

Computers and the Threat to Privacy

Information, virtually all of it stored in computer databases, is the lifeblood of the public and private bureaucracies that dominate postindustrial society. The quest for every-greater levels of efficiency has led to a scramble to obtain more and more information about individual citizens and consumers. Many observers fear, however, that this trend poses an increasingly serious threat to privacy, a right that, clearly, is precious to most Canadians.

Whereas in some countries citizens are comfortable with the government keeping population registers, for example, many Canadians see the government as potentially the greatest offender of private information. The massive data banks on taxation, census information, unemployment, police records, and marriage, birth and death registers contain a plethora of information. By linking these data banks, the government can learn intricate details about each and every citizen.

Most would agree that a certain amount of snooping is appropriate, especially when it comes to such socially approved ends as tracking down people engaged in laundering drug money, but there is a vast gray area in which the limits of privacy have yet to be adequately defined.

The mistrust by Canadians in our government may sometimes be well-founded, as in a recent case involving Revenue Canada and the Employment Insurance Commission (EIC). In this case, the EIC received data collected by Revenue Canada on customs forms filled out at the border by people entering Canada. The reason behind the release of this information was to catch people who were collecting employment insurance when they were out of the country and thus unavailable for work. Though the scheme was economically successful (the EIC recovered \$98.2 million), the Federal Court of Canada ruled that the Revenue Department erred when it released data on all people entering Canada, and the practice has since been deemed illegal (McCarthy 1999).

Critics who wonder whether the safeguards that we have under the Privacy Act are really important need only look to the Orwellian steps now being taken by the Thai government. By 2006, information on “65 million Thais (was stored) in a single, integrated computer network. Each citizen over age 15 (is) required to carry a card bearing a color photo... (and) and identification number” (Elmer-Dewitt). With this number, the government will be able to obtain the citizen’s fingerprints, height, home address, parents’ and children’s names, marital status, education, occupation, income, nationality, religion, and, potentially, criminal records.

Despite the possibility for abuse by governments, Canadians should probably be more concerned with the personal information that we freely give to businesses because this practice may pose a more immediate threat to personal privacy. Some of the largest data banks that include personal information belongs to the Loyalty Management Group Canada Inc. the owners of the Airmiles program. Over half of Canadian households now use their Airmiles card to rack up travel points through purchases at participating businesses. These businesses have access to the personal information that card holders supply

when applying for the cards in addition to the spending habits at their own business. These businesses can also get access to the data from the other participating businesses by purchasing these data from the Loyalty Group. The viewing preferences (Blockbuster Video) combined with the alcohol consumption and spending (Ontario liquor stores), credit limit (Bank of Montreal Master Card), magazine subscriptions (Maclean Hunter), gas purchases (Shell Canada) and kind of clothing bought (Holt Renfrew) paint a vivid picture of you and me (Noble, 1998). Some more examples:

“The Employers’ Information Service, a company based in Gretna, La., is creating a massive data bank on workers who have reported on-the-job injuries. For a fee, employers can request a report on prospective employees, including a history of prior job injuries and a record of worker’s compensation claims and lawsuits” (Lacayo, P.34).

“Public uproar forced Lotus Development ... and Equifax ... to shelve their scheme to market a data base that would have allowed anyone with a personal computer to purchase a list of names, buying habits and income levels of selected households” (Ibid).

“The American Business Conference and the National Alliance of Business have... joined with the Educational Testing Service...in creating a pilot program for a nationwide data base of high school records. It would give employers access to a job applicant’s grades, attendance history and the ancient evaluations of teachers” (Lacayo, p.36).

“Until recently...Equifax sold lists of consumers who used their credit cards more frequently than the average. Combining that with census data, the company then used a statistical model to estimate the general range of each card user’s income, though not to specify the actual amount” (Lacayo, p. 37).

“Three giant credit bureaus — TRW, Equifax and Trans Union —dominate the consumer-data industry, which also includes about 450 smaller outfits. Every month the Big Three purchase computer records, mostly from banks and retailers, that detail the financial activity of virtually every adult American. TRW and Equifax each have 150 million individual files” (Ibid). The industry defends its operations principally on the basis of its property rights to the data that it has purchases.

On the other hand, “critics complain that the reports are frequently riddled with errors and that it is difficult and expensive for consumers to correct or even know about them. Earlier this year Consumers’ Union reported that nearly half the credit reports it studied from the nation’s largest credit bureaus contained some inaccuracies” (Lacayo, p. 38). In response to such charges, TRW is now supplying consumers with free copies of their credit files upon request, but Trans Union and Equifax have refused to follow suit.

Another controversial technology is called Caller ID. Phone “customers get an electronic screen that displays the phone number of every incoming call” (Lacayo, p. 40). The service helps reduce obscene and harassing calls and allows businesses to be sure that orders are legitimate. But it also allows businesses to record and sell the numbers of callers to 800 numbers, and it may “discourage anonymous police tipsters and callers to telephone hot lines that

serve drug abusers, runaways and other people in trouble” (Ibid).

In spite or resistance to these pools of private information, the means of accessing some basic data about individuals seems to be growing easier. Through search engines on the Internet’s World Wide Web such as Lycos and Yahoo, anyone with Internet access can enter an individual’s name to look for his or her phone number, residential address, e-mail address, and—in some cases—a map showing where in a city that person lives. Anecdotal evidence suggests that unlisted numbers may even be available without restriction in some cases.

Sources

Elmer-Dewitt, Philip. “Peddling Big Brother.” *Time*, June 24, 1991, p. 62.

Lacayo, Richard. “Nowhere to Hide.” *Time*, November 11, 1991, pp. 34-040.

Markoff, John. “Remember Big Brother” Now He’s a Company Man.” *New York Times*, March 31, 1991.

McCarthy, Shawn. “Customs Wrong to Flag UI Cheats, Court Says.” *The Globe and Mail*, February 3, 1999.

Miller, Michael W. “More Households Dial ‘U’ For Unlisted.” *New York Times*, May 7, 1991.

Miller, Michael W. “Lawmakers Begin to Heed Calls to Protect Privacy and Civil Liberties as Computer Usage Explodes.” *Wall Street Journal*, April 11, 1991.

Mukenegge, Muadi, and Margaret Mannix. “Sorry, No Number,” *U.S. News & World Report*, June 10, 1991, p. 75.

Noble, Kimberley. “The Data Game”. *Maclean’s*. <http://www.macleans.ca/newsroom081798/cov1081798.html>. Accessed February 9, 1999.

Discussion Questions

What sorts of personal data should be kept private? Should data-gathering companies be allowed to sell information about your income? Bill-paying history? Medical history? Product purchases? Arrest history?

Should data-collection firms be required to ask permission from individuals before selling their names?

Is this an area in which government should play an active role, or will marketplace forces adequately protect the consumer?