BOOK REVIEW:

Data Banks & Privacy

Databanks in a Free Society, by Alan F. Westin and Michael A. Baker. Quadrangle Books, 501 pages, $12.50.

By Abner J. Mikva

Professor Alan Westin has written a book with a surprise ending, an ending, quite likely, that surprised even the author. In his book *Data Banks in a Free Society: Computers, Record-Keeping and Privacy*, Professor Westin and his associate, Michael A. Baker, conclude that the computers have not eaten up our privacy—yet. Indeed, Professor Westin finds the fact to be that data banks have not yet caused any erosion of our civil liberties, particularly, if we do not "romanticize the pre-computer era as a time of robust privacy, respect for individuality in organizations and 'face to face' relations in decision making."

It is true that the FBI and the House UnAmerican Activities Committee (since sanitized in name to the House Internal Security Committee) both managed to fill their houses with dossiers collected, filed, collated and retrieved without the use of modern machines. Even when the army used some computer technology in its super-spy activities on officeholders and other civilians a few years ago, hardly any use was made of interfacing techniques which could have hooked up their material with that of other domestic spy outfits like the FBI. Most of their input came from sleuthing rather than data-banking. All told, the author's conclusion seems tenable: that while the right to privacy has long been a pigeon for government snooping, so far the technology of data banks has not escalated the problem. The important phrase is "so far." The technological developments make all the concerns legitimate, even if premature. The apathy about the problem, however, is caused only in part by the fact that it is in *futuro*. Another cause is that the right to privacy itself is so poorly defended and regarded.

Secret Invasion

Alan Westin is a good enough civil libertarian to know that the right to privacy is more difficult to maintain because the interdictions to it are frequently unknown or muted as to their impact. A citizen knows when his individual right to assemble has been taken away. He may or may not know that some government agency has put together an accurate or inaccurate dossier of how the citizen spent his life. It is the *ex parte* nature of the problem which causes so much concern. That is why the struggles to preserve the right to privacy so frequently take on a theoretical, almost ephemeral nature.

People do not know when someone is tinkering with their privacy and certainly do not know when the information that has been collected is accurate or inaccurate. If we start with the simple (!) income tax return, the problem becomes apparent. The government has a legitimate interest in the life style of the taxpayer only to the extent of determining whether that taxpayer is paying his or her fair share of taxes. If, however, the Internal Revenue Service turns over the information on the return to the FBI, which concludes that the taxpayer has a penchant for contributing to left-wing charities, and if the taxpayer is subsequently denied a job or a promotion based on an adverse FBI report, then that taxpayer has been tinkered without ever knowing about it. And if the FBI confuses the Friends of the Atlantic Speaking Union with the Friends of the Soviet Union, that taxpayer has had a compound tinkering from which he or she may never recover.

Aside from the almost mystical fear of any kind of big machines, there was and is reason to be concerned about the computer impact on these problems. Modern technology makes data so easy to collect, exchange, store and retrieve that such data becomes omnipresent and indestructible matter. (When the Army Intelligence Corps were finally persuaded that it was not right to spy on civilians or even congressmen, they agreed to destroy their databanks—except for one printout. Even this neophyte in computers knows that one printout can recreate the entire databank instantly.)

Credit Records

It is not just official government snooping that portends the difficulty. In the past, an argument with a creditor (legitimate or illegitimate) created a manageable difficulty. That same dispute with an interfaced computer network among all the nation's creditors could create instant and permanent discredit.

Not too long ago, a Chicagoan paid by a perfectly valid check for some antiques which she had purchased out of town. The check suffered some physical damage before it went through her bank's identifying machine. When the machine spit out the check, events were set in motion which finally led to the woman's arrest and jailing. The bank reassured everybody that the mechanical failure of the computer was a fluke which would not happen very often. They found it necessary to give the woman some additional assuagement by way of a cash settlement.

That "horrible" is paraded only to show the results of a simple failure of one machine. Actually the woman may continue to have credit troubles wherever she goes, since the bad check charge may well have been interfaced to a lot of other computer systems of a lot of other credit institutions. The technology has not yet learned how to retrieve and destroy such boo-boos. Notwithstanding this potential for evil, Professor Westin finds that so far, the interferences with privacy are largely man-made. The real problems are still ahead, and therefore avoidable.

Law Needed

While Professor Westin offers some very important ideas on how to avoid a future computer shock, it is clear that effort will have to be achieved in the political arena rather than in academia. Unfortunately, the right to privacy does not have much of a political surface. Organizations like ACLU will have to do a better job in sensitizing people to the importance of the right to privacy and the potential for its loss. Ultimately, we must build a statutory framework which limits the amount of information that is requested by government and by private sources, which defines specifically the purposes for which such information may be sought, which severely limits the situations where such information may be exchanged or passed on to other agencies or organizations, and which gives the individual the right to inspect such data on a regular basis to determine its accuracy and relevancy.

That kind of legislation will only come about when people are *very* angry about their loss of privacy, real or threatened. Unfortunately that may occur only after the computers have eaten a much bigger chunk out of the right to privacy than they have thus far.

Abner J. Mikva, a Chicago attorney, is a former member of Congress. He is a member of the Illinois ACLU's Advisory Committee.