DP 1/17 5.60.01

COMPUTERS

Don't Tread on My Data

Protecting individual privacy in the information age

Richard Kusserow is a new kind of gumshoe. He is the master datatective of the Reagan Administration. Soon after becoming inspector general for the Department of Health and Human Services in 1981, Kusserow decided to crack down on fraud. The new boss directed that the agency's mammoth IBM computer system be used to compare a list of everyone on the Social Security rolls with a compilation of every Medicare recipient known to have died. The project uncovered 8,000 dead people to whom Social Security checks were still being mailed, like clockwork, once a month. In some cases, the checks were being cashed by imposters, and the U.S. Treasury was being robbed.

Kusserow's search—one of thousands of computer matching projects conducted by the Administration—points up the power and the perils of computer data banks. Removing the deceased from the Social Security rolls has saved taxpayers about $50 million and led to more than 500 convictions for fraud. But to ferret out the cheats, the computer had to open and examine, however briefly, the records of more than 30 million presumably innocent Americans. That, say civil libertarians on both sides of the political spectrum, is an invasion of privacy and comes perilously close to violating the Constitution, particularly the Fourth Amendment "right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures."

Individuals' papers and effects today can be scattered far beyond their physical persons and homes. The U.S. Government alone maintains some 3 billion personal computer files, a treasure trove through which an army of bureaucrats can search and snoop. Even more extensive are the records maintained by local governments, private credit agencies, banks, insurance companies, schools and hospitals. It is hard to live in modern society without leaving a long, broad electronic trail. Computers record where you reside and work, how much money you make, the names of your children, your medical and psychiatric history, your creditworthiness and indebtedness, your arrest record, the number of bathrooms in your home, the phone numbers you dial and even the time you last used a street-corner bank machine.

What privacy rights apply to this vast dossier of data? When can it be searched, shared or published? And if the information it contains is outdated, injurious or just plain false, what redress does an individual have? Not much, it turns out. Ostensibly, citizens are protected from overzealous use of the Government's computer files by the Privacy Act of 1974. It requires the Government to obtain the consent of individuals if an agency collects information on them for one purpose and then uses it for another. In most cases, however, the agency merely has to publish a notice of its plans in the Federal Register.

Many of the ways in which the Government uses its data banks seem at least reasonable. The Internal Revenue Service, for example, uses computer searches to withhold tax refunds from people who have defaulted on federal loans. But other intrusions on privacy are far more dubious. One agency concerned with press leaks matched the telephone records of its employees to the phone numbers of prominent Washington reporters.

Private data banks offer further opportunities for electronic surveillance, and the public has few safeguards against prying by companies. The only major law pertaining to private computer files is the Fair Credit Reporting Act of 1970. Under its provisions, credit-rating bureaus must give people access to their own credit files and the opportunity to correct mistakes. But the law is weakened by the fact that companies are not required to inform people that files on them have been opened.

The spread of computer data banks would be less disturbing if the information in them were not so freely passed around. Insurance companies, for example, exchange the medical histories of prospective customers. Credit bureaus often sell their data to employers who are screening job applicants. Other companies have developed computer blacklists that help alert landlords and physicians to prospective tenants and patients who have a history of filing lawsuits.

New efforts by lawmakers to address concerns about computerized invasions of privacy are still embryonic. A bill to create "data integrity boards" to oversee Government computer matching programs is expected to pass Congress this year. But civil libertarians argue that tighter restrictions are needed. The alternative, they say, is a frightening drift toward an Orwellian society in which Big Brother is always watching. Says Jerry Berman, director of the Project on Privacy and Technology of the American Civil Liberties Union: "If you have a surveillance system looking over a wide range of activities, the message is clear: don't deviate. That means don't cheat on your taxes—which is good. But it also means don't dissent." The danger, though not new, is intensified. As useful as computers are, the increasing pressure they put on personal privacy could threaten personal liberty. —*By Philip Elmer-DeWitt*

CYNTHIA JOHNSON

Inspector General Kusserow with the new tools of his trade

To the extent that Americans of 1787 thought about privacy, they conceived of it in terms of property, not individuals. Society was based on property, and restrictions on its acquisition or retention were resisted. Bans on undue government searches were common in the states. But it was assumed that society could enforce shared norms of morality, either through laws or simply through meddling. Obscenity, blasphemy, adultery were all restricted. Anyone who did not like the community's values was still free to do as he pleased, but only by exercising his freedom to move on.