Discussion

Eugene Oscapella
Office of the Privacy Commissioner of Canada

It is always difficult to beat the privacy drum about uses of personal information that individually may seem relatively benign. Privacy intrusions are somewhat like environmental contaminants. The odd release of a contaminant will not overwhelm the environment; repeated releases, however, will. Sometimes the environment cannot recover. In the privacy world, the phenomenon of small but multiple attacks on privacy, known as "privacy creep," is perhaps the most dangerous manifestation of today's many threats to privacy; it comes upon us quietly, minor intrusion after minor intrusion -- incrementally -- until there is almost no sphere of personal information or personal behaviour that is not under someone else's watchful eye. And because the effects are incremental, almost imperceptible in some cases, there is usually little public outcry.

And, unlike the environment, which can sometimes be regenerated, privacy often cannot. Once a person loses his or her privacy -- once information about them is removed from their control -- they have lost that element of privacy for good.

That is the approach we take to privacy. Individual intrusions may not appear to damage this fundamental human right -- the right to be let alone, as two American jurists described the right almost a century ago. Collectively, however, these intrusions threaten to bury any notion of privacy in a society increasingly dominated by computers, social welfare programs that involve governments in private activities, and hotly competitive private marketplaces.

That is the global context in which I make these remarks. That is the broader environment in which you must situate your thinking on the use of administrative information for statistical purposes. You must look at what is happening to privacy as a whole in society:

- The ability of private sector and government organizations to collect and manipulate personal information has increased exponentially. The much touted "information highway" now under development will expedite this process.

- In the name of efficiency, governments are collecting vast amounts of information and linking them; in the name of competitive advantage, private sector organizations are collecting and linking vast databases of personal information. The pressures for efficiency and competitive advantage suggest that the problem will grow, not diminish. The Knott paper highlights just how extensive data matching can be. The paper seems to confirm the very fears that people have -- that they will be tracked through the assemblage of material about them from a multitude of sources.

- Governments and the private sector are becoming less shy about violating the last bastion of privacy -- your body: drug testing, genetic testing.

- Your personal data have value for the private sector and for government; your personal data are someone else's treasure.

- People are becoming increasingly concerned about their privacy. In a 1992 survey conducted for the Privacy Commissioner of Canada and several other organizations, over 90 percent of those responding expressed at least moderate levels of concern about their privacy. Sixty percent felt they had less privacy than a decade ago; must deal with people's perceptions, even if distorted; and are increasingly conscious of the threat to privacy posed by technology, including data matching and the

potential abuses of the information highway -- such as transactional data.

■ Perceptions About the Adequacy of Legislation

It is important to dispel any notions that current legislation offers adequate privacy protection in Canada or -- I suspect -- in the United States. To argue that an activity of a government department protects fundamental notions of privacy simply because it does not violate current legislation overlooks just how weak many privacy laws are in Canada and, likely, in the United States.

In Canada, we have a law called the *Privacy Act* to regulate the collection, use, and disclosure of personal information by federal government institutions. Most provincial governments in Canada have enacted similar legislation to regulate provincial government institutions.

However, calling these "privacy" laws is somewhat misleading. Most of these laws set down minimum levels of conduct relating to personal information held by governments; in short, they protect *confidentiality* of information, not *privacy* of information. The only provision in the Federal *Privacy Act* that effectively limits what information can be collected about a person is Section 4. It reads:

> No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.

Thus, Section 4 is the "gateway" provision in the Federal *Privacy Act*. But it is a very broad gateway. If the *Statistics Act* says it is permissible to assemble hoards of personal information, this will be sufficient to satisfy the weak strictures of Section 4. Thus, the law does not truly protect privacy in the sense of the right to control who is able to acquire information about us.

Extremely intrusive forms of collection of personal information might, of course, violate Canada's constitutional privacy protection, but this is largely an assumption. Canada's *Charter of Rights and Freedoms* does not contain an explicit privacy right. To date, the *Charter's* protection against unreasonable search or seizure, in Section 8, has been interpreted as providing some privacy protection. However, this has occurred mainly in the field of criminal law and the courts might not interpret it as providing any useful level of privacy protection in the non-criminal sphere, such as that occupied by Statistics Canada.

