Privacy Wrongs

Corporations have more right to your data than you do

By James Rule and Lawrence Hunter

Beverly Dennis is an Ohio grandmother and bona fide American consumer. Several years ago, she completed a questionnaire for the Metromail Corp., a direct marketing firm, in order to get free product samples. In her responses, she disclosed things like her income level, date of birth, the fact that she was divorced, her interest in physical fitness, and choice of "personal care" products, according to a lawsuit she is filing.

Dennis got more than free product samples. She got a "sexually graphic and threatening" letter from a convicted rapist in a Texas penitentiary. It turned out he knew quite a lot about Dennis, thanks to her questionnaire. He had written his highly personalized letter after being assigned the task of entering data from the questionnaire by a Metromail subcontractor. The use of inmates to answer 800-number calls, process consumer information, and even act as telemarketers, it seems, is widespread. "If it said [on the circular] it would be sent to a prison," Dennis later said in an interview, "I certainly wouldn't have filled it out."

Dennis is suing Metromail and the Texas criminal justice system for "outrageous disregard of public safety ... and dangerous invasion of privacy," among other things. It's hard not to feel that she has a point.

In fact, the manipulation of personal data that have been fed into the maw of the information society is, to cop an oft-used metaphor, like making sausage. If we really knew what was involved, we probably would want to have as little to do with the process as possible. The trouble is, we don't have that option. The relentless and systematic collection, compilation, and selling of personal information are built into the texture of everyday life. You may imagine that you can keep your distance from the vacuum-like data intakes by making shrewd choices about when, where, and to whom you disclose. But unless you're prepared to adopt a lifestyle like Theodore Kaczynski's, you're wrong.

Beverly Dennis, we trust, will bounce back from the nasty experience caused by the misappropriation of her data. But there's evidence that other types of misuse could be even more harmful.

With rising public anxiety about the victimization of children, for example, parents and other concerned adults are noticing how easy it is to get data that could be put to sinister use. To dramatize the point, a Los Angeles television reporter recently purchased from Metromail a list of 5,500 children, with their family names and addresses. Not to make the exercise too subtle, the reporter placed the order in the name of Richard Allen Davis, the man convicted for abducting, sexually assaulting, and murdering 12-year-old Polly Klaas.

It's hard to say precisely where these particular data originated. We do know that lists like this are compiled from such sources as the "birthday clubs" that retailers encourage parents to enroll their kids in, subscription lists for children's magazines, and toy store discount cards. What is almost certain is that whoever provided the information did not realize he or she was helping to feed a commercial data bank.

The most alarming uses of personal data often involve the least obtrusive forms of collection. Take getting a prescription filled. Increasingly, this involves feeding the patients' and physicians' names, along with other identifying data on the people and drugs involved, into a computer. Sometimes the acknowledged purpose of the data entry is to determine whether the charges are covered by insurance. In some places, laws require prescription data to be fed into government sys-

James Rule *is a professor of sociology at SUNY, Stony Brook, and is an editor of* Dissent. Lawrence Hunter *is a computer scientist at the National Institutes of Health, and the Washington, D.C. chapter chair of Computer Professionals for Social Responsibility.*

tems aimed at curbing prescription drug abuse. But whatever the ostensible purposes, people lose control over their information once it enters the data stream.

Often pharmacists sell information to "switchers"—operations that find buyers for such data. Some switchers, for example, collate information on users of specific drugs for sale to manufacturers of over-the-counter companion drugs. Then manufacturers direct advertising appeals to the targeted patients. Are these practices beneficial to patients? Conceivably, if the companion drug helps. Can they be dangerous? Quite possibly, for those who use the new medication without seeking medical advice from their own physicians.

But for most Americans, the issue here is probably not whether these practices are medically beneficial. It is that people whose data are appropriated in these ways have no say in what happens to their information. Indeed, it's not even legally theirs. Patients may have thought that their prescriptions were a matter between themselves and their pharmacists, but that idea is going the way of vinyl records. There is just too much demand for personal information, and there are too many sophisticated techniques for getting it.

Some may consider this the inevitable by-product of living in an information age. But these leaks can lead to authentic tragedies. John Doe, an AIDS sufferer, was a middle-level manager of the Southeastern Pennsylvania Transportation Authority (SEPTA). He had disclosed his condition only to his immediate superior at SEPTA, someone he trusted. But then other managers at the organization noted that Doe's charges on the employer-backed prescription plan were unusually high and had his account audited. The investigation showed that Doe had been getting prescriptions for Retrovir, an anti-AIDS drug.

The result for Doe was stigmatization at work over matters that he had every right to keep to himself. Doe had maybe a year left in his work life, his attorney Clifford Boardman told *Newsday*, and every day was important to him. This disclosure took away his peace of mind. A federal jury awarded Doe $125,000, but the verdict was overturned on appeal. "We hold that a self-insured employer's need for access to employee prescription records ... outweighs an employee's interest in keeping his prescription drug purchases confidential," the U.S. Circuit Court of Appeals concluded.

