocent, law-abiding American citizens. There is no doubt that this project—in a democracy—constitutes an invasion of a person's privacy; it may also be a violation of the Constitutional Law.

In compliance with the Privacy Act, did the Department of Health and Human Services request consent from the individuals whose files were opened? Hardly. All HUD did was print a notice of their plans to ferret out fraud in the Federal Register.

Because the existing and emerging technologies enable governments and organizations to do things that could not be done before, there is incredible potential to abuse the civil rights of individuals and very few safeguards in place to protect personal privacy and freedom. When technology makes the handset of the phone on your desk—if it is part of a computerized telephone system—always a "hot" microphone whether on the hook or off, with the capability of recording conversations on the phone and in the room, what protects you from the risks inherent in how the information recorded by this technology is used? Even if a recorded conversation in your office cannot be used in a court of law, imagine all the other ways it could be used by friend and foe alike.

Suzanne E. Lindenau
Editor-in-Chief