Canada's privacy laws are designed mainly to regulate the flow of personal information, but not to protect privacy as such. For example, the Federal *Privacy Act* tries to do the following:

- ensure that persons from whom information is collected know the purpose of the collection;
- ensure that the information is as accurate, up-to-date and complete as possible;
- ensure that the information is used only for the purpose for which it was collected, or for a use consistent with that purpose;
- limit to whom the information can be disclosed; and
- allow the person affected to get access to the information and request its correction if the person thinks it is wrong.

These provisions are simply protecting confidentiality; they are not really protecting privacy. True privacy protection would require tighter strictures on the collection of personal information in the first place, not simply controls to protect confidentiality after privacy has been violated by the collection of the information in the first place. Remember that the East German STASI had an excellent record of preserving the confidentiality of information contained in millions of files on East Germans; few people would argue, however, that East German citizens had much privacy.

We must distinguish between confidentiality and privacy -- whether a promise of confidentiality sat-

isfies people's desire to be left completely alone. Does saying that "you must give information to me, but I won't disclose it to someone else," satisfy that need, or is something more required?

The Efficiency Argument

"Efficiency" seems to be the Holy Grail of government operations in many countries. But no democracy can tolerate efficiency at any cost. Police efficiency would arguably increase if we allowed cameras on every street corner, if we allowed the police to beat confessions out of people, if we denied people access to a lawyer until after interrogation, if we allowed the police to enter homes and search people and cars without requiring reasonable grounds to justify the search. Courts would convict more accused persons if we abolished certain evidentiary protections. People who defraud government welfare and health care programs could be more easily caught if we could freely match various databases held by government.

Yes, we would have a more efficient society. But would it be a more democratic society? Would the gains in efficiency outweigh the losses in democratic freedoms? Efficiency is a dangerous premise on which to base policy, unless the policy also honestly assesses the possible harms to other values as efficiency increases.

Increasing pressures to recover costs involved in obtaining census information may exert subtle, and perhaps not so subtle, pressures on organizations like Statistics Canada to ask questions that they might not otherwise ask if their mandate were simply to collect statistics necessary to satisfy the public interest.

Depersonalized Information

Many privacy problems can, of course, be avoided by depersonalizing information -- removing all information that connects it to a given person. However, depersonalizing information removes much of its value for researchers unless some means of encryption will allow the attributes of the information to be maintained without disclosing identities.

If data will be used in a way that no person can be identified, there is no real privacy issue, except to the extent that researchers can see individualized information. Who sees the personal information? How soon in the process is it depersonalized? If this information can be assembled with other information to develop a profile of a family or a small number of houses within a community, is that a privacy concern?

But is the use of the information to the point where it has been depersonalized a use without disclosure of the purpose? It does not appear to be a "consistent" use of the information under Canada's *Privacy Act.*

Information about identifiable groups, even if not strictly information relating to an individual, can still diminish privacy. If the information can be coupled with information from other sources to establish a profile of a small neighbourhood or to stigmatize members of a group (for example, an AIDS study that finds higher rates of infection among members of identifiable groups, such as gay men or prisoners), should it concern Statistics Canada that their information may be a part of the puzzle?

Consistent Use

Information collected for one purpose cannot be used for another without consent unless the use is consistent with the original purpose of the collection. (Section 7, *Privacy Act*). However, the *Privacy Act* can be overridden by other legislation. Therefore, if the *Statistics Act* allows use for another purpose, the rules in the *Privacy Act* do not apply.

Conclusion

Privacy is an important value -- a central value -- not one on the periphery of human existence. Will

the extensive use for statistical purposes of administrative records compiled for one purpose become -- or be perceived as -- just one more nail in the privacy coffin?

Ultimately, we must balance the value of information obtained by using administrative records with the *human* cost of obtaining that information. Does the value of the information obtained exceed the cost of violations of privacy -- real or perceived?

If perceptions about the privacy violations inherent in the use of administrative information for statistical purposes are distorted, it will be the responsibility of statisticians (and privacy advocates) to try to correct those misperceptions. In other words, you must be prepared more than ever to justify your actions by explaining your methodologies, your goals and your means of protecting privacy. And you must ask whether some information is simply too sensitive to be collected at all. Remember, above all, that research is a privilege. ■

"Protecting privacy in the computer age is like trying to change a tire on a moving car."
Chris Hibbert, Computer Professionals for Social Responsibility