Businesses are increasingly realizing there's a gold mine in personal data. Fortunes await those who can devise slick ways for distinguishing who should receive consumer credit, and on what terms; or for identifying profitable customers for insurance companies; or for specifying the best targets for marketing campaigns. These incentives have led to the growth of vast industries that depend on personal information as the essential raw material.

The sources for the data are all but endless, and often unobtrusive. Every call to an 800 number is apt to disclose the caller's phone number, giving resourceful data collectors access to the caller's name and address. One phone company recently created an electronic system that flashes information about the social characteristics of the caller's neighborhood. Internet transactions and website visits also may enable data collectors to infer the caller's identity. Every product coupon submitted for a rebate, every warranty slip filed with a manufacturer, every credit card sale—almost any identifiable fact about an American consumer—may provide grist for the commercial information mills.

Not all the sources are commercial enterprises. Charities, magazines, hospitals, and countless other not-for-profit organizations sell their data. Activist groups from right to left often sell lists of their supporters or trade them with other organizations. The U.S. Postal Service now routinely releases customers' change-of-address information—typically without their knowledge—to businesses who want it.

State motor vehicle registrars have long realized that records they compile—under legal compulsion—of accidents, driving infractions, and the like are valuable to insurance companies. Many states turn a pretty penny releasing driver data to insurance companies and the organizations that serve them. It makes financial sense; millions of requests per year at several dollars apiece help offset many a state budget deficit.

Record Sale

A typical mailing list company trumpets the availability of information on "83 million families, selectable by income, age, credit card use, mail-order buying, number (and age) of children, type of automobile, type of home. . . ." For an additional price, the same broker will provide "ethnic name selection," guessing the ethnicity of those in their databases by statistical analysis of names. Customers may wish to select, for example, names and phone numbers of all the black accountants in Washington, D.C., or contributors to gay charities, or purchasers of products for incontinence.

The ability to deal with vast numbers of individuals, while still attending to the fine detail of individual cases, yields stunning capabilities. And it's most alarming with medical data. The rise of third-party payment for medical needs and intense competition—among insurers, employers, and other businesses—to avoid people who might develop costly diseases have

fueled ferocious appetites for personal data.

In a case reported recently in *Time*, for example, a banker serving on a state health commission pulled a list of cancer patients in his area, determined which ones had loans with his bank, then called in the loans. And as with the AIDS sufferer mentioned earlier, prescription and other medical records are increasingly accessible to companies carrying medical insurance for their staffs. This dual role—employer and provider of medical insurance—tends inexorably to bring data together from relationships most of us would like to see hermetically walled off from one another.

In April 1996, *Newsday* reporter John Riley told the story of Veronica, a patient whose psychotherapy for depression was covered by her employer. Like many in the same situation, Veronica was alarmed to learn that, to extend the treatment, her therapist had to provide details of her problems to the managed care company paying the bills. Routinely, Riley writes, "doctors, patients and pharmacists ... must feed patient information up the system's food chain to insurers who may, in turn, share it with each other, with employers and with information vendors in a virtually unregulated process."

One's choices of video rentals are better protected under current American law than one's medical records.

This is not to say the manipulation of personal data has no advantages. We can be offered useful products and services we would otherwise miss. But what is at stake are the legal and social arrangements that will shape technological changes now in course. The current framework simply doesn't reflect the realities of a world where personal information has become the essential raw material for several major industries.

Of course, there are some important protections for personal information. The Privacy Act of 1974, which gave individuals access to data held by government agencies and allowed them to challenge its accuracy, was a positive step. If this law has a salient flaw, it is its failure in practice to achieve what was a key element of its original intent—to prevent data collected for one purpose from being used for other purposes that may not suit the interests of the provider.

Nothing so comprehensive as the Privacy Act exists for private-sector data. Coverage is piecemeal and chaotic. The occasional checks on appropriation of personal data—such as the right to review your credit record to make sure it's accurate—found in one sector are lacking elsewhere. As medical privacy specialist Sheri Alpert has commented, one's choices of video rentals are better protected under current American law than one's medical records. Under the "Bork law," passed after that judge's video rental choices were revealed during his Supreme Court confirmation hearings, video customers have the right to "opt out" from disclosure. In most other commercial areas (most medical contexts included) personal data belong to whoever has possession of them. Thus many hospitals, like the pharmacies we mentioned earlier, sell personal data from their records.

Americans are certainly realizing their privacy is increasingly at risk. In September, the database firm Lexis-Nexis found itself in the midst of a firestorm of public complaint after people discovered the firm was selling access to individuals' data—Social Security numbers, maiden names, addresses, and the like. Librarian Robert Gitlin told the *Los Angeles Times*, "It's private information that I don't want released without any opportunity to consent."

Though worsening, this problem is not new. For years, many have sought omnibus legislation to establish a blanket right to privacy. They have failed, though, because privacy is a contested value; the interest in protecting personal data often collides with other legitimate interests. My desire to keep my medical history to myself, for example, will always be at odds with the interests of insurers in auditing the care I receive. Any reasonable policy would give both privacy and "right-to-know" interests their due.

Righting the Wrong

That's why we propose the creation of personal property rights that would supersede the commercial exploitation of personal information. Without express authorization from the subject, no personal data could be sold or traded from any file for any commercial purpose. Release of credit card data to credit reporting agencies, "switching" of prescription information for marketing purposes, or the resale of records from mail order firms to direct marketing firms would all

be prohibited—unless the release of such data was explicitly authorized by the individual in question.

The immediate result of such a principle would be a new—and entirely healthy—set of choices and tensions. People would have to take careful stock of their interests in the use of their data, weighing privacy interests against other considerations. Imagine, for example, a consumer put off by a credit bureau's collection of information on her retail accounts, or unable to resolve a dispute with the credit bureau over her records. She could choose to prevent the release of further data to credit bureaus, or to prevent the current bureau from selling further reports. The bureau might then have the right to report that the record was sealed at the consumer's request, but no more.

Of course, consumers would have to weigh the consequences of their decisions—forgoing the benefits of having a credit record, or risking that creditors would choose not to do business with them or would charge them a higher rate of interest. Similarly, those denying their medical histories to insurance reporting firms might well find access to some forms of insurance blocked, or the costs of coverage raised. Because many consumers would probably choose to reap the benefits of releasing their information, commerce would not come grinding to a halt. But this system would place the onus of decision squarely where it belongs—on the individual who provides the data.

The information industry would then have incentives to make their activities acceptable to the people whose information they take, instead of just collecting it without their knowledge or permission. The credit reporting industry would have to sell its services to the public—presumably by promising more accurate, open reporting practices and by calling attention to the benefits of having an active and complete credit record. Direct marketers would have to convince the public that their attentions were, on balance, an advantage to the customer. Businesses would need to convince customers that the sale of their information really worked to their advantage—if not, customers would simply refuse their permission for release.

One end result of this new right would be a decrease in the quantity of privacy-invading experiences, from junk telephone calls to unwanted appropriations of medical information, and a rise in their quality—that is, the potential they will actually benefit the individual concerned.

Some legislative straws in the wind suggest that public opinion may now be open to a right like the one proposed here. GOP Congressman Bob Franks has proposed a bill to require parental consent before children's data can be commercialized. New Jersey state Sen. Richard Codey last February introduced a bill barring companies from renting or selling consumer names "without prior written or electronic consent" from the party concerned. About the same time, the Minnesota legislature was considering a similar bill applying to on-line service companies.

The courts are also starting to address the problem. In a case against Radio Shack, Robert Beken won $1,000 in damages for misuse of his personal data. Beken had written a contract on the back of his check to the electronics chain, committing them not to place him on the store's mailing list or send him any advertisements or mailings. The court rejected Radio Shack's defense that the clerk accepting the check had no authority to enter into such a contract with Beken.

But we believe that court decisions or piecemeal legislation will never provide the protection that would be afforded by a comprehensive right. The right we propose would not categorically block any of the useful forms of data exchange underlying today's information society. Nor would it prevent any organization from maintaining its own files on clients or customers—provided that the data involved were provided by, or with the consent of, those concerned. It would simply require their permission before their data could be released.

Who could take exception to the institution of personal data rights? Only the vast industries that now appropriate personal data for free. Information-collecting industries have often sought immunity from privacy-protecting legislation on freedom of expression grounds. But it hardly makes sense to identify the same value in "commercial speech" as in expression of opinion on public affairs, which would still be protected. Nothing proposed here, for example, should detract from the right of journalists or others to obtain personal data on public figures for news stories or other forms of public discussion.

This measure wouldn't solve all the sticky policy dilemmas associated with privacy protection. Some personal data no doubt should never be marketed for commercial use—those on children, for example, or individuals' DNA profiles. But establishing a general property right in personal data would create a potent new weapon for ordinary Americans to defend themselves against pressures on their privacy. With the information age hitting high gear in the 1990s, there's only so much time to get the genie back in the bottle. Otherwise, we will just have to adjust to living in see-through houses on the information highway. ●

Memo of the Month

LAW OFFICES
ALAN L. SPIELMAN, LTD.
2037 PINE STREET
PHILADELPHIA, PENNSYLVANIA 19103-6522
(215) 732-0471
TELEFAX 732-6462

June 28, 1996

New Bedford Standard-Times
555 Pleasant St.
New Bedford, MA 02742

Attention: Mr. Daniel L. O'Brien, Music Critic

Dear Mr. O'Brien:

We represent Iso Briselli. Mr. Briselli has brought to our attention false and defamatory statements concerning, among other inaccuracies, his inability to perform the third movement of Samuel Barber's "Violin Concerto, Op. 14." These defamatory statements have occasionally appeared in program notes and elsewhere as part of the history surrounding the commissioning of this work.

We are enclosing an article by George Diehl, Ph.D., which appeared in the November, 1995 issue of *Strad* magazine. This article presents an accurate version of the facts. If you are interested in Samuel Barber's Violin Concerto, we urge you to read the article before publicly commenting on the work's history. We must advise you, however, that your publication of the defamatory version of events may lead to the commencement of a defamation action against you on behalf of our client.

If you have any questions concerning this matter, please do not hesitate to contact us at your convenience.

Very truly yours,

Alan L. Spielman

sdb
enc